Erkennung und Analyse von Missbrauch in SIP-basierten Netzwerken

DISSERTATION

zur Erlangung des akademischen Grades
eines Doktors der Naturwissenschaften
(Dr. rer. nat.)

durch die Fakultät für Wirtschaftswissenschaften
am Institut für Informatik und Wirtschaftsinformatik der
Universität Duisburg-Essen (Campus Essen)

vorgelegt von
Dirk Hoffstadt, M.Sc.
geboren in Essen

Tag der mündlichen Prüfung:	15.12.2015
Erstgutachter:	Prof. Dr-Ing. Erwin P. Rathgeb
Zweitgutachter:	Prof. Dr. Tobias Hoßfeld

Zusammenfassung

Die Sprachkommunikation über „Voice over IP“-Netzwerke, basierend auf dem Session Initiation Protokoll (SIP), verbreitet sich auf Grund von Funktionalitäts- und Kostenvorteilen zunehmend und wird die klassischen Telefonnetze in den nächsten Jahren vollständig ablösen. Zusätzlich zu den Netzen der Telefonanbieter wird die Sprachkommunikation über das SIP-Protokoll auch im Unternehmens- und Privatanwenderumfeld unverzichtbar. So bietet VoIP die Möglichkeit, sich unabhängig von dem aktuellen Aufenthaltsort über das Internet bei dem jeweiligen Heimatnetzbetreiber oder der eigenen Firma anzumelden und über das dortige Nutzerkonto Gespräche zu führen. Da die Telefonie somit von einer geschlossenen und vergleichsweise sicheren Plattform auf eine viel offenere Plattform in das Internet migriert wird, ergeben sich neue Risiken und Missbrauchsmöglichkeiten im Bereich der Telefonie.

In dieser Dissertation werden Angriffe untersucht, die mit der Einführung von SIP-basierten Sprachdiensten im Internet entstehen und nicht aus Bedrohungen der Netzwerkschicht oder aus rechtlichen Vertragsbestimmungen resultieren. Das Ziel dieser Angriffe ist das Erlangen eines finanziellen Vorteils, indem ein Angreifer kompromittierte Zugänge für Auslandstelefonate oder für Anrufe zu Premiumnummern auf Kosten der Anschlussinhaber nutzt („Toll Fraud“).

Für die Realisierung der Bedrohungsanalyse und der Angriffserkennung wurden Konzepte, ein Versuchsnetzwerk sowie die notwendigen Softwarekomponenten ergebnisorientiert entwickelt. Im Vergleich zu anderen Forschungsarbeiten wurden Untersuchungen mit Ködersystemen (Honeypots) weiterentwickelt und es wurde ein System für eine verteilte, automatische Angriffserkennung entwickelt. Dafür wurden SIP-Verkehrsdaten über einen Zeitraum von sechs Jahren in zwei Class-C-Netzwerken aufgezeichnet und mit einem neuen Analyseansatz unabhängig von einzelnen SIP-Nachrichten automatisch ausgewertet.

Die Ergebnisse des Feldversuches in dieser Dissertation zeigen, dass die Bedrohungen für die SIP-Infrastruktur ansteigen und dass bereits eine Weiterentwicklung und Optimierung der Angriffswerkzeuge nachzuweisen ist. Die zunehmende Anzahl der Toll Fraud-Versuche mit internationalen Anrufzielen (und auch zu Premium-Rufnummern) verdeutlicht, dass bei einem unzureichenden Schutz der SIP-Server für die Nutzer und Betreiber sehr schnell ein erheblicher finanzieller Schaden entstehen kann. Es ist daher unerlässlich, die vorgeschalteten, systematischen Angriffsstufen frühzeitig zu erkennen und Abwehrkomponenten zu benachrichtigen.

Für die automatisierte, verteilte Angriffserkennung in Echtzeit und für die Maximierung des Beobachtungsgebietes wurde für diese Dissertation das „Security Sensor System“ entwickelt. Mit Hilfe von leichtgewichtigen Sensoren wurde eine weltweite signaturbasierte Angriffserkennung realisiert. Zusätzlich zu der standortbezogenen Angriffserkennung werden Angriffe durch einen zentralen Dienst korreliert. Dadurch können Angreifer netzwerkübergreifend bzw. länderübergreifend identifiziert und somit Gegenwehrkomponenten in Echtzeit benachrichtigt werden.

Der Vergleich der verschiedenen Messstellen im Internet belegt, dass die analysierten Angriffsmuster nicht nur im Netzwerk der Universität Duisburg-Essen, sondern zeitlich zusammenhängend auch an anderen Standorten auftreten. Dadurch wird deutlich, dass die ermittelten Ergebnisse auch für andere Netzwerke gültig sind und dass die Toll Fraud-Problematik bereits für alle Betreiber von SIP-Servern relevant ist.

Abstract

Voice over IP networks based on the Session Initiation Protocol (SIP) are becoming more and more widespread in the Internet due to functionality and cost advantages and will soon replace the classic telephony networks. Therefore, support of open SIP-based interfaces is an increasingly important requirement for IP-based Public Branch eXchanges (PBXs) and provider systems. The VoIP service allows using the personal or company VoIP account from any location worldwide. The migration of the telephony service from a closed and comparatively secure environment to a network with open interfaces creates security issues and opens up new opportunities for misuse and fraud.

In this thesis, attacks are analyzed which result from introducing SIP-based voice services and do not belong to the area of contract regulations or attacks on the network layer. The attacker's goal is to gain immediate financial benefit by making toll calls (international, cellular, premium services) via cracked third party accounts ("Toll Fraud").

To realize the threat analysis and the attack detection concepts, a SIP-based testbed and required software components were developed. In comparison to the related work, analyses with Honeypots were enhanced and a mechanism for automatic, distributed attack detection was realized. Therefore, for gathering the required data, a Honeynet with two class-C networks captured the SIP traffic for a period of six years. The automatic analysis is based on attacks and operates independently of single SIP messages.

The field test results of this thesis demonstrate that SIP-based threats increase over time and attack tools are optimized and enhanced. The increasing number of Toll Fraud attempts to international or premium numbers reveals that Toll Fraud attacks can cause the account owner substantial financial damage in a very short amount of time if there is insufficient attack detection and mitigation. Hence, it is necessary to implement an attack detection which is able to identify the different attack stages and sends a notification to mitigation components before a Toll Fraud call is established.

In this thesis, the Security Sensor System was developed to maximize the monitoring scope and to realize the distributed, automatic attack detection in real-time. The light-weight sensor component provides worldwide signature-based attack detection. Additional to the location-based attack detection, all attack notifications are sent to a central service which correlates the incoming alarm messages and provides a comprehensive attacker identification to inform mitigation components in real-time.

The comparison of different sensor nodes in the Internet shows that the analyzed attack patterns do not only occur in the University testbed, but also temporally coherent in other networks. Thus, the results are valid for different network environments and it is crucial to know that Toll Fraud attacks are already performed in reality.

Veröffentlichungen

M. Gruber, D. Hoffstadt, A. Aziz, F. Fankhauser, C. Schanes, E. Rathgeb und T. Grechenig, „Global VoIP Security Threats – Large Scale Validation" in IFIP Networking 2015 Conference, Toulouse, France, 2015

A. Aziz, D. Hoffstadt, E. Rathgeb und T. Dreibholz, „A Distributed Infrastructure to Analyse SIP Attacks in the Internet," in IFIP Networking 2014 Conference, Trondheim, Norway, 2014.

D. Hoffstadt, E. Rathgeb, M. Liebig, R. Meister, Y. Rebahi und T. Q. Thanh, „A comprehensive framework for detecting and preventing VoIP fraud and misuse," in International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 2014.

A. Aziz, D. Hoffstadt, S. Ganz und E. Rathgeb, „Development and Analysis of Generic VoIP Attack Sequences Based on Analysis of Real Attack Traffic," in Trust, Security and Privacy in Computing and Communications (TrustCom), Melbourne, VIC, 2013.

D. Hoffstadt, N. Wolff, S. Monhof und E. Rathgeb, „Improved detection and correlation of multi-stage VoIP attack patterns by using a Dynamic Honeynet System," in IEEE International Conference on Communications (ICC), Budapest, Hungary, 2013.

D. Hoffstadt, S. Monhof und E. P. Rathgeb, „SIP Trace Recorder: Monitor and Analysis Tool for threats in SIP-based networks" in TRaffic Analysis and Classification Workshop (IWCMC2012-TRAC), Limassol, 2012.

D. Hoffstadt, A. Marold und E. Rathgeb, „Analysis of SIP-Based Threats Using a VoIP Honeynet System," in Conference proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-2012), Liverpool, 2012.

M. Becke, K. Campowsky, C. Henke, D. Hoffstadt, J. Müller, C. Schmoll, A. Siddiqui, T. Magedanz, P. Müller, E. P. Rathgeb, and T. Zseby, "Addressing Security in a Cross-Layer Composition Architecture", in 10th Würzburg Workshop on IP: Joint ITG, ITC, and Euro-NF Workshop "Visions of Future Generation Networks" (EuroView 2010), , Würzburg, Germany, August, 2010

T. Zseby, C. Schmoll, C. Henke, D. Hoffstadt, A. Siddiqui, "G-Lab Deep: Cross-layer Composition and Security for a flexible Future Internet" in 6th International ICST Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities (Tridentcom 2010), Berlin, Germany, May, 2010

E. P. Rathgeb, Dirk Hoffstadt, "The E-Mail Honeypot System Concept, Implementation and Field Test Results" in Second International Conference on the Digital Society (ICDS 2008), Sainte Luce, Martinique, France, February 2008

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ASCII.....American Standard Code for Information Interchange
B2B.....Back-to-Back User Agent
BMBF.....Bundesministerium für Bildung und Forschung
BSI .....Bundesamt für Sicherheit in der Informationstechnik
bzw.....beziehungsweise
ca.....circa
CDR .....Call Detail Record
CPU .....Central Processing Unit / Hauptprozessor
CSV.....Comma-separated values
DDoS / DoS.....(Distributed) Denial of Service
DFN .....Deutsches Forschungsnetz
DHCP.....Dynamic Host Configuration Protocol
DNS .....Domain Name System
DSL .....Digital Subscriber Line
EEF .....Enable Extension Function
eRBL.....Extended Real-time Blacklist
etc. .....et cetera
EUR .....Euro (Währung)
evtl. .....eventuell
GB .....Gigabyte
HD .....High Definition
HTML.....Hypertext Markup Language
HTTP.....Hypertext Transfer Protocol
HTTPS.....Hypertext Transfer Protocol Secure
IAX.....Inter-Asterisk eXchange (Protocol)
ICMP.....Internet Control Message Protocol
ID.....Identifikator
IDS.....Intrusion Detection System
IETF .....Internet Engineering Task Force
inkl. .....inklusive
IP .....Internet Protocol
IPv4 / IPv6.....Internet Protocol Version 4 / Version 6
ISDN .....Integrated Services Digital Network
ITU-T .....International Telecommunication Union
LAN.....Local Area Network
LTE.....Long Term Evolution
LTS.....Long Term Support
MAC .....Media Access Control
MB.....Megabyte
MHz.....Megahertz
NAT .....Network Address Translation
NGN .....Next Generation Network
NP.....Notification Process
NUC.....Next Unit of Computing
OSI.....Open Systems Interconnection (Model)
PBX.....Private Branch eXchange

PC ..... Personal Computer
PCAP ..... Packet Capture (Format)
PHP ..... PHP: Hypertext Preprocessor
PIN ..... Persönliche Identifikationsnummer
POTS ..... Plain Old Telephone Service
PSTN ..... Public Switched Telephone Network
QoS ..... Quality of Service
RAM ..... Random Access Memory
RFC ..... Requests for Comments
RTP ..... Real-time Transport Protocol
SBC ..... Session Border Controller
SCP ..... Sensor Controller Process
SCS ..... Sensor Central Service
SCTP ..... Stream Control Transmission Protocol
SD ..... Secure Digital (Memory Card)
SDP ..... Session Description Protocol
SIP ..... Session Initiation Protocol
SIPS ..... Session Initiation Protocol Security
SMS ..... Short Message Service
SNI ..... SCS Notification Interface
SPIT ..... SPAM over Internet Telephony
SQL ..... Structured Query Language
SSD ..... Solid State Disk
SSH ..... Secure Shell
SSI ..... SCS Sensor Interface
SSL ..... Secure Sockets Layer
SSS ..... Security Sensor System
STR ..... SIP Trace Recorder
TB ..... Terrabyte
TCP ..... Transmission Control Protocol
TdR ..... Technik der Rechnernetze
TK ..... Telekommunikation
TLS ..... Transport Layer Security
u.a. ..... unter anderem
UAC / UAS ..... User Agent Client / User Agent Server
UDP ..... User Datagram Protocol
UMTS ..... Universal Mobile Telecommunications System
URI ..... Uniform Resource Identifier
URL ..... Uniform Resource Locator
USB ..... Universal Serial Bus
UTF-8 ..... UCS Transformation Format (Universal Character Set) 8 Bit
VLAN ..... Virtual Local Area Network
VM ..... Virtuelle Maschine
VoIP ..... Voice over IP
VPN ..... Virtual Private Network
W ..... Watt
WP ..... Worker Process
XML ..... Extensible Markup Language
z.B. ..... zum Beispiel

Inhaltsverzeichnis

1 Einführung und Motivation

Die Kommunikation mit „Voice over IP“ (VoIP) auf der Basis des Session Initiation Protokolls (SIP) [1] löst die klassische Telefonie zunehmend ab und macht die Unterstützung offener SIP-Schnittstellen deshalb auch im Bereich der IP-basierten Nebenstellenanlagen unverzichtbar. Dadurch wird allerdings die Telefonie von einer geschlossenen – und damit vergleichsweise sicheren – Basis auf eine offene, sehr viel verwundbarere Plattform migriert. Einhergehend mit dieser Entwicklung haben sich die Kosten für die VoIP-Telefonate stetig reduziert, wobei auch ein Trend zur Pauschalisierung der Nutzungsentgelte zu beobachten ist. Durch diese technischen und wirtschaftlichen Veränderungen sind neue Risiken und Missbrauchsmöglichkeiten im Bereich der Telefonie entstanden.

Eine Problematik besteht darin, dass die geringen Kosten für VoIP-Telefonate die Sprachdienste attraktiv für den Missbrauch von Anrufen zum Zwecke der Werbung oder Störung gemacht haben. Diese Problematik wird allgemein mit dem Begriff SPIT (SPAM over Internet Telephony) bezeichnet. „Toll Fraud“ ist eine zweite Problematik, die durch die flächendeckende Einführung von VoIP kritisch werden kann. VoIP bietet die Möglichkeit, sich unabhängig von dem aktuellen Aufenthaltsort über das Internet bei dem jeweiligen Heimatnetzbetreiber oder der eigenen Firma anzumelden und über das dortige Nutzerkonto Gespräche zu führen. Da Gespräche in die Mobilfunknetze, zu Sonderrufnummern und ins Ausland weiterhin oft nicht pauschaliert abgerechnet werden, ist es attraktiv, sich durch gefälschte Anmeldungen an fremden Nutzerkonten solche Gespräche kostenlos zu erschleichen. Da die neue Generation der Telefonie auf IP-Netzwerken basiert, darf eine dritte Problematik, „Denial of Service“-Angriffe auf VoIP-Server, ebenfalls nicht vernachlässigt werden.

Für diese Dissertation wurden Untersuchungen zu Bedrohungen in SIP-basierten Netzwerken mit dem Schwerpunkt Toll Fraud über einen Zeitraum von sechs Jahren durchgeführt [2]. Diese zeigen, dass an das Internet angeschlossene Kommunikations-anlagen mit SIP-Schnittstellen schnell entdeckt und in der Folge intensive Angriffsversuche mit bis zu 13 Millionen SIP-Paketen pro Account und Server unternommen wurden. Ähnlich wie bei der Entwicklung der Bedrohungen für Internetrechner durch Würmer, Denial of Service, SPAM und andere Angriffe sind die momentan auftretenden Angriffe als Vorboten eines stetig wachsenden neuen „Marktes“ anzusehen.

Ein für diese Dissertation durchgeführter Feldtest, der im September 2008 begann und bis Oktober 2014 ausgewertet wurde, zeigt, dass das Angriffsmuster Toll Fraud anfangs nur sporadisch auftauchte, seit Anfang 2010 jedoch kontinuierlich zunimmt. Dabei wurde deutlich, dass die Angreifer verschiedene Angriffsstufen für den Toll Fraud-Angriff kombinieren (siehe auch Kapitel 3.4). Dieser mehrstufige Toll Fraud-Angriff tritt inzwischen mit deutlich höherer Intensität auf (mehrere Millionen SIP-Nachrichten pro Tag). Die Analysen des Datenbestandes zeigen, dass neben weiterentwickelten automatisierten Angriffswerkzeugen für die Übernahme von Accounts auch manuelle, gezielte Angriffe mit „Softphones“ erfolgen, um die übernommenen Accounts zum Telefonieren zu verwenden (z.B. Anrufe in das Ausland). Es ist anzunehmen, dass das Aufkommen solcher Angriffe in den nächsten Jahren weiterhin steigen wird, da zunehmend umfangreiche SIP-

Funktionalitäten in weit verbreitete Home-Gateways (z.B. FritzBox[1]) und Telekommunikationsanlagen (TK-Anlagen) integriert und zukünftig auch direkte Verbindungen zwischen Endgeräten (ohne Mitwirkung von SIP-Infrastrukturkomponenten) möglich werden.

Für die Realisierung der Bedrohungsanalyse und der Angriffserkennung mussten Konzepte, ein Versuchsnetzwerk sowie die notwendigen Softwarekomponenten entwickelt werden. Zu Beginn war es wichtig, die Funktionsweise der SIP-basierten Angriffe zu verstehen. Um Angriffsmuster und Verhaltensänderungen identifizieren zu können ist eine theoretische Analyse nicht ausreichend. Daher war es notwendig, die SIP-Verkehrsdaten in einem realen Netzwerk aufzuzeichnen und über einen mehrjährigen Zeitraum im Rahmen eines Feldtests zu analysieren. Damit möglichst keine manuelle Analyse der gesammelten Verkehrsdaten erfolgen musste, wurden geeignete, automatisierte und flexible Auswertungs- und Erkennungsmechanismen implementiert, die stetig an das veränderte Angreiferverhalten angepasst werden konnten.

Für die Analyse der Bedrohungen in SIP-basierten Netzwerken wurde für die Dissertation ein Ködernetzwerk (Honeynet) aufgebaut, das auf verschiedenen Hosts (Honeypots) für Angreifer interessante SIP-Netzwerkdienste mit dem Ziel anbietet, angegriffen zu werden (siehe auch Kapitel 4.1 und 4.2). Dabei handelt es sich um ein speziell gesichertes und überwachtes Netzwerk, das keine Verbindung zu Produktivnetzen hat, um Schäden an anderen Systemen auszuschließen. Dazu wurden Honeypot-Systeme aufgesetzt, die eine angepasste Version der frei verfügbaren Telefonanlagen-Software Asterisk [3] beinhalten und somit für den Angreifer wie eine produktive SIP-Nebenstellenanlage wirken. Auf die Honeypots kann mit dem SIP-Protokoll aus dem Internet zugegriffen werden, da sich diese in einem öffentlichen Netzwerkbereich befinden.

Ein zentraler Aspekt bei einem Honeynet ist die vollständige Überwachung der Ködersysteme und des Angreiferverhaltens. Dabei muss sichergestellt werden, dass der Angreifer die Kontrollmechanismen nicht kompromittieren kann und diese möglichst unsichtbar sind, damit das Honeynet unentdeckt bleibt und nicht von produktiven Systemen unterschieden werden kann. Das entwickelte Monitoring-System „SIP Trace Recorder“ (STR) [4], siehe auch Kapitel 5.2, ermöglicht die Überwachung des gesamten Testbeds (zwei Class-C-Netzwerke), indem alle ein- und ausgehenden SIP-Nachrichten vollautomatisch aufgezeichnet, geparst und in einer SQL-Datenbank für die spätere Analyse gespeichert werden. Das Monitoring erfolgt vollständig passiv und unsichtbar für Angreifer, da der STR über einen Mirror-Port am Hauptswitch angebunden ist. Dadurch wird sichergestellt, dass die Überwachungskomponente aus dem Internet nicht erreichbar ist und somit nicht kompromittiert werden kann.

Die gesammelten Daten können zu jedem Zeitpunkt für Abfragen zu verschiedenen Fragestellungen verwendet werden. Darüber hinaus erfolgen automatisierte Analysen zu bereits vordefinierten Fragestellungen, die jede Nacht aktualisiert und auf dem zugehörigen Webinterface angezeigt werden. Mit dem STR kann das Angriffsverhalten in SIP-Netzwerken analysiert und eine Einschätzung der aktuellen Bedrohungslage gegeben werden.

Die Konzepte zur Analyse der Bedrohungen wurden fortlaufend weiterentwickelt. Neben den statistischen Analysen, die auf einzelnen Paketen bzw. auf der Paketanzahl in einem definierten Zeitraum basieren, erlauben tiefergehende Auswertungen, wie der Clustering-Ansatz (siehe Kapitel 4.3), genauere Aussagen zum Angreiferverhalten. Für das Clustering

[1] AVM FritzBox, http://avm.de/produkte/fritzbox/

wurden SIP-Nachrichten unter Berücksichtigung der SIP- und IP-Header (z.B. Quell-/Ziel-Adresse, SIP-Methode, SIP URI) und zeitlicher Schwellenwerte korreliert, so dass verschiedene Angriffstypen sichtbar und Kommunikationsbeziehungen (SIP-Sessions) berücksichtigt wurden. Da Angreifer nach der Übernahme eines Accounts typischerweise erst nach einigen Stunden bzw. Tagen die weitergehenden Toll Fraud-Angriffe durchführen, wurde eine Funktionalität benötigt, um Angreifer unabhängig von der Quell-IP-Adresse durch die SIP-Zugangsdaten identifizieren zu können. Das für diesen Einsatzzweck entwickelte dynamische Honeypot-System [5] erlaubt eine Verhaltensanpassung durch eine externe Überwachungskomponente während eines aktiven Angriffs (siehe auch Kapitel 4.5).

Die Analysen haben gezeigt, dass die Angriffe deutlich über die Testbed-Netzwerkgrenzen hinaus und somit großflächiger im Internet angelegt sind. Um jedoch verteilte SIP-Angriffe in verschiedenen Netzwerken untersuchen zu können, war es notwendig, ein geeignetes Analysewerkzeug zu entwickeln. Im Rahmen dieser Dissertation wurden das Konzept und die Architektur für ein verteiltes Sensorsystem zur Erkennung von Angriffen in SIP-basierten Netzwerken erstellt (siehe auch Kapitel 4.6).

Leichtgewichtige Sensoren wurden weltweit auf unterschiedliche Standorte verteilt und ermöglichen eine signaturbasierte Angriffserkennung [6]. Dazu wurde ein Konzept für XML-basierte Signaturen entwickelt (siehe auch Kapitel 4.4), damit die Ergebnisse der Honeynet-Untersuchungen für Erkennungsregeln abgeleitet werden konnten. Dabei ist hervorzuheben, dass nicht nur einzelne SIP-Pakete, sondern Abhängigkeiten zwischen Nachrichten und somit Kommunikationsbeziehungen berücksichtigt werden. Sobald eine Signatur verletzt und ein Angriff erkannt wird, erfolgt die Benachrichtigung eines zentralen Dienstes, der die Angriffsanalyse ausführt und das gesamte Sensornetzwerk überwacht und steuert.

Durch die Korrelierung von eingehenden Alarmmeldungen von verschiedenen Sensoren weltweit ermöglicht die zweistufige Analyse auf dem Zentraldienst eine Einschätzung der Bedrohungslage in SIP-Netzwerken. Eine anpassbare Schnittstelle zu Gegenwehr-Komponenten erlaubt eine Abschwächung bzw. Unterbindung eines Angriffes in Echtzeit.

Das verteilte Sensorsystem ist Teil des vom Bundesministerium für Bildung und Forschung geförderten Projektes "Schutz vor Missbrauch und Bedrohung von VoIP-Netzwerken (SUNSHINE)" [7]. Im Rahmen des Projektes und dieser Dissertation wurde in Zusammenarbeit mit einer weiteren Forschungseinrichtung und mit Industriepartnern ein Framework zur Verhinderung von Betrug und Missbrauch auf der Basis von VoIP-Kommunikationstechnologien entwickelt. Dazu wurden zwei Referenzimplementierungen des Sensorsystems entwickelt und erfolgreich getestet. Darüber hinaus wurde das Sensorsystem zur Erkennung von Angriffen innerhalb der Honeynet-Umgebung sowie bei Kooperationspartnern und in dem Forschungstestnetzwerk „NorNet“ [8] mit vielen internationalen Standorten eingesetzt. Durch den Einsatz in Honeynet-, Testbed- und Produktivumgebungen konnte das System für reale Angriffe evaluiert und optimiert werden.

Das Kapitel 2 beschreibt die Entwicklung von der klassischen Telefonie zu Voice-over-IP-Netzwerken und erklärt die relevanten Grundlagen des Session Initiation Protokolls. Weiterhin werden die Honeynets und die eingesetzten Software- und Hardware-Komponenten erläutert.

Kapitel 3 gibt einen Überblick über die Bedrohungen im Bereich Voice-over-IP und stellt die Missbrauchsszenarien vor. Nach der Abgrenzung des Arbeitsbereiches dieser Dissertation werden die unterschiedlichen Kommunikationsszenarien sowie die relevanten

Angriffsstufen für Toll Fraud erläutert. Abschließend erfolgt die Abgrenzung zu anderen wissenschaftlichen Arbeiten in diesem Forschungsbereich (Related Work).

Die Konzepte, die verwendete Methodik und die wissenschaftlichen Neuerungen dieser Dissertation werden in Kapitel 4 vorgestellt.

In Kapitel 5 werden die Architektur und die Implementierung der entwickelten Werkzeuge erläutert.

Die Ergebnisse des Honeynet-Feldversuches und die Evaluierung der implementierten Werkzeuge werden in Kapitel 6 vorgestellt. Darüber hinaus werden die Resultate der verteilten Erkennung an verschiedenen Standorten erläutert und Empfehlungen für die Angriffserkennung in SIP-basierten Netzwerken aufgezeigt.

Die Dissertation schließt mit einer Zusammenfassung und einem Ausblick in Kapitel 7.

2 Grundlagen

In diesem Kapitel werden die Unterschiede zwischen der Voice-over-IP-Telefonie und den herkömmlichen Telefonnetzen (z.B. ISDN) herausgestellt. Es erfolgt die Erläuterung des Session Initiation Protokolls (SIP) [1], da dieses Protokoll aktuell als Standard für die IP-Telefonie eingesetzt wird. Da für die Analysen dieser Dissertation Ködersysteme eingesetzt werden, werden die Architektur und die verschiedenen Typen der Honeypots / Honeynets vorgestellt. Darüber hinaus werden die eingesetzten Hardware- und Software-Komponenten beschrieben.

2.1 VoIP Kommunikation vs. POTS / ISDN

In der Vergangenheit gab es stets getrennte (durchschaltevermittelte) Telefon- und (paketorientierte) Datennetze. Eine kombinierte Nutzung fand nur im Heimbereich statt, wenn zum Beispiel ein Modem zur Interneteinwahl über eine analoge Telefonleitung verwendet wurde. Inzwischen ist es problemlos möglich, die heutigen Breitbandanschlüsse (z.B. DSL) und Datenleitungen für Internetanwendungen und zur parallelen Sprachübertragung zu nutzen.

„Next Generation Networks“ (NGN) [9] bestehen aus paketorientierten Netzwerken für möglichst alle Dienste. Auf Grund der Echtzeitanforderungen zur Sprach- und Videoübertragung stellen diese Netze „Quality of Service“ (QoS)-Optionen zur Verfügung, um die gewünschte Dienstgüte sicherzustellen. Ein wichtiger Aspekt in Hinblick auf die Kosten und auf die Offenheit für neue Dienste ist die vollständige Trennung der Verbindungssteuerung von dem Nutzdatentransport. So können in Zukunft weitere Anwendungen (z.B. Videotelefonie, Nachrichtenaustausch etc.) integriert werden, ohne dass das Signalisierungsprotokoll geändert werden muss. Somit können die Änderungen an der Infrastruktur und die entstehenden Kosten gering gehalten werden. Bestehende, herkömmliche Telefonnetze werden über Gateways integriert. Das anerkannte Konzept der Next Generation Networks wird zunehmend für das Festnetz sowie für Mobilfunknetze der 3./4. Generation (UMTS [10] / LTE [11]) in die Praxis umgesetzt.

Ein wesentlicher Bestandteil dieses Konzeptes ist die VoIP-Technologie, um Sprache in Echtzeit über IP-basierte Datennetze zu übertragen. Das Internet-Protokoll, Standard zur Datenübertragung im Internet, wird in der heutigen Zeit auch im größten Teil aller LANs in Firmen und bei Heimanwendern eingesetzt. Somit gibt es kaum Einschränkungen oder Probleme, wenn die Technik zur Sprachübertragung IP-basierte Netzwerke voraussetzt. Schon in den 90er Jahren hat diese Technik aus Kostengründen das Interesse der Öffentlichkeit geweckt[2]. Jedoch fehlte zu diesem Zeitpunkt die notwendige Infrastruktur im Internet und bei den Anwendern, um das Datenaufkommen in Echtzeit bewältigen zu können. Aussetzer und Gesprächsverzögerungen machten sich negativ bemerkbar und waren nicht akzeptabel. Inzwischen hat VoIP die Marktreife erreicht und ermöglicht das Telefonieren über Datennetze mit einem weltweit gültigen Standard. Die wichtigsten Protokolle (SIP, H.323 [12]) wurden von der International Telecommunication Union (ITU-T[3]) und der Internet Engineering Task Force (IETF[4]) standardisiert.

[2] http://www.heise.de/ct/artikel/Weltweit-waehlen-289336.html

[3] http://www.itu.int/

[4] https://www.ietf.org/

Um Anrufe zu tätigen, ist im Vorfeld eines Gesprächs eine Kommunikation zwischen den Endgeräten für den Verbindungsaufbau notwendig. Diese Verbindungssteuerung wird als Signalisierung bezeichnet. Für diesen Zweck wurde das Protokoll H.323 [12] von der ITU-T für paketbasierte Netze entwickelt. Ursprünglich stammt das Vorgängerprotokoll H.320 [13] aus der ISDN-Videotelefonie und wurde für leitungsgebundene Telefonie auf Paketnetzverfahren weiterentwickelt. Somit war es möglich, ISDN-typische Informationen über IP-basierte Netzwerke zu übertragen. Durch den hohen Reifegrad ist das Protokoll für VoIP-Netze geeignet, jedoch gilt es als starr und unflexibel, da es sich nicht über die ISDN-typische Kommunikation hinaus erweitern lässt. Inzwischen gilt das Session Initiation Protokoll [1] als Marktstandard für die Signalisierung in VoIP-Netzen. Bei diesem Protokoll wird im Gegensatz zu H.323 das im Internet weit verbreitete Hypertext Transfer Protokoll (HTTP) [14] zu Grunde gelegt. SIP fügt sich somit nahtlos in die bestehende Internet-Protokollarchitektur ein und kann für verschiedene Szenarien (z.B. Instant Messaging) neben der Signalisierung in VoIP-Netzen verwendet werden. In Kapitel 2.2 wird das Protokoll detailliert beschrieben. H.323 und SIP dienen allein der Signalisierung, während für die Nutzdaten das Real-time Transport Protokoll (RTP) [15] zum Einsatz kommt.

Unabhängig von der Signalisierung wird zur Sprachübermittlung das RTP-Protokoll eingesetzt. Dieses setzt auf eine ungesicherte Datenübertragung mit Hilfe des UDP-Protokolls auf und verwendet auf der OSI-Schicht 3 („Network Layer“) das IP-Protokoll. Es dient der kontinuierlichen, paketbasierten Übertragung von Multimedia-Inhalten (Audio, Video) über das Internet.

Länderspezifische Varianten oder Sonderlösungen, wie z.B. bei ISDN, gibt es nicht, so dass die Kompatibilität gewährleistet ist. Es ist davon auszugehen, dass VoIP nicht nur eine Alternative zu den herkömmlichen Telefonnetzen darstellt, sondern diese nach der aktuell laufenden Übergangszeit komplett ablösen wird[5]. Dies bedeutet, dass nur noch ein Datennetz existieren und die Koexistenz eines Telefonnetzes (z.B. ISDN) nicht mehr erforderlich sein wird. Auch im Mobilfunksektor ist mit der Inbetriebnahme der LTE-Netze ein Trend zu reinen Datennetzen zu erkennen. Somit sind große Kosteneinsparungen möglich. Hardware-Investitionen sind nur noch für die paketorientierten Netzwerke notwendig und kostenintensive Leitungsreservierungen pro Anschluss (unabhängig von der Nutzung) in herkömmlichen Telefonnetzen entfallen vollständig.

Bereits heute beginnen die großen Telekommunikationsanbieter in Deutschland mit der Umstellung der Infrastruktur im Neukundengeschäft. Die Telekom, als größter deutscher Netzbetreiber, möchte laut einer Absichtserklärung[5] alle herkömmlichen Telefonanschlüsse bis zum Jahr 2018 auf IP-Telefonie umgerüstet haben. Für die Bereitstellung eines Internetzugangs und einer Telefonleitung wird ausschließlich eine DSL-Leitung zum Endkunden geschaltet. Mit Hilfe des richtigen Endgerätes kann somit auch der Telefonanschluss per VoIP über die Datenleitung bereitgestellt werden. Der herkömmliche Analog- oder ISDN-Anschluss entfällt. Diese Technik ist natürlich auch für alle Gewerbebetriebe interessant, da eine bestehende Netzwerkverkabelung sowohl für das Firmen-LAN als auch für das Telefonsystem per VoIP genutzt werden kann. Eine kostenintensive Zweitverkabelung für Telefonie entfällt.

Für die Realisierung werden ein Server-System mit einer leistungsfähigen Telekommunikationssoftware sowie VoIP-fähige Endgeräte benötigt, die mit dem Firmen-LAN in den einzelnen Büros verbunden werden. Für die Anbindung der Computerarbeitsplätze und der VoIP-Telefone ist lediglich eine gemeinsame

[5] http://www.heise.de/newsticker/meldung/Telekom-beschleunigt-Umstieg-auf-IP-Telefonie-mit-Kuendigungen-2405049.html

Netzwerkverkabelung erforderlich. Im Bedarfsfall besteht jedoch die Möglichkeit, mit entsprechenden Schnittstellen (z.B. ISDN-Karte) herkömmliche Telefone in die VoIP-Umgebung zu integrieren. Über die VoIP-Telefonanlage werden Gespräche zu VoIP-Anbietern (DSL-Router) sowie zu dem herkömmlichen Telefonnetz (ISDN, analog) vermittelt.

Das Session Initiation Protokoll und das Real-time Transport Protokoll gelten heute als Standard für das Next Generation Network und werden somit von Vermittlungsstellen der Telekommunikationsanbieter und von Endgeräten diverser Hersteller (z.B. Cisco, Snom, AVM etc.) unterstützt.

2.2 Session Initiation Protokoll (SIP) – Aktueller Standard in VoIP-Netzwerken

Das SIP-Protokoll [1] wurde 1999 von der IETF als Signalisierungsprotokoll zur Verwaltung von Kommunikationssitzungen standardisiert. Dabei geht es nicht um die eigentliche Nutzdatenübertragung, sondern um die Aushandlung der Kommunikationsmodalitäten (z.B. Sprachcodec) und Sitzungssteuerungen für Sprach- oder Videodienste.

Das Session Initiation Protokoll ist ein Vermittlungsprotokoll in Anlehnung an Signalisierungsprotokolle aus der herkömmlichen Telekommunikationswelt. Gegenüber der von der ITU-T spezifizierten H.323-Protokollsammlung bietet SIP den Vorteil der einfachen, an typischen IP-Anwendungen orientierten Architektur. So können bei einer SIP-basierten Kommunikation viele Standardabläufe, wie z.B. der Verbindungsaufbau inklusive der Aushandlung der Medienoptionen, deutlich besser analysiert werden, da eine Decodierung oder Übersetzung für die Analyse entfällt. Im Vergleich zu anderen (binären) Protokollen (z.B. H.323) basiert der SIP-Nachrichtenaufbau auf dem HTTP-Protokoll, wodurch ein ASCII-kompatibler UTF-8-Zeichensatz verwendet wird. Das Protokoll ist heute in den Basis-RFCs 3261 [1], 3262 [16], 3263 [17], 3264 [18] und 3265 [19] mit einigen Erweiterungen und Verbesserungen im Vergleich zum RFC 2543 [20] spezifiziert.

Das SIP-Protokoll dient der Übermittlung von Signalisierungsnachrichten für die Etablierung von Kommunikationsverbindungen (Sessions) im Bereich VoIP. Bei einer Session kann es sich um eine Punkt-zu-Punkt-Verbindung oder um eine Konferenz mit mehr als zwei Teilnehmern handeln. In den SIP-Nachrichten werden Teilnehmer- und Signalisierungsinformationen übertragen, aber zusätzlich auch Parameter für die auszutauschenden Multimediadaten wie z.B. die möglichen Codecs. Mit Hilfe des SIP-Protokolls, in Kombination mit dem Session Description Protokoll (SDP) [21] zur Medienaushandlung, kann die gesamte Kommunikationsverbindung (Aufbau, Abbau, Steuerung der bestehenden Session) verwaltet werden.

Die SIP-Nachrichten können per TCP, SCTP oder UDP transportiert werden. Da SIP jedoch als Vermittlungs- und Signalisierungsprotokoll bereits geeignete Handshake-, Wiederholungs- und Timeout-Verfahren als Maßnahmen zur Kommunikationssicherung beinhaltet und somit verbindungsorientiert arbeitet, genügt die Verwendung von UDP als verbindungsloses Transportprotokoll. Ein zusätzlicher Verbindungsaufbau entfällt. Viele gängige Softwareprodukte bzw. IP-Telefone unterstützen inzwischen SIP über TCP, jedoch wird als Standard-Transportprotokoll UDP verwendet, so dass für diese Dissertation der Fokus auf SIP über UDP gesetzt wird. Unabhängig vom eingesetzten Transportprotokoll ist der Standard-Port für die SIP-Kommunikation 5060. Der Port 5061 wird verwendet, wenn „Transport Layer Security“ (TLS) für die verschlüsselte Kommunikation aktiviert ist. Die TLS-Verschlüsselung wird aktuell nur von wenigen Anbietern und Endgeräten unterstützt, so dass die Kommunikation standardmäßig unverschlüsselt abläuft.

2.2.1 SIP-Komponenten

Abbildung 1 gibt einen Überblick über die SIP-Komponenten, die bei der Kommunikation in SIP-basierten Netzwerken genutzt werden. Einen Sonderfall stellt nur die direkte Verbindung zweier Endgeräte dar, wenn zwischen zwei Teilnehmern eine SIP-Sitzung etabliert wird. Die Schnittstelle zwischen Anwender und Kommunikationsinfrastruktur bilden die „User Agents“. Dabei handelt es sich um Hardware-Telefone oder sogenannte „Softphones“, die als Softwareapplikation auf einem Computer oder Smartphone betrieben werden. Für die orts- und geräteunabhängige Kommunikation wird ein User Agent über einen „Registrar Server“, der für eine Domain zuständig ist, angemeldet (siehe Kapitel 2.2.2). Bei einer erfolgreichen Registrierung speichert der „Location Server“ eine oder mehrere Kontaktadressen pro User Agent. Die Aktualität dieser Kontaktdatenbank wird durch einen Timeout garantiert. Ein Endgerät muss bis zum vorgegebenen Zeitpunkt die Registrierung erneuern, bevor der Teilnehmer als nicht erreichbar gilt. Das Routing der SIP-Nachrichten zwischen den User Agents wird durch den „Proxy Server“ ausgeführt. Wird darüber hinaus eine Vermittlung von Gesprächen in das klassische Telefonnetz (z.B. ISDN) benötigt, so kann der Proxy Server mit einem geeigneten „Gateway“ erweitert werden. Die verschiedenen Nachrichtentypen und die Funktionsweise des SIP-Routings werden in Kapitel 2.2.3 erläutert. Rufumleitungen werden im „Redirect Server“ vermerkt, falls ein Teilnehmer unter einer anderen SIP-Adresse erreichbar ist. In aktuellen SIP-Telefonanlagen werden die Dienste des Location-, Redirect- und Registrar Servers direkt in Kombination mit dem Proxy Server implementiert.

2.2.2 Adressierung

Von HTTP wurde das Client-Server-Prinzip übernommen: Ein SIP-Software- oder Hardware-Telefon, das mittels einer SIP-Anfrage an ein anderes Endsystem eine Transaktion einleitet, wird als „User Agent Client“ (UAC) bezeichnet. Die andere Instanz der Kommunikationsverbindung wird dann als „User Agent Server“ (UAS) bezeichnet. Die Begriffe beschreiben eine Rolle, jedoch nicht die grundlegende Funktion, da diese je nach Transaktion (z.B. Verbindungsaufbau) geändert werden kann. Bei SIP-Proxy Servern und SIP-Registrar Servern handelt es sich um zentrale Netzelemente. Diese können jedoch als UAC fungieren, wenn z.B. eine Anfrage an ein Endsystem weitergeleitet wird.

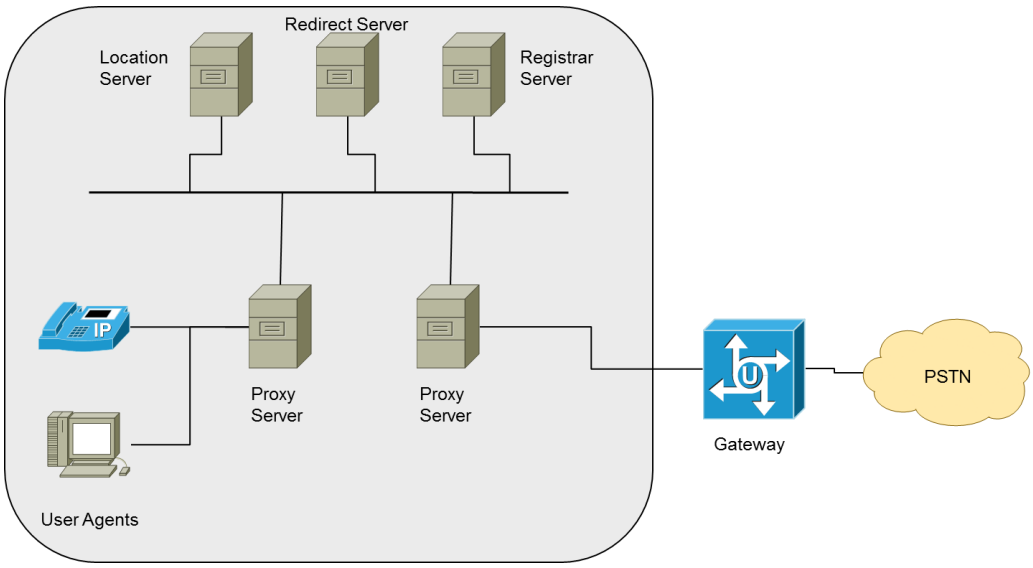


Abbildung 1: SIP-Komponenten

Für den Verbindungsaufbau werden als Kontaktadresse eines SIP-Endgerätes sogenannte „SIP Uniform Resource Identifier“ (SIP URI) verwendet. Der Aufbau entspricht einer E-Mail-Adresse mit vorangestellter Protokollbezeichnung. Sobald ein User Agent im Netzwerk aktiv wird, erzeugt dieser automatisch eine temporäre SIP URI. Abbildung 2 zeigt den Aufbau einer SIP URI sowie ein Beispiel für eine temporäre SIP URI. Diese ist grundsätzlich von dem Netzwerk (IP-Adresse) abhängig, in dem sich das Endgerät gerade befindet. Wenn keine zentrale SIP-Infrastruktur (SIP-Server) vorhanden ist, kann das Endgerät nur von einem anderen Endgerät erreicht werden, wenn die aktuelle, temporäre SIP URI bekannt ist. Bei einem Wechsel in ein anderes Netzwerk verändert sich auch die temporäre SIP URI, die aber innerhalb eines Netzwerkes eindeutig ist.

Ein Betreiber einer vermittelnden SIP-Infrastruktur kann einem Teilnehmer, wie in Abbildung 3 gezeigt, eine „permanente SIP URI“ zuordnen. Unter dieser permanenten SIP URI ist der Anwender grundsätzlich und überall erreichbar. Dazu wird die temporäre SIP URI bei dem SIP-Provider registriert und dieser stellt mit Hilfe eines SIP-Registrar- und Location Servers den Zusammenhang zwischen der permanenten und der temporären SIP URI her. Die permanente SIP URI beinhaltet keine IP-Adresse, sondern einen gültigen Domainnamen und ist wie eine E-Mail-Adresse weltweit über DNS auflösbar. Typischerweise entspricht die Benutzerkennung einer Telefonnummer, so dass Kompatibilität zum klassischen Telefonnetz gegeben ist. Darüber hinaus kann ein Anwender mehr als einen User Agent pro permanenter SIP URI registrieren, so dass eine erhöhte Mobilität sichergestellt werden kann. Ein Beispiel wäre die gleichzeitige Nutzung eines IP-Telefons am Arbeitsplatz und eines Smartphones mit Softphone-Applikation mit nur einer Rufnummer bzw. SIP URI.

2.2.3 SIP-Nachrichten

Bei der Kommunikation mittels SIP werden zwei Arten von Nachrichten unterschieden: „SIP-Requests“ und „SIP-Responses“ (Antwort auf SIP-Requests). Durch SIP-Requests werden Transaktionen, wie z.B. der Verbindungsaufbau, eingeleitet. Die enthaltene Methode definiert den grundlegenden Zweck eines SIP-Requests. In der Tabelle 1 werden die Standardmethoden erläutert, die für diese Dissertation relevant sind. Bei den erweiterten SIP-Methoden (SUBSCRIBE, REFER, NOTIFY, MESSAGE, PRACK, UPDATE, INFO, PUBLISH) handelt es sich um Zusatzfunktionen, die z.B. in Enterprise-Umgebungen wichtig sind (z.B. Teilnehmerstatus für Besetztlampenfelder).

Eine SIP-Response wird durch einen dreistelligen Statuscode sowie durch einen definierten Bezeichner beschrieben. In Anlehnung an das HTTP-Protokoll werden die SIP-Responses anhand der ersten Ziffer des Statuscodes in sechs Gruppen eingeteilt. Tabelle 2 zeigt die verschiedenen Gruppen der SIP-Responses und deren Bedeutung.

```
sip:<User>@<Host>
sip:123@192.168.100.254
```

Abbildung 2: Beispiel für temporäre SIP URI

```
sip:987654@sip.uni-due.de
sip:mustermann@sip.uni-due.de
```

Abbildung 3: Beispiel für eine permanente SIP URI

Für die Bedrohungsanalyse in SIP-basierten Netzwerken sind die Statuscodes neben den SIP-Requests von ähnlich großer Bedeutung, da hierdurch der Erfolg der Angriffe beurteilt werden kann.

2.2.4 Nachrichtenaustausch mit SIP-Transaktionen und Dialogen

Eine SIP-Transaktion besteht aus genau einem SIP-Request und einer oder mehreren SIP-Responses zwischen UAC und UAS. Die Zuordnung der verschiedenen SIP-Nachrichten zu einer Transaktion erfolgt über das Header-Feld „CSeq“ und den Parameter „Branch“ im „Via“-Header-Feld (siehe Kapitel 2.2.5). Die Werte werden durch den UAC festgelegt und

Tabelle 1: SIP-Methoden

SIP-Methode	Beschreibung
INVITE	Aufbau einer SIP-Sitzung zwischen UAC und UAS Im Messagebody sind bereits die SDP-Informationen zur Aushandlung der Medienverbindung enthalten
ACK	Bestätigung der finalen Statusinformation für das „3-Way-Handshake“ des Verbindungsaufbaus Eine ACK-Nachricht wird nicht durch eine SIP-Response beantwortet
BYE	Einleitung des Verbindungsabbaus durch UAC oder UAS
CANCEL	Abbruch einer SIP-Transaktion, z.B. während des Verbindungsaufbaus
OPTIONS	Abfrage von Eigenschaften des User Agents, ohne eine SIP-Sitzung aufzubauen
REGISTER	Registrierung eines User Agents bei einem Registrar Server und Übergabe der temporären und permanenten SIP URI

Tabelle 2: SIP-Responses

Statuscode	Beschreibung
1xx	Provisorische Statusinformationen werden verwendet, wenn eine Anfrage noch nicht abgeschlossen ist, z.B. während eines Verbindungsaufbaus „180 Ringing“
2xx	Erfolgreiche Bearbeitung einer Anfrage, z.B. „200 OK“
3xx	Umleitung einer Anfrage: Der Absender muss die Anfrage erneut an die Adresse senden, die in der Umleitungs-statusnachricht angegeben ist, z.B. „301 MOVED PERMANENTLY“
4xx	Fehler bei der Bearbeitung einer Anfrage, z.B. „400 BAD REQUEST“
5xx	Anzeigen von Serverfehlern, z.B. „500 SERVER INTERNAL ERROR“
6xx	Allgemeiner Fehler: Die Anfrage hat den SIP-Server erreicht, jedoch konnte diese nicht bearbeitet werden, z.B. „600 BUSY EVERYWHERE“

für die SIP-Response unverändert übernommen. Als Sonderfall gilt die SIP-Methode ACK, da diese während des Verbindungsaufbaus als eigene Transaktion definiert ist.

Der SIP-Dialog dient der verbindungsorientierten Kommunikation und wird z.B. mit der SIP-Methode INVITE eingeleitet. Sobald eine SIP-Sitzung erfolgreich durch das 3-Way-Handshake aufgebaut wurde, werden alle zugehörigen Transaktionen (z.B. Modifikation oder Beendigung der SIP-Sitzung) dem SIP-Dialog zugeordnet. Dieser wird über das Header-Feld „Call-ID“ sowie über die „tag“-Parameter der Header-Felder „From“ und „To“ eindeutig identifiziert. Die ersten beiden Werte werden durch den UAC und der letzte Wert durch den UAS vorgegeben. Nachfolgend werden die für diese Dissertation wichtigen SIP-Transaktionen erklärt. In den Abbildungen sind die Nachrichten des UAC jeweils mit einem schwarzen Pfeil und die des UAS mit einem roten Pfeil gekennzeichnet.

Abbildung 4 zeigt den Nachrichtenaustausch zur Abfrage der unterstützten Server bzw. User Agent-Funktionsmerkmale wie z.B. SIP-Methoden oder Codecs ohne den Aufbau einer SIP-Session. Die SIP-Methode OPTIONS wird laut RFC von jedem Endgerät unterstützt und muss mit einer Status-Nachricht („200 OK“) beantwortet werden. Diese Möglichkeit ist für Angriffsszenarien besonders interessant, um z.B. die Existenz eines SIP-Servers zu überprüfen.

Abbildung 5 zeigt die Registrierung von Endgeräten (User Agents) bei einem SIP-Server mit der SIP-Methode REGISTER. Für die Registrierung werden die temporäre und permanente SIP URI übermittelt. Ist die Registrierung erfolgreich, so versendet der SIP-Server eine „200 OK“-Statusnachricht (a) als Bestätigung. Im Fehlerfall gibt es typischerweise drei verschiedene Statusnachrichten:

- Der Anwender wird mit der Nachricht „401 UNAUTHORIZED“ (b) aufgefordert seine Zugangsdaten zu übermitteln.
- „403 FORBIDDEN“ (c) lehnt die Registrierung auf Grund von falschen Zugangsdaten ab.
- „404 NOT FOUND“ (d) deutet auf eine nicht existierende Nebenstelle hin.

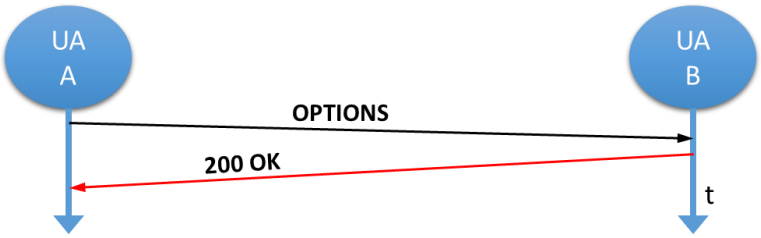


Abbildung 4: Abfrage von UAC/UAS-Eigenschaften

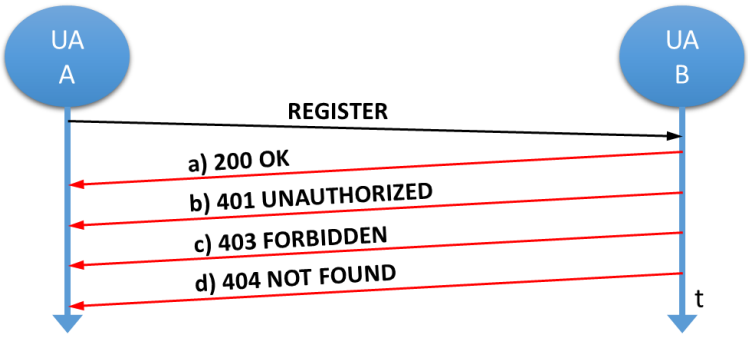


Abbildung 5: Registrierung von User Agents

Die SIP-Methode REGISTER ist für die im späteren Verlauf angesprochenen Bedrohungsszenarien von großer Bedeutung.

Für den Aufbau einer SIP-Sitzung wird die Transaktion mit der SIP-Methode INVITE eingeleitet, so dass eine verbindungsorientierte Kommunikationsverbindung auf Basis eines SIP-Dialogs ermöglicht wird.

Abbildung 6 zeigt den vorgeschriebenen 3-Way-Handshake für den Verbindungsaufbau sowie den Abbau einer SIP-Sitzung initiiert durch den SIP-Server. Die INVITE-Nachricht enthält bereits die wesentlichen Kommunikationsparameter (z.B. den gewünschten Codec) und muss mit der Meldung „200 OK“ bestätigt werden, gefolgt von einer ACK-Nachricht seitens des Clients. ACK dient der Bestätigung einer finalen Statusanfrage, wird im Protokollablauf aber niemals quittiert, obwohl es sich laut Definition um einen SIP-Request handelt. Weiterhin besteht vor der endgültigen Bestätigung durch die Nachricht „200 OK“ die Möglichkeit, provisorische Nachrichten als Statusmeldungen zu senden, die für Telefonverbindungen wichtig sind (z.B. „100 TRYING“, „180 RINGING“), so dass z.B. ein Freizeichen für den Anrufer generiert werden kann. Die Nachricht BYE bewirkt den sofortigen Abbau einer Verbindung und kann durch beide teilnehmenden Endgeräte erfolgen und muss mit einer SIP-Response beantwortet werden.

Die SIP-Methoden INVITE, BYE und CANCEL werden auch für die Abrechnung der Telefonate in den SIP-Servern verwendet, indem die Dauer des Gespräches über den Startzeitpunkt (3-Way-Handshake mit INVITE) und den Endzeitpunkt (BYE/CANCEL-Nachricht von Anwender oder Server) ermittelt wird. Da der Anwender zuvor über die Methode REGISTER an dem SIP-Server angemeldet wurde, ist eine eindeutige Identifizierung anhand der Zugangsdaten möglich. Je nach Zielrufnummer (z.B. Auslands-, Mobilfunk- und Premiumrufnummern) variieren üblicherweise die Tarife der Anbieter. Daher wird die gewählte Rufnummer aus der INVITE-Nachricht erfasst und zu Abrechnungszwecken temporär gespeichert.

2.2.5 SIP-Nachrichtenaufbau

Grundsätzlich ist der Aufbau von SIP-Requests und SIP-Responses identisch. Die SIP-Nachricht besteht aus einer Start-Zeile, einem Header und einem Body. Die Start-Zeile beinhaltet grundlegende Informationen zu der verwendeten Protokollversion und die Bezeichnung des Anfragetyps (Methode) bzw. Statuscodes. Bei SIP-Anfragen werden weiterhin die „Request URIs“ hinzugefügt. Dabei handelt es sich um die Zieladresse, an die

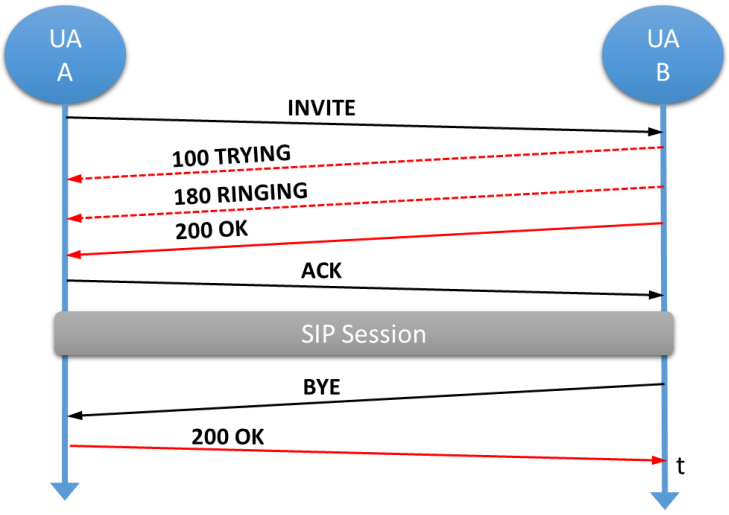


Abbildung 6: SIP-Verbindungsaufbau/-abbau und 3-Way-Handshake

sich die Anfrage richtet. Der Aufbau einer SIP-Nachricht wird in Abbildung 7 dargestellt. Der Header enthält Parameter, die den Nachrichteninhalt näher beschreiben und für den eigentlichen Nachrichtentransport von Bedeutung sind. Einige Parameter, wie z.B. „To“, „From“, „Via“ und „Call-ID“, sind für eine SIP-Nachricht zwingend vorgeschrieben, andere hingegen, wie z.B. „User Agent“ oder „Proxy-Authenticate“, sind optional.

Für die einzelnen SIP-Header-Felder gilt die folgende Syntax:

```
Header-Feld: Feldwert[;Feldparameter=Wert]
```

Das Via-Feld beinhaltet die SIP-Versionsnummer, das verwendete Transportprotokoll sowie die IP-Adresse bzw. Domain des versendenden SIP User Agents. Diese Informationen werden auf der UAS-Seite für das Zurücksenden der Statusinformationen an den anfragenden Client benötigt. Werden Anfragen z.B. über einen SIP-Server geleitet, so fügen diese Netzelemente, unter Angabe der eigenen IP-Adresse bzw. Domain, weitere Via-Felder oberhalb des bestehenden Via-Eintrags ein. Die Felder From und To definieren in Form einer SIP URI den rufenden bzw. gerufenen Teilnehmer der Kommunikationsverbindung. Über die Call-ID sowie die tag-Parameter im From- und To-Header-Feld erfolgt eine eindeutige Zuordnung einer SIP-Nachricht zu einem bestimmten SIP-Dialog zwischen zwei Endgeräten. Alle Anfragen und Statusinformationen eines SIP-Dialogs beinhalten die gleiche Call-ID, die vom initiierenden Endgerät zufällig generiert und durch die Hostadresse ergänzt wird. Die Parameter CSeq und Branch identifizieren die SIP-Transaktion. Die temporäre SIP URI wird im Feld „Contact“ durch den Absender der Nachricht vermerkt. Im Feld „Max-Forward“ ist der maximale Wert für das Weiterleiten der SIP-Nachricht definiert (Anzahl der Hops). Die Netzelemente dekrementieren diesen Wert um eins. Sobald der Wert Null erreicht wird, muss die Nachricht verworfen werden. Die Felder „Content-Type“ und „Content-Length“ spezifizieren den Typ und die Größe des nachfolgenden Message-Bodys.

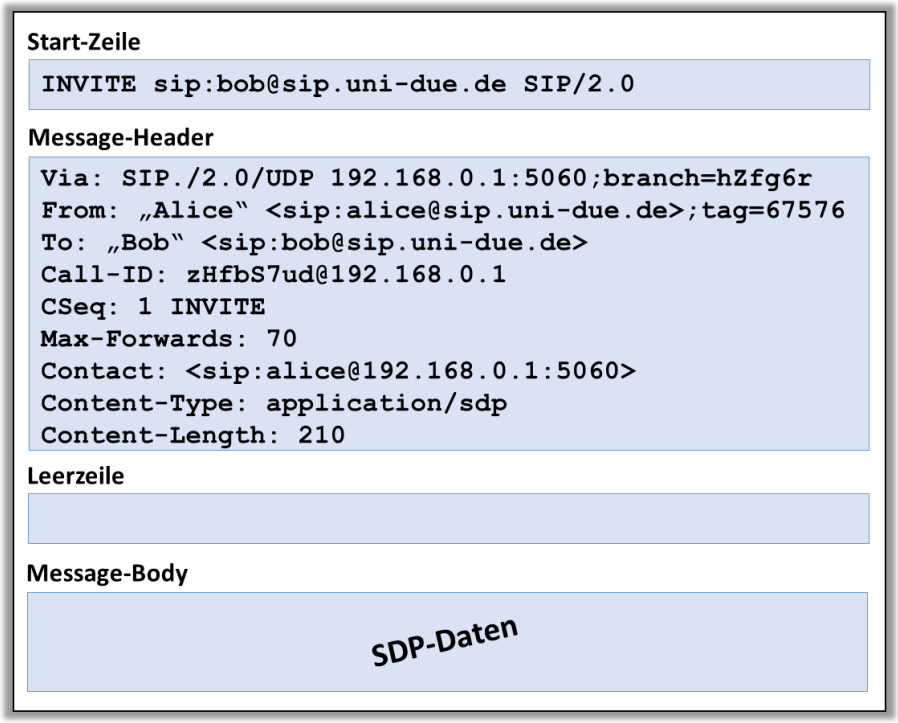


Abbildung 7: SIP Nachrichtenaufbau

Weitere Informationen für die Aushandlung der zu verwendenden Sprachcodecs werden im Message-Body übertragen. Der Austausch dieser Parameter wird per Session Description Protokoll (SDP) [18] vollzogen. Bei SDP handelt es sich um ein Standardprotokoll für die Medienaushandlung auf Basis des Offer-/Answer-Modells. Die User Agents tauschen wechselseitig die SDP-Informationen aus, die in den INVITE- und „200 OK“-Nachrichten enthalten sind. Mit Hilfe dieses Protokolls werden die Medientypen (Audio, Video), die Kontaktparameter (IP-Adresse und Port-Nummer) sowie die unterstützten Codecs der Endgeräte für die bevorstehende Kommunikationsverbindung ausgehandelt. Wie auch bei SIP wird ein ASCII-kompatibler UTF-8 Zeichensatz verwendet.

2.3 Honeypots und Honeynets

Bei einem Honeypot handelt es sich um ein Ködersystem, das bewusst interessante Netzwerkdienste mit dem Ziel anbietet, angegriffen zu werden. Das System muss ausreichend geschützt und von produktiven Umgebungen getrennt sein. Das Ziel von Honeypot-Experimenten ist die frühzeitige Erkennung von Gefahren sowie die Analyse von unterschiedlichen Angriffsmustern zur Gefahrenabwehr, so dass ein Netzwerk vor zukünftigen Angriffen möglichst geschützt ist. Daher ist es wichtig, unerlaubte Zugriffe sofort zu protokollieren und eine sorgfältige Überwachungskomponente zu installieren. Ein Honeynet ist ein aus mehreren Honeypots bestehendes Netzwerk.

2.3.1 Architektur

Bei dem Honeypot handelt es sich um einen physikalischen Computer oder um eine virtuelle Maschine mit einer speziell präparierten Software. Der Honeypot soll für den Angreifer als reales, produktiv genutztes System erscheinen. Das System ist unabhängig vom Produktivnetzwerk über eigene IP-Adressen und DNS-Einträge ansprechbar und emuliert je nach Aufgabenstellung einzelne Dienste, Applikationen oder Serversysteme mit verschiedenen Betriebssystemen. Je nach Honeypot-Typ können mehr oder weniger Interaktionsmöglichkeiten bereitgestellt werden. Dabei muss sichergestellt werden, dass der Angreifer durch die angebotene Funktionalität keinen Zugriff auf das Produktivnetz oder Kontrolle über den Honeypot erlangen kann. Die Absicherung des Honeypots stellt somit eine besondere Aufgabe dar.

Eine internationale Forschungsorganisation mit dem Namen „Honeynet-Project“ wurde 1999 gegründet und hat zahlreiche Veröffentlichungen [22] über die Definition, Architektur und den Betrieb von Honeypot-Systemen publiziert. Abbildung 8 zeigt die klassische Architektur einer Honeypot-Umgebung. Der Honeypot muss direkt mit dem Internet verbunden sein, jedoch wird dem Honeypot eine Überwachungskomponente vorgeschaltet, die typischerweise eine Firewall und ein „Intrusion Detection System“ (IDS)

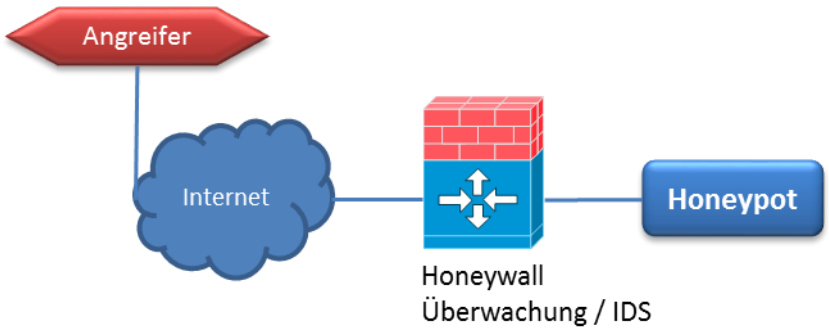


Abbildung 8: Klassische Honeypot-Umgebung

beinhaltet. Diese Komponente wird als Honeywall bezeichnet. Darüber hinaus erfolgt auf dem Honeypot und auf der Überwachungskomponente eine detaillierte Protokollierung des Angriffsverkehrs. Die gesammelten Daten werden zur Auswertung manuell oder über eine gesonderte Netzwerkschnittstelle an ein System übertragen, das für den Angreifer nicht erreichbar ist.

2.3.2 Honeypot-Typen

In der Literatur [23] wird hauptsächlich zwischen Low und High Interaction Honeypots unterschieden. Die Klassifizierung beschreibt die Intensität der Interaktionsmöglichkeiten. Bei einem Low Interaction Honeypot handelt es sich um einen sehr einfachen Typ, da lediglich Betriebssysteme, einzelne Dienste oder nur Teilfunktionen eines Netzwerkdienstes emuliert werden. Dabei wird nur so viel Funktionalität für den Angreifer bereitgestellt und implementiert, wie es für die Untersuchungen notwendig ist. Typischerweise werden keine realen Softwareprodukte eingesetzt. Die Funktionalität wird hingegen mit Skriptsprachen oder einer speziellen Honeypot-Software (z.B. HoneyD [24], Dioanea [25]) nachgebildet. So können z.B. mit der Software HoneyD ohne großen Aufwand ein Honeypot aufgesetzt und vordefinierte Netzwerkdienste in der Konfiguration aktiviert werden. Da es sich nur um eine Dienstemulation handelt, ist das Risiko einer missbräuchlichen Nutzung des Gesamtsystems durch den Angreifer relativ gering. Auf Grund der eingeschränkten Interaktionsmöglichkeiten können allerdings weitergehende Angriffe nicht analysiert und bewertet werden. Darüber hinaus besteht die Möglichkeit, dass ein Angreifer das System als Honeypot enttarnt.

Der High Interaction Honeypot hingegen bietet vollwertige Dienste an, die von produktiven Systemen nicht zu unterscheiden sind. In diesem Fall werden keine Dienste emuliert, sondern es erfolgt der Einsatz von vollwertiger Anwendungssoftware. Es werden jedoch gezielt nur die Dienste installiert, die für die Untersuchungen notwendig sind, so dass kein unnötiger Netzwerkverkehr generiert wird und keine Sicherheitslücken geöffnet werden. Im Vergleich zu Low Interaction Honeypots ist die Einrichtung deutlich komplexer, da ein Betriebssystem und die Anwendungssoftware konfiguriert und abgesichert werden müssen. Darüber hinaus muss eine geeignete Überwachung installiert werden, da dem Angreifer Zugriff auf ein vollwertiges System und somit die Möglichkeit, schadhafte Handlungen auszuführen, gegeben wird. Zusätzlich müssen Maßnahmen ergriffen werden, um kompromittierte Honeypots zu erkennen. Auf Grund der optimalen Interaktionsmöglichkeiten eignen sich High Interaction Honeypots sehr gut für die Analyse des Angriffsverhaltens und um Informationen über die Angriffswerkzeuge zu sammeln.

2.3.3 Honeypot-Software

Niels Provos entwickelte im Jahr 2002 die Honeypot-Software HoneyD, die als Open Source Software frei verfügbar ist. Die Software ermöglicht die Emulation verschiedener Netzwerkdienste (z.B. DNS). Über eine Konfigurationsdatei kann das gewünschte Antwortverhalten vordefiniert werden. Neben der Emulation von Diensten bietet die Software die Nachbildung verschiedener TCP/IP-Stacks, so dass dem Angreifer verschiedene Betriebssysteme präsentiert werden. Bei HoneyD handelt es sich somit um ein Low Interaction Honeypot, das auf einem einzelnen Host verschiedene Routing-Topologien und mehrere Honeypots mit unterschiedlichen Diensten emulieren kann. Die Protokollierung erfolgt lokal, so dass in diesem Fall ein zusätzliches externes Auswertungssystem notwendig ist.

Ende 2009 haben Markus Koetter und Mark Schlösser mit dem Dioanea-Framework [25] ein Low Interaction Honeypot entwickelt, das aktuellen Anforderungen (wie z.B. IPv6, SIP,

TLS) gerecht werden sollte. Da es auf der Skriptsprache Python [26] basiert, kann die Software sehr einfach erweitert werden. Dioanea kombiniert die bisher verfügbaren Tools in einer aktuellen Software mit stark erweiterten Interaktionsmöglichkeiten und wird daher neben den High Interaction Honeypots auch in dieser Dissertation eingesetzt (siehe Kapitel 2.4.2).

2.3.4 Honeynets

Für die Untersuchungen in dieser Dissertation wird ein Honeynet eingesetzt, das High und Low Interaction Honeypots beinhaltet. Dabei handelt es sich um ein Netzwerk von Honeypots, das aus dem Internet erreichbar ist. Der Low Interaction Honeypot basiert auf Dioanea und der High Interaction Honepot basiert auf Asterisk [3] (siehe Kapitel 2.4.1). Bei dem aufgebauten Honeynet handelt es sich um ein reales Netzwerk, das mit Hilfe von Monitoring-Komponenten stark überwacht wird und von der produktiven Umgebung komplett getrennt ist. Eine vorgeschaltete Firewall begrenzt den Zugriff auf die zu analysierenden SIP-Dienste, so dass die Honeypots, abgesehen von ICMP, auf den übrigen Netzwerkports nicht erreichbar sind. Honeynets bieten dem Angreifer einen größeren Anreiz und ganz bewusst ein größeres Angriffspotenzial sowie mehr Interaktionsmöglichkeiten als ein einzelner Host. Durch die Betrachtung mehrerer verschiedener Hosts kann das Verhalten der Angreifer im Netzwerk beobachtet und verstanden werden.

Da das Honeynet keine Produktivaufgabe hat, wird jeglicher Datenverkehr zu den Honeypots als Angriffsverkehr klassifiziert. Üblicherweise erfolgt die Überwachung mit einer Honeywall (Firewall- und Monitoring-Komponente) zwischen Internet und Honeynet. In dem entwickelten VoIP-Honeynet sollte ein möglicher Angriff auf die Analyse- und Überwachungskomponenten auf jeden Fall verhindert werden, so dass für diese Dissertation bewusst ein anderer Netzwerkaufbau gewählt wurde, der in Kapitel 4.1 und 4.2 erläutert wird.

2.4 Eingesetzte Software

Im Rahmen dieser Dissertation werden verschiedene Softwarekomponenten benötigt, die für die Untersuchungen und das entwickelte Testbed von zentraler Bedeutung sind. Nachfolgend werden diese vorgestellt. Die konkrete Konfiguration wird in Kapitel 5 erläutert.

2.4.1 Asterisk

Die frei verfügbare Software PBX „Asterisk“ [3] ist ein zentrales Softwarepaket für die VoIP-Honeypots. Zum Einsatz kommt die Version 1.6. Asterisk ist eine quelloffene Software-Telefonanlage und ermöglicht in Kombination mit einem Linux-System den Aufbau einer leistungsfähigen VoIP-Telefonanlage mit Schnittstellen zum herkömmlichen Telefonnetz. Dabei besteht die Möglichkeit, einerseits gängige „klassische“ Protokolle wie T1 oder Loopstar, andererseits neue wie die zunehmende Zahl an VoIP-Protokollen (z.B. SIP, SIPS [27], IAX [28], H.323 [12]) zu verwenden. Neben Konkurrenzprodukten wie FreeSwitch [29] oder Yate [30] ist Asterisk am weitesten verbreitet und bietet darüber hinaus eine umfassende Dokumentation sowie Unterstützung in der Community. Die Software Asterisk wird immer stärker zur Konkurrenz von proprietären, kommerziellen Telefonanlagen und ermöglicht den Betreibern von Telefonsystemen große Freiheiten und somit Eigenentwicklungen. Verschiedene Unternehmen vertreiben auf Basis von Asterisk

kommerzielle Produkte (wie z.B. Askozia[6]) mit Support und ausgefeilten Business-Funktionen. Asterisk wird über eine Vielzahl von Konfigurationsdateien individuell eingestellt und verwaltet, so dass diese Software für einen SIP-basierten Honeypot sehr gut geeignet ist. Das System arbeitet ressourcenschonend und ist sehr gut skalierbar.

2.4.2 Dionaea

Das Dionaea-Framework [25] ist quelloffen, modular und entstand 2009 im Rahmen des „Google Summer of Code“. Der Quellcode in Python ist somit frei verfügbar und kann verändert bzw. weiterentwickelt werden, so dass Anpassungen für das VoIP-Honeypot sehr einfach möglich sind. Die Vorteile von Dionaea sind die Unterstützung von aktuellen Protokollen wie z.B. IPv6 oder TLS, besonders jedoch die Implementierung des Session Initiation Protokolls (SIP). Es werden die folgenden, wichtigen SIP-Methoden unterstützt: OPTIONS, REGISTER, INVITE, ACK, CANCEL und BYE. Über eine dateibasierte SQlite[7]-Datenbank können für das SIP-Modul Nebenstellen und Zugangsdaten definiert werden, die nach dem Systemstart für Angreifer zur Verfügung stehen. Dionaea bietet über die Features eines Low Interaction Honeypots hinaus umfangreiche Protokollierungs-funktionen. Aus Sicherheitsgründen und zur Korrelierung der Angriffe erfolgt das gesamte Monitoring des VoIP-Honeynets für diese Dissertation zentral, so dass keine Messdaten von eventuell missbräuchlich genutzten Honeypots abgerufen werden müssen. Daher bleiben die Dioanea-Protokollierungsfunktionen deaktiviert.

2.4.3 Sipvicious

Bei SIPvicious [31] handelt es sich um eine White-Hacking-Toolsuite, die quelloffen, frei verfügbar und in Python [26] programmiert ist. Es werden fünf Programme angeboten:

(1) SVMAP wird für das Durchsuchen von Netzwerken nach SIP-Komponenten verwendet, indem SIP-Anfragen der Methode OPTIONS an typischerweise alle IP-Adressen in einem zuvor definierten Subnetz gesendet werden. Anhand der Statusantwort werden aktive SIP-Server erkannt. Darüber hinaus kann das Durchsuchen auch mit INVITE- oder REGISTER-Paketen erfolgen.
(2) SVWAR ermöglicht die Abfrage von aktiven Nebenstellen eines SIP-Servers, indem REGISTER-Pakete für einen definierten Wertebereich versendet und ausgewertet werden. Das Tool erkennt anhand von Antwortpaketen automatisch, ob eine Nebenstelle existiert.
(3) Mit SVCRACK sollen die Kennwörter mittels Brute-Force-Attacke von den detektierten Nebenstellen erraten werden. Hier können zufällige Zeichenketten oder vorhandene Wörterbücher für den Angriff verwendet werden.
(4) SVREPORT dient der Auswertung und Aufbereitung der Angriffsergebnisse.
(5) Das Zusatzprogramm SVCRASH soll fehlgeschlagene SVWAR- und SVCRACK-Angriffe abbrechen.

2.5 Hypervisor und Hardwarekomponenten

Für die Umsetzung der im Rahmen dieser Dissertation benötigten Softwarekomponenten wurde eine in Hinblick auf Ressourcen flexible Hardware-Umgebung benötigt, die jederzeit angepasst und erweitert werden konnte. Darüber hinaus wurden für die verteilten Sensoren möglichst mobile und stromsparende Hardware notwendig, so dass ein Einsatz

[6] AskoziaPBX IP-Telefonanlage, http://askozia.com/de/

[7] SQLite software library, http://www.sqlite.org/

der Sensoren an verschiedenen Standorten möglich war. In Kapitel 5.5 wird eine Übersicht über die nachfolgend beschriebenen Komponenten gegeben.

2.5.1 VMware ESXi Hypervisor

Für das VoIP-Honeynet und das verteilte Sensorsystem werden unterschiedliche Anforderungen an Hard- und Software sowie an die Netzwerkarchitektur gestellt. Damit die Versuchsumgebung schnell auf neue Bedürfnisse (z.B. Ressourcenverbrauch und Netzwerkanbindungen) angepasst werden kann, wird auf der VMware ESXi-Umgebung [32] des Lehrstuhls aufgebaut. Hier handelt es sich um einen Verbund von drei ESXi-Servern in der Version 5.1 mit insgesamt 52 physikalischen CPU-Kernen (104 logische CPUs), 480 GB Arbeitsspeicher sowie 25 TB Massenspeicher. VMware ESXi ist ein Bare-Metal-Hypervisor, so dass mehrere virtuelle Maschinen auf nur einer Hardware eingesetzt werden können.

Alle eingesetzten Komponenten sind als virtuelle Maschinen aufgesetzt worden. Dadurch können diese bei Bedarf leicht neu konfiguriert oder dupliziert werden. Auch die Zuweisung der Ressourcen kann bedarfsorientiert verändert werden. Die notwendige Netzwerkanbindung und Zuordnung von benötigten Subnetzen ist so mit geringstem Aufwand über die Steuerungssoftware der virtuellen Umgebung möglich.

2.5.2 Intel NUC

Die Firma Intel stellt mit der „Next Unit of Computing“ (NUC[8]) eine sehr kompakte x64-Hardwareplattform mit aktueller Prozessortechnologie bereit, so dass jedes aktuelle Betriebssystem installiert werden kann. Das System bietet auf kleinstem Raum die Leistungsdaten eines aktuellen Computers bei geringem Stromverbrauch. So wird ein Intel Core-i5-4250U Prozessor (2,6 MHz) mit zwei Kernen (vier logische CPUs), vier GB Arbeitsspeicher sowie einer 64 GB SSD-Festplatte (SATA-Anbindung) eingesetzt. Der Arbeitsspeicher lässt sich bis auf 16 GB und die SSD aktuell bis ein TB erweitern. Eine Gigabit-Netzwerkschnittstelle, USB3.0-Anschlüsse und eine HD-Grafikkarte vervollständigen diesen Mini-PC. Trotz der großen Leistungsreserven liegt der Stromverbrauch im Leerlauf bei unter 10 W. Die Kosten liegen pro Stück bei ca. 250 EUR. Durch die kompakte Bauform, den geringen Stromverbrauch und die gebotenen Ressourcen ist das Gerät für den verteilten Sensor sehr interessant und kann auch in Umgebungen mit großem Datendurchsatz eingesetzt werden.

2.5.3 Raspberry Pi

Der Raspberry Pi[9] ist im Vergleich zum Intel NUC nochmals kleiner und deutlich preiswerter (ca. 70 EUR). Dieses Gerät kam 2012 auf den Markt und wird überwiegend zum Experimentieren und Programmieren eingesetzt. Es handelt sich um einen Single Board Computer mit Broadcom ARM11-Prozessor (ein Kern mit 700 MHz) und 512 MB Arbeitsspeicher. Eine zusätzliche Grafikeinheit erlaubt das Verarbeiten von HD-Material. Als Massenspeicher kann jedoch nur auf eine SD-Karte zugegriffen werden. Da auf diesem Gerät Linux installiert werden kann, wurde auch der Raspberry Pi für das verteilte Sensorsystem vorgesehen, da der günstige Preis gerade in kleinen Netzwerkumgebungen die Verteilung der entwickelten Sensoren ermöglichen soll. Der Stromverbrauch ist mit ca. vier Watt im Leerlauf sehr gering.

[8] Intel NUC, http://www.intel.de/content/www/de/de/nuc/overview.html

[9] http://www.raspberrypi.org/

3 Bedrohungen und Stand der Wissenschaft

Dieses Kapitel gibt einen Überblick über die Bedrohungen in VoIP-Netzwerken und grenzt den Arbeitsbereich dieser Dissertation ab. Nachfolgend werden die möglichen Kommunikationsszenarien erläutert und die für den Schwerpunkt dieser Arbeit relevanten Angriffsstufen vorgestellt. Das Kapitel schließt mit der Diskussion von Veröffentlichungen, die in den Arbeitsbereich dieser Dissertation fallen.

3.1 Bedrohungen im Bereich Voice over IP

Bedingt durch Voice over IP kommt es zu einer neuen Netzkonvergenz: Die klassischen Telefonnetze werden aufgelöst und in die IP-Netzwerke werden Telefoniedienste integriert. Für eine Bedrohungsanalyse müssen Missbrauchsszenarien betrachtet werden, die sich durch die Kombination von Telefoniediensten mit IP-basierten Netzwerken ergeben.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in der umfangreichen VoIP-SEC-Studie [33] die klassischen Sicherheitsziele für eine sichere IP-Kommunikationsverbindung angeführt: Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität. Da es sich bei VoIP-Diensten um IP-basierte Anwendungen handelt, sind diese auch von den Bedrohungen der zugrunde liegenden IP-Netzwerke betroffen. Nachfolgend wird die Notwendigkeit der Schutzziele verdeutlicht:

- **Vertraulichkeit**
  Die traditionelle Telefonie läuft über getrennte Transportnetze, so dass ein Angreifer üblicherweise zunächst Zugriff auf das Transportnetz erlangen muss. Bei der VoIP-Telefonie wird das IP-Netz des Datenverkehrs mitbenutzt, so dass ein Zugriff deutlich erleichtert wird. Darüber hinaus können die IP-basierten Standardprotokolle (z.B. SIP) mit verfügbaren Werkzeugen sehr einfach überwacht werden.
- **Integrität**
  Da es sich bei IP-Telefonen und VoIP-Telefonanlagen um computerbasierte Systeme handelt, muss die Integrität des Gesamtsystems (Betriebssystem, VoIP-Software) sichergestellt sein, da ein Angreifer ein kompromittiertes System steuern und manipulieren könnte. Neben dem Abhören von Gesprächen könnten diese gezielt umgeleitet oder unter anderer Identität initiiert werden.
- **Verfügbarkeit**
  Die Verfügbarkeit des Telefoniedienstes mit einer ausreichenden Sprachqualität ist für viele Wirtschaftszweige, aber auch für Rettungskräfte elementar wichtig. Durch die Verschmelzung von Telefonie- und Datennetzwerk kann die Verfügbarkeit durch bekannte IP-basierte Angriffe beeinträchtigt werden.
- **Authentizität**
  Im Gegensatz zu den klassischen leitungsgebundenen Telefonnetzen muss die Identität des Anwenders mit Hilfe von Zugangsdaten geprüft werden. Gelingt es einem Angreifer, die Identität gegenüber dem VoIP-Server zu fälschen, so können Gespräche auf Kosten Dritter geführt werden (siehe Kapitel 3.1.2.3).

3.1.1 Bedrohungen in IP-basierten Netzwerken

Die vom BSI erstellte VoIP-SEC-Studie unterscheidet zwischen den passiven Angriffen in IP-basierten Netzwerken, die das Mitlesen von Nachrichten ermöglichen (Sniffing) und den deutlich kritischeren aktiven Angriffen, die Nachrichten an Opfersysteme versenden oder manipulieren. Die folgenden Angriffe der Netzwerkebene in IP-basierten Netzwerken sind laut der VoIP-SEC-Studie auch für die VoIP-Kommunikation relevant:

- **Man-in-the-Middle**
  Ein Angreifer befindet sich zwischen zwei kommunizierenden Systemen und kann die übermittelten Pakete manipulieren oder eigene Nachrichten unter fremden Namen versenden.
- **Netzwerk- und Port-Scans**
  Der Angreifer ermittelt durch das Versenden von Nachrichten aktive Dienste in einem Subnetz und versucht mittels Fingerprinting möglichst viele Informationen über ein System zu sammeln.
- **Spoofing Angriffe**
  Für diesen Angriff werden Nachrichten mit gefälschten Informationen versendet, so dass das Opfersystem auf Grund der gefälschten Adressierungsinformationen dem Angreifer vertraut (z.B. IP-/DNS-Spoofing).
- **Replay Angriffe**
  Der Angreifer protokolliert authentisierte Nachrichten, um diese zu einem späteren Zeitpunkt zu verwenden.
- **DoS und DDos Angriffe**
  Denial of Service Angriffe sollen die Verfügbarkeit von Systemen stören, indem Ressourcen wie Rechenleistung, Arbeitsspeicher oder die Bandbreite einer Kommunikationsverbindung bewusst herabgesetzt werden. Weitere Angriffe zielen jedoch bewusst auf Implementierungsschwachstellen ab. Bei einem Distributed Denial of Service Angriff werden ausgehend von mehreren Systemen gezielt Angriffe auf ein Opfersystem ausgeführt. Dieser Angriffstyp wird von einem Angreifer gezielt gesteuert.

Bezogen auf die Applikations- und Anwenderebene werden Bedrohungen wie SPAM, Phishing, Malware, Wörterbuchangriffe und der Diebstahl von Zugangsdaten in der Studie genannt und sind somit auch für die Missbrauchsszenarien in VoIP-Netzwerken relevant.

3.1.2 Missbrauchsszenarien in VoIP-Netzwerken

Anbieter von VoIP-Dienstleistungen verfolgen das gleiche Geschäftsmodell wie bei der herkömmlichen Telefonie, d.h. ein Anbieter ermöglicht einem Kunden den Zugriff auf das Telefonnetz und erhält für diesen Service Gebühren. Da der Zugang im Vergleich zum herkömmlichen Telefonnetz nicht über eine dedizierte Leitung bzw. ein getrenntes Transportnetz erfolgt und somit dieses eindeutige Identifizierungsmerkmal entfällt, muss eine Identifizierung über die IP-Adresse oder die Zugangsdaten (Benutzername, Kennwort) erfolgen. Falls der VoIP-Anbieter jedoch nicht der Betreiber des IP-Netzwerkes ist oder eine Anmeldung von einem externen Netzwerk erfolgt, kann der Anwender nicht über die IP-Adresse identifiziert werden. Da VoIP die weltweite, standortunabhängige Nutzung des Telefonanschlusses ermöglicht und eine Dienstnutzung z.B. bei einer Auslandsreise möglich ist, kann die Anmeldung bzw. Anwenderidentifizierung nur über individuelle Benutzerkennungen erfolgen.

In Kombination mit den Bedrohungen aus den IP-basierten Netzen ergeben sich im Vergleich zur klassischen Telefonie neue Missbrauchsszenarien, die im Rahmen des durchgeführten BMBF-Projektes SUNSHINE[10] [7] identifiziert wurden:

3.1.2.1 Abhören von Telefonaten

Da die Signalisierung und Sprachübertragung in SIP-basierten Netzwerken üblicherweise unverschlüsselt abläuft, sind Anwender in öffentlichen Netzwerken besonders gefährdet (z.B. öffentlicher WLAN-Hotspot). Aber auch ein Eingriff in die Signalisierung und Umleitung der Datenströme an Angreifer ist denkbar (z.B. anderer Registrar Server über DNS-Manipulation).

3.1.2.2 Stören von Telefonaten

Hier muss zwischen generischen Kommunikationsstörungen bedingt durch bekannte IP-basierte Angriffe und VoIP-spezifischen Angriffen unterschieden werden.

Da VoIP-Endgeräte auf eine funktionierende IP-Verbindung zu dem VoIP-Dienst angewiesen sind, kann über eine DNS-Manipulation die Verbindung zum Provider gestört und somit das Telefonat unterbunden werden. Weiterhin handelt es sich bei einem IP-Telefon um einen vollwertigen Mini-PC, der über Diagnose- bzw. Managementschnittstellen (Webserver) angegriffen werden kann (Ausnutzung von Schwachstellen bzw. Implementierungsfehlern). Die VoIP-Infrastruktur des Providers kann mit DDoS-Angriffen gestört werden, so dass keine Telefonate mehr möglich sind.

Unabhängig von den bekannten IP-basierten Bedrohungen sind Angriffe auf VoIP-Signalisierungsprotokolle auf der Anwendungsebene möglich, so dass z.B. durch fehlerhafte Pakete die Telefonanlagen-Software abstürzt.

3.1.2.3 Finanzieller Vorteil

Da die Identitätserkennung nur auf Basis von Zugangsdaten erfolgt, wird die Anmeldung bei einem Providersystem mit einer fremden Identität durchgeführt. Dies wird möglich, wenn durch vorausgegangene Angriffe Zugangsdaten erbeutet wurden. Hier sind Angriffe auf der Netzwerkebene (z.B. Man-in-the-Middle, Sniffing im WLAN), aber auch Angriffe auf der Anwendungsschicht möglich (z.B. Phishing, Brute-Force-Attacken auf VoIP-Dienste). Zusätzlich kann ein Angreifer über einen kompromittierten Account Telefondienste für Dritte anbieten, um selber Gewinne auf Kosten anderer erwirtschaften zu können. Darüber hinaus werden Anwender durch Bedrohungen wie z.B. Phishing oder SPAM dazu gebracht, Mehrwertnummern anzurufen. Alternativ kann ein Angreifer die eigenen Mehrwertnummern durch einen kompromittierten Account anrufen bzw. Anrufe gezielt umleiten lassen und somit finanzielle Vorteile generieren.

3.1.2.4 Unerwünschte Anrufe (SPIT)

In Anlehnung an die SPAM-Problematik im E-Mail-System besteht in VoIP-Netzwerken die Bedrohung durch SPIT-Anrufe (SPAM over Internet Telephony). Diese werden durch kostenlose Gespräche innerhalb der durch Provider betriebenen Telefonnetze, aber auch durch nun mögliche Direktverbindungen zwischen den SIP-Komponenten, im Vergleich zu den klassischen Telefonnetzen, begünstigt.

3.1.2.5 Unterlaufen der Flatrate Mischkalkulation

Der Missbrauch von privaten Telefontarifen für geschäftliche Zwecke ist im VoIP-Umfeld durch die standortunabhängige Nutzung besonders einfach möglich. Es handelt sich jedoch

[10] BMBF-Projekt SUNSHINE, http://www.sunshineproject.net/index.html

um einen Missbrauch durch den Anwender und nicht um Bedrohungen über die Netzwerk- bzw. Applikationsebene.

3.2 Arbeitsbereich und Abgrenzung der Dissertation

Da der Ausbau der IP-basierten Sprachkommunikation auf Basis des SIP-Protokolls schnell voranschreitet und große Provider die Migration bis zum Jahr 2018[11] abgeschlossen haben wollen, wird die Notwendigkeit der Untersuchung von SIP-spezifischen Angriffen deutlich. In dieser Dissertation werden Angriffe untersucht, die mit der Einführung von SIP-basierten Sprachdiensten im Internet entstehen und nicht aus Bedrohungen der Netzwerkschicht oder aus rechtlichen Vertragsbestimmungen resultieren. Das Ziel dieser Angriffe ist das Erlangen eines finanziellen Vorteils, indem ein Angreifer kompromittierte Zugänge für Auslandstelefonate oder für Anrufe zu Premiumnummern auf Kosten der Anschlussinhaber nutzt.

Angriffe, die sich auf den Sprachdienst auswirken, jedoch durch Bedrohungen auf der Netzwerkebene bedingt sind (z.B. DDos, DNS-Spoofing, Sniffing), werden in dieser Dissertation nicht betrachtet, da diese Angriffe auch bei normalen Rechnersystemen funktionieren. Für diese Angriffe existieren bereits Lösungen aus den IP-Netzwerken, die bei Bedarf aktiviert werden können. Um das Abhören von Gesprächen in öffentlichen Netzwerken zu verhindern, wäre der Einsatz von VPN-Verbindungen bzw. Verschlüsselungsfunktionen möglich. DDoS-Angriffe sind ebenfalls ein Problem aus IP-Netzwerken und können durch Intrusion Detection Systeme bzw. durch Aktivierung von gezielten Stateful-Firewall-Regeln abgeschwächt werden. Sind diese darüber hinaus durch das gezielte Ausnutzen von Sicherheitslücken bedingt, so müssen auch die VoIP-Komponenten (Endgeräte und Server) stets auf dem aktuellsten Stand der Software gehalten werden.

Das Unterlaufen der Flatrate-Mischkalkulation ist ein Vertragsbruch durch den Anwender. Dieses kann durch die providerseitige Überwachung des Gesprächsaufkommens kontrolliert werden und bei einer deutlichen Überschreitung der festgelegten Parameter erfolgt eine veränderte Abrechnung bzw. Anpassung des Vertrages. Auf diesem Gebiet gibt es Verfahren, die von einem SUNSHINE-Projektpartner entwickelt wurden und auf der Auswertung von Call Detail Records (CDR) [34] basieren [7].

Zu Beginn der Untersuchungen für diese Dissertation wurden auch unerwünschte Anrufe (SPIT) in die Voruntersuchungen miteinbezogen. In einem Kooperationsprojekt mit einem Hersteller von VoIP-Telefonanlagen wurde ein SPIT-Filter zur Abschwächung von unerwünschten Anrufen erarbeitet. Es stellte sich jedoch heraus, dass es zwar einzelne SPIT-Anrufe gab, diese jedoch in der Honeynet-Umgebung während des Feldtests kaum nachweisbar waren.

Daher liegen die Schwerpunkte dieser Arbeit in den folgenden Bereichen:

1. Analyse von Bedrohungsszenarien mit dem Ziel, kostenlose Telefonverbindungen auf Kosten Dritter mit einhergehendem Identitätsdiebstahl zu führen (Toll Fraud) oder finanzielle Gewinne durch den Betrug mit Mehrwertdiensten zu erreichen.
2. Entwicklung von Mechanismen für die automatische Angriffserkennung in Echtzeit mit dem Ziel, aktive Angriffe abschwächen zu können.

[11] http://www.heise.de/newsticker/meldung/Telekom-beschleunigt-Umstieg-auf-IP-Telefonie-mit-Kuendigungen-2405049.html

3.3 Kommunikationsszenarien für das Angriffsziel Toll Fraud

Nachfolgend werden drei relevante Kommunikationsszenarien in SIP-basierten Netzwerken vorgestellt, die auch bei der Erkennung von Toll Fraud-Angriffen berücksichtigt werden müssen.

3.3.1 Endanwender-Szenario

Im Endanwender-Szenario (siehe Abbildung 9) wird davon ausgegangen, dass ein Kunde einen SIP-basierten Telefonanschluss bei einem Provider hat und ein Home-Gateway (wie z.B. die weitverbreitete FritzBox) zum Registrieren der SIP-Accounts einsetzt. Da die Kommunikation über das Internet stattfindet, gibt es zwei potenzielle Angriffsmöglichkeiten: Zum einen die SIP-Schnittstelle auf Kundenseite und zum anderen den SIP-Server des Providers. Auf beiden Seiten besteht die Gefahr, dass ein Angreifer die aktiven SIP-Komponenten durch Subnetz-Scans auffinden und die eingerichteten SIP-Accounts mit entsprechenden Angriffen übernehmen kann. Das Ziel sind sogenannte Toll Fraud-Anrufe, d.h. der Angreifer telefoniert auf Kosten des Kunden.

3.3.2 Firmen-Szenario

Mittelständische Unternehmen betreiben meist eigenständig Telefonanlagen, die eine SIP-Schnittstelle über das Internet anbieten. Dies ist z.B. notwendig, damit Außendienstmitarbeiter weltweit die Möglichkeit haben, die eigene Nebenstelle zu nutzen und somit unter einer gleichbleibenden Rufnummer erreichbar zu sein. Darüber hinaus können Telefonate zu Standardkonditionen geführt werden. Abbildung 10 zeigt, dass sowohl die Mitarbeiter als auch die Angreifer die SIP-Schnittstelle über das Internet erreichen können. Ziel des Angreifers ist es, mit mehrstufigen Angriffen eine Nebenstelle zu kompromittieren und diese für Toll Fraud-Anrufe zu nutzen.

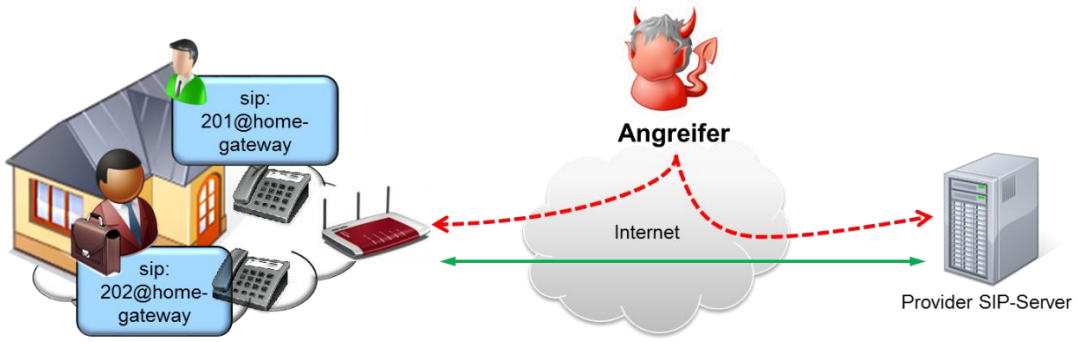


Abbildung 9: Endanwender SIP-Szenario

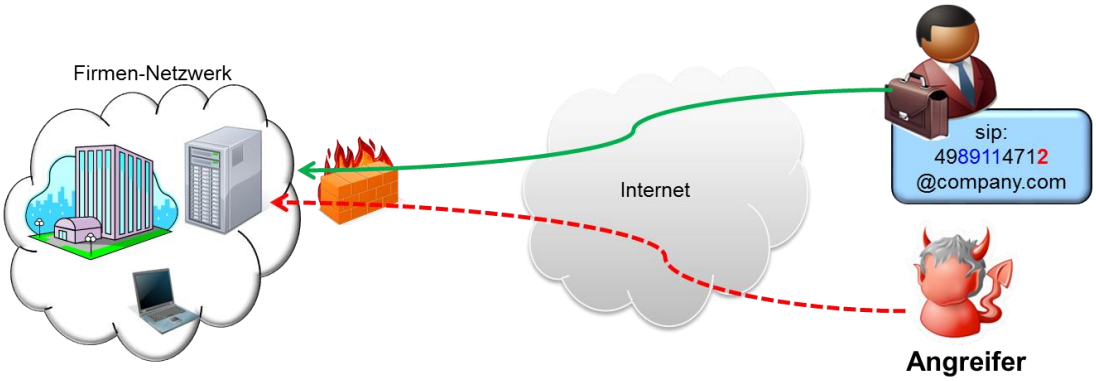


Abbildung 10: Firmen SIP-Szenario

3.3.3 Enterprise- / Provider-Szenario

Im Gegensatz zu den vorherigen Szenarien setzen große Firmen oder Provider aus dem Enterprise-Umfeld mehrere SIP-Server ein, die über einen „Session Border Controller“ (SBC) [35] an das Internet angebunden sind. Abbildung 11 zeigt, dass die Kommunikation in diesem Fall immer über den SBC läuft, so dass die einzelnen SIP-Server nach außen hin nicht sichtbar sind. Der SBC trennt das interne Firmennetzwerk vom Internet. Ein SBC ist ein B2B-User Agent, so dass dieser nach Definition der SIP-Transaktionen in die Signalisierung mit einbezogen ist. Darüber hinaus gibt es Sicherheitsmerkmale, die vor defekten SIP-Paketen und DoS-Angriffen schützen sollen. Da Außendienstmitarbeitern die Möglichkeit geboten wird, die eigene Nebenstelle über das Internet zu verwenden, können auch potenzielle Angreifer mit möglichst unauffälligen Angriffen (niedrige Paketanzahl für Angriffe zur Vermeidung der Firewall-Abwehr) eine Nebenstelle auffinden und übernehmen. Eine kompromittierte Nebenstelle kann von den Angreifern für den eigenen finanziellen Vorteil genutzt werden, indem z.B. Telefoniedienste für Dritte angeboten oder die eigenen Mehrwertrufnummern gewählt werden.

3.4 Relevante Angriffsstufen für Toll Fraud

Die Erfahrungen mit den frei verfügbaren Angriffswerkzeugen und die Honeynet-Analysen dieser Dissertation haben gezeigt, dass vier relevante Angriffstypen existieren, die notwendig sind, um als Angreifer eine SIP-Nebenstelle übernehmen zu können. Das Ziel dieser Angriffe ist, Telefonate über das kompromittierte Serversystem zu Premium-Rufnummern (z.B. 0900) oder zu Auslandsrufnummern zu führen.

3.4.1 Server Scan

Abbildung 12 zeigt, dass für den Angriffstyp „Server Scan“ ein Angreifer versucht, aktive SIP-Komponenten in einem Netzwerkbereich aufzufinden, indem einzelne IP-Adressen oder alternativ ganze Subnetze ähnlich wie bei einer „Ping“-Anfrage abgefragt werden. Dazu nutzt der Angreifer die Tatsache, dass nach Vorschrift im SIP-RFC ein Endgerät SIP-Nachrichten der Methode OPTIONS beantworten muss. Ist ein SIP-Gerät in einem gescannten Subnetz aktiv, so beantwortet dieses die OPTIONS-Anfrage mit der Statusnachricht „200 OK“ und wird somit identifiziert. Für diesen Angriffstyp wird mindestens eine SIP-Nachricht pro Host verwendet. Wird hingegen ein Server ohne aktiven

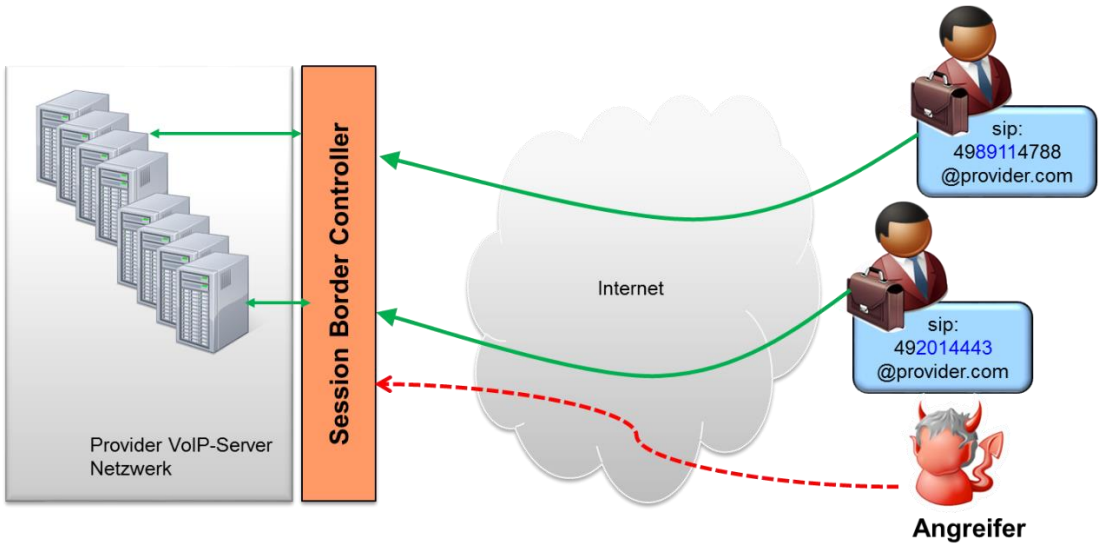


Abbildung 11: Enterprise SIP-Szenario

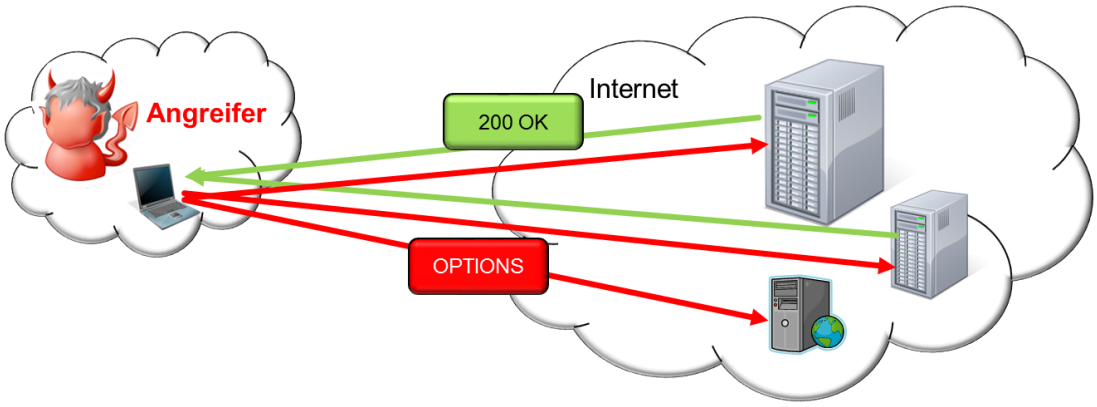


Abbildung 12: Angriffstyp Server Scan

SIP-Dienst angesprochen (z.B. ein Webserver), erfolgt keine Rückmeldung. Mit dem Angriffswerkzeug kann in diesem Fall geprüft werden, ob es sich um eine SIP-Komponente mit einem veränderten, nicht standardkonformen SIP-Stack handelt. Dafür kann der Server Scan auch mit den SIP-Methoden REGISTER oder INVITE durchgeführt werden.

3.4.2 Extension Scan

Der zweite Angriffstyp „Extension Scan“ dient zur Identifizierung von aktiven Nebenstellen auf einem zuvor erkannten SIP-Server. Üblicherweise erfolgen systematische Registrierungsversuche (SIP-Methode: REGISTER) für verschiedene Nebenstellen, jedoch ohne Zugangsdaten. Dies zeigt deutlich, dass zunächst aktive Nebenstellen identifiziert werden sollen. Als Nebenstellenkennung werden aufsteigende Zahlen im Bereich von 100 bis 9999, aber auch Buchstabenkombinationen gewählt. Abbildung 13 zeigt, dass der SIP-Server in Abhängigkeit von der gewählten Nebenstelle mit verschiedenen SIP-Statusnachrichten antwortet. Bei einer korrekten Nebenstellenkennung wird die REGISTER-Anfrage vom Server mit einer „401 UNAUTHORIZED“- (fehlende Zugangsdaten) oder „403 FORBIDDEN“-Nachricht (falsches Kennwort) beantwortet. Existiert die angefragte Nebenstelle hingegen nicht, so erhält der Angreifer eine „404 NOT FOUND“-Nachricht. Das Ergebnis dieses Angriffstyps ist eine vollständige Liste aktiver Nebenstellen eines Servers. Die Analysen dieser Dissertation haben gezeigt, dass ein Angreifer für einen Angriff dieses Typs bis zu 40.000 SIP-Nachrichten an ein Serversystem sendet.

3.4.3 Registration Hijacking

Die Liste der Nebenstellen wird für den nachfolgenden Angriffstyp „Registration Hijacking“ verwendet. Pro aktiver Nebenstelle versucht der Angreifer das Passwort zu erraten. Dazu

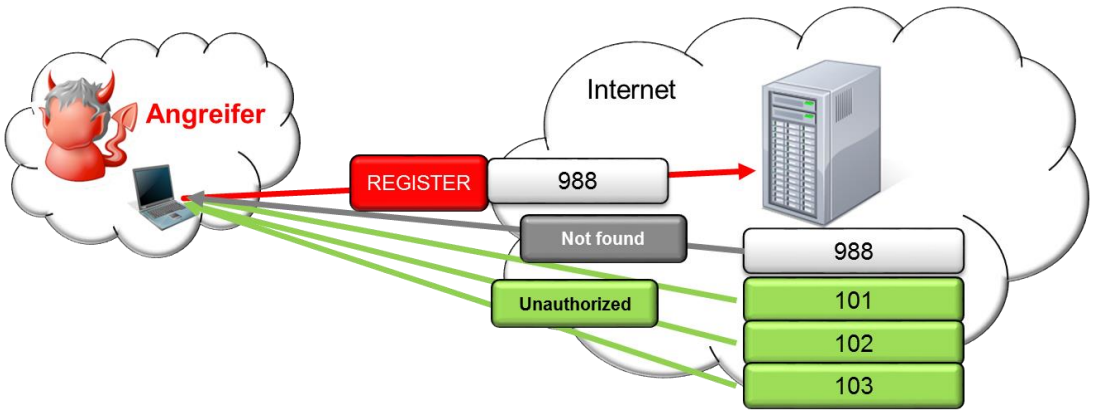


Abbildung 13: Angriffstyp Extension Scan

werden zahlreiche REGISTER-Nachrichten mit unterschiedlichen Passwörtern an den Server gesendet. Diese Angriffsstufe kann im Vergleich zu den vorherigen Stufen enorme Ausmaße annehmen (bis zu 13 Millionen Pakete pro Nebenstelle). Wie in Abbildung 14 gezeigt, wird bei einem falschen Kennwort die SIP-Statusnachricht „403 FORBIDDEN“ von dem SIP-Server an den Angreifer gesendet. Bei einem korrekten Passwort für die Nebenstelle 103 empfängt der Angreifer den Statuscode „200 OK“ und speichert diese Information für eine spätere Registrierung an dieser Nebenstelle. Typischerweise werden für diesen Angriff zufällige numerische Passwörter, aber auch unterschiedlich umfangreiche Wörterbücher mit alphanumerischen Kennwörtern verwendet.

3.4.4 Toll Fraud

Der Toll Fraud-Angriff ist der vierte Angriffstyp. Wie in Abbildung 15 gezeigt, registriert sich ein Angreifer an einer zuvor identifizierten Nebenstelle (a). Diese Registrierung unterscheidet sich nicht von herkömmlichen Anwendern, da dem Angreifer alle notwendigen Informationen zu diesem Zeitpunkt bekannt sind. Auf SIP-Ebene sind eine einzelne, erfolgreiche Registrierung sowie INVITE-Nachrichten für die Anrufe sichtbar. Der Angreifer hat nun die Möglichkeit, über eine fremde Nebenstelle internationale Anrufe oder Anrufe zu Premium-Diensten (0900) zu tätigen, indem INVITE-Nachrichten mit der gewünschten Zielrufnummer gesendet werden (b). Darüber hinaus besteht die Möglichkeit, Telefoniedienste für Dritte über eine gehackte Nebenstelle anzubieten und über diesen Weg anonym zu bleiben. Daher ist es möglich, dass die Toll Fraud-Versuche von unterschiedlichen Quell-IP-Adressen ausgehen, wenn die Angreifer die Zugangsdaten untereinander austauschen.

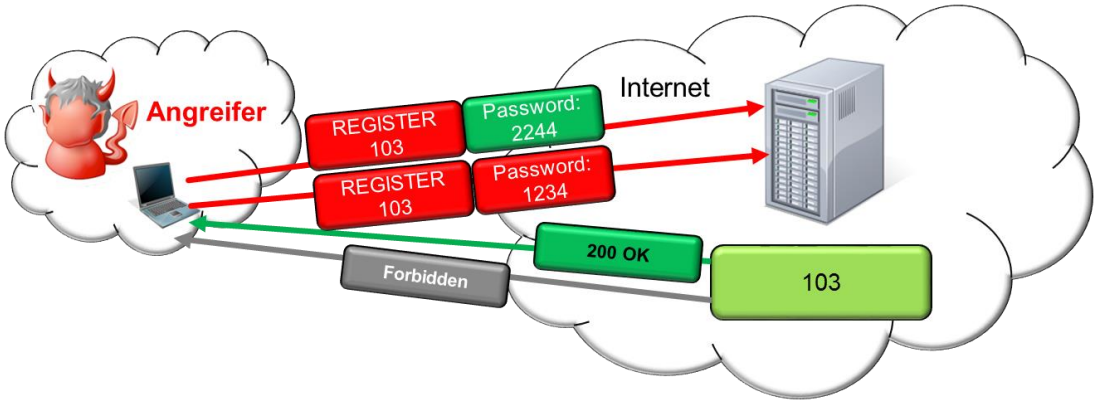


Abbildung 14: Angriffstyp Registration Hijacking

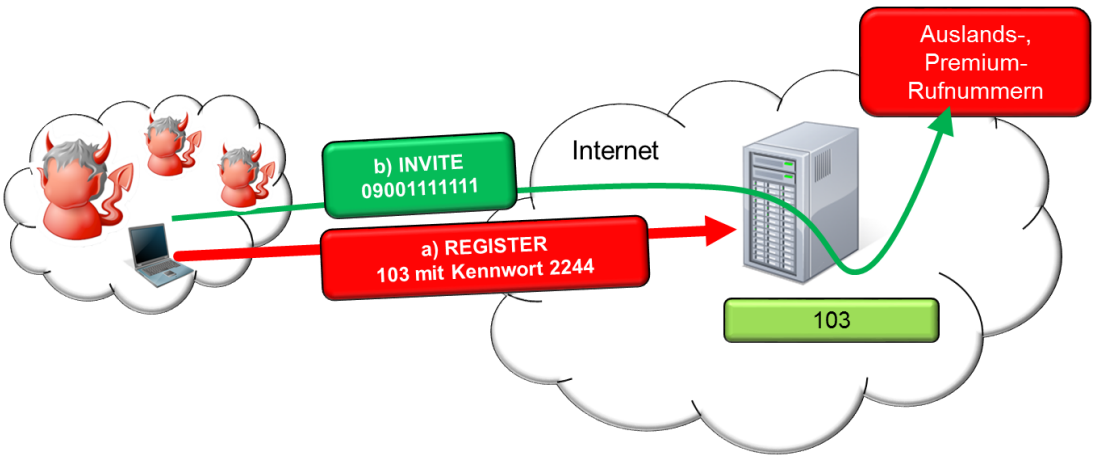


Abbildung 15: Angriffstyp Toll Fraud

3.5 Stand der Forschung

Da SIP auf IP basiert, erläutern J. Rosenberg et al. in [1], dass die existierenden Bedrohungen der IP-basierten Netzwerke auch auf SIP übertragen werden können (z.B. DoS-, Spoofing-, Man-in-the-Middle-Attacken). Zusätzlich werden SIP-spezifische Angriffsmuster genannt, wie z.B. Registration/Call-Hijacking, illegaler Aufbau/Abbau von SIP-Sessions oder SPIT. Als möglicher Lösungsansatz wird nur eine Ende-zu-Ende-Verschlüsselung genannt, die jedoch nicht das Betrugs- und Missbrauchsproblem von SIP-Servern durch mehrstufige Toll Fraud-Angriffe lösen kann. Daher wird in dieser Dissertation der Schwerpunkt auf die Missbrauchserkennung von SIP-Komponenten gelegt.

Für die Erkennung von DoS-Angriffen in SIP-Netzwerken zeigt S. Ehlert in [36] einen Lösungsansatz auf. Es werden drei Algorithmen vorgestellt, um DoS und DDoS-Angriffe detektieren und abwehren zu können. Um zwischen regulärem SIP-Verkehr und DoS-Angriffen unterscheiden zu können, wird ein Erkennungsschema spezifiziert. Diese Arbeit stellt einen vielversprechenden Ansatz für die DoS-Problematik dar. Um jedoch andere Angriffstypen erkennen zu können, ist eine viel detailliertere Analyse der SIP-Daten notwendig. Dies wird in dieser Dissertation mit der forensischen Analyse und der verteilten Echtzeiterkennung aufgegriffen.

Für Honeypots gibt es unterschiedliche Konzepte und Ansätze für verschiedene Fragestellungen, die I. Mokube et al. in [23] erläutern. Das Ziel der Honeypot-Konzepte ist die Erkennung von unautorisierten Zugriffen auf IT-Systeme. Während Low Interaction Honeypots nur bestimmte Funktionen eines Dienstes simulieren und Zugriffe protokollieren, basieren High Interaction Honeypots auf realen Implementierungen und bieten eine vollständige Dienstfunktionalität. Üblicherweise werden mehrere Honeypots zu einem Honeynet zusammengeschlossen, das als reales produktives Netzwerk erscheint, jedoch aus Sicherheitsgründen strikt überwacht und separiert werden muss. Zur Beantwortung einer Fragestellung zum Angreiferverhalten wurde für diese Dissertation zusätzlich ein Low Interaction Honeypot eingesetzt, da dieses individuell angepasst werden kann und somit eine Reaktion auf das Angreiferverhalten ermöglicht (siehe Kapitel 4.5).

In [37] beschreiben Nassar et al. ein Intrusion Detection System, das für die Erkennung von SIP-Angriffen entwickelt wurde. Dieses System basiert auf einem Low Interaction Honeypot, das in [38] beschrieben wird. Bei diesem Ansatz handelt es sich um eines der ersten VoIP-Honeypots, das speziell für die Erkennung von Denial of Service- und Anruf-Angriffe (wie z.B. SPIT) ausgelegt wurde. Darüber hinaus sollen mit dem Honeypot Informationen über den Angreifer gesammelt werden (Fingerprinting), indem eine aktive Interaktion stattfindet (z.B. Portscan des Angreifer-Systems).

Da nur ein Low Interaction Honeypot verwendet wurde und der Schwerpunkt auf DoS- und Anruf-Attacken lag, stellt dieser Ansatz nur eine begrenzte Funktionalität zur Verfügung und hat somit eine sehr eingeschränkte Sicht auf das Netzwerk und die Funktionsweise anderer Angriffstypen. Für das Verständnis und die Erkennung vielfältiger Angriffe wird ein Honeypot mit möglichst vollständiger SIP-Funktionalität benötigt, das von einem produktiven SIP-Server nicht zu unterscheiden ist. Darüber hinaus sollte die Überwachung nicht auf ein einzelnes System oder eine einzelne IP-Adresse begrenzt sein.

In [39] wurde durch C. Valli eine erste, einfache statistische Analyse zu Angriffen in SIP-basierten Netzwerken durchgeführt. Die Verkehrsdaten für diese Analyse wurden in mehreren virtuellen Low Interaction Honeypots dateibasiert aufgezeichnet und anschließend für die paketbasierte Auswertung abgerufen. Die Ergebnisse zeigen, dass für die Angriffe auf die Honeypots primär das Tool Sipvicious benutzt wurde und dass ein weiteres Tool mit der Bezeichnung „sipsscuser“ gefunden wurde. Der Autor spekuliert über

ein Verhalten, das an ein Bot-Netz oder eine wurmähnliche Aktivität erinnert. Bei diesem Ansatz werden die Messdaten auf den einzelnen Honeypots gespeichert. Dies sollte vermieden werden, da die Opfersysteme jederzeit von Angreifern kompromittiert werden können. Berücksichtigt man die Funktionalität des White-Hacking-Tools SIPvicious, so ist eine möglichst globale Überwachung notwendig, die sich nicht auf einige wenige IP-Adressen im Netzwerk beschränkt.

Um die genannten Probleme abzuschwächen, wurde für diese Dissertation eine Honeynet-Lösung gewählt, die zusätzlich auf einem High Interaction Honeypot basiert. So ist die bestmögliche Interaktion mit dem Angreifer gewährleistet. Zusätzlich erlauben ein zentrales und entkoppeltes Monitoring und eine automatisierte Analysekomponente die sichere Überwachung gesamter Subnetze und eine bidirektionale Korrelierung von SIP-Nachrichten für eine statusbehaftete Auswertung. Für das Verständnis des Angreiferverhaltens ist es über die paketorientierte Analyse hinaus notwendig, die SIP-Nachrichten verschiedenen Angriffstypen zuordnen zu können. Dazu wurde der Ansatz in dieser Dissertation mit einem regelbasierten Clustering-Algorithmus optimiert (siehe Kapitel 4.3), der die unterschiedlichen Angriffe in SIP-basierten Netzwerken automatisiert erkennt.

In [40] beschreiben Y. Wu et al. eine IDS-Architektur zur Erkennung von Angriffen in VoIP-Netzwerken. Sollen SIP-Missbrauchsversuche mit bestehenden Intrusion Detection Systemen, wie z.B. Snort [41] oder Bro [42] erkannt werden, so ergeben sich einige Probleme: Die Erkennung von Angriffen basiert bei einem IDS auf einzelnen Paketen, indem der Inhalt jeder eingehenden Nachricht mit den vorhandenen Signaturen verglichen wird. Da die SIP-Kommunikation jedoch auf Sitzungen beruht, müssen die SIP-Pakete untereinander korreliert und zu unterschiedlichen Angriffstypen zugeordnet werden, so dass die Untersuchung auf Auffälligkeiten in einem einzelnen Paket nicht ausreicht. Eine weitergehende Erkennung von Bedrohungen durch die Korrelierung der SIP-Nachrichten und die Einbeziehung unterschiedlicher Netzwerkstandorte wird durch die verteilte Echtzeiterkennung ermöglicht (siehe Kapitel 4.6).

Parallel zu den Entwicklungen und Untersuchungen dieser Dissertation wurde an der Technischen Universität Wien von M. Gruber et al. ein VoIP-Honeynet aufgesetzt und die Verkehrsdaten wurden ausgewertet [43] [44] [45]. Der Ansatz basiert auf High Interaction Honeypots, die über eine Honeywall zwecks Monitoring nach dem klassischen Honeynet-Konzept an das Internet angebunden sind. Der eingehende Traffic wird auf der Honeywall in PCAP-Dateien gespeichert, die täglich von einer Analysekomponente abgerufen werden. Das IDS Snort generiert Alarme, sobald eine vordefinierte Regel bei einem Datenpaket zutrifft.

Das System überwacht nur die wenigen Honeypot-IP-Adressen in zwei verschiedenen Netzwerken und ermöglicht eine einfache statistische Analyse in Bezug auf die Anzahl der eingehenden Pakete, die Herkunftsländer der Angreifer und die verwendeten User Agents. Die vorliegenden Ergebnisse beziehen sich auf einen Zeitraum von August 2011 bis Dezember 2012.

Ein interessanter Aspekt ist die Möglichkeit, die missbräuchlich getätigten Anrufe der Angreifer zeitweise in das klassische Telefonnetz zu vermitteln, um weitere Informationen durch das Aufzeichnen von Audio-Daten zu erhalten. Aus rechtlichen und aus Kostengründen wurde dieser Ansatz an der Universität Duisburg-Essen nicht verwendet, jedoch implementiert. Da der genutzte Ansatz auf dem Honeywall-Prinzip aufbaut, muss diese gegen Angriffe im Internet sehr gut geschützt werden, da hier die Messdaten gespeichert werden und die Überwachungskomponenten des Honeynets eingerichtet sind.

Könnte ein Angreifer die Honeywall kompromittieren, so hätte dies fatale Folgen für das Forschungssystem. Darüber hinaus werden nur wenige IP-Adressen überwacht, so dass die Sicht auf das Angreiferverhalten begrenzt ist. Durch das tägliche Abrufen und Einlesen der Verkehrsdaten aus den PCAP-Dateien entsteht eine erhebliche Verzögerung für die Analysekomponenten.

Die genannten Probleme sollen durch den in dieser Dissertation entwickelten Honeynet-Überwachungsansatz gelöst werden, indem gesamte Subnetze überwacht, die Verkehrsdaten direkt geparst und in eine SQL-Datenbank für die Analyse geschrieben werden. Die Ergebnisse der automatischen Analysen werden direkt auf einer zugehörigen Management-Website angezeigt. Damit die Überwachungs- und Analysekomponente für Angreifer unsichtbar und nicht angreifbar ist, erfolgt die Anbindung passiv über einen Mirror-Port des Routers.

Die Einbeziehung unterschiedlicher Netzwerkstandorte zur umfassenden Analyse der Angriffsaktivitäten in SIP-basierten Netzwerken wird auch von J. Safarik in [46] thematisiert. Nur durch die Vergrößerung des Beobachtungsgebietes kann das Angreiferverhalten genauer untersucht werden. Das vorgestellte System basiert auf vorgefertigten Software-Images des Honeypots Dionaea [25], das an verschiedenen Standorten installiert wird. Die Verkehrsdaten werden in der Dioanea-Datenbak lokal gespeichert und periodisch zu einem zentralen Server übertragen, um eine weitergehende Analyse zu ermöglichen. Für die Realisierung des Ansatzes wird die Installation und Wartung von ressourcenaufwändigen Hardware- und Softwarekomponenten notwendig.

Die Erfahrungen während dieser Dissertation haben jedoch gezeigt, dass derartige Honeypot- und Monitoring-Lösungen, die in [46] und [43] gezeigt werden, nur sehr selten von Dritten akzeptiert werden. Dies ist durch den Installationsaufwand, den Ressourcenverbrauch, den Managementaufwand und die Datenschutzbedenken der Unternehmen oder der Netzanbieter begründet. Um diese Probleme abzuschwächen, wurde für diese Dissertation das verteilte Sensor System entwickelt, das leichtgewichtige Sensoren zur signaturbasierten Erkennung auf Remote-Systemen einsetzt und nur im Alarmfall Nachrichten an einen zentralen Dienst zur Auswertung und Korrelierung der erkannten Angriffe sendet.

Auch bei VoIP-Umgebungen besteht die Möglichkeit, dass Bot-Netze für den Angriff eingesetzt werden. A. Dainotti et al. beschreiben in [47] die Ergebnisse einer durchgeführten Analyse zu Bot-Netzen in einem „/8“-Forschungsnetzwerk. Die Autoren ordnen die empfangenen Pakete dem „Sality botnet“ zu, das einen sehr umfangreichen Scan im IPv4-Adressraum (mutmaßlich /0-Scan) durchgeführt und auch SIP-Pakete für den Angriff verwendet hat. Bei den Analysen für diese Dissertation wird daher berücksichtigt, ob es bei den vorliegenden SIP-Verkehrsdaten der unterschiedlichen Messstellen Hinweise auf Bot-Netze gibt.

4 Konzept und wissenschaftliche Neuerungen

Aktuelle Sicherheitsprobleme, wie der Missbrauch von VoIP-Servern und Betrugsversuche, sind auch in SIP-basierten Netzwerken bekannt und in den letzten Jahren enorm angestiegen. Aktuelle Softwareprodukte für das Monitoring von Unternehmens- und Providernetzwerken auf NetFlow-Basis [48] zeigen in aggregierter Form die Verkehrsdaten (z.B. IP-Adressen der Verbindungen, übertragenes Datenvolumen).

Bei Experimenten mit der Monitoring-Software IsarFlow[12] eines Kooperationspartners wurde jedoch deutlich, dass der SIP-Angriffsverkehr in den überwachten Netzwerken im Verhältnis zu den übrigen Protokollen (z.B. HTTP, SSH) auf Grund der geringen Datenmenge nicht als auffällig ausgewiesen wurde. Darüber hinaus konnte keine Unterscheidung zwischen den Angriffstypen getroffen werden, da die Verbindungsinformationen nur aggregiert vorliegen und ein Zugriff auf die SIP-Header nicht möglich ist. Gängige Intrusion Detection Systeme, wie z.B. Snort [41], verwenden üblicherweise statische Regeln mit Suchmustern für einzelne Datenpakete und verzichten auf eine Korrelierung verschiedener Nachrichten einer oder mehrerer Verbindungsbeziehungen.

Für eine detaillierte Sicht und die Entwicklung von effektiven Lösungen zur Erkennung und Abwehr von SIP-Angriffen sind andere Systeme notwendig. Zunächst müssen die aktuellen Angriffe detailliert untersucht und das Angriffsverhalten muss verstanden werden. Zu diesem Zweck wurden für diese Dissertation seit Oktober 2008 umfangreiche Untersuchungen mit Ködersystemen durchgeführt und Ansätze für die automatische SIP-Angriffserkennung entwickelt. Die Konzepte und wissenschaftlichen Neuerungen werden nachfolgend vorgestellt. Am Ende dieses Kapitels erfolgt eine Einordnung der Konzepte dieser Arbeit sowie der in Kapitel 3.5 vorgestellten relevanten Veröffentlichungen.

4.1 Analyse von Angriffen mit einem Honeypot

Um Angriffe auf SIP-basierte Serversysteme besser verstehen und analysieren zu können, wird ein dienstspezifischer Honeypot benötigt, der sich in seinem Verhalten nicht von produktiven SIP-Servern unterscheiden darf und im realen Internet zu Messzwecken eingesetzt werden kann. Somit können verfügbare Angriffswerkzeuge in einer Laborumgebung getestet und die Funktionalitäten verstanden werden. Darüber hinaus erlaubt der Einsatz eines Honeypots mit Anbindung an das Internet eine Aussage über die Existenz und die Intensität der aktuell laufenden Angriffe.

In Anlehnung an den aus der Literatur bekannten klassischen Honeypot-Ansatz wird ein Rechnersystem mit dem Betriebssystem Linux und der Open Source Telefonanlage Asterisk [3] aufgesetzt und als Honeypot konfiguriert. Die Anbindung an das Internet und die Absicherung des Systems sind durch eine vorgeschaltete Firewall sichergestellt, so dass ausschließlich SIP-Pakete auf dem Standard-Port 5060 akzeptiert und weitergeleitet werden. Abbildung 16 zeigt den Netzwerkaufbau. Für die Angreifer sind vier Nebenstellen mit einfachen Kennwörtern konfiguriert, so dass das System über das Internet auffindbar und für einen Angreifer potenziell interessant ist. Die Überwachung des SIP-Verkehrs erfolgt mit dem Werkzeug tcpdump [49], das alle eingehenden und ausgehenden SIP-Pakete lokal im PCAP-Format [50] aufzeichnet. Durch eine zusätzliche, detaillierte

[12] IsarFlow, http://isarflow.de/home/

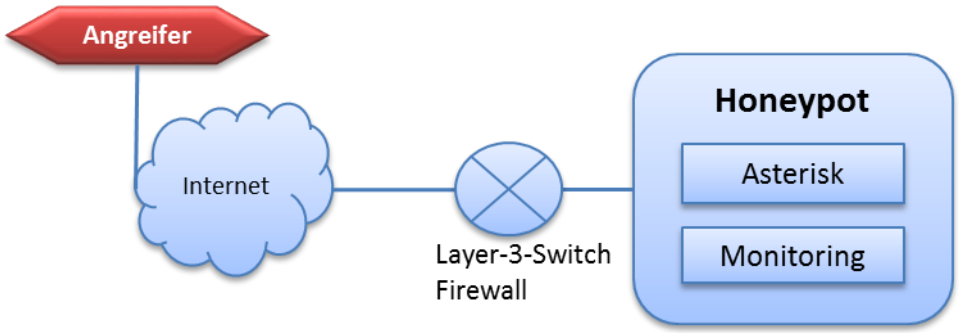


Abbildung 16: Single Honeypot Netzwerkaufbau

Protokollierung des Asterisk-Servers wird eine spätere Offline-Analyse der Angriffe ermöglicht.

Mit Hilfe dieses Systems wird geklärt, ob eine öffentliche IP-Adresse aus dem Universitätsnetzwerk bereits Ziel von Angriffen ist bzw. mit welcher Intensität diese ablaufen. Parallel kann das Angriffsverhalten der verfügbaren Angriffswerkzeuge an dem eingerichteten Honeypot überprüft und nachvollzogen werden.

Obwohl die IP-Adresse des Honeypots nicht veröffentlicht wurde, ist das System nach wenigen Tagen von Angreifern aus dem Internet gefunden und angegriffen worden. Abbildung 17 zeigt für wenige Tage intensive Angriffe der Angriffstypen Extension Scan und Registration Hijacking mit über 80.000 SIP-Paketen pro Tag. Darüber hinaus wurden einzelne OPTIONS-Pakete aufgezeichnet. Diese deuten auf einen Server Scan im Netzwerk hin und lassen vermuten, dass auch weitere Netzwerkbereiche angegriffen wurden. Die eingeschränkte Sicht mit nur einem Honeypot und die sicherheitskritische lokale Protokollierung müssen somit für umfassendere Untersuchungen optimiert werden.

4.2 Netzwerkweite Analyse des Angriffsverhaltens

Damit die Untersuchungen nicht nur auf die manuelle Auswertung einzelner Hosts begrenzt sind, wird eine großflächige Überwachung für gesamte Subnetze benötigt. Darüber hinaus muss die lokale Protokollierung verändert werden, damit eine möglichst detaillierte und automatische Auswertung des SIP-Verkehrs möglich ist.

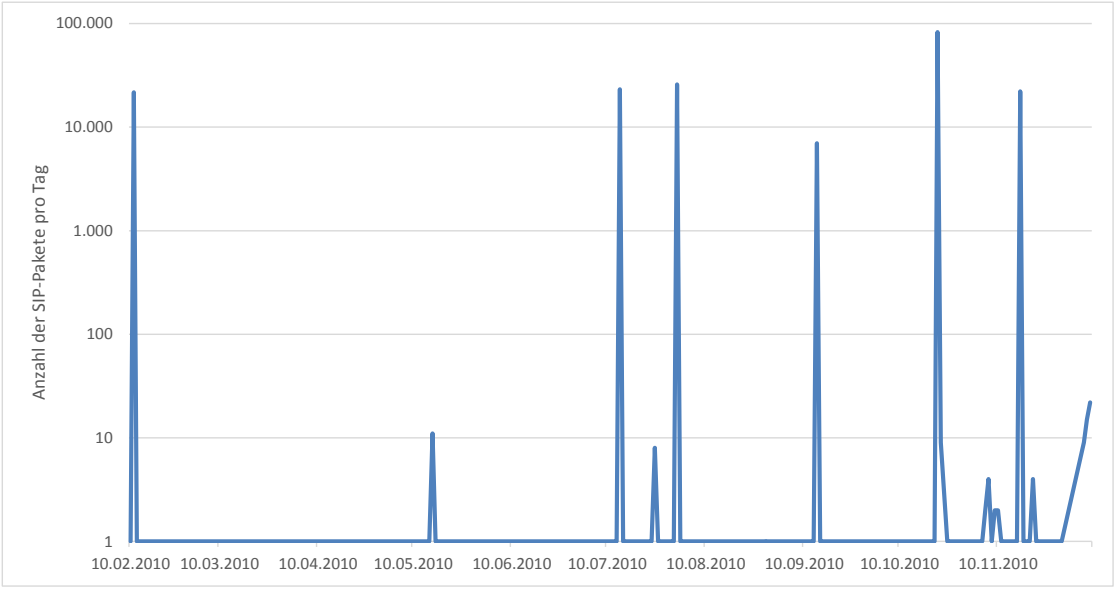


Abbildung 17: Single Honeypot System: Anzahl der SIP-Pakete pro Tag

Dafür müssen die folgenden Aspekte berücksichtigt werden:

- Einrichtung weiterer Honeypots zur Etablierung mehrerer Messpunkte im Netzwerk, so dass eine großflächige Analyse möglich wird
- Virtualisierung der Honeypots zur besseren Skalierbarkeit und Ressourcen-optimierung (VMware ESXi [32])
- Sammlung der Verkehrsdaten an einem zentralen Punkt zur Vermeidung der lokalen Aufzeichnung pro Honeypot und Erleichterung der Auswertung
- Sichere und für den Angreifer unsichtbare Anbindung der Überwachungs-komponenten
- Vergleich von Netzwerken mit und ohne SIP-Komponenten für die Analyse des Angreiferverhaltens in unterschiedlichen Umgebungen
- Möglichst einfache bzw. automatisierte Analyse der aufgezeichneten SIP-Nachrichten und Abwendung von einer dateibasierten Aufzeichnung (PCAP-Dateien)
- Webbasierte Darstellung von wiederkehrenden statistischen Auswertungen
- Berücksichtigung der Datenschutzproblematik in produktiven Firmen-Netzwerken

Abbildung 18 zeigt die erweiterte Honeynet-Umgebung, die aus dem Internet erreichbare SIP-Server zur Verfügung stellt und den gesamten ein- und ausgehenden SIP-Datenverkehr mit dem für diese Dissertation entwickelten Analysewerkzeug SIP Trace Recorder (STR) [4] überwacht (siehe Kapitel 5.2). Eine Firewall verbindet zwei Class-C-Netzwerke mit dem Internet und verhindert alle Zugriffe, die sich nicht auf das SIP-Protokoll beziehen. Das erste Netzwerk beinhaltet mehrere SIP-Honeypots und das zweite Netzwerk enthält keine SIP-Komponenten, so dass ein Vergleich zwischen diesen Netzwerken möglich ist.

Im Vergleich zu Tools wie z.B. tcpdump, die den gesamten Datenverkehr auf einer Netzwerkschnittstelle aufzeichnen und in PCAP-Dateien für die weitergehende Analyse (z.B. mit Wireshark [51]) abspeichern, hat der STR einige entscheidende Vorteile:

- Filterung auf das SIP-Protokoll
- Ausblendung der nicht relevanten OSI-Schichten und Protokolle
- Die gesammelten Daten werden nicht chronologisch in vielen, großen Dateien abgelegt, sondern strukturiert und nach benötigten Header-Feldern gefiltert in

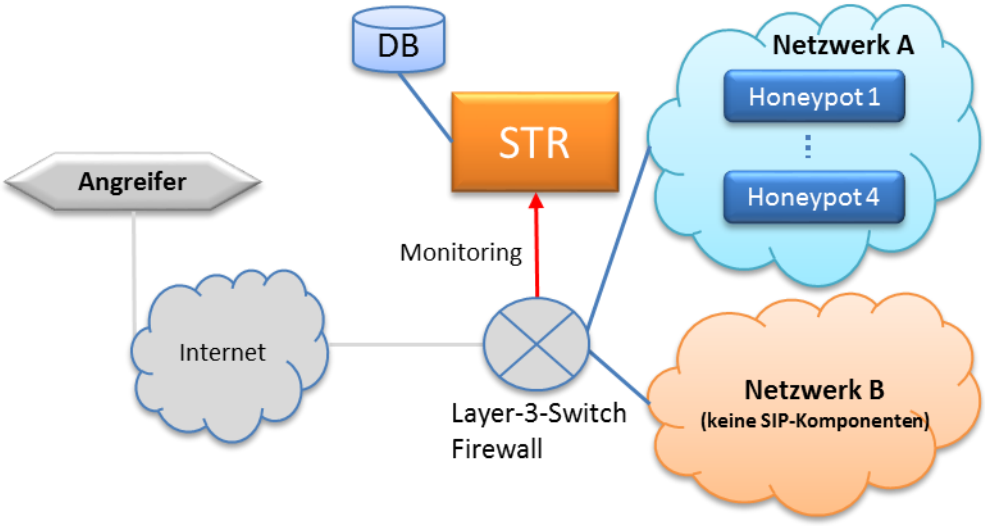


Abbildung 18: Architektur Honeynet

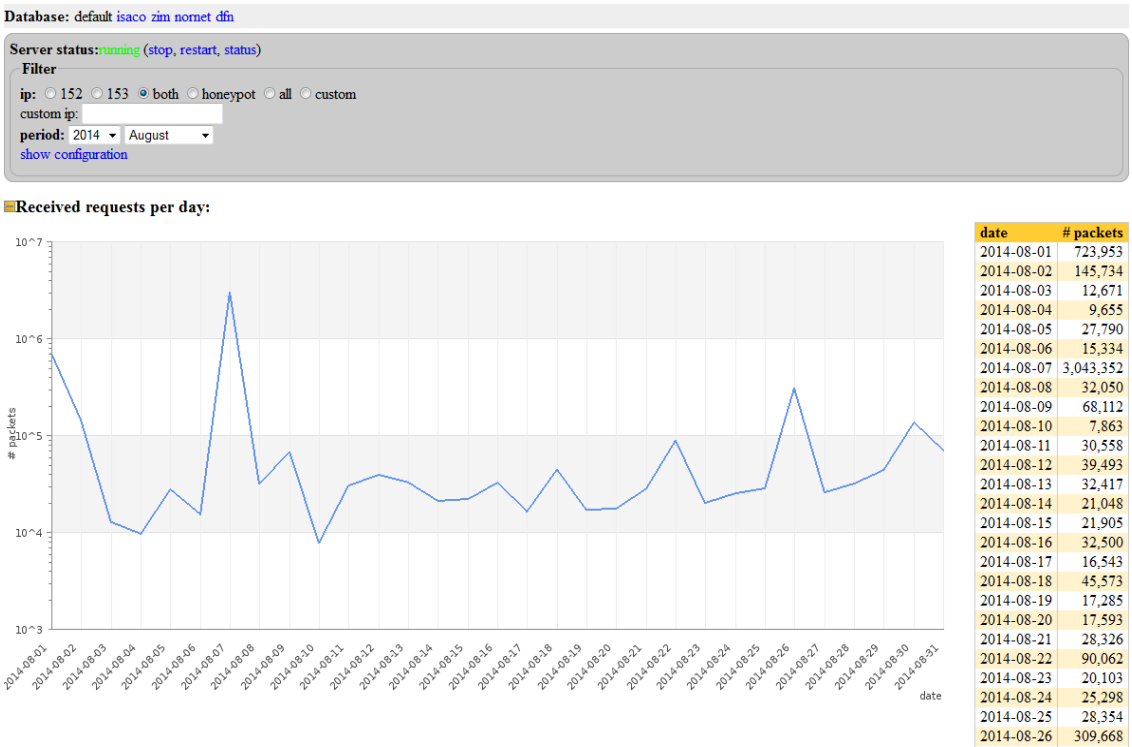
einer SQL-Datenbank unter Berücksichtigung der Abhängigkeiten zwischen den SIP-Nachrichten abgespeichert.

- Bei einer Analyse entfällt das Suchen und Öffnen verschiedener Dateien abhängig vom Zeitraum.
- Durch die SQL-Datenbank sind alle Daten der aufgezeichneten SIP-Pakete sofort für eine Auswertung auf Basis von standardisierten SQL-Abfragen verfügbar.
- Die Funktionen einer höheren Programmiersprache (z.B. PHP [52]) können verwendet werden, so dass auch komplexe Abfragen unproblematisch sind.

Über eine Management-Website sind vordefinierte statistische Auswertungen (z.B. Anzahl der Pakete pro Tag bzw. pro IP-Adresse, Herkunft der IP-Adressen), die täglich automatisch aktualisiert werden, abrufbar. Die Filteroptionen erlauben eine übersichtliche Darstellung und Auswahl der gewünschten Daten. Neben den statistischen Ergebnissen können zu jedem aufgezeichneten SIP-Paket die Header-Informationen abgerufen werden. Abbildung 19 zeigt einen Ausschnitt der STR-Management-Website mit den SIP-Nachrichten pro Tag für den Monat August 2014.

Sollen in einem Netzwerk verschiedene Bereiche durch den STR überwacht werden, so können mehrere Aufzeichnungsmodule mit einem zentralen Datenbankserver verbunden werden, wodurch das Kopieren von Aufzeichnungsdateien, wie z.B. bei tcpdump, von verschiedenen Standorten entfällt. Darüber hinaus ist es möglich, PCAP-Dateien, die an anderen Standorten aufgezeichnet wurden, zur Analyse in den STR zu importieren. Alternativ können STR-Datenbanken anderer Standorte eingelesen werden, damit eine vergleichende Analyse für verschiedene Standorte durchgeführt werden kann.

Damit der STR auch in produktiven Umgebungen mit hohen Datenschutzanforderungen eingesetzt werden kann, erlaubt die „Privacy“-Funktion eine Teilanonymisierung der SIP-Verbindungsdaten, indem einige Header-Felder mit einer SHA-2-Hashfunktion mit



date	# packets
2014-08-01	723,953
2014-08-02	145,734
2014-08-03	12,671
2014-08-04	9,655
2014-08-05	27,790
2014-08-06	15,334
2014-08-07	3,043,352
2014-08-08	32,050
2014-08-09	68,112
2014-08-10	7,863
2014-08-11	30,558
2014-08-12	39,493
2014-08-13	32,417
2014-08-14	21,048
2014-08-15	21,905
2014-08-16	32,500
2014-08-17	16,543
2014-08-18	45,573
2014-08-19	17,285
2014-08-20	17,593
2014-08-21	28,326
2014-08-22	90,062
2014-08-23	20,103
2014-08-24	25,298
2014-08-25	28,354
2014-08-26	309,668

Abbildung 19: STR-Management-Website (Ausschnitt)

unterschiedlichen Seed-Werten anonymisiert werden. Es ist somit kein Rückschluss auf den Sender oder Empfänger bzw. die gewählten Telefonnummern und Nebenstellen möglich.

In einem Honeynet oder einer produktiven VoIP-Umgebung kann der STR über einen Mirror-Port des Switches oder Routers angebunden und für die Analyse von Angriffen verwendet werden.

In Netzwerken ohne aktive SIP-Komponenten stellte sich heraus, dass nur SIP-Pakete der Methode OPTIONS aufgezeichnet und keine weitergehenden Angriffsversuche erkennbar waren. Um das vollständige Angriffsverhalten überwachen zu können, wurde der STR mit einem Honeypot auf Asterisk-Basis kombiniert und als virtuelle Maschine (VM) an Projektpartner übergeben. Mit Hilfe dieser VM war es möglich, an einer beliebigen öffentlichen IP-Adresse das Angreiferverhalten unabhängig von produktiven SIP-Servern zu untersuchen.

Die Vorteile der netzwerkweiten Analyse [2] mit dem STR werden in Abbildung 20 deutlich: Zunächst sind die einzelnen Peaks der lokalen Überwachung des Single Honeypot-Systems sichtbar. Ab Dezember 2010 zeigt die blaue Kurve alle Angriffspakete, die an das Netzwerk A mit SIP-Komponenten gerichtet wurden, wodurch die eingeschränkte Sicht des Single Honeypots deutlich wird. Das Vergleichsnetzwerk B (ohne SIP-Komponenten) wurde kontinuierlich auf einem konstant hohen Niveau mit dem Angriffstyp Server Scan angegriffen. Das neue Setup bestätigt u.a. die zuvor getätigte Annahme, dass ganze Netzwerkbereiche nach aktiven SIP-Komponenten durchsucht und angegriffen werden. So können nur durch das erweiterte Monitoring die an unterschiedliche Hosts verteilten Server Scan-Angriffe erkannt werden.

4.3 Angriffsbasierte, erweiterte Analyse (Clustering)

Die vorausgegangenen statistischen Analysen sowie die in Kapitel 3.5 bekannten Arbeiten anderer Autoren basieren nur auf der Betrachtung und Zählung einzelner SIP-Nachrichten. Daher fehlen wichtige Informationen zu der Anzahl der Angriffe bzw. zu dem eigentlichen Angriffsverhalten und der verwendeten Angriffstypen. Nur durch eine Analyse des IP- und SIP-Headers in Hinblick auf die Quell-/Zieladresse, SIP-Methode und SIP URI unter Berücksichtigung des Zeitverhaltens ist eine Korrelierung der aufgezeichneten SIP-Nachrichten überhaupt erst möglich, so dass diese den Kommunikationsbeziehungen (SIP-Sessions) und Angriffstypen zugeordnet werden können.

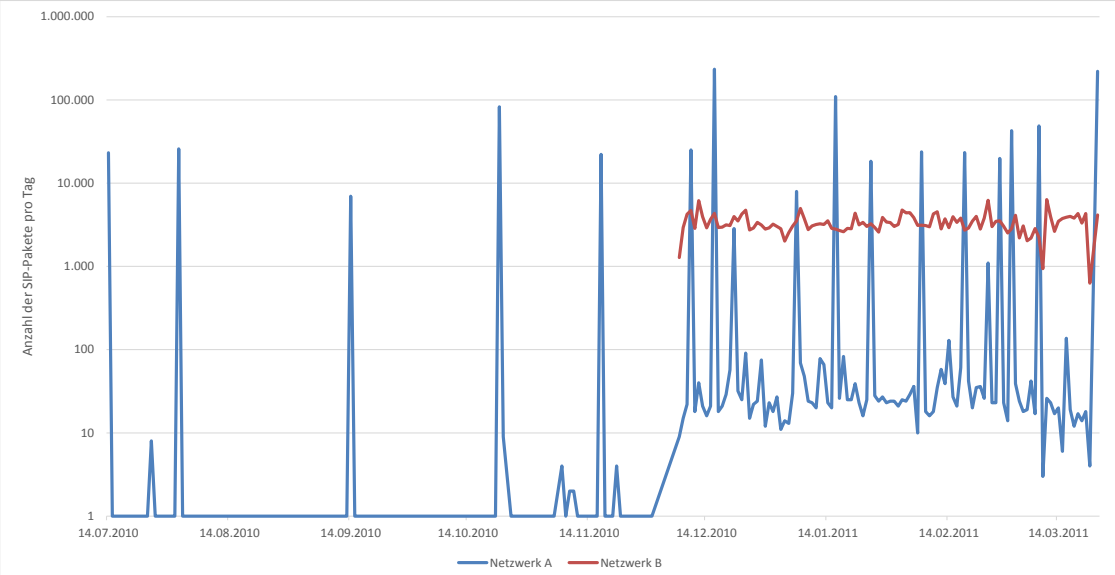


Abbildung 20: Lokale vs. globale Überwachung (SIP-Pakete pro Tag)

Da z.B. für die Angriffsstufen Extension Scan und Registration Hijacking die gleiche SIP-Methode REGISTER verwendet wird, ist eine umfassendere Auswertung notwendig, die nicht nur auf einzelnen SIP-Paketen basieren darf. Darüber hinaus wird für verschiedene Angriffe innerhalb einer Angriffsstufe eine unterschiedliche Anzahl an SIP-Nachrichten benutzt. So benötigt typischerweise ein Wörterbuchangriff mehr SIP-Pakete als eine numerische, iterative Brute-Force-Attacke. Bei beiden Angriffen handelt es sich jedoch um Registration Hijacking. Die absolute Anzahl der SIP-Pakete erlaubt keine Aussage über die Gefährlichkeit eines Angriffs. So benötigen z.B. kritische Toll Fraud-Angriffe zu verschiedenen Rufnummern nur sehr wenige Pakete (typischerweise 10 bis 100), währenddessen Extension Scan-Angriffe mit bis zu 40.000 Paketen unkritischer, jedoch deutlich auffälliger sind, wenn nur die reine Paketanzahl betrachtet wird.

Für die automatische Identifizierung der Angriffsstufen werden die zugehörigen Nachrichten zu einem „Attack-Cluster“ kombiniert, indem die Quell-IP-Adresse, die Angriffsstufe sowie das Zeitverhalten berücksichtigt werden. Um die auftretenden Angriffsversuche besser verstehen zu können, werden auf Grundlage der gesammelten Messdaten vier Attack-Cluster definiert:

1. **Server Scan**
   Ziel-IP-Adresse: unterschiedlich
   SIP-Methode: OPTIONS
2. **Extension Scan**
   Ziel-IP-Adresse: gleichbleibend
   Ziel-Nebenstelle: unterschiedlich
   SIP-Methode: REGISTER
3. **Registration Hijacking**
   Ziel-IP-Adresse: gleichbleibend
   Ziel-Nebenstelle: gleichbleibend
   SIP-Methode: REGISTER
   Anmeldedaten: unterschiedlich
4. **Toll Fraud**
   Ziel-IP-Adresse: gleichbleibend
   Ziel-Nebenstelle: bekannte Nebenstelle aus vorausgegangenen Angriffsstufen
   SIP-Methode: INVITE
   Anmeldedaten: bekannte Zugangsdaten aus vorherigen Angriffsstufen

Die Definitionen für die Attack-Cluster werden in SQL-Abfragen und PHP-Skripten abgebildet, so dass die Auswertungen täglich und automatisiert aktualisiert und auf der STR-Management-Website dargestellt werden können. Da bei einem Server Scan einzelne OPTIONS-Pakete an verschiedene Hosts im Netzwerk gesendet werden, ist hier das großflächige Monitoring essentiell.

Tabelle 3 und Tabelle 4 zeigen einen Ausschnitt aus der Clustering-Auswertung für die Angriffstypen Server Scan und Registration Hijacking. Dies soll die Vorteile dieses neuen Ansatzes verdeutlichen: Pro Monat werden die Anzahl der Angriffe und die Anzahl der SIP-Pakete gegenübergestellt. Zur Verdeutlichung der Ergebnisse sind die beiden nachfolgenden Tabellen pro Spalte in Abhängigkeit zu den Werten (rot: hoher Wert, grün: niedriger Wert) eingefärbt.

Im Februar 2011 wurden 96.648 SIP-Pakete der Angriffsstufe Server Scan zugeordnet. Diese Pakete gehörten zu 274 Angriffen. Für den Zeitraum Juni bis August 2013 zeigt Tabelle 3, dass die Anzahl der Angriffe auf bis zu 65 zurückgegangen ist, jedoch wurden bis zu 519.025 SIP-Nachrichten dem Angriffstyp Server Scan pro Monat zugeordnet. Dies macht deutlich,

Tabelle 3: Clustering Beispiel 1

Monat	Server Scan	
	Angriffe	Pakete
2011-02	274	96.648
2011-03	241	103.666
2013-06	65	476.572
2013-07	82	519.025
2013-08	72	473.526

Tabelle 4: Clustering Beispiel 2

Monat	Registration Hijacking	
	Angriffe	Pakete
2011-06	8	13.963.419
2011-07	40	10.483.106
2011-08	20	772.207
2011-09	148	3.243.164
2014-03	761	370.317

dass anhand der Anzahl der Pakete keine Aussagen über die Anzahl der Angriffe getroffen werden können. Weiterhin ist eine einfache, statistische Auswertung nicht ausreichend, da von der Paketanzahl pro Tag bzw. Monat ausgehend keine Aussage zu der Gefährlichkeit der aufgezeichneten Angriffe getätigt werden kann. Dies hängt damit zusammen, dass eine Zuordnung zu den Angriffstypen und deren Intensität fehlt. Tabelle 4 verdeutlicht diese Aussage: Im Monat Juni 2011 wurden für acht Registration Hijacking-Angriffe über 13,9 Millionen SIP-Pakete verwendet, währenddessen im März 2014 für 761 Angriffe nur 370.317 SIP-Nachrichten benutzt wurden.

4.4 Automatisierung der Angriffserkennung mit Signaturen

Die bisher vorgestellten Konzepte basieren auf einer Offline-Analyse von zuvor gesammelten SIP-Verkehrsdaten. Um jedoch Gegenwehrkomponenten (z.B. eine Firewall) noch während eines laufenden Angriffs informieren zu können, wird eine Angriffserkennung in Echtzeit benötigt. Dazu müssen bekannte Angriffstypen in Form von vordefinierten Signaturen formuliert werden, um eine automatisierte Erkennung zu ermöglichen. Nur so ist eine Abschwächung und Abwehr von Angriffen möglich. Darüber hinaus wird durch die Echtzeit-Erkennung die Möglichkeit geschaffen, im Honeynet-Bereich mit dem Angreifer zu interagieren (siehe Kapitel 4.5). Im Vergleich zu den Offline-Analysen entfällt für bekannte Angriffsmuster die Verzögerung bei der Erkennung. Im Gegensatz zu klassischen Intrusion Detection Systemen, die nach verdächtigen Mustern in einzelnen Datenpaketen suchen, müssen bei der Angriffserkennung in SIP-basierten Netzwerken verschiedene SIP-Pakete miteinander korreliert und in Zusammenhang mit den Kommunikationsverbindungen (SIP-Sessions) analysiert werden.

Für die signaturbasierte Angriffserkennung wurden Regeln aus den gesammelten Honeynet-Daten abgeleitet. Die in „Extensible Markup Language“ (XML) [53] formulierten Signaturen enthalten eine Beschreibung der bekannten Angriffstypen. Durch die Verwendung von XML sind die Signaturen leicht verständlich, klar strukturiert und standardisiert. Weiterhin können für jeden neuen Angriffstyp weitere Signaturen für die automatische Erkennung erstellt werden. Da es sich bei dem Honeynet-Datenverkehr per Definition um Angriffsdaten handelt, kann dieser in der Laborumgebung mit dem

Normalverkehr von SIP-Endgeräten und SIP-Servern verglichen werden, so dass die erstellten Signaturen nur bei verdächtigen SIP-Kommunikationen zutreffen. Um dies sicherzustellen, kann eine Abfolge von SIP-Nachrichten über die IP- und SIP-Header-Felder untereinander verglichen und in Relation gesetzt werden. Die Vorgehensweise soll an dem nachfolgenden Beispiel erläutert werden.

Abbildung 21 zeigt eine vereinfachte Beispiel-Signatur für die Erkennung des Angriffstyps Extension Scan. Der detaillierte Aufbau und die Funktionsweise der Signaturen wird in Kapitel 5.3.1 beschrieben. Jede Signatur enthält eine eindeutige ID, einen Namen sowie eine optionale Beschreibung, so dass alle beteiligten Komponenten einen erkannten Angriff eindeutig zuordnen können. Mit Hilfe von Signaturparametern können eine oder mehrere Aktionen definiert werden, die ausgelöst werden, sobald der spezifizierte Angriffstyp zutrifft (z.B. Protokollierung oder Benachrichtigung einer zentralen Überwachungskomponente). Zusätzlich kann das Zeitverhalten berücksichtigt werden. Dafür muss eine Abfolge von SIP-Nachrichten innerhalb eines vorgegebenen Zeitraums eingegangen sein (z.B. drei SIP-Nachrichten innerhalb von drei Sekunden), damit ein Regelsatz zutrifft. Im Bereich <sippackets> werden mehrere SIP-Pakete definiert. Die Definitionen enthalten Angaben zu den Header-Werten sowie Abhängigkeiten zu vorausgegangenen SIP-Paketen.

Bei einem Extension Scan-Angriff wird typischerweise eine Vielzahl von Paketen der SIP-Methode REGISTER an einen bestimmten Server gesendet. Dabei variiert jedoch die Zielnebenstelle, so dass im To-Header bei jedem Paket eine andere Nebenstelle angegeben ist. In der vorliegenden Beispielregel soll der Angriff mit einer Abfolge von zwei SIP-Nachrichten erkannt werden. Als Voraussetzung für die Aktivierung dieser Signatur wird ein SIP-Paket der Methode REGISTER definiert. Das nachfolgende Paket muss von der gleichen Quell-IP-Adresse an die gleiche Zieladresse gesendet werden (Vergleich mit dem ersten Paket). Weiterhin muss es sich ebenfalls um ein REGISTER-Paket handeln, jedoch im Vergleich zum ersten SIP-Paket mit abweichender Zielnebenstelle.

Um eine Abgrenzung zum Normalverkehr sicherzustellen und zur Vermeidung von „False Positives“ bzw. „False Negatives“, können die Signaturen um weitere Überprüfungen erweitert bzw. durch eine Erhöhung der analysierten Paketanzahl optimiert werden. Dafür existieren Deklarationen, um eine einfache Definition von langen Paketabfolgen zu ermöglichen (z.B. 100 SIP-Pakete mit nur einem <siprequest>-Bereich).

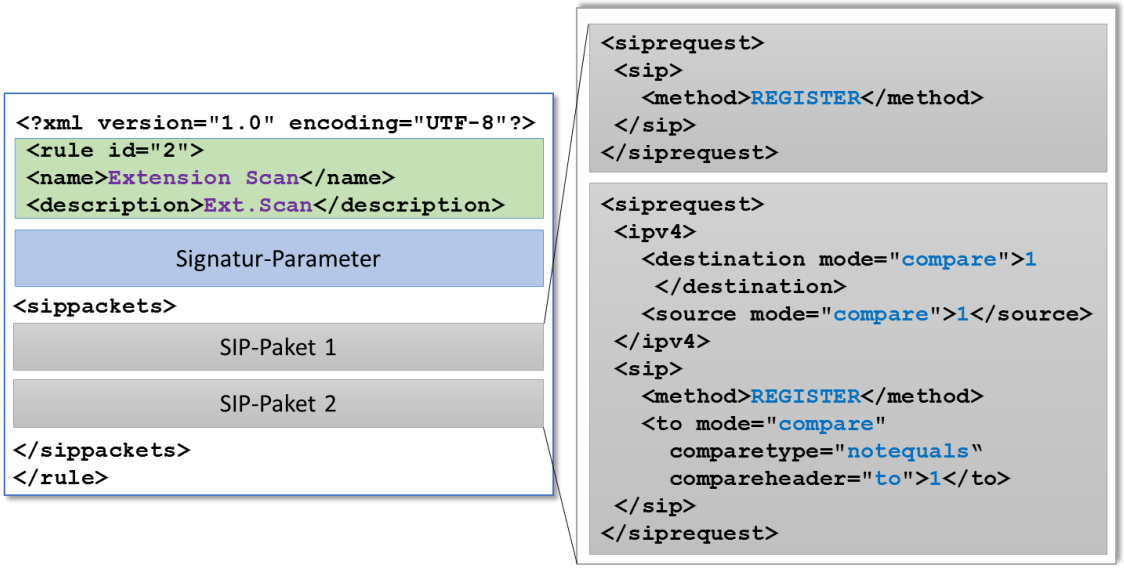


Abbildung 21: Beispiel für die signaturbasierte Angriffserkennung

4.5 Identifizierung der Angreifer unabhängig von der Quell-IP-Adresse

Während der mehrjährigen Untersuchungen war zu beobachten, dass Angreifer die ersten drei Angriffsstufen von der gleichen Quell-IP-Adresse ausführten. Die eigentlichen Toll Fraud-Angriffe erfolgten jedoch oftmals von einer anderen IP-Adresse ohne vorausgegangene Scans. Somit ergab sich die Fragestellung, ob Angreifer die erlangten Anmeldedaten einer Nebenstelle der Honeypots weitergeben bzw. untereinander austauschen. Um diese Fragestellung genauer betrachten zu können, war eine Erweiterung der bisherigen Honeypots notwendig, da die Zuordnung der Angreifer auf Grund der wechselnden Quell-IP-Adressen nicht möglich war [5].

Die Identifizierung der Angreifer musste unabhängig von der wechselnden Quell-IP-Adresse erfolgen. Dazu wurden die SIP-Zugangsdaten (Benutzername/Kennwort) verwendet, die bei der Registrierung einer Nebenstelle von dem Angreifer verwendet wurden. In diesem Fall wurde jedoch eine dynamische Konfigurationsanpassung des Honeypots für den Angriffsfall notwendig, so dass die angegriffene Nebenstelle noch während des Angriffs exklusiv für den Angreifer reserviert und mit neuen Zugangsdaten angepasst wurde. Da in einem ersten Schritt der eigentliche Angriff zunächst erkannt werden musste, konnte der STR auf Grund der fehlenden Echtzeiterkennung nicht verwendet werden.

Für diesen Zweck wurde eine Sensorkomponente entwickelt (siehe Kapitel 5.3.2), die eine Angriffserkennung auf Basis der Signaturen sowie eine Schnittstelle zur Anpassung der Honeypot-Konfiguration in Echtzeit bereitstellt. Für die Interaktion mit einem Angreifer und dessen Identifizierung über die SIP-Zugangsdaten war während eines Angriffes eine erhebliche Konfigurationsanpassung des SIP-Servers notwendig. Dies war jedoch mit dem Asterisk-Server nicht umsetzbar, so dass für das Konzept des dynamischen Honeypots auf den Low Interaction Honeypot Dioanea zurückgegriffen wurde. Kapitel 5.4 beschreibt die Architektur und die detaillierte Funktionsweise.

Das neue Konzept wurde im Zeitraum vom 01.08. bis 30.09.2012 in einem Feldtest evaluiert. Das dynamische Honeypot wurde in diesem Zeitraum von 132 Angreifern mit insgesamt 12.548.485 SIP-Paketen angegriffen. In Abbildung 22 werden anhand eines konkreten Angriffes die Vorteile des dynamischen Honeypot-Konzeptes sowie der typische Ablauf des Angriffsverhaltens erklärt. Am 23.08.2012 fand um 13:01:45 Uhr ein Server Scan (A), ausgehend von einer IP-Adresse, mit 9.538 SIP-Paketen statt. Nur wenige Sekunden

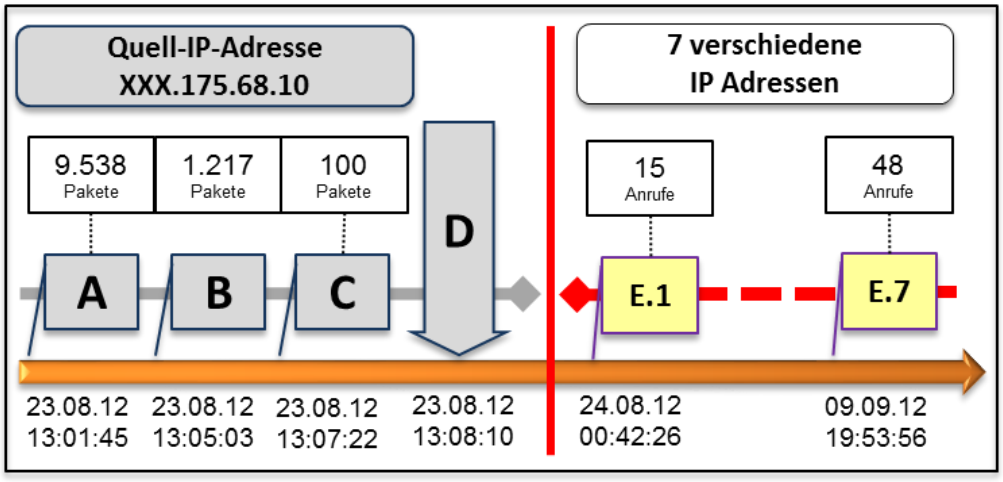


Abbildung 22: Funktionsweise des dynamischen Honeypots (Beispielangriff)

nach dem Server Scan (ab 13:05:03 Uhr) wurde das Honeypot-System nach aktiven Nebenstellen mit einem Extension Scan (B) durchsucht. Ab 13:07 Uhr begann der Registration Hijacking-Angriff (C). Typischerweise senden die Angreifer erst bei der Angriffsstufe Registration Hijacking zur Übernahme der Nebenstelle SIP-Zugangsdaten in den REGISTER-Paketen mit. Daher wurde für den Sensor eine Signatur definiert, die bei einem Schwellenwert von 100 REGISTER-Paketen für die gleiche Nebenstelle eine Benachrichtigung an den Low Interaction Honeypot sendet (D). Sobald eine Benachrichtigung für eine bestimmte Nebenstelle von dem Honeypot empfangen wird, erfolgt die Umkonfigurierung, indem der nächste Registrierungsversuch akzeptiert und die gesendeten Zugangsdaten gespeichert werden. Eine umkonfigurierte Nebenstelle steht für andere Angreifer nicht mehr zur Verfügung. Direkt nach der erfolgreichen Registrierung erfolgen typischerweise keine Toll Fraud-Angriffe.

Am 24.08.2012 um 0:42 Uhr konnte mit Hilfe der STR-Aufzeichnungen eine erfolgreiche Registrierung an der kompromittierten Nebenstelle von einer bisher unbekannten IP-Adresse nachvollzogen werden (E.1). Dabei ist anzumerken, dass die erste Registrierung sofort erfolgreich verlief und dem Angreifer die Zugangsdaten von dem vorausgegangenen Registration Hijacking-Angriff bekannt waren. Ein vorheriger Server oder Extension Scan von dieser IP-Adresse fand nicht statt. Bis zum 09.09.2012 wurden insgesamt sieben Toll Fraud-Angriffe mit den gleichen Zugangsdaten von unterschiedlichen IP-Adressen mit jeweils bis zu 48 Anrufen durchgeführt (E.1 bis E.7). Durch diesen neuen Ansatz wird es möglich, Registration Hijacking-Versuche und Toll Fraud-Anrufe zu korrelieren und unabhängig von der Quell-IP-Adresse eine Identifizierung des Angreifers vorzunehmen.

4.6 Verteilte Echtzeiterkennung von Angriffen

Auf Grund der vollständigen SIP-Datenaufzeichnung mit hohem Ressourcenaufwand war es äußerst schwer, Kooperationspartner bzw. Universitäten von dem Einsatz des STRs zu überzeugen und somit Messdaten von unterschiedlichen Standorten zu erhalten. Bedingt durch die Aufzeichnung der gesamten SIP-Kommunikation war es trotz Anonymisierungsfunktion besonders schwierig, Industriepartner zu gewinnen. Neben dem Honeynet des Lehrstuhls konnte das STR-Aufzeichnungsmodul an zwei weiteren Standorten installiert werden. Auf Grund der lokalen Datenaufzeichnung mussten die gesammelten Daten jedoch in regelmäßigen Abständen in den zentralen Datenbankserver zur Auswertung nach Essen übertragen werden.

Für das Verständnis der Angriffe in SIP-basierten Netzwerken mit der Möglichkeit verschiedenster Offline-Analysen mit Standard-Werkzeugen (SQL, PHP, Microsoft Excel[13]) ist der STR sehr gut geeignet. Da es sich bei den Angriffen in SIP-basierten Netzwerken nach den bisherigen Erkenntnissen jedoch um ein globales Problem im gesamten Internet handelt, ist eine Erkennung an verschiedenen Standorten notwendig. Darüber hinaus müssen verteilte Angriffe an einer zentralen Stelle korreliert werden können und schützenswerte Systeme rechtzeitig benachrichtigt werden. Nur durch eine Echtzeit-Erkennung in möglichst vielen Netzwerken können Angriffe abgeschwächt (z.B. durch eine Firewall) bzw. SIP-Server geschützt werden (z.B. Sperrung eines Accounts). Für eine verteilte Echtzeiterkennung von Angriffen an verschiedenen Standorten im Internet mit möglichst geringem Ressourcenaufwand und der Berücksichtigung des Datenschutzes musste das bisherige Konzept weiterentwickelt werden.

[13] Microsoft Excel 2013, https://products.office.com/de-de/excel

Basierend auf den Ergebnissen der forensischen Auswertungen und den abgeleiteten Angriffssignaturen wurde für diese Dissertation das Konzept der lokalen, signaturbasierten Angriffserkennung zu einem Sensor-Netzwerk für die verteilte Erkennung von SIP-Angriffen erweitert. Dieser Lösungsansatz ist auch im Rahmen des BMBF-Projektes SUNSHINE gefördert worden. Das verteilte Sensorsystem erlaubt, auf der Anwendungsebene die verschiedenen Angriffstypen (siehe auch Kapitel 3.4 und Kapitel 5.3.1) in Echtzeit zu detektieren. Ebenso ermöglicht es eine sehr genaue, feingranulare Interpretation der Aktivitäten. Damit die Ergebnisse nicht nur für einen kleinen Ausschnitt eines Netzwerkes repräsentativ sind, wird ein Sensor über einen Mirror-Port an einer zentralen Netzwerkkomponente (Switch, Router) angeschlossen bzw. werden Sensoren an unterschiedliche Standorte im Internet verteilt, so dass möglichst große Netzbereiche überwacht werden können. Dabei ist es wichtig, dass die Sensoren einerseits in bestehende SIP-Komponenten (SIP-Proxys, Gateways, Endgeräte) integriert werden, andererseits – basierend auf dem Honeynet-Ansatz – dedizierte, autonome Sensorkomponenten entwickelt werden, die an strategisch günstigen Stellen im Netz positioniert werden können.

Darüber hinaus wird untersucht, welche Vorteile sich durch eine Korrelierung von Angriffsinformationen unterschiedlicher Sensor-Standorte erreichen lassen. So können die verteilten Angriffssensoren auf der Dienstebene räumlich verteilte Angriffe erfassen, auch wenn diese mit geringer Gesamtintensität erfolgen und somit bei einem Standard-Netzwerk-Monitoring keinen Alarm auslösen würden. Zusätzlich können die erkannten Angriffe an Schutzkomponenten (z.B. Firewall) in Echtzeit gemeldet werden, um den Angriff abzuschwächen oder zu beenden. Um eine Korrelierung der Alarmmeldungen von verschiedenen Standorten bzw. Sensoren zu erreichen, ist es notwendig, einen zentralen Dienst für die Analyse bereitzustellen. Da Gegenwehrkomponenten möglichst in Echtzeit benachrichtigt werden müssen, sind eine zentrale, automatisierte Analyse mit einem ausreichenden, komplexen Regelwerk sowie eine leistungsfähige Schnittstelle zur Anbindung vieler Sensor-Standorte notwendig.

Abbildung 23 zeigt das Konzept des „Security Sensor Systems“ [7] bestehend aus dem erweiterten Sensor zur signaturbasierten Angriffserkennung sowie aus dem „Sensor Central Service“ (SCS) zur Korrelierung der Angriffsmeldungen der verbundenen Sensoren. Im Vergleich zum STR werden keine SIP-Pakete mehr aufgezeichnet, so dass die Sensoren

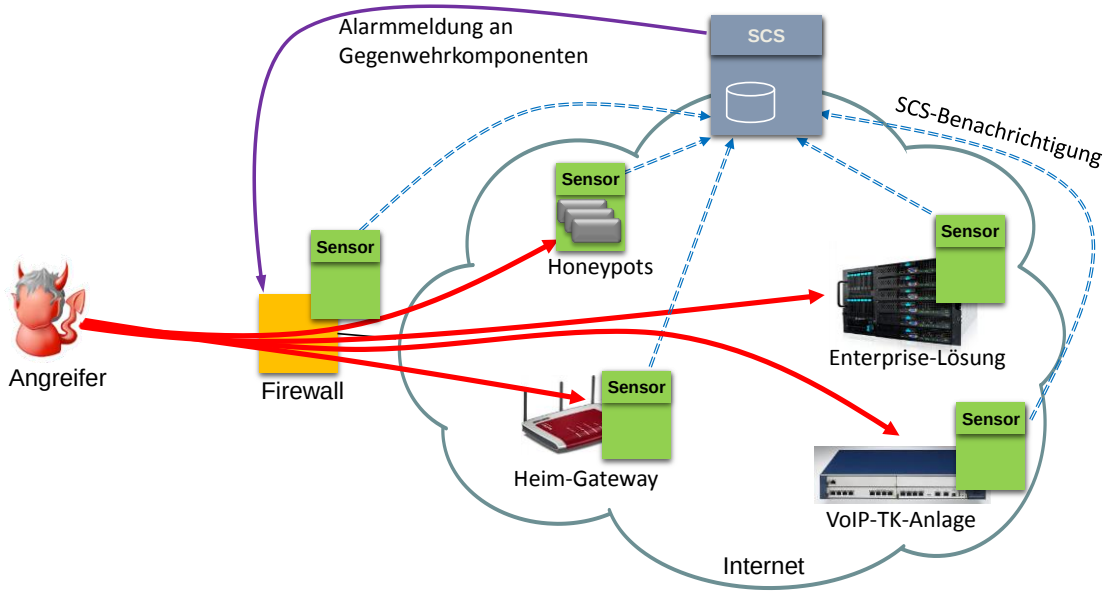


Abbildung 23: Übersicht Security Sensor System

auch in produktiven Netzwerken eingesetzt werden können. Im Enterprise-Umfeld erfolgt die Anbindung über einen Mirror-Port am Switch des VoIP-Netzwerkes, damit im Fehlerfall ein Einfluss auf die produktiven Systeme ausgeschlossen werden kann. In kleineren Umgebungen kann der Sensor direkt auf der Hardware der Telefonanlage oder auf dem Heim-Gateway installiert werden. Für Netzwerke ohne aktive SIP-Komponenten wurde ein Kombisystem aus Honeypot und Sensor entwickelt, das sowohl in kleinen (Port-Forwarding bedingt durch NAT) als auch in großen Netzwerken mit mehreren statischen, öffentlichen IP-Adressen installiert werden kann. Diese Kombilösung eignet sich auch für Forschungs-Testbeds wie z.B. NorNet [8], damit möglichst viele Sensoren an unterschiedlichen Standorten weltweit betrieben werden können [6].

Das verteilte Sensorsystem basiert auf einer zweistufigen Angriffsanalyse: Sobald ein Angriff an einem Netzwerkstandort von einem Sensor erkannt wird und somit eine Signatur zutrifft, erfolgt umgehend eine Benachrichtigung an den SCS (erste Stufe der Angriffsanalyse). Dabei werden alle relevanten Informationen zu dem erkannten Angriff mitgesendet (ID des Sensors, zutreffende Signatur ID, Quell- und Ziel-IP-Adresse des Angriffs, Zeitstempel). Weitere Daten aus dem SIP-Header können bei Bedarf ebenfalls zur Verfügung gestellt werden.

Für die zweite Stufe der Angriffsanalyse werden eingehende Benachrichtigungen auf dem SCS in einer SQL-Datenbank gespeichert, so dass die Angriffe korreliert werden und die empfangenen Angriffsdaten bei Bedarf auch zu einem späteren Zeitpunkt als Grundlage für erweiterte Analysen zur Verfügung stehen. Die zweistufige Erkennung von Angriffen hat den Vorteil, dass Angriffe aus unterschiedlichen Netzwerken weltweit korreliert und Zusammenhänge erkannt werden können. Da die Analyse auf dem SCS auf einem Regelsatz basiert, wird in Abhängigkeit von den SCS-Regeln bei einer oder mehreren eingehenden Sensor-Benachrichtigungen eine Alarmmeldung an die angebundenen Gegenwehr- bzw. VoIP-Komponenten gesendet. Ein Angriff auf die VoIP-Server im Netzwerk kann in diesem Fall durch eine Firewall abgeschwächt werden. Die Architektur und Funktionsweise des Security Sensor Systems wird in Kapitel 5.3 detailliert erläutert.

4.7 Zusammenfassung und Einordnung der Konzepte

Die zuvor vorgestellten Konzepte für diese Dissertation werden in Abbildung 24 in den wissenschaftlichen Kontext und in Relation zu bestehenden Veröffentlichungen eingeordnet. Dabei wird unterschieden, ob das Ziel der Arbeiten forensische Analysen sind oder ob es sich um eine Angriffserkennung bzw. Alarmierung im Angriffsfalle handelt (X-Achse). Zusätzlich wird der Beobachtungsbereich (von der einzelnen IP-Adresse bis zu verteilten Messstellen) berücksichtigt und auf der Y-Achse dargestellt. Darüber hinaus wird für jeden Entwicklungsschritt bei den Konzepten der wissenschaftliche Mehrwert angegeben.

Im Bereich von forensischen Analysen mit Single Honeypot-Systemen, die für das Verständnis und die Analyse von SIP-basierten Angriffen genutzt werden, haben auch andere Arbeitsgruppen [38] [39] [43] einzelne VoIP-Honeypots in unterschiedlichen Ausprägungen eingesetzt (Low/High Interaction Honeypots). Im Bereich der Single-Honeypots unterscheiden sich die Systeme dieser Dissertation von den anderen Konzepten wie folgt:

- Durch den Einsatz von High Interaction Honeypots auf Basis der Software Asterisk steht für den Angreifer ein realer und vollständiger SIP-Server wie in produktiven Umgebungen zur Verfügung. Dies gewährleistet, dass die analysierten Angriffe auch unabhängig von der Laborumgebung zutreffend sind und es dem Angreifer nicht

ermöglicht wird, anhand des Systemverhaltens eine Honeypot-Infrastruktur zu erkennen.

- Alle bisher bekannten Honeypot-Systeme basieren auf einer Angreiferidentifizierung auf Basis der Quell-IP-Adresse. Durch die dynamische Zuteilung von IP-Adressen in vielen Provider-Netzwerken oder durch den Einsatz von Network Address Translation (NAT) können sich die Quell-IP-Adressen eines Angreifers verändern. Das Konzept der dynamischen Honeypots (Kapitel 5.4) [5] erlaubt hingegen eine Angreiferidentifizierung auf Basis der während eines Registration Hijacking-Angriffs verwendeten Zugangsdaten. Somit kann eine Attacke einem Angreifer auch nach dem Wechsel der Quell-IP-Adresse weiterhin zugeordnet werden.

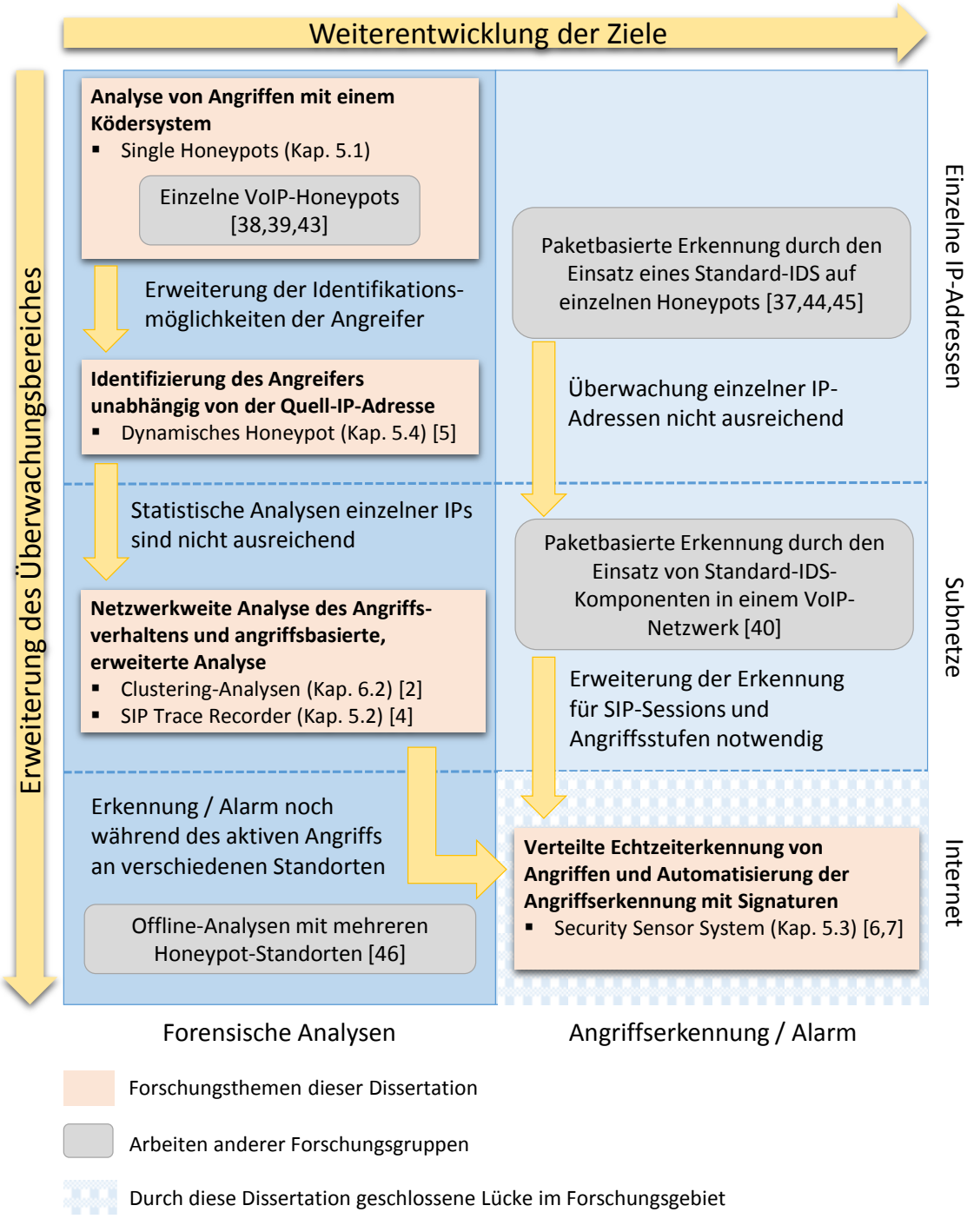


Abbildung 24: Einordnung der Konzepte in den Forschungsbereich

Bisherige wissenschaftliche Untersuchungen waren auf wenige IP-Adressen und auf die Betrachtung einzelner Pakete begrenzt. Da die Analysen mit Single Honeypot-Systemen nur eine sehr begrenzte Sicht auf das Netzwerk erlauben und sich während der ersten Analysen Hinweise auf Scan-Versuche von Netzbereichen herausstellten, musste der Überwachungsbereich vergrößert werden. Darüber hinaus waren die bisher typischerweise durchgeführten statistischen Auswertungen auf Paketbasis nicht ausreichend, da der Verbindungsstatus und die Zuordnung zu Angriffen nicht berücksichtigt wurden. Daher wurden neue Ansätze als Alleinstellungsmerkmal für diese Dissertation erarbeitet [4]:

- Erweiterung der statistischen Analysen zu verbindungs- und angriffsorientierten Auswertungen durch die Korrelierung von SIP-Nachrichten (Clustering) [2].
- Entwicklung einer komplett passiven, zentralen Überwachung und Protokollierung der eingesetzten Honeypots durch die Anbindung über einen Mirror-Port. Dadurch sind die Überwachungskomponenten im Vergleich zu dem klassischen Honeynet-Konzept für den Angreifer nicht erreichbar und auf keinen Fall erkennbar. Eine dezentrale Aufzeichnung der Daten und eine aufwändige Zusammenführung entfallen.
- Eine beliebige Erweiterung des Überwachungsbereiches ist möglich, da die Aufzeichnungskomponenten in Kombination mit der Anbindung über Mirror-Ports große und zahlreiche Netzwerkbereiche überwachen können.
- Automatisierte Analyse von gesammelten SIP-Verkehrsdaten in der zentralen Überwachungskomponente mit vordefinierten Abfragen und Präsentation auf der Management-Website, ohne dass ein manueller Eingriff notwendig ist.

Da die Honeynet-Analysen gezeigt haben, dass es sich bei den SIP-spezifischen Toll Fraud-Angriffen um ein globales Problem handelt, wurde die Zielsetzung dieser Dissertation auf die verteilte Erkennung von Angriffen in Echtzeit gesetzt. Nur so besteht die Möglichkeit, einen laufenden Angriff rechtzeitig erkennen und mit geeigneten Gegenmaßnahmen (z.B. Firewall-Systeme) abschwächen zu können. Durch [46] wurde deutlich, dass die Verteilung identischer Honeypots an unterschiedlichen Standorten mit einer dezentralen Datensammlung und einer daraus resultierenden Offline-Analyse für eine Erkennung von Angriffen nicht geeignet ist. Diese Systeme sind auf Grund der Software-Images ressourcenintensiv und erfordern einen hohen Aufwand bei der Datenabfrage. Bei Gesprächen mit Kooperationspartnern in der Industrie stellte sich heraus, dass Systeme mit hohem Wartungsaufwand unerwünscht sind. Darüber hinaus müssen datenschutzrechtliche Aspekte berücksichtigt werden, so dass die Aufzeichnung und der spätere Export des SIP-Verkehrs keine Option darstellen.

Im Bereich der Angriffserkennung gibt es Veröffentlichungen anderer Arbeitsgruppen, die jedoch eine paketbasierte Erkennung auf der Basis von Standard-IDS-Systemen einsetzen. Die Systeme unterscheiden sich in der Größe des Überwachungsbereiches, beginnend bei einzelnen IP-Adressen [37] [44] [45] bis zu einer Subnetz-Überwachung [40].

Im Vergleich zu dem verteilten Honeynet in [46] und den IDS-basierten Systemen muss für das Erkennungssystem für diese Dissertation sichergestellt sein, dass die Erkennung auch eine Korrelierung der Pakete zur Identifizierung der Angriffsstufen ermöglicht. Bei der Betrachtung des Forschungsgebietes wurde festgestellt, dass auf dem Gebiet der automatischen SIP-basierten Angriffserkennung in Echtzeit eine Lücke existiert (siehe Markierung in Abbildung 24), die mit dieser Dissertation geschlossen wird.

Dabei besteht der wissenschaftliche Mehrwert des Security Sensor Systems [6] [7] in folgenden Punkten:

- Durch den Einsatz von leichtgewichtigen Sensoren kann die Anzahl der Messstandorte maximiert werden. Darüber hinaus erlaubt die passive Anbindung der Sensoren einen Einsatz in privaten sowie in produktiven Enterprise-Systemen.
- Die Sicherstellung des Datenschutzes wird gewährleistet, da keine Aufzeichnung des SIP-Verkehrs auf Grund der Echtzeit-Analyse vor Ort notwendig ist. Die langfristige Speicherung von persönlichen Daten entfällt.
- Für die automatische Erkennung der SIP-Sessions und der Angriffsstufen wird die Paket-Korrelierung direkt auf den Sensoren eingesetzt.
- Das System erlaubt eine einfache Anpassung der Erkennung bei veränderten Angriffsmustern durch den Einsatz von Signaturen.
- Zusätzlich zu der standortbezogenen Angriffserkennung werden Angriffe durch einen zentralen Dienst korreliert. Dadurch wird es möglich, Angriffe netzwerkübergreifend bzw. länderübergreifend zu erkennen und in einen Zusammenhang zu bringen.
- Durch die Zusammenführung aller Angriffsinformationen in dem zentralen Dienst ist eine frühzeitige Benachrichtigung der Gegenwehrkomponenten möglich, so dass auch Netzwerkstandorte geschützt werden können, an denen noch kein Angriff oder nur ein erster Scan-Versuch stattgefunden hat.
- Die integrierten Management-Funktionen stellen die automatische Konfiguration der Sensoren und die Verteilung von Signaturen sicher und minimieren somit den Wartungsaufwand in produktiven Netzwerken. Der Einsatz von Zertifikaten für die Identitätsprüfung und die aktive TLS-Verschlüsselung zwischen Sensor und Zentraldienst berücksichtigen die Sicherheitsanforderungen.

5 Architektur und Implementierung

In diesem Kapitel werden die Architektur und die Implementierung der entwickelten Komponenten erläutert. Für die forensischen Analysen wurden zu Beginn die Single Honeypot Systeme eingesetzt. Für die umfassende Analyse (Überwachung ganzer Subnetze) der SIP-basierten Angriffe wurde der SIP Trace Recorder in Kombination mit einem Honeynet verwendet. Die verteilte Angriffserkennung erfolgte mit dem Security Sensor System. Das dynamische Honeypot wurde benötigt, wenn das Angreiferverhalten unabhängig von der Quell-IP-Adresse untersucht werden sollte. Das Kapitel schließt mit einem Vergleich der Systeme in Hinblick auf den Einsatzzweck.

5.1 Single Honeypot System

Um die verfügbaren Hardware-Ressourcen des bereitgestellten Servers optimal nutzen zu können und eine gute Skalierbarkeit bei der Einrichtung weiterer Honeypots zu erreichen, wurde die Virtualisierungslösung VMware ESXi [32] eingesetzt. Das eigentliche Honeypot wurde als virtuelle Maschine (VM) aufgesetzt, so dass mehrere, unterschiedliche Honeypots unabhängig voneinander auf derselben Hardware lauffähig waren. Für die Untersuchungen in dieser Dissertation wurden zwei verschiedene Honeypot-Lösungen eingesetzt, die nachfolgend vorgestellt werden.

5.1.1 Asterisk-Honeypot

Die virtuelle Maschine beinhaltet ein Standard-Linux-System sowie den frei verfügbaren SIP-Server Asterisk [3]. Der Asterisk-Server wurde für den Betrieb als Honeypot mit einer vordefinierten Konfiguration eingestellt: Jede Honeypot-VM stellt eine genau definierte Anzahl von Nebenstellen (Accounts) mit schwachen Kennwörtern bereit und beantwortet eingehende SIP-Nachrichten auf dem UDP-Port 5060. Die einfachen Kennwörter entsprechen den Nebenstellennummern (z.B. 400) oder setzen sich aus kurzen Ziffernfolgen (z.B. 1234) zusammen. Das Verhalten entspricht somit einem Standard SIP-Server. Angreifer sind in der Lage, die aktiven Nebenstellen zu finden und zu übernehmen. Dadurch wird es möglich, die ersten drei Angriffsschritte (Server Scan, Extension Scan und Registration Hijacking) mit dem Honeypot als Opfersystem zu realisieren (siehe Kapitel 3.4).

Erfolgreich registrierte Angreifer können an einer normalen SIP-Telefonanlage beliebige Telefonnummern auf Kosten des Benutzers anrufen. Aus rechtlichen Gründen und zum Schutz der eigenen Infrastruktur sind die Honeypots so konfiguriert, dass externe Anrufe an eine interne Nebenstelle umgeleitet werden und der Rufaufbau für den Angreifer nur simuliert wird. Dies bedeutet, dass der Angreifer die vierte Angriffsstufe Toll Fraud durchführen kann und wichtige Daten, wie z.B. die gewählte Rufnummer, aufgezeichnet werden, der Angriff jedoch keinen Schaden verursacht. Um die optimale Auswertung zu gewährleisten, sind alle aktiven Nebenstellen der Honeypots im STR hinterlegt, so dass zwischen aktiven und inaktiven Nebenstellen verglichen werden kann. Aus rechtlichen Gründen werden nur Signalisierungsinformationen verarbeitet. Es erfolgt keine Aufzeichnung der Sprachdaten, die über das Real-time Transport Protokoll (RTP) [15] übertragen werden.

Für die Asterisk-Honeypots wurden die Nebenstellen 201, 302, 333 und 400 eingerichtet. Der Wertebereich entspricht einer Standard-Nebenstellenanlage und kann somit von den bekannten Angriffswerkzeugen gefunden werden. In Kombination mit dem STR ist es nicht

mehr notwendig, den SIP-Verkehr auf dem eigentlichen Honeypot aufzuzeichnen oder zu analysieren. Dadurch sind für die Auswertung keine Managementzugriffe auf die Honeypot-VM mehr erforderlich, so dass die Systeme bis auf den SIP-Port mit der Firewall komplett gegen Angreifer abgeschirmt werden können.

5.1.2 Dioanea-Honeypot

Das Dioanea-Framework [25] (siehe auch Kapitel 2.4.2) wurde als Alternative zu den High Interaction Asterisk-Honeypots ausgewählt und als SIP-Honeypot eingesetzt. Dazu wurden alle übrigen Dienstsimulationen und die interne Protokollierung abgeschaltet und nur die SIP-Implementierung auf UDP- und TCP-Port 5060 aktiviert. Am 17. Mai 2011 wurde auch das Dioanea-Honeypot in das Honeynet am Lehrstuhl integriert. Auf Grund der eingeschränkten SIP-Funktionalität musste ein selbst entwickeltes SIP-Modul implementiert werden, da eine Registrierung von Nebenstellen nicht möglich war. Parallel wurde Dioanea durch die Entwicklungsgemeinschaft weiterentwickelt und mit einem erweiterten SIP-Modul ausgestattet. Erst diese aktuelle Generation des Dioanea-Honeypots, die Ende 2013 veröffentlicht wurde, bietet die notwendige Unterstützung für die Registrierung von Nebenstellen (SIP Methode REGISTER) an. Diese ist eine elementare Voraussetzung für die Erkennung von mehrstufigen Toll Fraud-Angriffen.

Mit diesem System sollte geklärt werden, wie sich das Angreiferverhalten ändert, wenn ein weiterer Honeypot verfügbar ist und ob sich die Angriffe auch gegen den SIP TCP-Port richten. Auf der Grund der fehlenden zentralen Überwachung handelt es sich nicht um ein Honeynet, sondern um unabhängige Honeypots mit eigenständiger Protokollierung. Durch den Low Interaction Honeypot sollte für die Angreifer ein möglichst interessanter SIP-Server geschaffen werden, der mit dem Asterisk-Honeypot vergleichbar ist. Darüber hinaus sollte analysiert werden, ob die Angreifer je nach Honeypot-Typ ein unterschiedliches Interesse bzw. Angriffsverhalten zeigen. Um auch die Nebenstellenbereiche der Enterprise-VoIP-Telefonanlagen abzudecken, wurde für das Dioanea-Honeypot ein Nebenstellenbereich zwischen 1000 und 9999 gewählt. Aus rechtlichen Gründen erfolgt auch mit diesem Honeypot keine Aufzeichnung der Sprachdaten.

Da die bereitgestellten Nebenstellen in einer Datenbank verwaltet werden, ist die Konfiguration auch im laufenden Betrieb einfach möglich. Dadurch entfällt die arbeitsintensive Veränderung von Konfigurationsdateien wie bei dem Asterisk-Server. Es stellte sich jedoch schnell heraus, dass sich bedingt durch die skriptbasierte Implementierung (Python [26]) im Vergleich zum Asterisk-Server keine Ressourcenvorteile in der virtuellen Umgebung ergaben. Auf leistungsschwächeren Hardwarekomponenten, wie z.B. dem Raspberry Pi (siehe Kapitel 2.5.3), konnte mit dem Asterisk-Honeypot ein deutlich besseres Antwortzeitverhalten erreicht werden.

5.2 SIP Trace Recorder und Honeynet

Das entwickelte SIP-Honeynet, das am Lehrstuhl Technik der Rechnernetze eingesetzt wird, besteht aus mehreren SIP-Honeypots, die alle an das gleiche öffentliche Class-C-Netzwerk angeschlossen sind. Dabei handelt es sich jeweils um eine virtuelle Maschine auf VMware-Basis. Für Vergleichsuntersuchungen wird parallel ein weiteres öffentliches Class-C-Netzwerk betrieben, das keine SIP-Komponenten enthält.

Das Analysewerkzeug SIP Trace Recorder (STR) wird zur Aufzeichnung und Aufbereitung des SIP-Angriffsverkehrs benötigt, so dass eine automatische Auswertung ermöglicht wird. Wie in Abbildung 25 dargestellt, ist der STR in großen Netzwerkumgebungen (Enterprise)

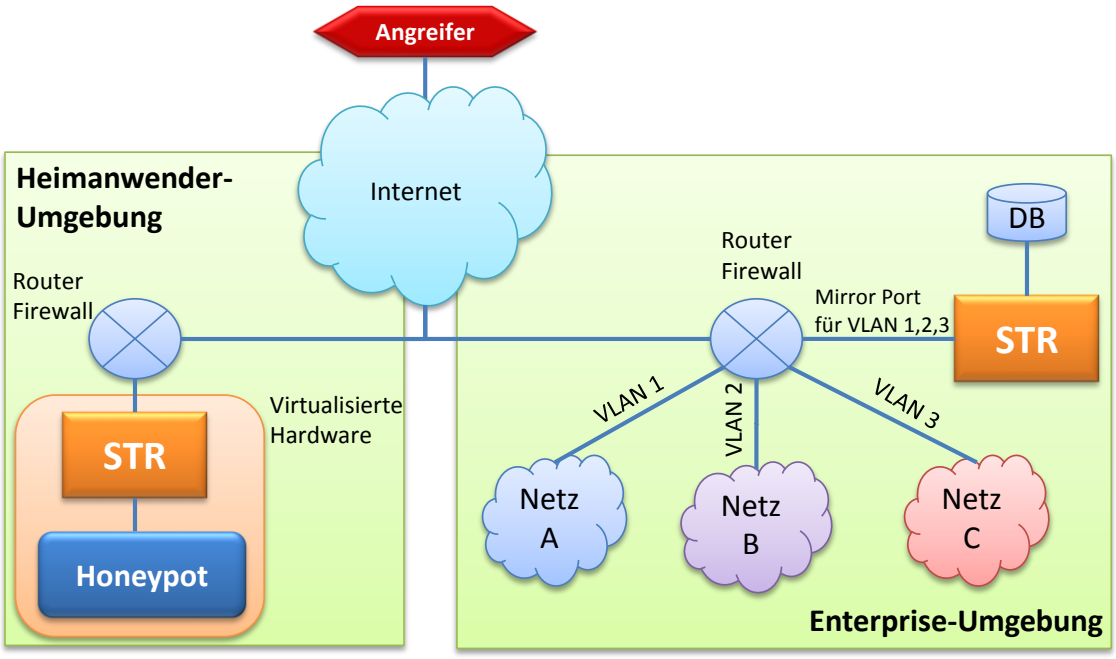


Abbildung 25: Netzwerkanbindung SIP Trace Recorder (STR)

an den Hauptrouter angeschlossen, der die Datenpakete der überwachten VLANs[14] als Kopie über einen Mirror-Port an den STR sendet. Dies soll ausschließen, dass der STR über das Internet angegriffen werden kann bzw. dass es bei einem Ausfall in produktiven Netzwerken zu einer unerwünschten Einflussnahme kommt. Darüber hinaus ist der STR für den Angreifer nicht sichtbar, da zwischen den Honeypot-Komponenten und der Überwachungskomponente keine Kommunikationsverbindung existiert. Die verarbeiteten Datenpakete der überwachten Netzwerke werden in einer zentralen Datenbank gespeichert.

In kleineren Umgebungen kann der STR auch mit einem einzelnen Honeypot kombiniert und in Form einer virtuellen Maschine bzw. auf einer kompakten Hardware (z.B. Intel NUC, siehe Kapitel 2.5.2) bereitgestellt werden. Diese Art der Installation eignet sich für kleine Netzwerkstandorte ohne konfigurierbare Netzwerk-Switche sowie ohne aktive SIP-Komponenten. Die Verkehrsdaten werden in diesem Szenario lokal gespeichert und müssen periodisch abgerufen werden. Die virtualisierte Hardware wird an den Router angeschlossen. Dabei leitet die STR-VM die Daten auf Schicht 2 für den Angreifer transparent (keine IP-Bindung) an die Honeypot-VM weiter und verarbeitet gleichzeitig den SIP-Verkehr.

5.2.1 Architektur

Der STR besteht aus zwei Hauptmodulen, die über eine SQL-Datenbank verbunden sind: Das Aufzeichnungsmodul ist in Java [54] implementiert und basiert auf den frei verfügbaren Bibliotheken JNetPcap [55] und libpcap [50]. Dadurch wird der Einsatz auf unterschiedlichen Hardware- und Softwareplattformen ermöglicht. Das Auswertungs-modul ist in PHP [52] geschrieben und greift auf die Datenbank des Aufzeichnungsmoduls zu. Es bietet automatisierte Analysen des aufgezeichneten SIP-Verkehrs auf einer Management-Website. Das objektorientierte Softwaredesign ermöglicht eine einfache Erweiterung, so dass ohne Veränderung der Architektur weitere Funktionen hinzugefügt werden können.

[14] IEEE 802.11Q, http://standards.ieee.org/findstds/standard/802.1Q-2011.html

Abbildung 26 zeigt die Architektur des STR-Aufzeichnungsmoduls. Zunächst wird ein „Listener“-Prozess an eine Netzwerkschnittstelle gebunden, so dass der SIP-Echtzeitverkehr mit Hilfe der libpcap-Bibliothek zur weiteren Bearbeitung in einer Nachrichtenwarteschlange für den nächsten Prozess zur Verfügung gestellt wird. Für Systeme mit mehr als einer Netzwerkkarte können weitere Listener-Prozesse aktiviert werden. Neben der Echtzeitanalyse erlaubt der Listener-Prozess auch das Einlesen von Dateien im PCAP-Format [50], so dass der SIP-Verkehr von anderen, entfernten Systemen im Nachhinein analysiert werden kann (z.B. Aufzeichnungen mit dem Tool tcpdump [49]). Für die durchgeführten Analysen wurde ein PCAP-Filter verwendet, der im STR frei konfiguriert werden kann und nur Datenpakete auf dem UDP/TCP-Port 5060 weiterleitet. Somit wird der übrige Datenverkehr direkt verworfen und die folgenden Prozesse werden nicht mit den Daten anderer Protokolle belastet.

Bevor die Datenpakete in die Warteschlange eingefügt werden, erfolgt eine auf regulären Ausdrücken basierende Überprüfung, ob es sich bei den eingehenden Paketen um SIP-Payload handelt. Dies soll die Last im „Parser“-Modul reduzieren, falls das Paket keine SIP-Daten enthält. Im nachfolgenden Parser-Modul werden die wichtigen Kommunikations-daten aus dem SIP-Header mit String-Operationen und regulären Ausdrücken ausgelesen und über eine SQL-Datenverbindung in eine MySQL-Datenbank [56] geschrieben. Die folgenden IP- und SIP-Header-Werte werden für das Auswertungsmodul gespeichert:

- Source IP Address/Port
- Destination IP Address/Port
- SIP-Method
- Call-ID
- User Agent
- Contact user/host
- To/from
- Via
- Authorization information
- Time stamp
- SIP Version
- Statuscode/Reasonphrase

Bei der Aufzeichnung wird zwischen SIP-Anfrage und SIP-Antwort unterschieden. Schon während der Aufzeichnung des SIP-Verkehrs wird versucht, eine logische Korrelation zwischen den SIP-Paketen herzustellen, so dass eine sofortige Zuordnung der Pakete zu den SIP-Sessions ermöglicht wird. Das Ergebnis der Korrelation wird in einer Datenbank-Tabelle gespeichert.

Damit die gesammelten SIP-Nachrichten nicht periodisch manuell ausgewertet werden müssen, verfügt der STR über ein Auswertungsmodul, das in Abbildung 27 gezeigt wird. Über sogenannte Plug-Ins (siehe Kapitel 5.2.3) werden täglich aktualisierte Ergebnisse auf vordefinierte Fragestellungen automatisch auf einer Management-Website präsentiert

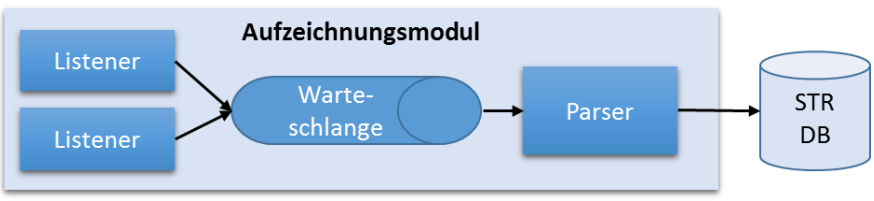


Abbildung 26: Architektur STR-Aufzeichnungsmodul

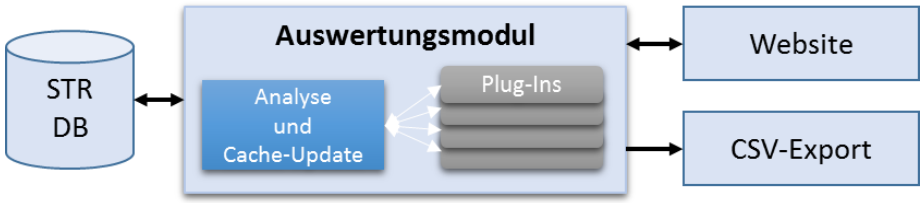


Abbildung 27: Architektur STR-Auswertungsmodul

oder als CSV-Export zur Verfügung gestellt. Das Aktualisierungsintervall kann beliebig angepasst werden. Darüber hinaus ist eine sofortige Neuberechnung und Filterung (z.B. Veränderung des Zeitraums oder des Netzwerkbereiches) der Ergebnisse pro Plug-In durch eine Benutzeraktion möglich. Jedes Plug-In basiert auf der Programmiersprache PHP und der Abfragesprache SQL, so dass der gesamte Funktionsumfang einer etablierten Skript- und Abfragesprache für die Analyse zur Verfügung steht. So können z.B. die eingehenden SIP-Pakete pro Tag in Tabellenform oder als Diagramm auf der Website angezeigt werden. Zur besseren Übersicht wurde ein Filter implementiert, der eine Selektierung nach verschiedenen Netzwerken und Zeiträumen erlaubt.

5.2.2 Datenbankstruktur

Die STR-Datenbank läuft auf einem MySQL-Datenbankserver und besteht zur Speicherung der Angriffsdaten aus vier Haupttabellen sowie aus weiteren Tabellen, die für die Konfiguration des Auswertungssystems notwendig sind. Tabelle 5 zeigt die wichtigsten Datenbanktabellen mit den zugehörigen Attributen.

Die für die Analyse wichtigen Header-Felder jeder eingehenden SIP-Anfrage werden in der Tabelle „requests“ gespeichert. Die Antworten des Honeynets werden in der Tabelle „responses“ aufgezeichnet. Mit Hilfe der Call-ID aus dem SIP-Header und der SIP-Methoden kann z.B. der Beginn, das Ende und die Dauer einer SIP-Sitzung festgestellt werden. In der Tabelle „conversations“ wird das Ergebnis der automatischen Korrelierung von SIP-Paketen gespeichert. Dadurch wird ersichtlich, wie lange eine SIP-Sitzung aufrechterhalten wird, bis die Verbindung durch das Honeynet oder den Angreifer beendet wird. Sobald der SIP-Header einer REGISTER- und INVITE-Nachricht einen „Authorization“-Header beinhaltet, werden diese Informationen in die Datenbanktabelle „credentials“ eingefügt.

Neben den vorgestellten Haupttabellen werden für die Konfiguration und für die Optimierung der Anzeigegeschwindigkeit des Auswertungsmoduls weitere Datenbanktabellen mit den Namen „conf_*“ und „cache_*“ verwendet. In den Tabellen mit den Namen „conf_*“ werden Netzwerkbereiche oder einzelne IP-Adressen für die

Tabelle 5: STR-Datenbank Haupttabellen

Name	Attribute
requests	id, sourceip, sourceport, destinationip, destinationport, method, callid, useragent, contactuser, contacthost, touser, tohost, fromuser, fromhost, via, time
responses	id, sourceip, sourceport, destinationip, destinationport, callid, sipversion, statuscode, reasonphrase, time
conversations	callid, invitetime, byetime
credentials	requestid, headerfield, username, realm, nonce, response, uri, algorithm

komfortable Filterung im Webinterface hinterlegt oder notwendige Informationen für die automatisierten Abfragen gespeichert (z.B. IP-Adressen und Nebenstellen der Honeypots). Die Tabellen mit den Namen „cache_*“ enthalten zwischengespeicherte Analyseergebnisse der periodischen Auswertungen, damit für die Anzeige der Ergebnisse nicht für jeden Anwender eine erneute Generierung in Echtzeit erfolgen muss und der Datenbankserver nicht stark belastet wird.

5.2.3 Plug-Ins zur Datenauswertung

Durch das implementierte Plug-In-Verfahren muss die Auswertungslogik für jede Fragestellung in einer getrennten Datei definiert werden. Alle Plug-In-Dateien befinden sich in einem bestimmten Verzeichnis und werden durch das Auswertungsmodul aufgerufen, wenn das Plug-In in der Datenbank aktiviert ist. Alle Plug-Ins haben eine identische Struktur (siehe Abbildung 28) und müssen bestimmte Methoden beinhalten. Die Methode „getContent“ wird aufgerufen, sobald ein Plug-In auf der Management-Seite

```php
<?php
class Auswertung1 implements Widget, CSVExport
{
    private $year;
    private $month;
    private $ip_filter;
    private $custom_ip_filter;
    private $content;
    public function __construct($year=-1, $month=-1, $ip_filter="",
     $custom_ip_filter="")
    {
        $this->year = validatedYear($year);
        $this->month = validatedMonth($month);
        $this->ip_filter = (IpFilter::isValid($ip_filter)) ? $ip_filter : "all";
        $this->custom_ip_filter = $custom_ip_filter;
    }
    public function getContent($force_update=false)
    {
        if ($force_update)
            self::updateCache($this->year, $this->month, $this->ip_filter,
            $this->custom_ip_filter);
        $this->loadContent();
        return $this->content;
    }
    private function loadContent()
    {
        $this->content = $this->generateAnalysis($this->year, $this->month,
        $this->ip_filter, $this->custom_ip_filter)
        $this->content .= '<div style="clear:right; font-size: small;">
        <a href="javascript:loadanalysis(true);">refresh cache</a></div>';
    }
    private function generateAnalysis()
    {
         /* Logik für die Auswertung */

        return $output;
    }
     public static function export_csv($startMonth=-1, $startYear=-1, $endMonth=-1,
     $endYear=-1, $ip_filter="", $custom_ip_filter="")
    {
         return $csv;
    }
    public static function updateCache($year=-1, $month=-1, $ip_filter="",
    $custom_ip_filter="") {
    }
}
?>
```

Abbildung 28: STR-Plug-In für Analysen

angezeigt wird. Ein Parameter legt fest, ob die zwischengespeicherten Daten der letzten Berechnung („loadContent“) oder Daten per Echtzeitberechnung („updateCache“) benutzt werden. Für die eigentliche Analyse wird eine eigene Methode definiert, die vollständigen Datenbankzugriff hat und die Ergebnisse für die Methoden loadContent und updateCache aufbereitet. Hilfsvariablen ermöglichen den Zugriff auf den vom Benutzer ausgewählten Zeitraum und Netzwerkbereich.

Die Ausgabe für die Management-Website kann in Form von HTML-Code und Grafiken erfolgen, so dass jede Art von Ergebnisdarstellung möglich ist. Das Zwischenspeichern von Daten für eine höhere Performance des Webinterfaces kann sowohl in einer Datenbanktabelle als auch in Dateiform erfolgen. Um die Analyseergebnisse auch in anderen Programmen weiterverwenden zu können (z.B. Excel), ist in jedem Plug-In die Methode „export_csv“ definiert. Dadurch können die Ergebnisse direkt von der Webseite im CSV-Format heruntergeladen werden. Einmal täglich werden durch einen Scheduler die updateCache-Methoden aller aktiven Plug-Ins aufgerufen, so dass die zwischengespeicherten Daten auf der Management-Website möglichst aktuell sind und nur bei hohem Aktualitätsbedarf in Echtzeit neu berechnet werden müssen.

5.2.4 Skalierbarkeit und Performance

In Hinblick auf die Skalierbarkeit wurde das Auswertungsmodul so konzipiert, dass mehrere STR-Datenbanken in einem Webinterface verwaltet werden können. Dadurch wird es möglich, mehrere STR-Aufzeichnungsmodule auf verschiedenen Hosts zu betreiben, die Angriffsdaten jedoch zentral auf einem Datenbankserver zu speichern und auszuwerten. Somit können die beiden Hauptmodule und die Datenspeicherung auf getrennten physikalischen Maschinen eingerichtet werden. In sehr großen Umgebungen können dadurch mehrere Aufzeichnungsinstanzen und Datenbankserver eingesetzt werden, um die notwendige Performance sicherzustellen und eine Lastaufteilung herbeizuführen.

Für die Überwachung des Honeynets sind die STR-Module in einer virtuellen Maschine mit Ubuntu[15] 12.04 LTS-Betriebssystem installiert. Da sowohl das Aufzeichnungsmodul als auch das Auswertungsmodul inkl. Datenbankserver in dieser VM betrieben werden, müssen die verfügbaren Ressourcen entsprechend der zu erwartenden Last dimensioniert sein. Für die Bewertung der Performance und der notwendigen Systemressourcen wurden die Angriffe auf das Honeynet mit dem Tool tcpdump aufgezeichnet und ausgewertet.

Die VM musste so konzipiert werden, dass das Aufzeichnungsmodul mehrere parallele Angriffe bearbeiten kann. Darüber hinaus mussten ausreichend Ressourcen für den MySQL-Datenbankserver bereitstehen, so dass die Speicherung der Daten gewährleistet war. Liegt die Datenrate der eingehenden Pakete über der Verarbeitungsrate oder kommt es bei der Weiterverarbeitung der Pakete im Parser zu einer Verzögerung (z.B. durch Performance-Probleme der Datenbank oder durch die Korrelierung von SIP-Paketen eines Calls), muss für die Nachrichtenwarteschlange zwischen Listener und Parser genügend Arbeitsspeicher als Puffer verfügbar sein. Es stellte sich im Probebetrieb heraus, dass die Nachrichtenwarteschlange schnell anwuchs und Paketverluste auftraten, sobald parallel komplexe Auswertungen in der Datenbank vorgenommen wurden. Daher wurde dem STR-Aufzeichnungsmodul zwei GB Arbeitsspeicher fest zugewiesen, so dass genügend Pakete zwischengespeichert werden können.

Um Verzögerungen durch eine zu hohe Datenbankauslastung zu reduzieren, die durch das Auswertungsmodul verursacht wird, erfolgen komplexe Auswertungen auf einem

[15] Ubuntu Linux, http://www.ubuntu.com/

getrennten System. Dies wird durch die Replizierung der Datenbank zwischen zwei Datenbankservern möglich. Die MySQL-Datenbank wird aus Performance-Gründen mit acht GB Arbeitsspeicher betrieben; weitere sechs GB stehen für System- und Webserver-Prozesse bereit. Zur Sicherstellung der Rechenleistung für alle Prozesse verfügt die virtuelle Maschine über acht Prozessoren.

Ein typischer Angriff mit dem Tool SIPvicious erzeugt in der Laborumgebung im Mittelwert zwischen 310 und 360 SIP-Pakete pro Sekunde (Sende- und Empfangsrichtung) in Abhängigkeit von dem gewählten Angriffstyp. Bedingt durch parallele Angriffe im Honeynet wurde ein Maximalwert von 51.234 SIP-Paketen pro Sekunde gemessen. Zusätzlich zu der Prüfung mit tcpdump wurde auch das Netzwerkmonitoring System IsarFlow[16] von einem Kooperationspartner für die Validierung des STRs eingesetzt. Bei Lastspitzen konnte in unregelmäßigen Abständen festgestellt werden, dass einzelne SIP-Pakete nicht vom STR verarbeitet wurden. Dies ist auf die JNetPcap/libpcap-Implementierung zurückzuführen und konnte auch nicht durch den Einsatz neuerer Versionen vollständig unterbunden werden. Eine Überlast des Parsers konnte ausgeschlossen werden, da die Nachrichtenwarteschlange nur minimal gefüllt war und nicht anstieg.

5.2.5 Anonymisierung

Da der STR auch in produktiven Umgebungen mit hohen Datenschutzanforderungen eingesetzt werden sollte, ermöglicht die „Privacy“-Funktion eine Teilanonymisierung der SIP-Verbindungsdaten. In produktiven Firmenumgebungen wurde der STR nur mit aktiver Anonymisierungsfunktion betrieben. Die Felder „Source IP“, „Destination IP“, „Call-ID“, „From“, „To“ und „Contact“ werden mit einer SHA-2-Hashfunktion mit unterschiedlichen Seed-Werten anonymisiert, so dass kein Rückschluss auf den Sender oder Empfänger bzw. gewählte Telefonnummern und Nebenstellen möglich ist. Die Felder „Version“, „User Agent“, „Port“, „SIP method“, „statuscode“ und der Zeitstempel werden hingegen im Klartext gespeichert, da diese Daten aus datenschutzrechtlicher Sicht nicht kritisch sind. Es hat sich jedoch gezeigt, dass durch die Anonymisierung wichtige Informationen verloren gehen bzw. eine Korrelierung von SIP-Nachrichten behindert wird.

Wegen der fehlenden Informationen können jedoch einige Analyse-Plug-Ins nicht verwendet werden. Um die fehlenden Daten zu kompensieren, müssten diese Informationen schon während der Verarbeitung der SIP-Pakete im Parser ermittelt und sofort analysiert werden, da eine Speicherung von Verbindungsinformationen nicht zulässig ist. Neben der Erhöhung der Systemlast bei der Echtzeitverarbeitung der eingehenden Datenpakete müsste die gesamte Systemarchitektur stark verändert werden, da in diesem Fall Analysefunktionen in das Aufzeichnungsmodul ausgelagert werden müssten.

So ist z.B. die Analyse mit einem Geolocation-Dienst [57] zur Bestimmung der Herkunft des Angreifers nicht möglich, da die Quell-IP-Adresse nicht im Klartext vorliegt. Daher müsste diese Analyse in das Aufzeichnungsmodul verlegt werden, wodurch unnötig Last in der Echtzeitverarbeitung erzeugt würde. Aber auch die wichtige Korrelierung von Angriffspaketen für den Clustering-Ansatz und die Zuordnung zu den Angriffsstufen ist z.B. im Fall eines Extension Scan-Angriffs nicht möglich, da die Überprüfung der aufsteigenden Zielnebenstellen im To-Header nicht durchführbar ist. Statistische Auswertungen, die auf der Paketanzahl basieren, und Analysen zu den Angriffswerkzeugen (User Agent) sind auch bei aktiver Anonymisierung ohne Änderung der Systemarchitektur möglich.

[16] IsarFlow, http://isarflow.de/home/

5.2.6 Management-Website

Die STR-Management-Website zeigt die Ergebnisse der vordefinierten, automatischen Analysen geordnet nach den STR-Plug-Ins an. Wie Abbildung 29 zeigt, kann über einen Filter festgelegt werden, für welchen Zeitraum und für welche Netzwerkbereiche die Ergebnisse angezeigt werden sollen. Standardmäßig werden der aktuelle Monat und die Datenbasis des TdR-Lehrstuhls angezeigt. Damit die Verkehrsdaten von anderen Netzwerkstandorten importiert werden können, unterstützt der STR mehrere Datenbanken für die Analyse. Auf der Website kann die gewünschte Datenbank für die Ergebnisanzeige ausgewählt werden. In Abbildung 29 werden durch das Setzen des Filters für den Monat Februar 2014 die eingegangenen SIP-Nachrichten für das Netzwerk A (mit aktiven Honeypots) pro Tag als Ergebnis eines STR-Plug-Ins grafisch aufbereitet. Dabei zeigen sich die charakteristischen Peaks, die durch die aufgezeichneten Registration Hijacking Angriffe zu begründen sind.

Mit Hilfe eines weiteren STR-Plug-Ins wird die Herkunft der Angreifer-IP-Adressen untersucht und in Abhängigkeit von der Anzahl der IP-Adressen bzw. der verwendeten SIP-Anfragen grafisch und tabellarisch präsentiert (Abbildung 30). So ist der aktuelle Status der Bedrohungslage sofort ohne manuelle Analysen ersichtlich.

Da von den Toll Fraud-Angriffen eine besondere Gefahr für SIP-Server ausgeht und diese für den Betreiber einen enormen finanziellen Schaden verursachen können, werden auf der STR-Website auch die letzten Toll Fraud-Anrufe in dem Honeynet-System angezeigt. Die Liste in Abbildung 31 zeigt die letzten 25 Toll Fraud-Anrufe. Alle Angreifer in dieser Liste haben nach einer erfolgreichen Registrierung an einer Honeypot-Nebenstelle einen Anrufversuch zu einer internationalen oder Premium-Rufnummer durchgeführt. Darüber hinaus wird in der Spalte „destination user“ deutlich, wie die Angreifer durch das Variieren von Amtskennzahlen versuchen, die Nebenstellenanlage zu verlassen.

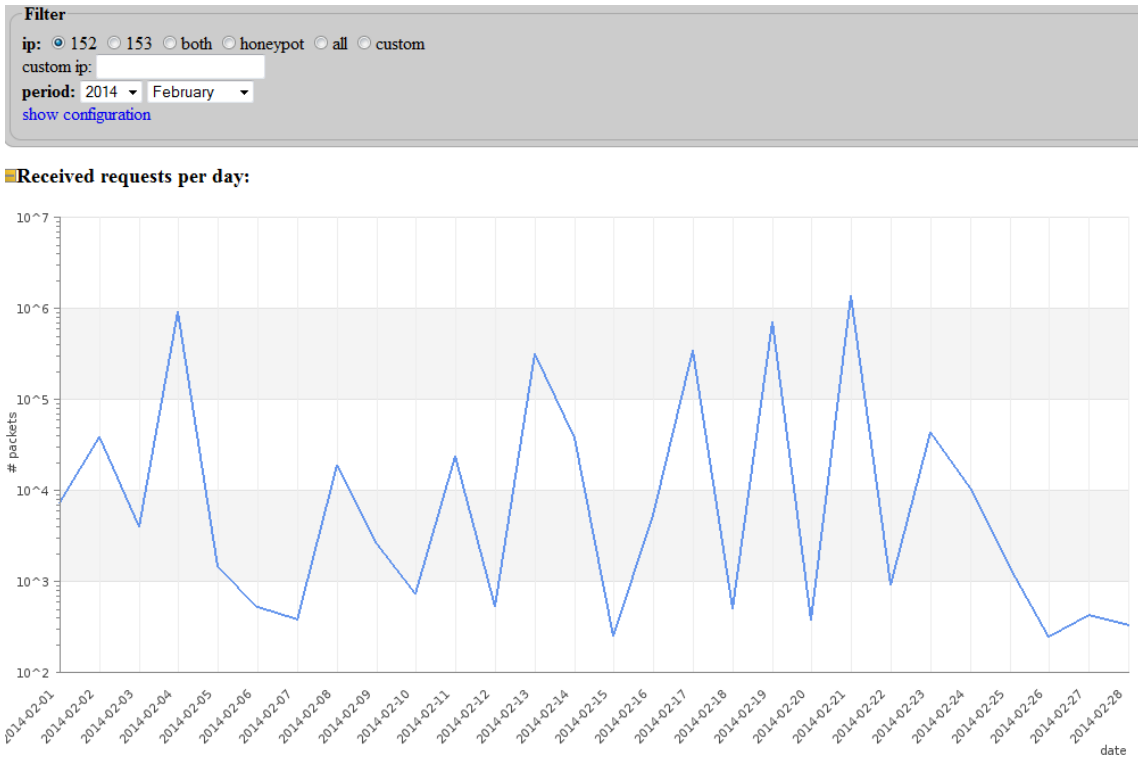
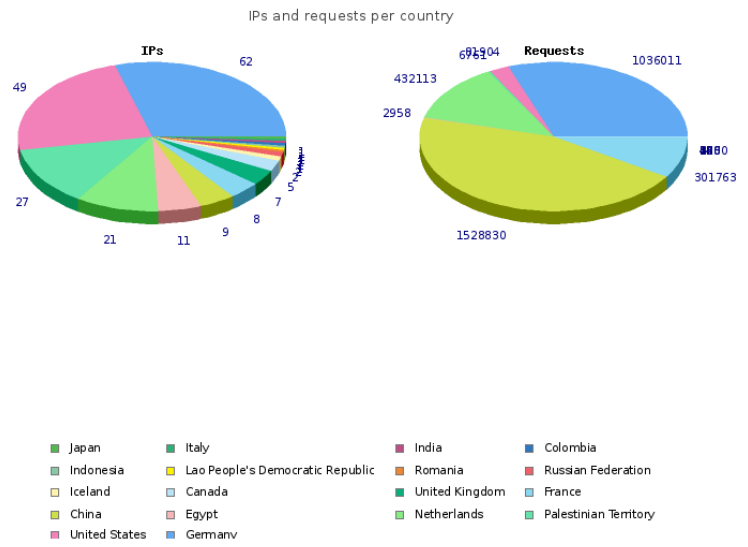


Abbildung 29: STR-Website: SIP-Pakete pro Tag und Filteroptionen



country	# ips	# requests
Canada	5	4,500
China	9	1,528,830
Colombia	1	18
Egypt	11	2,958
France	8	301,763
Germany	62	1,036,011
Iceland	2	5
India	1	18
Indonesia	1	18
Italy	1	24
Japan	1	153
Lao People's Democratic Republic	1	8
Netherlands	21	432,113
Palestinian Territory	27	6,761
Romania	1	3
Russian Federation	2	32
United Kingdom	7	366
United States	49	81,904

Abbildung 30: STR-Website: Herkunft der Angreifer

Last 25 calls (honeypot):

time	call id	source ip	destination ip	duration	destination user	source
2014-11-12 23:48:03	9695f19e5cf408cb32993cf730215d38	195.154.252.144	132.252.152.203		002972599770270	1000
2014-11-12 22:07:11	b70b2acffa973347fb9186f3362a5b7a	195.154.252.144	132.252.152.203		011972599770270	1000
2014-11-12 22:06:52	2953c16dfde78ba5b4a518ed1308e72a	69.30.232.202	132.252.152.203		+972598273072	100
2014-11-12 20:40:13	da44c6252290a75fd88fc042be1cd71a	195.154.252.144	132.252.152.203		972599770270	1000
2014-11-12 19:12:57	f60fc8104b059c15d2444592dd0dd62f	195.154.252.144	132.252.152.203		+972599770270	1000
2014-11-12 17:45:33	70e05faae72d2addd3a3968e6f9c2ff0	195.154.252.144	132.252.152.203		000972599770270	1000
2014-11-12 16:19:05	17593abdf824769c3d23885b645e4861	195.154.252.144	132.252.152.203		00970599770270	1000
2014-11-12 14:52:22	42979a50c98811fd0ebfb5091f722f3d	195.154.252.144	132.252.152.203		00972599770270	1000
2014-11-11 21:25:57	2df38f74e9e4083b838589a52867300c	69.30.232.202	132.252.152.203		00972598273072	100
2014-11-11 00:42:24	226ed4a510ca126cb2dcbf7576b4627c	192.187.122.234	132.252.152.203		900972599375251	2001
2014-11-11 00:08:07	7cefc4775c003282dacfb49bf2d2d526	192.187.122.234	132.252.152.203		000972599375251	2001
2014-11-10 23:33:55	92985ec7d0830204e8326512bb44facf	192.187.122.234	132.252.152.203		00972599375251	2001
2014-11-10 22:58:18	4e787e358526cb9dbe2ade32ea73c8ca	192.187.122.234	132.252.152.203		900972599375251	2000
2014-11-10 22:23:39	45db820bb28e4e6e56e2e92608004bcf	192.187.122.234	132.252.152.203		000972599375251	2000
2014-11-10 21:50:15	16f4f492bdb8d5c1517f21209c441918	192.187.122.234	132.252.152.203		00972599375251	2000
2014-11-10 21:15:52	f4e578c4d0acd0cf3d3ebeaf22f1035a	192.187.122.234	132.252.152.203		900972599375251	109
2014-11-10 20:41:32	5159c9bc4fe0b3adbf7b8bd174fbe093	192.187.122.234	132.252.152.203		000972599375251	109
2014-11-10 20:07:18	7f6af3fb588ff53bc5d84b26390d8260	192.187.122.234	132.252.152.203		00972599375251	109

Abbildung 31: STR-Website: Liste der aktuellen Toll Fraud-Anrufe

5.3 Security Sensor System

Für die verteilte Erkennung von Angriffen an unterschiedlichen Standorten im Internet in Echtzeit und deren Korrelierung wurde das Security Sensor System entwickelt. Die Echtzeiterkennung basiert auf XML-Signaturen, die in Kapitel 5.3.1 erklärt werden. Das Gesamtsystem besteht aus zwei Kernkomponenten: Der Sensorkomponente und dem „Sensor Central Service“ (SCS), der den zentralen Dienst für die Sensorinstanzen darstellt. In den nachfolgenden Unterkapiteln werden der Sensor (Kapitel 5.3.2), die Architektur und die Funktionsweise des SCS (Kapitel 5.3.3) sowie die Korrelierung der eingehenden Sensormeldungen anhand von SCS-Regeln erläutert (Kapitel 5.3.5). Um eine automatisierte, verteilte Erkennung und eine zentrale Analyse der Bedrohungen in Echtzeit zu realisieren, musste eine Schnittstelle zwischen Sensor und SCS entwickelt werden (Kapitel 5.3.4). Die Abschwächung bzw. Abwehr der Angriffe erfolgt durch die Benachrichtigung der betroffenen SIP-Server und der Gegenwehrkomponenten über eine gesonderte Schnittstelle (Kapitel 5.3.7), die im Rahmen des BMBF-Projektes SUNSHINE mit Industriepartnern spezifiziert wurde. Die möglichen Einsatzszenarien und die Hardwareplattformen werden in Kapitel 5.3.6 beschrieben.

5.3.1 Angriffserkennung durch XML-Signaturen

Die Signaturen zur Erkennung von VoIP-Angriffen werden in XML (Extensible Markup Language) [53] spezifiziert. Pro Signatur wird eine eigene XML-Datei benutzt. Abbildung 32 zeigt die Grundstruktur der Signaturen im Überblick. Der detaillierte Aufbau wird in Abbildung 34 bis Abbildung 37 gezeigt. Jede Signatur wird auf ein <rule>-Element abgebildet. Das „ID“-Attribut enthält eine eindeutige Zahl und wird zur Identifizierung der Regel verwendet. Ein <rule>-Element enthält drei unterschiedliche Unterelemente, die im Bereich Signatur-Header (grün hinterlegt) definiert werden: <name>, <description>, <action>. Für jede Regel kann auch das Zeitverhalten für eingehende Pakete berücksichtigt oder das Verhalten für den Versand von Benachrichtigungen beeinflusst werden. Dazu werden im Bereich „Signatur-Parameter“ (blauer Bereich) die Optionen <timeconditions> und <repcount> definiert.

Die Elemente <name> und <description> werden zur Benennung von Angriffsberichten, so genannte Reports, verwendet. Das Element <action> enthält ein Schlüsselwort, das die Aktion benennt, die ausgeführt wird, falls die Regel zutrifft, z.B. „log“ zum Speichern des Reports in einer Log-Datei oder „report“ zum Melden des Angriffs an den Zentraldienst. Das <timeconditions>-Element hat ein oder mehrere Unterelemente vom Typ <condition>, welche die maximale Zeit in Sekunden enthalten, in der zwei oder mehrere SIP-Nachrichten empfangen worden sein müssen. Die SIP-Nachrichten, für die das definierte Zeitintervall gültig ist, sind durch die Attribute „start“ und „end“ festgelegt.

Mit Hilfe des Elementes <repcount> kann festgelegt werden, in welchen Zeitabständen eine Benachrichtigung an den Zentraldienst gesendet werden soll, so dass die Netzwerklast zwischen Sensor und Zentraldienst minimiert wird. Damit die Echtzeiterkennung jedoch gewährleistet bleibt, wird bei der ersten zutreffenden Signatur grundsätzlich ein Report gesendet. Weitere Reports werden automatisch gezählt und nach Ablauf des definierten Zeitraums an den Zentraldienst durch einen zusammenfassenden Report gemeldet. Die Funktion „RepCount“ ist abhängig von der Signatur und der Angreifer-IP-Adresse, so dass identische oder andere Angriffstypen anderer Angreifer sofort an den Zentraldienst gemeldet werden.

Die Angriffssignaturen beschreiben eine Folge von SIP-Nachrichten (grauer Bereich), für die gewisse zeitliche Bedingungen gelten (z. B. „alle Nachrichten einer Regel müssen innerhalb

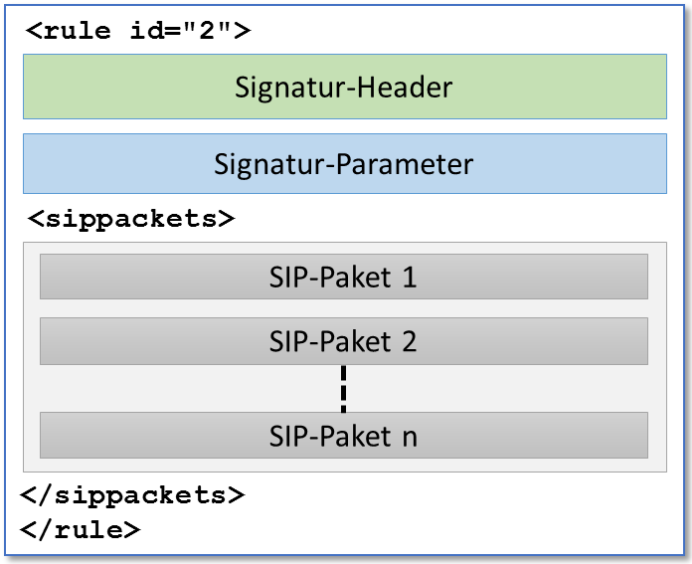


Abbildung 32: Signaturaufbau

von fünf Sekunden empfangen werden“). Die SIP-Header-Felder sowie Netzwerk- und Transportschichtinformationen (IP-Adressen und Ports) können innerhalb der Signaturen mit fest vorgegebenen Werten oder mit Werten von früheren Nachrichten der Folge verglichen werden.

Eine Signatur umfasst mindestens eine SIP-Nachricht. Die Reihenfolge der SIP-Nachrichten wird in dem Element <sippackets> spezifiziert. Die möglichen Unterelemente sind <siprequest> und <sipresponse>, deren Bedeutung aufgrund des Namens definiert ist. Für jedes dieser beiden Elemente können die in Tabelle 6 gezeigten Unterelemete verwendet werden. Tabelle 6 zeigt nur einen Auszug der SIP-Header-Werte. Weitere SIP-Header-Felder können durch die Definition gleichnamiger Elemente (protokoll-konforme SIP-Feldbezeichnung in Kleinbuchstaben und ohne Sonderzeichen) verwendet werden.

Zur Vereinfachung und besseren Übersichtlichkeit der Regeldefinitionen kann den Elementen <siprequest> und <sipresponse> der Parameter „count=“ angehängt werden. Ein Integer-Wert gibt an, wie oft das definierte SIP-Paket auftreten muss, bis eine Signatur zutrifft. Das Verhalten ist mit einer for-Schleife vergleichbar. Für den Vergleich von Nachrichten stehen die in Tabelle 7 angegebenen Attribute zur Verfügung.

Die Reihenfolge der Nachrichten in der XML-Struktur definiert die Reihenfolge der Nachrichten in der Regel. Dies ist für den Vergleich von eingehenden Nachrichten relevant,

Tabelle 6: XML-Elemente zur Definition von SIP-Paketen

Element	Unterelement	Beschreibung
ipv4 / ipv6		Enthält Felder aus dem IPv4/IPv6-Header
	source / destination	Quell- bzw. Ziel-IP-Adresse
sip		Unterschiedliche SIP-Header
	method	Beschreibt die SIP-Methode
	status	Status-Code der Antwort
	to / from	Quell- / Ziel-Nebenstelle (User)
	user-agent	Eingesetzte SIP-Software des Clients
	Call-ID	Eindeutige ID der Session

Tabelle 7: XML-Attribute für den Vergleich von Nachrichten

Attribut-Name	Beschreibung
mode	Ein „mode“-Attribut kann benutzt werden, falls das Element mit einer anderen SIP-Nachricht einer Regel (mode=“compare“) oder mit einem festen Wert (mode=“fixed“, Standardeinstellung) verglichen werden soll
compareType	Der Parameter „compareType“ wird verwendet, um zu definieren, wie die Werte mit einem weiteren Header einer anderen SIP-Nachricht verglichen werden. Mögliche Werte sind: „equals“ (Standardeinstellung), „notequals“, „contains“ und „notcontains“
compareHeader	Für einen Vergleich muss der Zielwert mit dem Parameter „compareHeader“ spezifiziert werden

so dass die Nachrichten in einer Signaturdefinition untereinander referenziert werden können.

Abbildung 33 zeigt anhand eines Beispiels die Definition von zwei SIP-Nachrichten sowie den Vergleich von Header-Werten. Für diese Signatur wird zunächst ein SIP-Request der Methode REGISTER definiert. Für die nachfolgende SIP-Nachricht werden der IP- und SIP-Header überprüft und mit der ersten Nachricht verglichen. Die Ziel- und Quell-IP-Adresse müssen bei Paket eins und zwei übereinstimmen. Es wird festgelegt, dass auch die zweite Nachricht die SIP-Methode REGISTER enthalten muss. Darüber hinaus erfolgt ein Vergleich des SIP-Header-Feldes To der zweiten Nachricht mit dem To-Feld der ersten Nachricht. Der Parameter „compareType“ mit dem Wert „notequals“ gibt an, dass sich die zu vergleichenden Werte unterscheiden müssen, damit die Definition für das zweite SIP-Paket zutrifft.

Nachfolgend wird für jeden bekannten Angriffstyp die jeweilige Signatur erläutert, die während des ersten Feldversuches für die verteilte Angriffserkennung verwendet wurde.

5.3.1.1 Server Scan

Ein Server Scan wird genutzt, um die SIP-Server in einem Netzwerk zu identifizieren. Dabei wird ausgenutzt, dass ein SIP-Server gemäß RFC eine OPTIONS-Anfrage immer beantworten muss. Die Anfragen werden an alle Hosts/IP-Adressen eines Netzes geschickt. Die antwortenden Hosts sind SIP-Server. Um einen Server Scan zu erkennen, muss der Sensor mehr als eine IP-Adresse überwachen, idealerweise das gesamte Subnetz. Überwacht er nur eine IP-Adresse, so kann nicht erkannt werden, ob nur dieser eine Host eine OPTIONS-Anfrage erhalten hat oder ob tatsächlich das gesamte Subnetz gescannt wird.

Zur Erkennung des Angriffs wird in Abbildung 34 eine Signatur gezeigt, die OPTIONS-Anfragen berücksichtigt. Damit SIP-Nachrichten von produktiven Komponenten nicht als Angriff gewertet werden, wird ein Schwellenwert von drei OPTIONS-Nachrichten in drei Sekunden festgelegt. Mehr als eine OPTIONS-Nachricht an verschiedene IP-Adressen muss als verdächtig gewertet werden, da ein solches Verhalten nicht dem normalen SIP-Protokollablauf entspricht. Die Quelle (Quell-IP-Adresse) ist dabei immer gleichbleibend. Das Ziel unterscheidet sich aber jeweils vom Ziel der vorherigen Nachricht. Alle drei

```
<siprequest>
 <sip>
   <method>REGISTER</method>
</sip>
</siprequest>
```

```
<siprequest>
 <ipv4>
   <destination mode="compare">1</destination>
   <source mode="compare">1</source>
 </ipv4>
 <sip>
   <method>REGISTER</method>
   <to mode="compare" comparetype="notequals"
     compareheader="to">1</to>
 </sip>
</siprequest>
```

Abbildung 33: Signatur mit Paketdefinitionen und Vergleichsfunktion

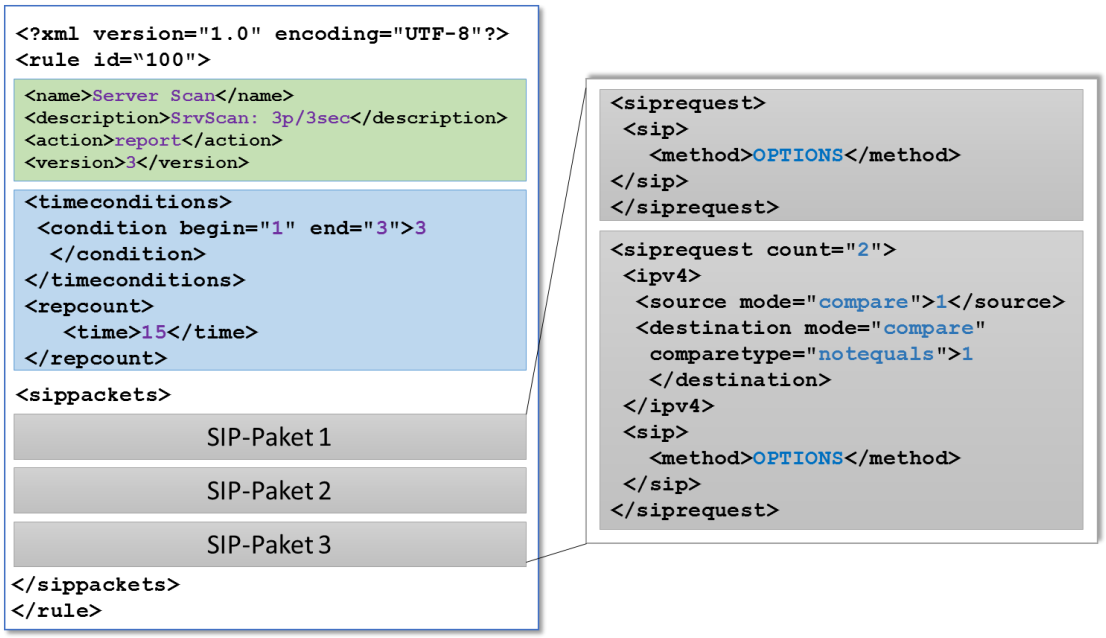


Abbildung 34: Signatur für Server Scan-Angriffe

definierten Nachrichten sind vom Typ „siprequest“ und müssen die Methode OPTIONS beinhalten. Ab dem zweiten SIP-Paket wird verglichen, ob die Angreifer-IP-Adresse mit dem ersten Paket der Regel übereinstimmt und ob das zweite bzw. dritte Paket an eine andere Ziel-IP-Adresse gesendet wird als die erste SIP-Nachricht. Die Regel ist mit dem Parameter „count“ vereinfacht, so dass die Bedingungen für die SIP-Pakete zwei und drei nur einmal definiert werden müssen.

Im Header der Signatur ist definiert (<timeconditions>), dass die drei definierten SIP-Nachrichten innerhalb von drei Sekunden empfangen werden müssen. Wird dieser Timeout überschritten, wird die Regel automatisch verworfen. Sollte es sich um einen längeren Angriff eines Angreifers handeln, so wird der Zentraldienst nach der ersten Benachrichtigung alle 15 Sekunden zusammenfassend informiert (abhängig von der RepCount-Einstellung). Wird der Sensor in entfernten Netzwerken mit einer geringeren Leitungsbandbreite eingesetzt, kann dieser Wert entsprechend erhöht werden, so dass die Benachrichtigungen zum Zentraldienst z.B. nur alle 60 Sekunden erfolgen.

5.3.1.2 Extension Scan

Ein Extension Scan wird für die Suche nach aktiven Nebenstellen einer Telefonanlage benutzt. Die gefundenen Nebenstellen können später das Ziel von SPIT-Anrufen oder Registration Hijacking-Angriffen sein. Für einen Extension Scan wird die REGISTER-Methode mit unterschiedlichen Werten im To-Header verwendet. Typischerweise werden zahlreiche REGISTER-Anfragen in einer sehr kurzen Zeitspanne verwendet (bis zu 40.000 SIP-Pakete in wenigen Minuten).

Die in Abbildung 35 gezeigte XML-Signatur beinhaltet vier Paketdefinitionen von derselben Quell-IP-Adresse (gleicher Angreifer) zu derselben Ziel-IP-Adresse (gleicher SIP-Server), jedoch mit unterschiedlichen Zielnebenstellen innerhalb von vier Sekunden. Auf Grund der wechselnden Zielnebenstellen bei einem Extension Scan muss für jede eingehende SIP-Nachricht geprüft werden, ob diese im Vergleich zur vorherigen Nachricht einen unterschiedlichen To-Header-Wert aufweist. Der Schwellenwert für die notwendige Anzahl von SIP-Nachrichten wurde auf mindestens vier Pakete festgelegt, da z.B. bei einigen SIP-Anschlüssen bis zu drei Rufnummern einzeln an einem SIP-Server registriert werden müssen. Im Vergleich zu der Honeynet-Umgebung macht es in Netzwerkumgebungen mit

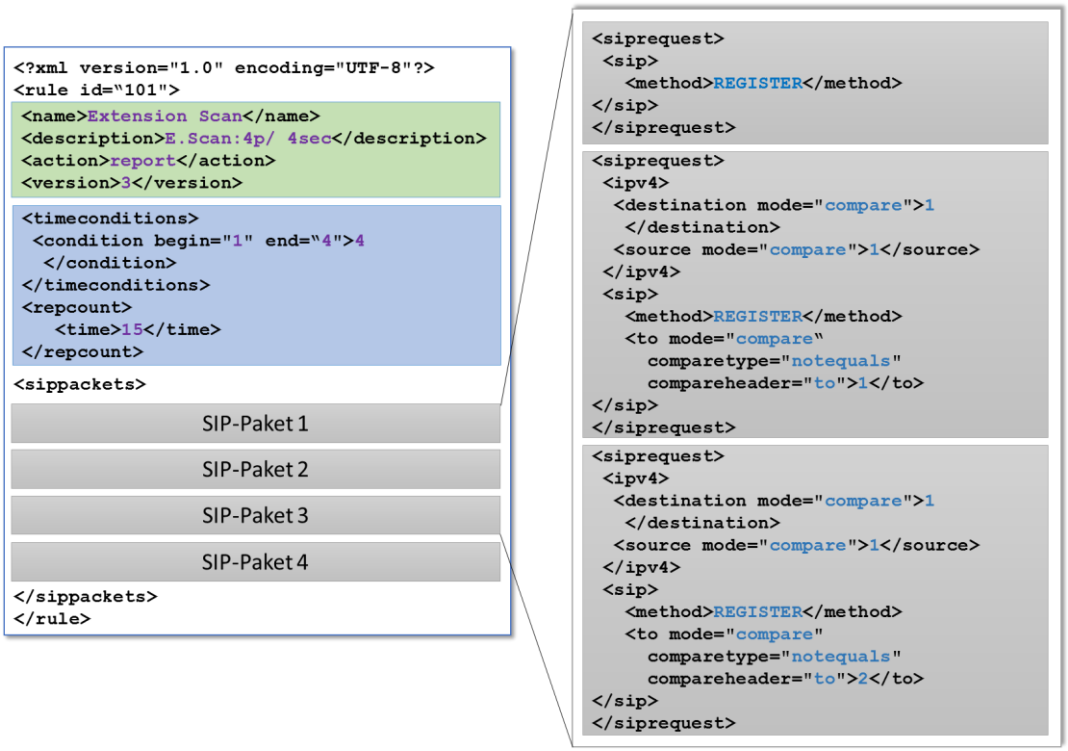


Abbildung 35: Signatur für Extension Scan-Angriffe

produktiven Komponenten Sinn, die Anzahl der Pakete in dieser Signatur auf mindestens 10 zu erhöhen, so dass „False Positives“ möglichst ausgeschlossen werden können. So kann ein privater VoIP-Anschluss als Nachfolger des ISDN-Mehrgeräteanschlusses bis zu 10 unabhängige Telefonnummern haben.

Zur Erfüllung dieser Signatur wird zunächst ein SIP-Paket der Methode REGISTER benötigt. Die Bedingungen für die Pakete zwei bis vier sind bis auf das zu vergleichende Paket identisch: Für jedes Folgepaket wird geprüft, ob die Quell- und Ziel-IP-Adresse identisch sind und ob sich der To-Header-Eintrag von dem des Vorgängerpaketes unterscheidet. Der Sensor versendet die Reports maximal alle 15 Sekunden (RepCount-Wert im blauen Bereich Signatur-Parameter).

5.3.1.3 Registration Hijacking

Bei der Angriffsstufe Registration Hijacking wird versucht, eine existierende (durch Extension Scan ermittelte) Nebenstelle an einem SIP-Server anzumelden. Dabei werden bis zu 13 Millionen SIP-Nachrichten der Methode REGISTER mit derselben Zielnebenstelle (To-Header) und unterschiedlichen Authentisierungsinformationen in kurzer Zeit verschickt. Die eingesetzte Signatur (siehe Abbildung 36) beinhaltet 100 SIP-Requests, die innerhalb von 30 Sekunden von einer Quelle zu einem Ziel gesendet werden müssen. Der Wert des To-Headers ist dabei immer derselbe, da eine Nebenstelle mittels Brute-Force-Attacke übernommen werden soll. Die verschiedenen Authentisierungsinformationen werden ignoriert, da diese für die Angriffserkennung nicht relevant sind und so auch die Systemlast reduziert werden kann.

Da Registration Hijacking-Angriffe typischerweise sehr massiv ausfallen, wurde der Schwellenwert von 100 SIP-Paketen definiert (siehe auch Kapitel 6.4.1). Fehlgeschlagene Anmeldeversuche von normalen SIP-Komponenten oder reguläre Anmeldungen von SIP-DECT-Anlagen mit zahlreichen Mobiltelefonen in produktiven Umgebungen werden so vollständig ignoriert, so dass „False Positives“ minimiert werden können. „False Negatives“ sind in diesem Falle möglich, da Angriffe mit weniger als 100 SIP-Paketen nicht

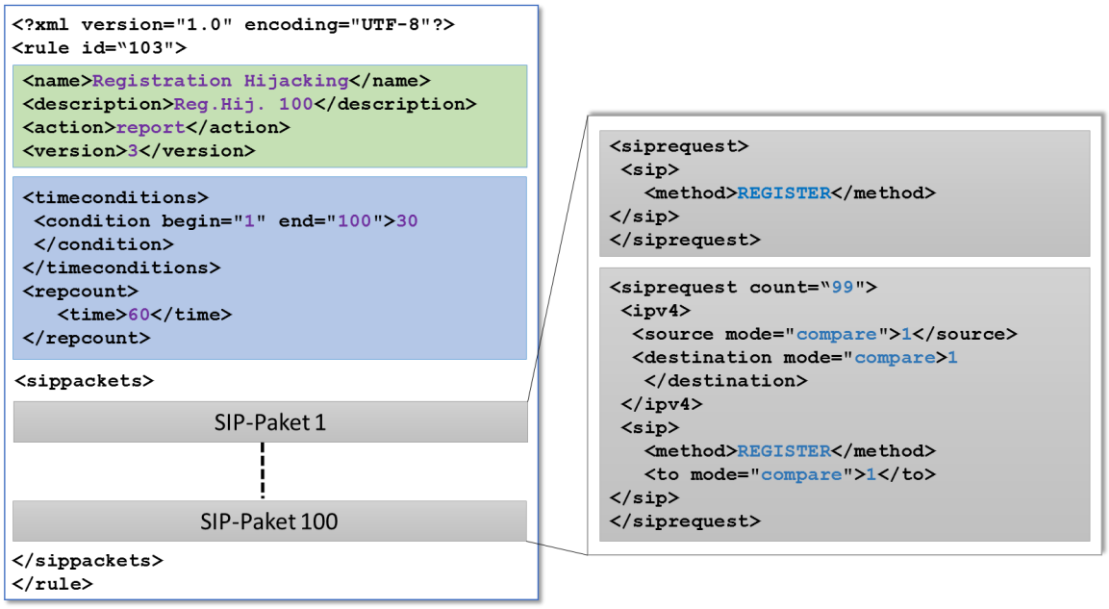


Abbildung 36: Signatur für Registration Hijacking-Angriffe

berücksichtigt werden. Sollen auch weniger intensive Angriffe erkannt werden, so müsste eine weitere Signatur mit einem geringeren Schwellenwert definiert werden.

Die Signatur für den Registration Hijacking-Angriff erfordert auch die Definition eines SIP-Requests der Methode REGISTER. Die folgenden 99 SIP-Nachrichten werden mit dem Parameter „count“ als Schleife definiert. Dabei wird geprüft, ob die Werte für die Quell- und Ziel-IP-Adresse sowie der Wert für das To-Header-Feld mit dem ersten SIP-Paket übereinstimmen.

Sobald die definierten Bedingungen für die 100 SIP-Nachrichten zutreffen, wird automatisch ein Report an den Zentraldienst gesendet. Nach dem Empfang weiterer 100 Pakete wird nur ein Report versendet, wenn die letzte Benachrichtigung bereits 60 Sekunden zurückliegt. Andernfalls wird die Erfüllung der Signatur für diesen Angreifer im Speicher vermerkt und nach Ablauf des Timeouts als Sammelreport gemeldet. Da die Brute-Force-Attacken oftmals über viele Minuten bis hin zu Stunden aktiv sind, wird zur Reduzierung der Netzwerk- und Systemlast die Anzahl der Folgereports durch die RepCount-Funktion eingeschränkt.

5.3.1.4 Toll Fraud

Toll Fraud bezeichnet das unrechtmäßige Führen von Telefongesprächen auf Kosten Dritter. Bei der Erkennung besteht die Schwierigkeit darin, legitime Anrufer von Angreifern zu unterscheiden. Die IP-Adresse des Angreifers könnte als Erkennungsmerkmal dienen, sofern dieselbe IP-Adresse vorher für einen anderen Angriffstyp genutzt wurde. Beobachtungen mit Hilfe eines Honeynets haben allerdings gezeigt, dass die vorbereitenden Angriffe (Server Scan, Extension Scan und Registration Hijacking) von anderen IP-Adressen als die späteren Anrufe erfolgen.

Wenn ein Registration Hijacking-Versuch erkannt wurde, kann aber beispielsweise eine Regel definiert werden, die anschlägt, wenn versucht wird, über eine kompromittierte Nebenstelle zu telefonieren. Dies wird durch das zweistufige Erkennungssystem (Sensor und Zentraldienst) möglich, indem für die Korrelierung eine SCS-Regel auf dem Zentraldienst eingesetzt wird, wobei ein eingehender Sensor-Report als Trigger verwendet wird (siehe Kapitel 5.3.5). Mit Hilfe des SCS wird ermittelt, ob eine Nebenstelle vor dem Toll Fraud-Versuch bereits angegriffen wurde (z.B. Extension Scan, Registration Hijacking). Für

eine optimale Erkennung von Toll Fraud-Angriffen in produktiven Umgebungen werden eine Signatur mit entsprechenden Schwellenwerten sowie eine zentrale Korrelierungskomponente benötigt, damit ein Zusammenhang zwischen vorausgegangenen Angriffen erkannt werden kann und die False Positives-Rate minimal gehalten wird.

Der erste Feldversuch mit dem Security Sensor System hat jedoch auch gezeigt, dass Angreifer bei Toll Fraud-Versuchen in nur wenigen Sekunden zahlreiche Zielrufnummern mit variierenden Amtskennzahlen ausprobieren. In diesem Fall wäre eine Erkennung unabhängig von vorausgegangenen Angriffen möglich, da unterschiedliche Rufnummern an nur einer Nebenstelle in einem kurzen Zeitabstand getestet werden und dieses Verhalten in produktiven Systemen nicht zu finden ist. Zur Absicherung gegen False Positives können auch die SIP-Antworten berücksichtigt werden, so dass z.B. festgestellt werden kann, ob eine gewählte Rufnummer ungültig ist. Dadurch wird eine Unterscheidung von einem normalen Anwender möglich, der z.B. die Wahlwiederholung verwendet.

In einem Honeynet hingegen gelten alle getätigten Anrufe und somit jedes INVITE-Paket als verdächtig, da in diesem keine produktiven Komponenten installiert sind. Als Ergebnis des durchgeführten Feldversuches wird nachfolgend eine Regel beschrieben, die eingesetzt werden kann, wenn nicht jedes INVITE-Paket als Angriff gewertet werden soll.

Diese Regel dient der Meldung von allen abgehenden Anrufversuchen zu unterschiedlichen Zielrufnummern über aktive Honeypot-Nebenstellen. Basierend auf den forensischen Analysen wird bei dieser Signatur berücksichtigt, dass ein Angreifer verschiedene Zielrufnummern testet. Innerhalb von 10 Sekunden muss ein Angreifer drei Anrufversuche (SIP-Nachrichten der Methode INVITE) zu unterschiedlichen Zielrufnummern über die gleiche Honeynet-Nebenstelle ausführen, damit die in Abbildung 37 dargestellte Signatur zutrifft und der Sensor einen Report an den Zentraldienst sendet. Da die Angreifer typischerweise verschiedene Amtskennzahlen ausprobieren, liegt die False Negatives-Rate nach Honeynet-Analysen bei dieser Regel unter 1%.

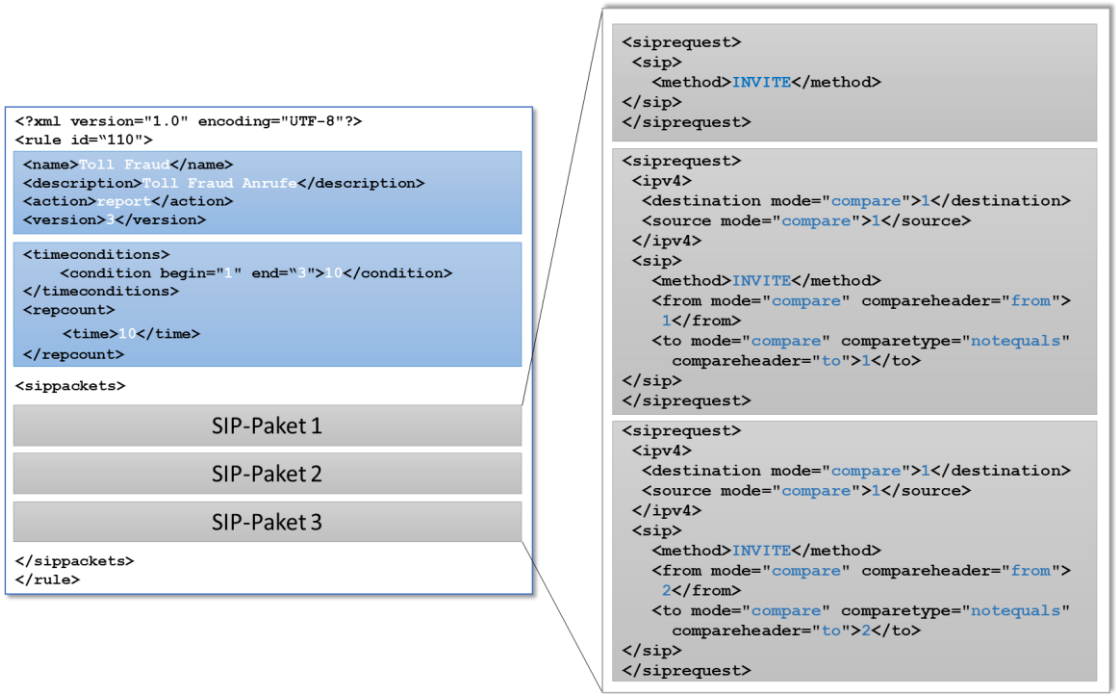


Abbildung 37: Signatur für Toll Fraud-Anrufe

Die Ergebnisse der verschiedenen Signaturen zur Angriffserkennung werden in Kapitel 6.3.4 erläutert.

5.3.2 Sensor

Der Sensor ist ein Werkzeug zur signaturbasierten Erkennung von Angriffen in SIP-basierten VoIP-Netzwerken. Die in Kapitel 5.3.1 vorgestellten XML-Signaturen können von dem Sensor direkt eingelesen und zur Erkennung von Angriffen benutzt werden. Während der Forschungsprojekte wurde auf Grund von unterschiedlichen Hardware-Plattformen jeweils ein Prototyp in C++ [58] sowie in Java [54] implementiert und im Honeynet des Lehrstuhls getestet und optimiert. Die Software ist objektorientiert unter Zuhilfenahme der Bibliotheken libpcap [49], libboost [59] und libcurl [60], welche u.a. die einfache Arbeit mit Netzwerkschnittstellen und eine Plattformunabhängigkeit ermöglichen. Verschiedene Prozessorarchitekturen, wie x86/x64, MIPSEL (FritzBox) oder ARM (Raspberry Pi), werden unterstützt. Die dabei eingesetzten Betriebssysteme basieren auf Linux.

Die Sensorarchitektur und der Datenfluss werden in Abbildung 38 gezeigt und in den nachfolgenden Unterkapiteln anhand der Komponenten erläutert. Der Sensor besteht aus vier Hauptkomponenten (Listener, Analyse, Aggregation, Aktion), die durch Hilfskomponenten unterstützt werden. Konfiguriert wird der Sensor entweder lokal über eine Konfigurationsdatei sowie über Programmparameter oder durch einen zentralen Dienst, der die Konfiguration pro Sensorinstanz zur Verfügung stellt. In diesem Fall muss in der Konfigurationsdatei die URL des Zentraldienstes, eine eindeutige Sensor-ID inkl. Kennwort sowie ein Zertifikat zur Überprüfung der Vertrauenswürdigkeit angegeben werden. Die technische Beschreibung der Schnittstelle zwischen Sensor und Zentraldienst erfolgt in Kapitel 5.3.4.

5.3.2.1 Listener

Die erste Komponente wird als Listener bezeichnet und dient der Sammlung und Filterung der SIP-Nachrichten basierend auf der Bibliothek libPcap. Mit Hilfe dieser Komponente werden die SIP-Pakete auf Port 5060 (TCP/UDP) aus dem gesamten Datenverkehr herausgefiltert, so dass nur die relevanten Pakete weiterbearbeitet werden und die Systemlast nicht unnötig ansteigt. Aktuell existieren drei verschiedene Implementierungen dieser Komponente, die es ermöglichen, die SIP-Nachrichten über eine Netzwerkschnittstelle im „promiscuous mode“, aus einer Datei im PCAP-Format (z. B. mit tcpdump erzeugt) oder per UDP-Tunnel zu sammeln. Alle gesammelten SIP-Nachrichten werden sofort in eine Warteschlange gestellt, auf die auch die nächste Komponente zugreifen kann. Somit kann das Empfangsmodul unabhängig von der Analysekomponente die SIP-Nachrichten durch nebenläufige Prozesse verarbeiten.

5.3.2.2 Analyse

Mit der Analysekomponente werden alle SIP-Nachrichten aus der Warteschlange durch den SIP-Parser eingelesen und mit den definierten Angriffssignaturen verglichen. Der Analysekomponente sind unter Zuhilfenahme der Speicher-Hilfskomponente alle

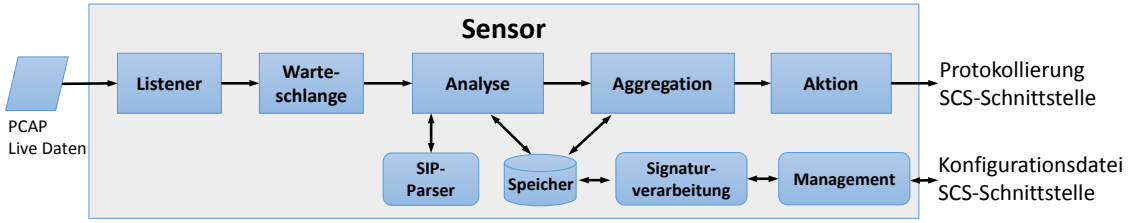


Abbildung 38: Sensor-Architektur

Angriffssignaturen bekannt, da diese bei Programmstart über die Management- und Signaturverarbeitungskomponente bereits eingelesen wurden. Die Angriffssignaturen können dabei entweder aus lokal gespeicherten Dateien geladen oder von einem zentralen Dienst abgerufen werden. Neben den Angriffssignaturen verwaltet die Speicherkomponente auch den Zustand der Angriffssignaturen, für die schon eine oder mehrere SIP-Nachrichten empfangen wurden, sowie alle SIP-Nachrichten, die für Vergleiche mit später empfangenen Nachrichten benötigt werden. Der Speicher, der für den Zustand von Angriffssignaturen und SIP-Nachrichten benötigt wird, wird sofort wieder freigegeben, sobald die Daten nicht mehr relevant sind.

Die Analysekomponente entnimmt die SIP-Nachrichten einzeln der Warteschlange und bringt diese mithilfe des SIP-Parsers in eine interne Objektstruktur. Anschließend wird jede SIP-Nachricht mit der ersten Nachricht jeder Angriffssignatur verglichen. Sollte der Vergleich positiv ausfallen, wird ein „Stateful-Objekt“ für diese Regel unter Berücksichtigung der Quell-IP-Adresse erstellt, so dass weitere eingehende Nachrichten mit der zweiten Nachricht der aktiven Angriffssignatur verglichen werden können.

Sollten für eine Nachricht alle Vergleiche negativ ausfallen, da keine passenden Signaturdefinitionen vorhanden sind, wird die Nachricht ignoriert. Sollte bei einem Vergleich festgestellt werden, dass die zeitlichen Bedingungen nicht erfüllt sind, so wird das entsprechende Zustandsobjekt der Angriffssignatur entfernt. Sofern die Nachrichten, die mit diesem Zustand verknüpft waren, nicht mehr für andere Zustände benötigt werden, werden auch diese zur Speicherfreigabe entfernt. Fällt der Vergleich einer eingehenden SIP-Nachricht mit der letzten Nachrichtendefinition eines Zustandsobjektes einer Angriffssignatur positiv aus, so wird ein Report erzeugt und die nachfolgende Aggregationskomponente informiert.

5.3.2.3 Aggregation

Bei massiven Angriffen besteht die Möglichkeit, dass einige feingranulare Signaturen sehr häufig auslösen und bedingt durch die große Anzahl von Reports die Netzwerklast zwischen Sensor und Zentraldienst stark ansteigen lassen. So würden zum Beispiel bei einem Registration Hijacking-Angriff mit 100.000 SIP-Nachrichten und einer Signaturdefinition von 100 Paketen 1.000 Reports in wenigen Minuten versendet. Die Aggregationskomponente verwaltet die ausgehenden Reports unter Berücksichtigung der RepCount-Werte der jeweiligen Signatur sowie der IP-Adresse des Angreifers.

Der erste Report eines Angriffs wird von der Aggregationskomponente sofort an die Aktionskomponente weitergeleitet. Die nachfolgenden Reports eines Angriffs werden aggregiert und gezählt, so dass nach Ablauf des Timeouts (definiert durch den RepCount-Wert, z.B. 60 Sekunden) ein erweiterter Report weitergegeben wird. Der Versand wird nur für Reports der gleichen Signatur-ID und der gleichen Quell-IP-Adresse für die Dauer des festgelegten Timeouts verzögert. Attacken anderer Angreifer oder andere Angriffstypen werden unabhängig behandelt. Da der erste Report grundsätzlich versendet wird, ist die Echtzeitfähigkeit der Angriffserkennung nicht beeinträchtigt. Auch der Anfang sowie das Ende eines Angriffs sind weiterhin feststellbar.

5.3.2.4 Aktion

Die Aktionskomponente dient dazu, eine bestimmte Aktion auszuführen, wenn ein Angriff erkannt wird. Der Aufruf erfolgt über die Aggregationskomponente, wobei der zu bearbeitende Report übergeben wird. Derzeit implementierte Aktionen sind beispielsweise das Speichern eines Angriffsreports in einer lokalen Logdatei, die Benachrichtigung des Low Interaction Honeypots Dioanea oder das Senden eines Angriffsreports an einen zentralen

Dienst über die Sensor/SCS-Schnittstelle (siehe Kapitel 5.3.4). Welche Aktion ausgeführt wird, ist in den einzelnen Angriffssignaturen definiert. Es ist auch möglich, mehrere Aktionen für eine Angriffssignatur auszuführen. Durch den modularen Aufbau können weitere Aktionen implementiert werden.

5.3.3 Architektur und Funktionsweise des Sensor Central Service (SCS)

Der Sensor Central Service (SCS) stellt für alle Sensoren die Konfiguration sowie die Verteilung der Erkennungssignaturen bereit. Pro Sensor können die zu verteilenden Signaturen festgelegt werden, so dass nicht jeder Sensor alle Signaturen verarbeiten muss. Die SCS-Architektur und die Funktionsweise sind in Abbildung 39 dargestellt und werden nachfolgend erläutert.

Sobald eine Signatur auf einer Sensorinstanz für einen aktiven Angriff zutrifft, wird durch den Sensor ein erster Report erzeugt und in Abhängigkeit von dem RepCount-Parameter der Signatur werden in definierten Zeitabständen Folgereports versendet. Die empfangenen Sensorreports werden über das „SCS Sensor Interface“ (SSI) an den SCS übertragen und durch den „Sensor Controller Process“ (SCP) in einer MySQL-Datenbank gespeichert. Dieser Prozess dient neben dem Empfang und der Speicherung der Reports dem Management der verteilten Sensoren.

Die Management-Website stellt den aktuellen Status der angebundenen Sensoren inklusive des Standortes und der eindeutigen Sensor-ID dar. Weiterhin können die eingehenden Reports der Sensoren eingesehen und die Verarbeitung der Regelsätze kontrolliert werden. Darüber hinaus ist die gesamte Konfiguration sowie die Erstellung und

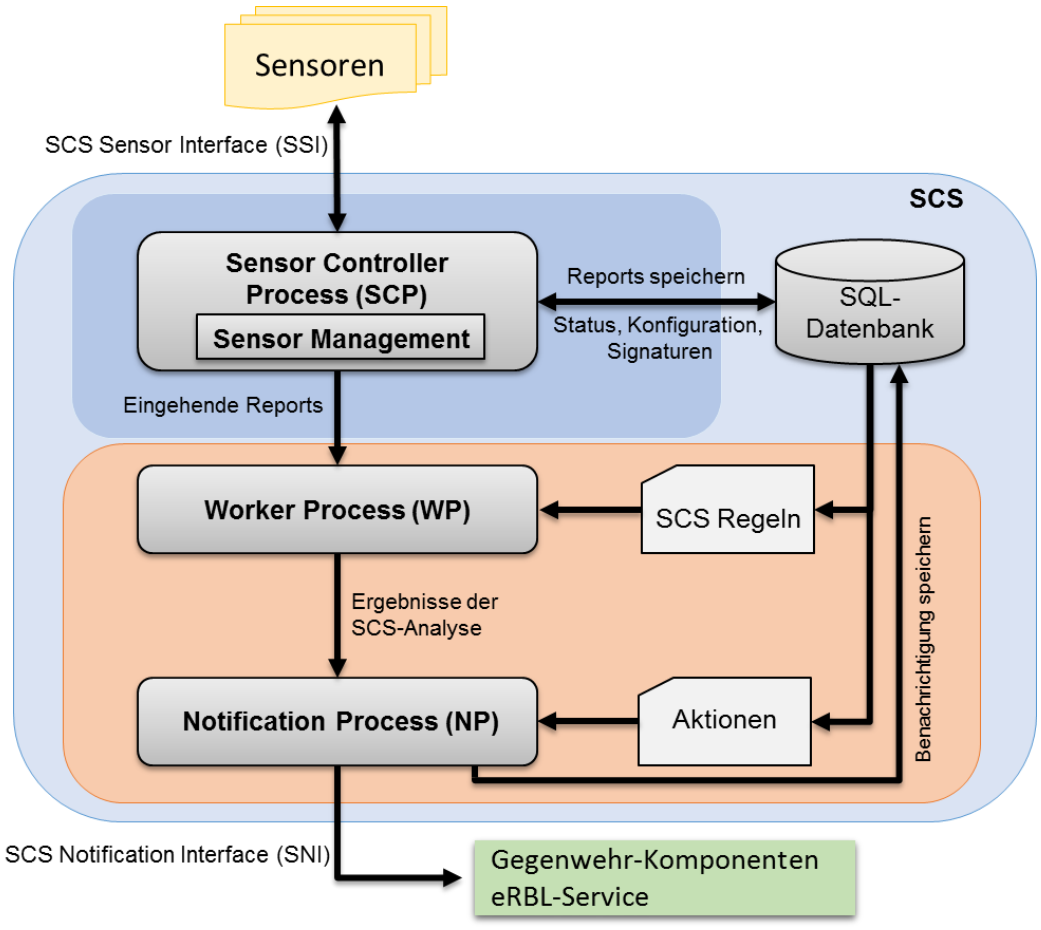
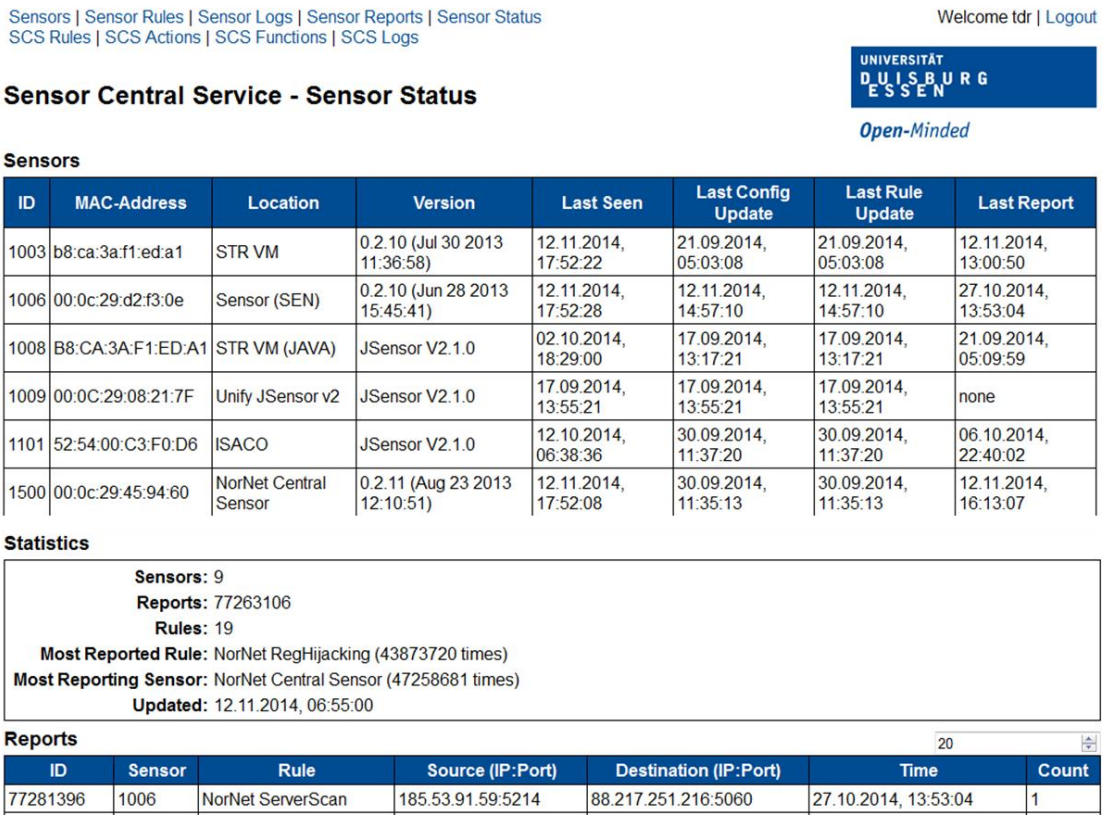


Abbildung 39: SCS-Architektur

Verwaltung von SCS-Regeln und Sensorsignaturen möglich. Abbildung 40 zeigt einen Ausschnitt der SCS-Management-Website mit dem Status der angebundenen Sensoren, der aktuellen Statistik (Anzahl der aktiven Sensoren, empfangene Reports, aktive Regeln, die am häufigsten gemeldete Regel und der Sensor mit der höchsten Aktivität) sowie den letzten empfangenen Report des Sensors mit der ID 1006. Über die Menüführung am oberen linken Rand gelangt der Anwender auf die Konfigurationsseiten des Security Sensor Systems, z.B. für das Einrichten neuer Sensoren und Signaturen bzw. SCS-Regeln und Aktionen.

Das zentrale Management ist besonders wichtig, da nur so eine komfortable Verwaltung der Messstellen möglich wird, ohne für eine Signatur- oder Konfigurationsänderung physikalischen Zugang zu fremden Netzwerken an weit entfernten Standorten haben zu müssen. Um einen „Single Point of Failure“ auszuschließen, können die Komponenten des zentralen Managements (z.B. Datenbank-Server, Sensor-Schnittstelle) auf unterschiedlichen physikalischen Systemen betrieben werden. Damit periodische „Pull-Requests“ der nachfolgenden Analyseprozesse, die eine unnötige Belastung der Ressourcen darstellen würden, vermieden werden können, werden neue Reports neben der Speicherung in der SQL-Datenbank direkt an den „Worker Process“ (WP) gemeldet.

Der Worker Process stellt das zentrale Modul der Angriffsanalyse auf dem SCS dar. Unter Berücksichtigung der SCS-Regeln (siehe Kapitel 5.3.5) werden eingehende Reports analysiert. Mit Hilfe der SCS-Regeln können Zusammenhänge bzw. Abhängigkeiten zwischen einzelnen Sensorregeln definiert werden. Ist eine SCS-Regel zutreffend, z.B. weil ein Angreifer einen Server Scan in verschiedenen Netzwerken ausführt, können verschiedene Aktionen über den „Notification Process“ (NP) initiiert werden, wie z.B. das Informieren einer Firewall zum Blockieren eines aktuell laufenden Angriffs. Jeder SCS-Regel können eine oder mehrere Aktionen zugewiesen werden, die bei Zutreffen der Regel ausgeführt werden. Eine Aktion kann aus vordefinierten Funktionen bestehen (wie z.B. das



Sensors | Sensor Rules | Sensor Logs | Sensor Reports | Sensor Status
SCS Rules | SCS Actions | SCS Functions | SCS Logs

Welcome tdr | Logout

UNIVERSITÄT DUISBURG ESSEN
Open-Minded

Sensor Central Service - Sensor Status

Sensors

ID	MAC-Address	Location	Version	Last Seen	Last Config Update	Last Rule Update	Last Report
1003	b8:ca:3a:f1:ed:a1	STR VM	0.2.10 (Jul 30 2013 11:36:58)	12.11.2014, 17:52:22	21.09.2014, 05:03:08	21.09.2014, 05:03:08	12.11.2014, 13:00:50
1006	00:0c:29:d2:f3:0e	Sensor (SEN)	0.2.10 (Jun 28 2013 15:45:41)	12.11.2014, 17:52:28	12.11.2014, 14:57:10	12.11.2014, 14:57:10	27.10.2014, 13:53:04
1008	B8:CA:3A:F1:ED:A1	STR VM (JAVA)	JSensor V2.1.0	02.10.2014, 18:29:00	17.09.2014, 13:17:21	17.09.2014, 13:17:21	21.09.2014, 05:09:59
1009	00:0C:29:08:21:7F	Unify JSensor v2	JSensor V2.1.0	17.09.2014, 13:55:21	17.09.2014, 13:55:21	17.09.2014, 13:55:21	none
1101	52:54:00:C3:F0:D6	ISACO	JSensor V2.1.0	12.10.2014, 06:38:36	30.09.2014, 11:37:20	30.09.2014, 11:37:20	06.10.2014, 22:40:02
1500	00:0c:29:45:94:60	NorNet Central Sensor	0.2.11 (Aug 23 2013 12:10:51)	12.11.2014, 17:52:08	30.09.2014, 11:35:13	30.09.2014, 11:35:13	12.11.2014, 16:13:07

Statistics

Sensors: 9
Reports: 77263106
Rules: 19
Most Reported Rule: NorNet RegHijacking (43873720 times)
Most Reporting Sensor: NorNet Central Sensor (47258681 times)
Updated: 12.11.2014, 06:55:00

Reports 20

ID	Sensor	Rule	Source (IP:Port)	Destination (IP:Port)	Time	Count
77281396	1006	NorNet ServerScan	185.53.91.59:5214	88.217.251.216:5060	27.10.2014, 13:53:04	1

Abbildung 40: SCS-Status-Website

Melden eines Angreifers an einen Real-time-Blacklist-Service) oder Informationen über eine externe Schnittstelle anderen Softwareprodukten zur Verfügung stellen.

5.3.4 SSI-Schnittstelle zwischen Sensor und SCS

Die Sensoren und der SCS-Zentraldienst kommunizieren, indem der Sensor bei Programmstart sowie periodisch unter einer vordefinierten URL über das Internet ein PHP-Skript aufruft und dabei per HTTP-POST eine definierte XML-Struktur mitsendet. Die Antwort des Zentraldienstes erfolgt ebenso in einer definierten XML-Struktur sowie mit HTTP-Status-Codes und ermöglicht mithilfe mehrerer Parameter die zentrale Steuerung der verteilten Sensoren. Die Kommunikation erfolgt verschlüsselt per HTTPS. Die Identität des Zentraldienstes wird durch eine eigene Stammzertifizierungsstelle, deren Wurzelzertifikat den Sensoren bekannt ist, überprüft. Die Verwendung von HTTP-Keep-Alive[17] ermöglicht den Austausch vieler Anfragen und Antworten, ohne dass neue TCP- oder SSL-Verbindungen aufgebaut werden müssen.

Die Sensorauthentifizierung am Zentraldienst erfolgt über die eindeutige Sensor-ID und das Passwort, die bei jeder Anfrage mitgesendet werden. Zusätzlich wird die MAC-Adresse des Sensors übermittelt und bei dem ersten Login gespeichert, damit festgestellt werden kann, ob eine Sensor-ID von mehreren Sensorinstanzen an unterschiedlichen Standorten genutzt wird. Da die Messstandorte bei einer doppelten Nutzung einer Sensor-ID nicht mehr eindeutig sind, werden Anmeldungen von anderen MAC-Adressen nicht zugelassen. Bei einer Standortänderung oder einem Hardwarewechsel muss die Verknüpfung von Sensor-ID und MAC-Adresse zuvor über die SCS-Management-Website aufgehoben werden.

5.3.4.1 Nachrichtenaustausch

Abbildung 41 zeigt den Nachrichtenfluss zwischen einem Sensor und dem SCS-Zentraldienst. Aus Sicherheitsgründen erfolgen die Anfragen grundsätzlich von der Seite des Sensors und nicht umgekehrt. Dadurch ist es für die Kommunikation zwischen SCS und Sensor nicht notwendig, einen öffentlich zugänglichen Port in der Firewall des Sensor-Hosts

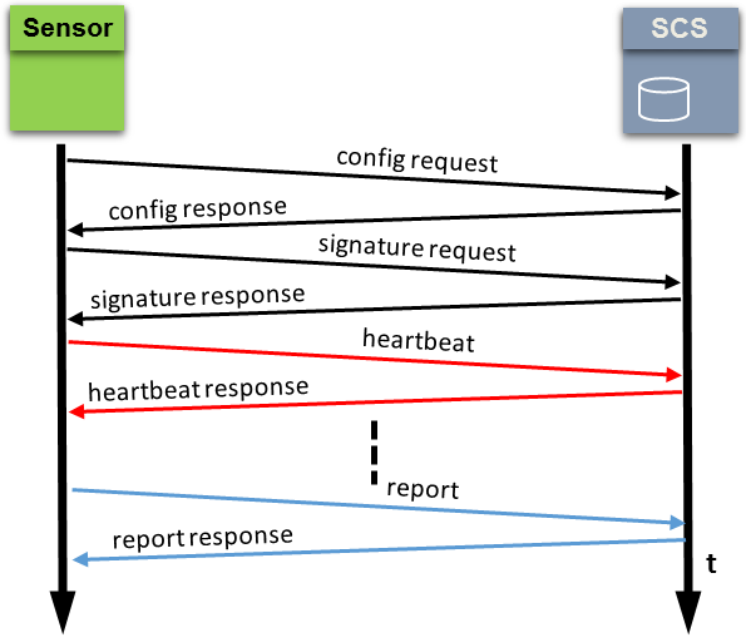


Abbildung 41: Nachrichtenfluss zwischen Sensor und Zentraldienst

[17] RFC7230, Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing, Keep-Alive Connections

zu öffnen. Eine Anfrage des Sensors wird mit einer Statusnachricht beantwortet, so dass in regelmäßigen Abständen eine Rekonfiguration des Sensors mit Hilfe der Antwortpakete möglich ist.

Beim Start des Sensors wird zunächst die Konfiguration per „config-request“ abgerufen und anschließend werden die Angriffssignaturen per „signature-request“ übertragen. Wurden die Konfiguration und die Signaturen durch den Sensor erfolgreich verarbeitet, ist die Angriffserkennung des Sensors aktiv und es werden periodisch „heartbeat“-Nachrichten versendet, falls kein Report generiert wird. Das Versenden der heartbeat-Nachrichten ist bei der aktuellen Sensor-Version auf 30 Sekunden eingestellt. Eine heartbeat-Nachricht wird durch den SCS bestätigt. Bei einem erkannten Angriff wird eine „report“-Nachricht versendet und durch den SCS bestätigt. Wird eine Sensorinstanz beendet, so erfolgt keine Abmeldenachricht an den SCS, da das Ausbleiben der heartbeat-Nachrichten automatisch einen Fehlerzustand des entsprechenden Sensors im SCS erzeugt.

5.3.4.2 Anfragetypen

Für die SSI-Schnittstelle wurden fünf Anfragetypen spezifiziert, die von einer Sensor-Instanz an den SCS gesendet werden können:

- **config**
  Der config-request dient dem Abruf der Sensorkonfiguration (z.B. Netzwerkschnittstelle und PCAP-Filter für die Listener-Komponente).
- **rule**
  Der zweite Anfragetyp rule wird benutzt, um die Angriffssignaturen zu übertragen, die im SCS für eine Sensor-ID festgelegt wurden.
- **report**
  Wird durch einen Sensor ein Angriff erkannt, weil eine Signatur zutrifft, so kann dieser per report-Anfrage an den Zentraldienst gemeldet werden.
- **log**
  Eine log-Anfrage erlaubt beispielsweise die Meldung von Fehlern an den Zentraldienst, falls Teile der Konfiguration nicht verarbeitet werden können (z.B. fehlerhafter PCAP-Filter).
- **heartbeat**
  Eine heartbeat-Anfrage wird periodisch versendet, damit dem Zentraldienst bekannt ist, welche Sensoren aktiv sind, und damit dieser im Antwortpaket Steuerungsinformationen an die Sensoren senden kann. Heartbeat-Anfragen werden allerdings nur verschickt, sofern in einer definierten Zeit keine andere Anfrage versendet wird. Werden z.B. viele Angriffe gemeldet, kann der Versand von heartbeat-Nachrichten über längere Zeit ausbleiben, damit die Netzwerkverbindung nicht unnötig belastet wird.

In Abbildung 42 ist ein Beispiel für eine report-Anfrage dargestellt, die vom Anfragetyp „request“ ist. Das XML-Schema gibt vor, dass die Anmeldeinformationen im Element <authinfo> übertragen werden müssen. In jeder Nachricht wird das Element <version> vermerkt, so dass über den Zentraldienst ermittelt werden kann, welche Sensoren nicht der aktuellen Version entsprechen. Die dargestellten Informationen im <report>-Element sind die Pflichtinformationen, welche in jedem Report vorhanden sein müssen. Damit ein Report im SCS analysiert werden kann, müssen die eindeutige Signatur-ID und zur Kontrolle der Regelübereinstimmung zwischen Sensor und SCS auch die Versionsnummer der Signatur vermerkt werden. In einem Standardreport werden nur die folgenden Angriffsdaten bereitgestellt, so dass die Privatsphäre und der Datenschutz berücksichtigt

```
<?xml version="1.0" encoding="UTF-8"?>
<request>
 <authinfo>
  <sensorid>123</sensorid>
  <secret>qwertzuiopasdfghjklyxcvbnm</secret>
  <mac>AB:CD:EF:12:34:56</mac>
 </authinfo>
 <version>1.0-20120508</version>
 <type>REPORT</type>
 <report>
  <ruleid>103</ruleid>
  <ruleversion>5</ruleversion>
  <sourceip>132.252.154.77</sourceip>
  <sourceport>5060</sourceport>
  <destinationip>132.252.152.203</destinationip>
  <destinationport>5060</destinationport>
  <time>20120508T08:53:38</time>
  <repcount>9</repcount>
 </report>
</request>
```

Abbildung 42: Beispiel für SSI-Report-Nachricht (Standard)

sind: Quell- und Ziel-IP-Adresse, Portnummern und Zeitstempel. Handelt es sich nicht um den ersten Report, der für einen identischen Angreifer und die gleiche Signatur-ID generiert wird, so wird im Element <repcount> zusätzlich vermerkt, wie viele Reports innerhalb des für diese Signatur definierten Timeouts gesammelt wurden.

Darüber hinaus ermöglicht die SSI-Schnittstelle die Übermittlung weiterer SIP-Header-Werte im Element <sipvalues>, die in der Definition der Angriffssignaturen angegeben werden können. Die zusätzlichen Header-Werte müssen als Unterelemente nach dem Schema

<SIP-Header-Name>Wert</SIP-Header-Name>

in den Report eingebunden werden. Der SCP speichert die zusätzlichen SIP-Header-Werte automatisch in einer getrennten Tabelle der Datenbank und ordnet diese über eine 1:n-Verknüpfung dem entsprechenden Reporteintrag zu, so dass diese Werte auch für den Analyseprozess verwendet werden können. Dies ermöglicht z.B. den Vergleich der verwendeten Angriffswerkzeuge (User Agent-Header). Jedoch muss bei vielen weiteren Feldern der Datenschutz beachtet werden. Zum Beispiel entspricht der To-Header eines INVITE-Pakets der gewählten Zielrufnummer. Deshalb kann es in produktiven Umgebungen zu datenschutzrechtlichen Konflikten kommen.

5.3.4.3 Statusnachrichten

Der Zentraldienst nutzt HTTP-Status-Codes zur Beantwortung der Anfragen. Dies hat den Vorteil, dass die Menge der übertragenen Daten reduziert werden kann und der Sensor nur dann Rechenleistung für die Verarbeitung der (XML-)Antwort aufwenden muss, wenn tatsächlich Steuerungsinformationen vorliegen. Die genutzten Status-Codes sind „204 NO CONTENT“, wenn keine Daten mitgesendet wurden, „400 BAD REQUEST“, wenn die Anfrage des Sensors syntaktisch ungültig war, „403 FORBIDDEN“, wenn die Authentisierung fehlgeschlagen ist (ungültige Sensor-ID oder ungültiges Passwort bzw. falsche MAC-

Adresse). Der Status-Code „200 OK“ wird genutzt, wenn Daten im XML-Format im Nachrichtenkörper vorliegen.

Die XML-Nachricht (siehe Beispiel in Abbildung 43) enthält zwei Elemente, <newconfig> und <newrules>, welche auf den Wert „1“ gesetzt werden, wenn ein Konfigurations- bzw. Regel-Update durch den Sensor durchgeführt werden soll (der Zentraldienst sendet diese Informationen nicht automatisch mit). Das <action>-Element kann genutzt werden, um den Sensor neu zu starten (RESTART), zu stoppen (STOP) oder die aktuelle Softwareversion zu installieren (UPDATE). Das <type>-Element wird genutzt, wenn zusätzliche Informationen wie Angriffssignaturen (type=rules) oder Konfigurationsparameter (type=config) in der Antwort enthalten sind. Eine Antwortnachricht kann entweder Regeln oder Konfigurationsparameter oder kein <type>-Element beinhalten. Wird eine Aktualisierung der Regeln durchgeführt, so werden grundsätzlich alle Regeln innerhalb einer Nachricht übertragen, so dass alle bisherigen Signaturen auf dem Sensor verworfen und durch die neuen ersetzt werden.

5.3.5 Korrelierung von verteilten Angriffen mit SCS-Regeln

Die SCS-Regeln ermöglichen eine Korrelierung von eingehenden Sensor-Reports und sind im Gegensatz zu den Angriffssignaturen in der Skriptsprache PHP spezifiziert. Da besonders bei der Korrelierung unterschiedlicher Reports verschiedener Standorte eine möglichst dynamische und umfangreiche Definition von Regeln notwendig ist, kann der volle Umfang von PHP für die Analyse genutzt werden. Die SCS-Regeln können über die Management-Website definiert werden. Um diesen Vorgang möglichst komfortabel zu gestalten, muss lediglich die eigentliche Analysefunktion erstellt werden, die auf vordefinierte Objekte und die SCS-Datenbasis zugreifen kann.

Abbildung 44 zeigt das Editieren einer SCS-Regel mit Hilfe der SCS-Management-Website. Für jede Regel wird ein eindeutiger Name vergeben. Mit Hilfe von Bedingungen wird festgelegt, wann diese Regel für die Analyse verwendet werden soll. Eine Regel wird nur von dem SCS Worker Process aktiviert, wenn ein eingehender Sensor-Report den zugewiesenen Sensoren und Signaturen entspricht. In dem gezeigten Beispiel wurde die SCS-Regel sechs Sensoren und der Signatur „Honeypot Register (100x)“ zugeordnet. Trifft ein Registration Hijacking-Report von einem der sechs zugeordneten Sensoren ein, wird die Logik der SCS-Regel angewendet und bei einem erfolgreichen Ergebnis werden die aktivierten Aktionen durch den SCS ausgeführt (in diesem Fall „Hello World“ und „Notify Firewall“).

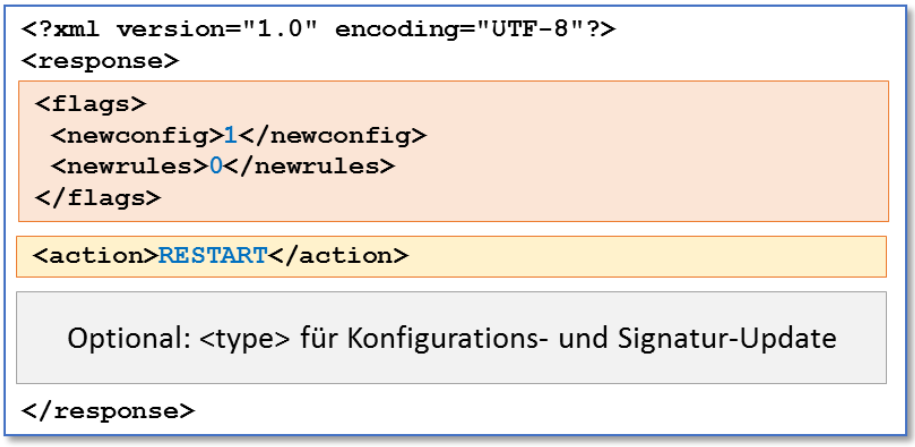


Abbildung 43: Antwortnachricht SCS-Interface

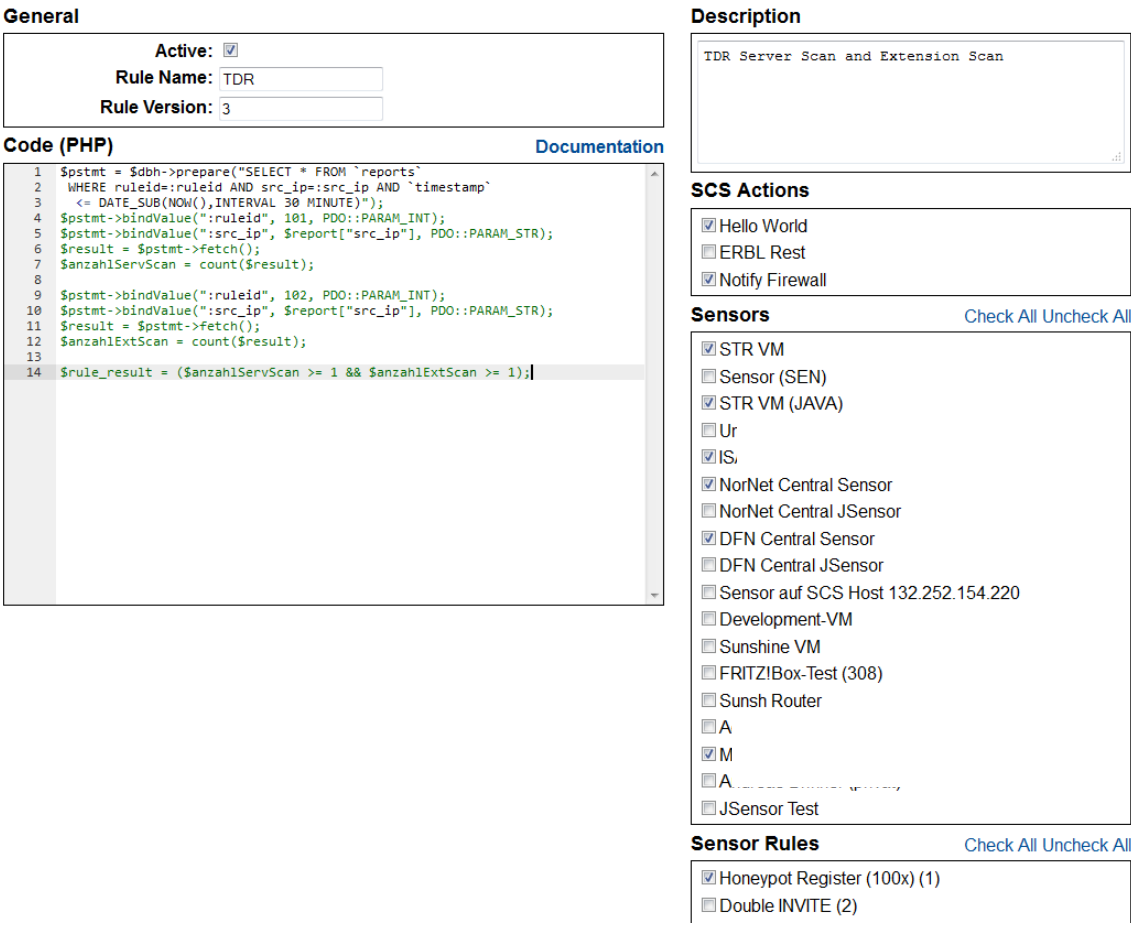


Abbildung 44: SCS-Regel Definition

Mit der Programmlogik aus dem abgebildeten Beispiel wird bei jedem eingehenden „Honeypot Register 100x“-Report, abhängig von den Angreifern, analysiert, ob vorausgegangene Server Scan- (RuleID 101) und Extension Scan-Angriffe (RuleID 102) innerhalb der letzten 30 Minuten erfolgten. Das Objekt „$pstmt“ bietet direkten Zugriff auf die Report-Datenbanktabelle des SCS, so dass beliebige SQL-Abfragen je nach Fragestellung benutzt werden können. Die letzte Zeile prüft, ob jeweils ein oder mehrere Server Scan- und Extension Scan-Angriffe an verschiedenen Standorten erkannt wurden und setzt in diesem Fall die Rückgabevariable auf „true“.

Wenn ein Angreifer neben dem aktuellen Registration Hijacking-Angriff bereits vor weniger als 30 Minuten weitere Angriffsstufen durchgeführt hat, gilt dieser als besonders verdächtig, so dass auch die Aktion „Notify Firewall“ ausgelöst wird. Über eine Schnittstelle in dieser Aktion wird die Angreifer-IP-Adresse übergeben, damit temporär die IP-Adresse dieses Angreifers geblockt werden kann und eine produktive Nutzung nicht gestört wird.

5.3.6 Einsatzszenarien und Hardware

In Kapitel 3.3 wurden die unterschiedlichen Kommunikationsszenarien und möglichen Angriffsziele erläutert. Für die verteilte Missbrauchserkennung im Internet muss der Sensor in verschiedenen Netzwerkbereichen installiert werden können und darf die Funktion der produktiven SIP-Komponenten nicht negativ beeinflussen. Darüber hinaus muss für die unterschiedlichen Umgebungen berücksichtigt werden, welche Voraussetzungen für die Installation und den Betrieb eines Sensors gegeben sind. So steht z.B. nicht in jedem Netzwerk ein Mirror-Port für die passive Anbindung des Sensors zur Verfügung oder es werden keine IP-Telefoniedienste betrieben, so dass nicht die vollständigen Angriffsketten

sichtbar werden. Darüber hinaus müssen die Anforderungen an die Hardware berücksichtigt werden, da besonders in kleinen Netzwerken keine leistungsfähigen Virtualisierungsserver für den Betrieb des Sensors und eines Honeynets verfügbar sind.

In Enterprise-Umgebungen werden typischerweise Session Border Controller (SBC) eingesetzt und diese sind den SIP-Servern vorgeschaltet. Für den Angreifer ist der SBC die öffentlich erreichbare Komponente. Der ein- und ausgehende SIP-Verkehr kann über einen Mirror-Port an die Sensor-Komponente weitergeleitet werden. In diesem Fall kann der Sensor als virtuelle Maschine zur Installation auf vorhandenen, leistungsfähigen Servern bereitgestellt werden. Auch im Small Business Umfeld kann der Sensor im Regelfall über einen Mirror-Port der Firewall oder an einem Switch problemlos betrieben werden. Steht hingegen kein Virtualisierungsserver für die Installation des Sensors zur Verfügung oder handelt es sich um eine Netzwerkumgebung ohne aktive SIP-Komponenten, wird eine unabhängige Hardwarelösung benötigt, die genügend Ressourcen für die Erkennung von Angriffen sowie für einen evtl. notwendigen Honeypot bereitstellt. Besonders in privaten Netzwerken, die typischerweise nur über einen Heim-Router mit beschränkter Funktionalität verfügen, müssen kompakte und stromsparende Hardwarekomponenten mit ausreichenden Ressourcen ausgewählt werden.

Auf den in Kapitel 2.5 vorgestellten kompakten Hardwareumgebungen Intel NUC und Raspberry Pi wurde das Linux Betriebssystem Debian[18] 7 installiert. Neben der Sensor-Komponente ist optional die Software Asterisk als High Interaction Honeypot eingerichtet, so dass die Kompakt-Hardware ohne großen Installationsaufwand besonders gut in kleineren und mittleren Netzwerkumgebungen installiert werden kann. Sollte keine öffentliche IP-Adresse für das System zur Verfügung stehen, so kann in „Network Address Translation“ (NAT)-Umgebungen eine Portweiterleitung des Ports 5060 eingerichtet werden.

Auf Grund des geringen Kaufpreises wäre das Raspberry Pi für den Sensor-Betrieb optimal. Das ähnlich kompakte Intel NUC-System bietet zeitgemäße Hardware, hat jedoch einen deutlich höheren Anschaffungspreis. In der Laborumgebung wurden verschiedene Angriffssignaturen bei aktivem Honeypot auf beiden Systemen in Hinblick auf die Performance wiederholt getestet:

- Reg. Hijacking 1: Diese Regel definiert einen Registration Hijacking-Angriff mit 100 REGISTER-Paketen, die innerhalb von 20 Sekunden eintreffen müssen.
- Reg. Hijacking 2: Mit dieser Regel soll überprüft werden, ob sich die Berücksichtigung des Zeitverhaltens positiv oder negativ auf die Systemlast auswirkt, indem keine zeitliche Einschränkung definiert wurde.
- Angriffsstufen 1-3: Für diesen Test wurden drei Regeln aktiviert, die einen Server Scan mit fünf Paketen (in fünf Sekunden), einen Extension Scan mit 10 Paketen (in 10 Sekunden) sowie einen Registration Hijacking-Angriff mit 100 Paketen (in 20 Sekunden) berücksichtigen.

Abbildung 45 zeigt, dass die Ergebnisse für die Tests Reg.Hijacking 1 und 2 nur marginal (ca. 0,5%) voneinander abweichen, so dass die Berücksichtigung des Zeitverhaltens keine nennenswerten Auswirkungen auf die Systemlast hat. Werden hingegen mehrere Signaturen pro Sensor aktiviert und somit komplexere Sachverhalte untersucht, steigt die Systemlast auf beiden Geräten um 4% an. Der Vergleich der Hardwarekomponenten zeigt jedoch deutlich, dass das Raspberry Pi-System im Angriffsfall eine Systemlast von fast 100% erreicht und somit für komplexere Signaturen oder Umgebungen mit parallelen Angriffen

[18] Debian Linux, https://www.debian.org/

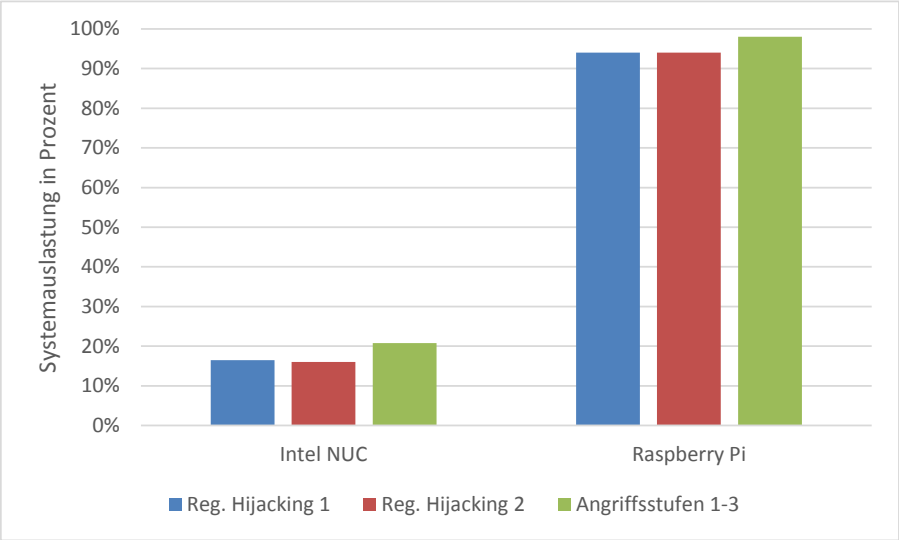


Abbildung 45: Systemlast der Intel NUC / Raspberry Pi Hardware je nach Signatur

nicht geeignet ist. Auf Grund der aktuellen Hardware (Zwei-Kern-Prozessor, vier GB Arbeitsspeicher, SSD-Festplatte) wird deutlich, dass der Intel NUC für den Sensor-Betrieb sehr gut geeignet ist und bei einem Stromverbrauch von ca. sieben Watt auch in privaten Netzwerken eingesetzt werden kann.

5.3.7 Abwehr von Angriffen

Eine zutreffende SCS-Regel kann eine oder mehrere Aktionen auslösen. Eine SCS-Aktion kann mit dem vollen Sprachumfang von PHP programmiert werden. Alternativ besteht die Möglichkeit, eine externe Schnittstelle mit gewünschten Parametern (z.B. Quell-IP-Adresse des Angreifers) aufzurufen.

Obwohl der Hauptfokus dieser Dissertation auf der Erkennung von SIP-basierten Angriffen liegt, wurden während der Untersuchungen im Rahmen des BMBF-Projektes SUNSHINE Ansätze zur Abwehr von Angriffen entwickelt und getestet. Dazu wurden zwei Aktionen implementiert: Die Schnittstelle zur Übertragung von Angriffsdaten in die „Extended Real-time Blacklist“ (eRBL) [7] und eine direkte Anbindung an ein Firewall-System eines Industrie-Projektpartners. Darüber hinaus werden Ideen für weitere Abwehrmaßnahmen vorgestellt, die im Projektumfeld und im Rahmen von Demonstratoren für Konferenzen entstanden sind.

5.3.7.1 eRBL-Dienst

Abbildung 46 zeigt, dass der eRBL-Dienst aus zwei Hauptkomponenten besteht: Aus dem REST-Server [61] für das Hinzufügen und Verwalten von verdächtigen IP-Adressen und aus dem DNS-Server für die einfache Abfrage von Angreifer-IP-Adressen. Beide Dienste nutzen eine gemeinsame SQL-Datenbank. Der DNS-Dienst stellt die Abfrage-Schnittstelle für die

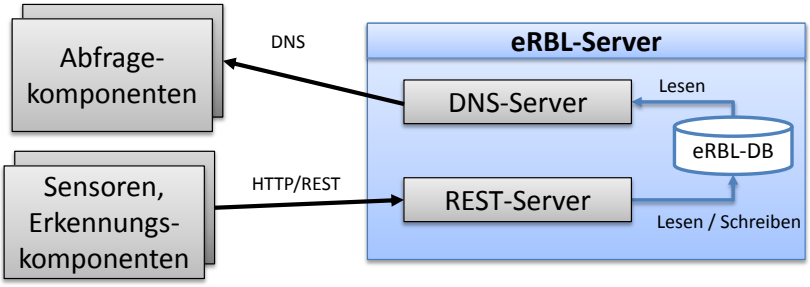


Abbildung 46: eRBL-Architektur

verschiedensten Softwareprodukte wie z.B. Firewall oder SIP-Server bereit, so dass diese bei einem Zugriff durch eine unbekannte IP-Adresse über eine Standardschnittstelle überprüfen können, ob eine Quell-IP-Adresse verdächtig ist. Eine komplizierte bzw. meist unerwünschte Erweiterung von bestehenden Softwareprodukten um proprietäre Schnittstellen kann somit vermieden werden.

5.3.7.2 Abwehrszenario

Die Abbildung 47 zeigt ein schützenswertes internes Netzwerk einer Firma, das SIP-basierte Dienste nach außen anbietet, damit Außendienstmitarbeiter die Sprachdienste von unterwegs oder von zuhause nutzen können. Dieses Netzwerk ist durch eine Firewall vom Internet oder anderen Netzwerken getrennt. In der Mitte ist ein nicht vertrauenswürdiges Netzwerk dargestellt, das in diesem Szenario als Internet angenommen wird und Angreifer beinhaltet. Darüber hinaus sind weitere Sensoren im Internet verteilt, wie z.B. auf einem Heimnetz-Router.

Die Firma betreibt eine eigene Telefonanlage (PBX), an die die internen VoIP-Telefone angebunden sind. Über dieses System werden auch die Sprachdienste für externe Teilnehmer zur Verfügung gestellt. Die Telefonanlage ist zur Kommunikation mit externen Teilnehmern durch die Firewall von außen erreichbar.

Zur Erkennung von Angriffen sind verteilte Sensoren installiert. In diesem Szenario ist ein interner Sensor auf der Telefonanlage im Firmen-Netzwerk positioniert. Des Weiteren ist ein zweiter Sensor auf dem Internet-Router integriert. Die beiden Sensoren leiten im Angriffsfall die Reports, basierend auf den geladenen Signaturen, an den SCS weiter. Alle installierten Sensoren erlauben eine verteilte Erkennung, so dass die Angriffsaktivität in verschiedenen Netzwerkbereichen möglichst frühzeitig erkannt werden kann.

Wird bei der Analyse der eingegangenen Sensor-Reports auf dem SCS ein Angriff erkannt, so wird eine Alarmnachricht an den eRBL-Server für die IP-Adresse des Angreifers gesendet. Die Angreifer-Daten stehen nun für verschiedene Komponenten über den eRBL-Dienst zur Verfügung.

Die Firewall ist so konfiguriert, dass Quell-IP-Adressen von eingehenden SIP-Verbindungen zu der IP-Telefonanlage vor der Weiterleitung der SIP-Pakete über den eRBL-Dienst geprüft werden. Falls die Verbindung nicht zulässig ist, besteht die Möglichkeit, entsprechende SIP-

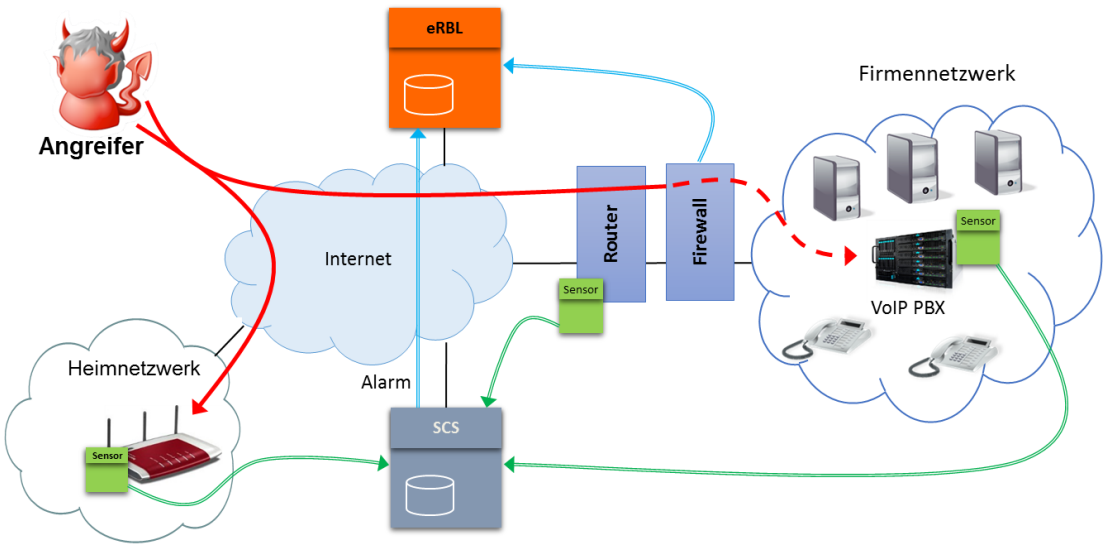


Abbildung 47: Abwehrszenario mit eRBL-Dienst

Antworten zu generieren, um die Verbindung protokollkonform zu beenden und für einen definierten Zeitraum zu unterbinden.

5.3.7.3 Weitere Abwehrmaßnahmen

Die Gegenmaßnahmen im Angriffsfall können auch unabhängig von einer vorgeschalteten Firewall direkt im SIP-Server bzw. Session Boarder Controller implementiert werden:

- Wurde ein Angriff auf eine bestimmte Nebenstelle erkannt, so kann der Anwender zur Eingabe einer nur ihm bekannten PIN oder zur Änderung des SIP-Kennwortes über eine Webschnittstelle zu Beginn eines Gespräches aufgefordert werden. Alternativ kann an die hinterlegte E-Mail-Adresse oder Mobilfunkrufnummer im Angriffsfall ein neues Kennwort oder eine benötigte PIN gesendet werden, so dass der Anwender rechtzeitig über den Betrugsversuch informiert ist und die Zugangsdaten der kompromittierten Nebenstelle für den Angreifer nutzlos werden.
- Liegt ein Verdachtsfall vor, so können Anrufe zu Mehrwert- oder internationalen Rufnummern vorerst unterbunden werden, so dass ein größerer finanzieller Schaden abgewendet werden kann.
- Erfolgt durch eine bereits an anderen Messstellen bekannte IP-Adresse ein Server- oder Extension Scan-Angriff, kann das Verhalten des SIP-Servers temporär angepasst werden. Sobald ein SIP-Paket der Methode OPTIONS oder REGISTER von dieser Quell-IP-Adresse eingeht, werden die SIP-Anfragen nicht beantwortet, so dass der SIP-Server für den Angreifer unentdeckt bleibt und nicht angegriffen werden kann.

5.4 Dynamischer Honeypot

Während der Honeynet-Untersuchungen war zu beobachten, dass Angreifer die ersten drei Angriffsstufen von der gleichen Quell-IP-Adresse ausführten, die eigentlichen Toll Fraud-Angriffe jedoch typischerweise von einer anderen IP-Adresse ohne vorausgegangene Scans erfolgten (siehe Abbildung 22 in Kapitel 4.5). Somit ergab sich die Fragestellung, ob Angreifer die erlangten Anmeldedaten einer Nebenstelle der Honeypots weitergeben bzw. untereinander austauschen. Auf Grund der wechselnden Quell-IP-Adressen war es notwendig, die Angreifer über andere Parameter zu identifizieren. Dazu wurde das bisherige Honeynet um eine dynamische Honeypot-Komponente erweitert. Dabei wurde die Tatsache genutzt, dass vor einem Toll Fraud-Anruf eine Registrierung an einer Nebenstelle mit gültigen Zugangsdaten erfolgen muss, die durch einen vorausgegangenen Angriff erlangt wurden. Der Angreifer wird somit unabhängig von der IP-Adresse über die verwendeten SIP-Zugangsdaten (Benutzername / Kennwort) identifiziert.

Für den dynamischen Honeypot (siehe Kapitel 5.4.1) wird eine signaturbasierte Angriffserkennung verwendet. Sobald ein Brute-Force-Angriff auf eine aktive Nebenstelle des Honeypots erkannt wird, wird eine in der Signatur definierte Aktion ausgelöst. Dadurch wird eine Benachrichtigung an den attackierten Honeypot versendet (siehe Kapitel 5.4.2). Dieser verändert auf Grund der empfangenen Benachrichtigung die Konfiguration der angegebenen Nebenstelle, so dass der Angreifer mit Hilfe der „Enable Extension“-Funktion (siehe Kapitel 5.4.3) über die SIP-Zugangsdaten und unabhängig von der Quell-IP-Adresse identifiziert werden kann.

5.4.1 Komponenten und Netzwerkarchitektur

Das dynamische Honeypot-System (siehe auch Kapitel 4.5) besteht aus zwei Modulen: Der Sensor-Komponente (siehe Kapitel 5.3.2) für die aktive, signaturbasierte Angriffsüberwachung und einem oder mehreren Dioanea-basierten Low Interaction

Honeypots (siehe Kapitel 5.1). Die Sensor-Komponente wird über einen Mirror-Port an den Hauptrouter angebunden, so dass der gesamte eingehende und ausgehende Angriffsverkehr überwacht werden kann. Abbildung 48 zeigt, dass zwischen Sensor und Honeypot eine von dem Angriffsverkehr unabhängige, sichere Verbindung zur Steuerung der Rekonfiguration des Honeypots existiert.

5.4.2 Schnittstelle zwischen Honeypot und Sensor

Zusätzlich zu der Netzwerkschnittstelle für die Internetanbindung ist für die virtuelle Maschine des dynamischen Honeypots eine weitere Netzwerkschnittstelle zu einem Steuerungsnetzwerk eingerichtet. Dabei handelt es sich um ein virtuelles, lokales Netzwerk, das nicht aus dem Internet erreichbar ist und nur den durch Firewall-Regeln gesicherten Austausch von Steuerungsbenachrichtigungen zwischen dem Sensor und den Honeypots erlaubt. Durch den Einsatz der Virtualisierungslösung VMware ESXi können getrennte virtuelle Netzwerke für sicherheitskritische Funktionen realisiert und ohne höheren Hardwareaufwand an die Komponenten angeschlossen werden.

Für das virtuelle Honeypot wurde die Sensorinstanz mit einer Signatur für die Erkennung eines Registration Hijacking-Angriffs konfiguriert. Diese wurde aus den Ergebnissen der forensischen Analyse abgeleitet. Die Signatur trifft zu, wenn 100 SIP-Pakete der Methode REGISTER an die gleiche Quell- und-Ziel-IP-Adresse sowie an die gleiche Zielnebenstelle (To-Header-Feld) gesendet wurden. Das Zeitintervall für diese Regel wurde auf 60 Sekunden begrenzt, da die SIP-Nachrichten bei Brute-Force-Angriffen üblicherweise in wenigen Sekunden eintreffen und das System nicht benötigte Erkennungszustände zum Einsparen von Ressourcen verwerfen kann. Durch die Flexibilität der signaturbasierten Erkennung kann die Identifizierung der Angreifer jederzeit an neue Verhaltensmuster angepasst werden.

Sobald ein Registration Hijacking-Angriff erkannt wird, wird die in der Signatur definierte Aktion „honeypotreport“ ausgeführt und eine Benachrichtigung über die „Sensor-Honeypot-Schnittstelle“ an das angegriffene Honeypot gesendet. Abbildung 49 zeigt, dass die IP-Adresse des Angreifers sowie die Kennung der angegriffenen Nebenstelle übertragen werden. Bei den Steuerungsnachrichten zwischen Sensor und Honeypot handelt es sich um SIP-Pakete der Methode NOTIFY, die im Messagebody eine definierte XML-Struktur aufweisen und über die getrennte und gesicherte Netzwerkverbindung gesendet werden.

In der Beispielnachricht hat die Sensor-Komponente im Steuerungsnetzwerk die IP-Adresse 192.168.99.94 und das dynamische Honeypot ist unter der IP-Adresse 192.168.99.105 erreichbar. Die Zuordnung der öffentlichen Honeypot-Adressen und der internen IP-Adressen im Steuerungsnetzwerk erfolgt in der Sensor-Konfigurationsdatei. In dem Beispiel

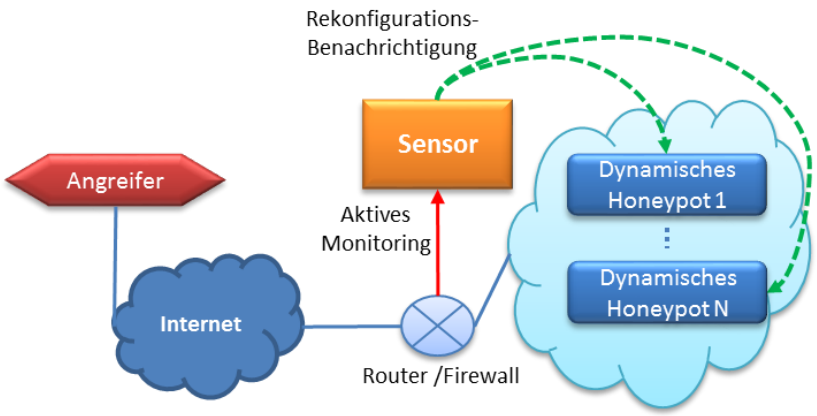


Abbildung 48: Netzwerkaufbau dynamisches Honeynet

```
NOTIFY sip:honeypotreport@192.168.99.105 SIP/2.0
To: <sip:honypotreport@192.168.99.105>
From: <sip:sensor@192.168.99.94>
Call-ID: 3027823560
CSeq: 282 NOTIFY
Content-Type: text/plain

<?xml version="1.0"?>
<dialog-info proto=SIP>
<state>method="auth"</state>
<param host="132.252.151.99" username="598"></param>
</dialog-info>
```

Abbildung 49: Beispiel für eine Steuerungsnachricht des dynamischen Honeypots

wurde ein Registration Hijacking-Angriff („method=auth“) von der Angreifer-IP-Adresse 132.252.151.99 auf die Nebenstelle 598 des Honeypots mit der internen IP-Adresse 192.168.99.105 erkannt.

Das Dioanea-Honeypot wurde um ein Skript erweitert, das die Sensorbenachrichtigungen über einen UDP-Socket empfängt und die Daten auf Gültigkeit überprüft. Die IP-Adresse des Sensors ist aus Sicherheitsgründen in dem Empfangsskript fest konfiguriert, so dass ausschließlich von einer bestimmten Sensorinstanz Befehle zur Rekonfiguration akzeptiert werden. Sobald eine gültige Benachrichtigung empfangen wird, erfolgt die Anpassung der Honeypot-Konfiguration für die in der Nachricht angegebene Nebenstelle, indem die SIP-Zugangsdaten der nächsten vom Angreifer gesendeten REGISTER-Nachricht akzeptiert werden. Die Anpassung erfolgt jedoch nur über die Enable Extension-Funktion (siehe Kapitel 5.4.3), wenn die Nebenstelle nicht bereits für einen anderen Angreifer verwendet wird. Dazu werden die aktuelle Konfiguration sowie alle durchgeführten Änderungen und die notwendigen SIP-Anmeldeinformationen in einer lokalen Datenbank gespeichert.

5.4.3 Dynamische Konfiguration: Enable Extension-Funktion

Die Enable Extension-Funktion (EEF) basiert auf den Ergebnissen von vorausgegangenen forensischen Analysen, die gezeigt haben, dass für einen Toll Fraud-Anruf eine vorausgegangene, erfolgreiche Registrierung an einer Nebenstelle notwendig ist. Daher werden bei der signaturbasierten Erkennung ausschließlich Registration Hjiacking-Angriffe berücksichtigt. Nach einem definierten Schwellenwert wird die angegriffene Nebenstelle für den aktuellen Angreifer aktiviert. Nachfolgend wird der Ablauf der EEF anhand von Abbildung 50 erläutert:

1. Die SIP-Authentifizierung basiert auf der HTTP-Digest-Authentifizierung[19]. Wenn ein Angreifer versucht, eine Nebenstelle mit einer Registration Hijacking-Attacke zu knacken, wird mit Hilfe des eingesetzten User Agents ein „response hash“ über die folgenden Parameter berechnet:
    - Nonce value
    - Username
    - SIP method
    - SIP URI
    - Geheime Zeichenfolge (Kennwort der Nebenstelle)

[19] HTTP Digest Authentication, RFC 4169, http://tools.ietf.org/html/rfc4169

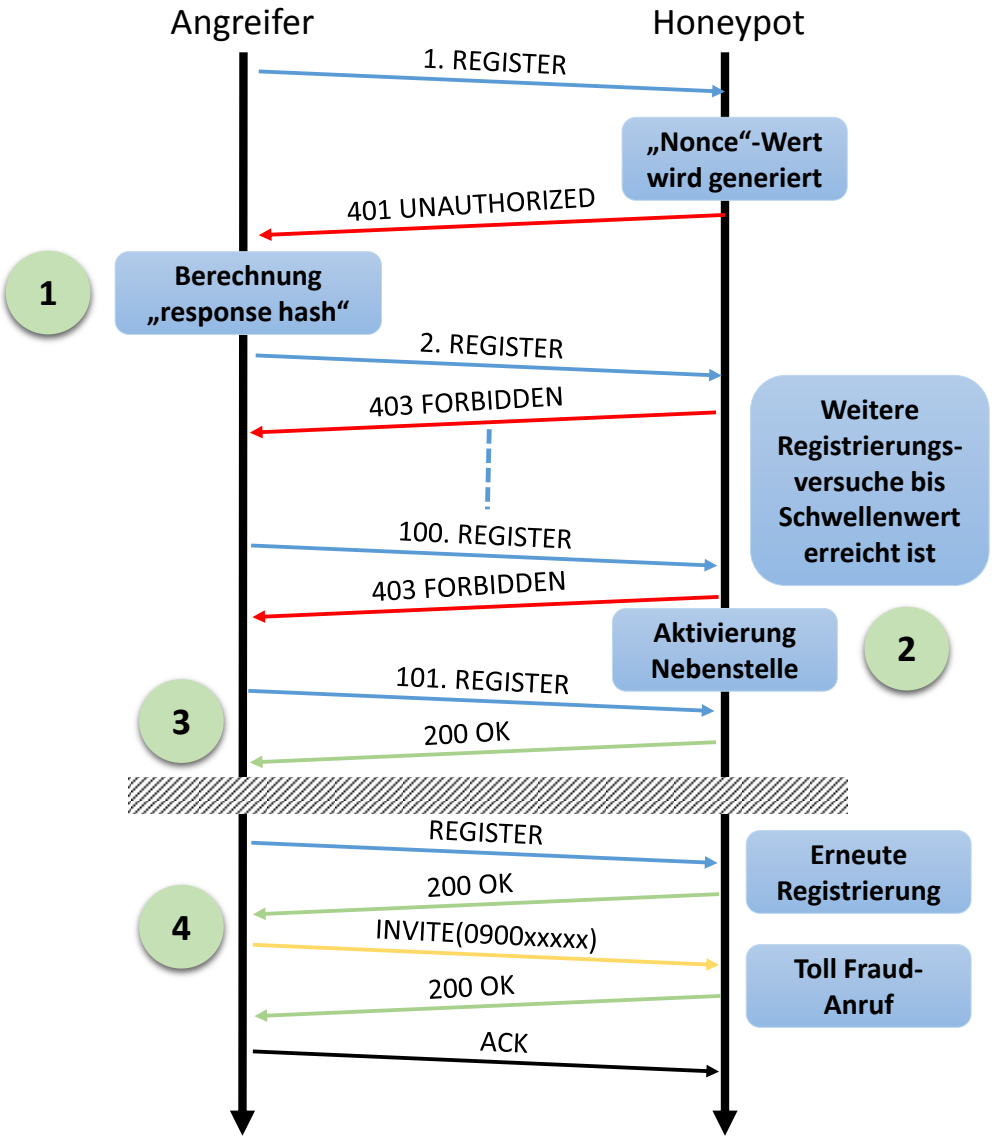


Abbildung 50: Funktionsweise Enable Extension-Funktion (EEF)

Bei der „nonce value“ handelt es sich um einen zufälligen base64-Wert, der durch den Honeypot generiert wird.

2. Wird ein Registration Hijacking-Angriff (identifiziert über die identische Quell/Ziel-IP-Adresse, Ziel-Nebenstelle und den Benutzernamen) mit einer größeren Anzahl von Paketen als der definierte Schwellenwert erkannt (z.B. 100 SIP-Pakete), erfolgt die Aktivierung der Nebenstelle für den aktuellen Angreifer, indem das Kennwort aus der nächsten REGISTER-Nachricht akzeptiert und die Anmeldeinformationen für diese Nebenstelle gespeichert werden. Alle Zugangsdaten und die aktiven Nebenstellen werden in einer lokalen Datenbank gespeichert. Der genannte Schwellenwert kann angepasst werden, so dass das Verhalten der Honeypots für Angreifer schwerer nachvollziehbar ist. Der generierte „nonce value“ wird für jede Registrierung an dieser Nebenstelle verwendet.
3. Nach einer erfolgreichen Aktivierung einer Nebenstelle sendet der Honeypot eine „200 OK“-Nachricht an den Angreifer, vorausgesetzt, der „response hash“ des Angreifers entspricht den in der Honeypot-Datenbank gespeicherten Informationen. Pro Nebenstelle können nicht mehrere SIP-Zugangsdaten hinterlegt

werden, so dass eine 1:1-Zuordnung von Angreifer und Nebenstelle gewährleistet bleibt.

4. Mit einer erfolgreichen Registrierung an einer aktivierten Nebenstelle ist es jetzt über eine INVITE-Nachricht möglich, einen Toll Fraud-Anruf aufzubauen.

Sobald eine Nebenstelle durch einen Angreifer aktiviert wurde, ist die Registrierung nur innerhalb von 10 Versuchen möglich. Weitere Versuche werden durch das System mit einer Fehlermeldung abgewiesen, da das Ausprobieren von Anmeldeinformationen auf Grund der eindeutigen Identifizierung nicht möglich sein darf. Ein Angreifer, der die gültigen Anmeldedaten durch einen vorherigen Angriff herausgefunden hat, sollte die Registrierung typischerweise mit nur einer REGISTER-Nachricht durchführen können.

Da pro Nebenstelle und Angreifer eine 1:1-Zuordnung stattfindet und das Ausprobieren von Anmeldeinformationen an bereits aktivierten Nebenstellen unterbunden wird, ist eine Identifizierung der Angreifer unabhängig von der verwendeten Quell-IP-Adresse über die SIP-Zugangsdaten möglich.

5.5 Übersicht über die Komponenten und deren Einsatzmöglichkeiten / Features

Dieses Unterkapitel gibt anhand von Tabelle 8 einen zusammenfassenden Überblick über die Funktionen der entwickelten Softwarekomponenten und berücksichtigt dabei die möglichen Einsatzzwecke und Szenarien.

Die beiden Single Honeynet-Systeme auf Basis von Asterisk und Dioanea sowie der dynamische Honeypot werden lokal an einem Standort eingesetzt und sammeln die Angriffsdaten in einer lokalen Datenbank auf dem Host. Während die genannten Systeme über eine einzelne IP-Adresse an das Internet angebunden sind, können mit Hilfe des STRs ein oder mehrere Subnetze überwacht werden. Die Aufzeichnung der Verkehrsdaten erfolgt in einer zentralen Datenbank für alle überwachten Netzwerke, so dass eine spätere Auswertung stark vereinfacht wird. Das Security Sensor System (SSS) kann sehr flexibel und verteilt in allen Netzwerkgrößen (auch im Internet) eingesetzt werden. Die Analyse der Angriffsdaten erfolgt vollautomatisch in Echtzeit auf Basis von Signaturen im Vergleich zu der notwendigen Offline-Analyse der anderen Systeme.

Während die Honeypot-Systeme die Verkehrsdaten und Angriffe auf Nebenstellen nur in einer Log-Datei aufzeichnen, erfolgt durch den STR eine Vorverarbeitung (Parsen der SIP-Pakete und Speicherung in einer SQL-Datenbank) und eine automatische Aufbereitung der gesammelten Daten für definierte Fragestellungen (z.B. Angriffe pro Tag, Herkunft der Angreifer). Die automatische Angriffserkennung des SSS stellt einen weiteren Entwicklungsschritt dar, so dass dieses System als IDS zur Erkennung von SIP-basierten Angriffen eingesetzt werden kann. Durch die implementierten Schnittstellen können Gegenwehrkomponenten direkt an den Sensor Central Service angebunden werden, so dass Angriffe unterbunden oder abgeschwächt werden.

Das STR-Honeynet und die Honeypot-Systeme sind statisch konfiguriert, der dynamische Honeypot erlaubt jedoch eine Reaktion auf das Verhalten der Angreifer, indem während eines Angriffs Nebenstellen für einen Angreifer aktiviert werden. Auch das SSS kann im laufenden Betrieb durch das Laden weiterer Signaturen an das neue Angreiferverhalten angepasst werden.

Alle Systeme können grundsätzlich in einer ausreichend dimensionierten Server-VM eingesetzt werden. In Skriptsprachen programmierte Systeme bzw. der STR mit einer leistungsfähigen SQL-Datenbank benötigen ausreichend Hardware-Ressourcen. Somit

Tabelle 8: Übersicht über die Features der entwickelten Komponenten

Features / Systeme		Honeypot Asterisk	Honeypot Dioanea	STR	Security Sensor System	Dynamisches Honeypot
Typ	Host	✔	✔	✔	✔	✔
	LAN	✘	✘	✔	✔	✘
	Internet	✘	✘	✘	✔	✘
Analyse	Echtzeit	✘	✘	✘	✔	✘
	Offline / zentral	✘	✘	✔	✘	✘
	Offline / lokal	✔	✔	✘	✘	✔
Einsatzgebiet	Forensik / Rohdaten	✔	✔	✔	✘	✔
	Forensik / Analyse	✘	✘	✔	✔	✘
	IDS	✘	✘	✘	✔	✘
	Abwehr	✘	✘	✘	✔	✘
Art	dynamisch	✘	✘	✘	✔	✔
	statisch	✔	✔	✔	✘	✘
Hardware	Server (VM)	✔	✔	✔	✔	✔
	Intel NUC	✔	✔	✘	✔	✔
	Raspberry Pi	✔	✘	✘	✔ *	✘
	FritzBox	✘	✘	✘	✔ *	✘
Szenario	Heimanwender	✔	✔	✘	✔	✘
	Small-Business	✔	✔	✔	✔	✔
	Enterprise	✘	✘	✘	✔	✘
	Forschung	✔	✔	✔	✔	✔

***** eingeschränkte Funktionalität

kann nur der Sensor auf kleinen Hardware-Komponenten wie z.B. dem Raspberry Pi oder der FritzBox installiert werden. Jedoch zeigt die Performance-Analyse in Kapitel 5.3.6, dass die Ressourcen für komplexere Signaturen nicht ausreichend sind. Ein einzelner Honeypot auf Asterisk-Basis ist im Vergleich zum Dioanea-Honeypot noch auf dem Raspberry Pi lauffähig.

Auf Grund von notwendigen Hardware- und Netzwerkvoraussetzungen können der dynamische Honeypot und das STR-Honeynet nicht in Heimanwenderszenarien eingesetzt werden. Aus datenschutzrechtlichen Gründen und der Notwendigkeit von hochverfügbaren Netzwerken können der STR und die Honeypots nur mit sehr großen Hürden in Enterprise-Szenarien integriert werden. Für alle aufgeführten Szenarien kann jedoch das Security Sensor System eingesetzt werden, da dieses optimal an die vorhandenen Netzwerkkomponenten anpassbar ist und darüber hinaus keine personenbezogenen Daten abspeichert.

6 Ergebnisse

In diesem Kapitel wird mit einem Feldversuch gezeigt, dass die entwickelten Konzepte und Werkzeuge für die Analyse und Erkennung von SIP-spezifischen Angriffen geeignet sind.

Zu Beginn werden die Datenquellen der durchgeführten Analysen erläutert. In dem Unterkapitel 6.2 werden die Ergebnisse der forensischen Analysen vorgestellt. Diese basieren auf den STR-Messdaten, die seit Dezember 2010 erhoben wurden. Anschließend werden zur Bestätigung der getätigten Aussagen und der gezeigten Effekte die aufgezeichneten Daten von drei verschiedenen Messstandorten verglichen (siehe Kapitel 6.3). Dadurch wird sichergestellt, dass es sich nicht um lokale Effekte im TdR-Honeynet handelt.

In dem Unterkapitel 6.3.4 werden die Ergebnisse des Feldversuches mit dem Security Sensor System vorgestellt und es wird das Angreiferverhalten an unterschiedlichen Standorten gezeigt. Zur Beurteilung der Funktionsfähigkeit der Angriffserkennung werden die Ergebnisse mit den STR-Aufzeichnungen verglichen (False Positives / False Negatives). Die Datenbasis bilden die auf dem SCS eingegangenen Sensor-Reports. Das Kapitel schließt mit einem Fazit und Empfehlungen für die Weiterentwicklung von Werkzeugen für die Angriffserkennung und -abwehr (siehe Kapitel 6.5).

6.1 Überblick über die Datenquellen

Die Tabelle 9 gibt einen Überblick über die verwendeten Datenquellen für die nachfolgenden Analysen. Pro Datenquelle wird angegeben, wie lange diese zur Verfügung stand, welches System zum Einsatz kam und wie viele Honeypot-Systeme betrieben wurden. Die Aufzeichnungen mit dem SIP Trace Recorder begannen am TdR-Lehrstuhl im Dezember 2010 und werden aktuell noch fortgeführt. Für die forensischen Analysen (Kapitel 6.2) und für den Vergleich der Messdaten von anderen Standorten (Kapitel 6.3) wurde der Datenbestand bis einschließlich Oktober 2014 berücksichtigt.

Die ersten beiden Sensoren des Security Sensor Systems wurden nach der Fertigstellung des Prototypen im Januar 2013 am Lehrstuhl und in Berlin für die Überprüfung der Funktionsweise eingesetzt. Nach der Optimierung der ersten Referenzimplementierung und Festlegung der Signaturen wurden weitere Standorte im September und Oktober 2013 in Betrieb genommen. Von September 2013 bis März 2014 erfolgte ein Feldversuch an verschiedenen Standorten. In dem Versuchszeitraum wurden weder die Signaturen noch

Tabelle 9: Überblick über die Datenquellen

Name der Datenquelle	Zeitraum der STR-Messungen	Zeitraum der Sensor-Messungen	Anzahl der SIP-Honeypots
TdR-Lehrstuhl (Honeynet und Referenz-Netz)	12/2010 - 10/2014	01/2013 - 10/2014	5
Berlin	01/2012 - 01/2013 (A)	01/2013 - 10/2014	IP-Telefonanlage
München	-	09/2013 - 10/2014	IP-Telefonanlagen
Wien	01/2013 - 10/2014 (I)	-	8
NorNet Testbed	10/2013 - 10/2014	10/2013 - 10/2014	30
Deutsches Forschungsnetz (DFN)	02/2014 - 10/2014	02/2014 - 10/2014	1
Rechenzentrum Uni Duisburg-Essen	02/2012 - 06/2012 (A)	-	IP-Telefonanlage

(A) = anonymisierte STR-Messdaten
(I) = importierte SIP-Verkehrsdaten

die Sensorimplementierung verändert, so dass die Vergleichbarkeit sichergestellt ist. Die Auswertung des Feldversuchs der verteilten Angriffserkennung in Kapitel 6.3.4 basiert auf den Messdaten des Security Sensor Systems sowie auf den gesammelten Verkehrsdaten des STRs, um die Erkennungsleistung der Sensoren überprüfen zu können.

Bei Kooperationspartnern bestand zu unterschiedlichen Zeitpunkten die Möglichkeit, den STR bzw. die Sensoren zu installieren und über einen bestimmten Zeitraum zu betreiben. So konnte der STR für ein Jahr in Berlin in einer produktiven VoIP-Umgebung und für fünf Monate im Rechenzentrum der Universität Duisburg-Essen getestet werden, jedoch mit aktivierter Anonymisierungsfunktion, so dass der Umfang der Analysen eingeschränkt war.

Durch die Einrichtung des Sensors in den Forschungsnetzen DFN [62] und NorNet [8] wurde es möglich, über 30 Messstandorte in verschiedenen Ländern (z.B. Norwegen und China) in Betrieb zu nehmen. Für die Kontrolle der Sensorfunktionalität wurde parallel das STR-Aufzeichnungsmodul installiert. An den Standorten München und Berlin wurde der Sensor in VoIP-Umgebungen von Kooperationspartnern installiert, die reale VoIP-Telefonanlagen beinhalten. Aus Datenschutzgründen war die zusätzliche Integration des STRs nicht möglich bzw. erfolgte nur temporär mit aktivierter Anonymisierungsfunktion.

Von einem Kooperationspartner in Wien wurden die dort gesammelten SIP-Verkehrsdaten für einen Zeitraum von 1,5 Jahren für eine vergleichende Auswertung zur Verfügung gestellt, so dass die für diese Dissertation am TdR-Lehrstuhl erhobenen Messdaten mit denen aus Wien korreliert werden konnten. Die bereitgestellten Daten wurden in den STR importiert und mit dem identischen Verfahren analysiert.

6.2 Forensische Analysen

Die nachfolgenden forensischen Analysen zu SIP-spezifischen Angriffen basieren auf den gesammelten SIP-Verkehrsdaten des Honeynets am TdR-Lehrstuhl bis einschließlich Oktober 2014.

6.2.1 Überblick und chronologische Auswertung

Zum Verständnis der SIP-basierten Angriffe und zur Entwicklung geeigneter Erkennungs- und Gegenmaßnahmen wird der SIP-Verkehr in den Honeynets seit Dezember 2009 (STR-Aufzeichnung ab Dezember 2010) aufgezeichnet und ausgewertet. Da sich in diesen Netzwerken keine produktiven SIP-Komponenten befinden, kann jede eingehende SIP-Nachricht als verdächtig eingestuft werden. Bis Dezember 2010 erfolgte das Monitoring nur auf einzelnen Honeypots. Dadurch ergab sich eine sehr begrenzte Sicht auf nur wenige Hosts, so dass keine verlässliche Aussage zu den übrigen IP-Adressen getroffen werden konnte.

Im Dezember 2010 wurde das SIP-Honeynet komplett umkonfiguriert und durch die Installation des STRs (Kapitel 5.2) wurde die komplette Überwachung von zwei unterschiedlichen Class-C-Netzwerken realisiert. Abbildung 51 zeigt den Unterschied zwischen der lokalen (Monitoring auf wenigen Hosts) und der globalen Sicht (STR-Einsatz). Es wird deutlich, dass die überwachten Netzwerkbereiche bis zum Ende des Messzeitraumes unter kontinuierlich steigenden Angriffen standen und dass der globale Überwachungsansatz als sinnvoll erachtet werden muss, da nur so großflächige Angriffsversuche sichtbar werden. Über den Messzeitraum zeigt sich eine steigende Tendenz der Angriffe mit einem leichten Einbruch Ende 2013. Dieser Rückgang ist auf einen Routing-Ausfall im Universitätsnetzwerk für das zweite Class-C-Netzwerk zurückzuführen. Dieser Umstand wird auch in Abbildung 52 deutlich.

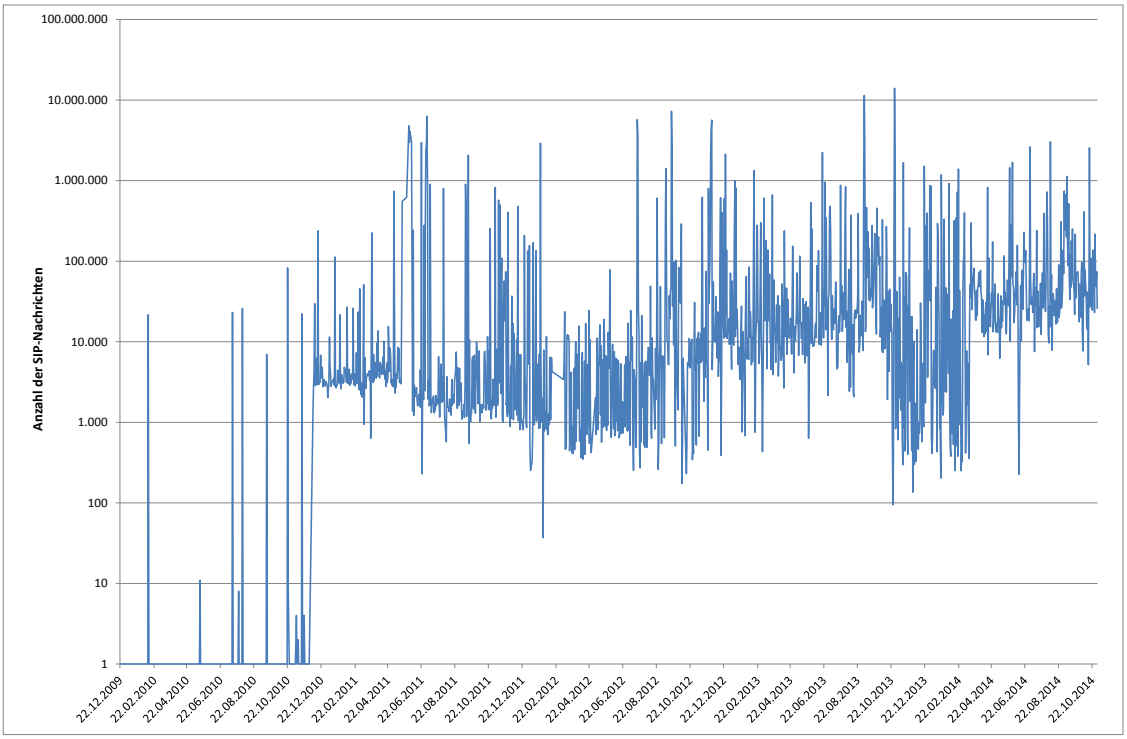


Abbildung 51: SIP-Nachrichten pro Tag seit Dezember 2009

Abbildung 52 zeigt, dass sich das Angriffsverhalten zwischen den beiden Netzwerken unterscheidet. Fast der gesamte SIP-Verkehr in Netzwerk B (keine SIP-Komponenten) ist auf OPTIONS-Pakete zurückzuführen, die dazu dienen, aktive SIP-Geräte zu erkennen. Dies macht deutlich, dass die kontinuierlichen, wiederkehrenden und intensiven Scan-Versuche auch unabhängig von einer Härtung des SIP-Stacks auftreten würden. In Netzwerk A (mit SIP-Honeypots) ist der Anteil der OPTIONS-Pakete vergleichsweise niedrig. Angreifer attackieren die SIP-Komponenten direkt, ohne vorausgegangene OPTIONS-Pakete. Dies wird besonders deutlich, wenn an die Honeypots direkt eine REGISTER-Nachricht ohne vorherige OPTIONS-Nachricht gesendet wird.

Darüber hinaus wird das Netzwerk A nur selten mit OPTIONS-Nachrichten attackiert. In diesem Fall muss davon ausgegangen werden, dass die aktiven SIP-Komponenten dem Angreifer bereits durch vorherige Scans bekannt sind, ein OPTIONS-Scan des Netzwerkes nach dem Auffinden des ersten Honeypots abgebrochen wird oder die IP-Adressen der bekannten SIP-Server unter den Angreifern ausgetauscht werden und somit eine Kooperation stattfindet. Weitere Server Scans wären in diesen Fällen nicht notwendig.

Um diese Überlegung zu überprüfen, wurde am 17. Mai 2011 ein neuer Honeypot in Betrieb genommen. Nur wenige Stunden nach Inbetriebnahme wurde dieser Honeypot durch einen Server Scan aufgefunden und in den folgenden Tagen von unterschiedlichen Quell-IP-Adressen massiv attackiert (über vier Millionen Nachrichten pro Tag). Nach sieben Tagen wurde im Vergleich zu den übrigen Honeypots eine normale Angriffsintensität erreicht. Im Netzwerk eines Kooperationspartners konnte dieses Verhalten reproduziert werden. Die auffälligen Peaks in der grünen Kurve zeigen weiterführende Angriffsstufen. Mit einer enorm großen Anzahl von Paketen versuchen die Angreifer, eine Nebenstelle zu übernehmen (bis zu 13 Millionen Pakete pro Nebenstelle), indem Passwörter geraten werden. Dieser enorme Aufwand wird deutlich, wenn berücksichtigt wird, dass seit Dezember 2010 in Netzwerk A über 185 Millionen Angriffspakete aufgezeichnet wurden. Die Scan-Versuche in Netzwerk B fallen im direkten Vergleich erwartungsgemäß mit über 12 Millionen SIP-Paketen vom Umfang her deutlich geringer aus.

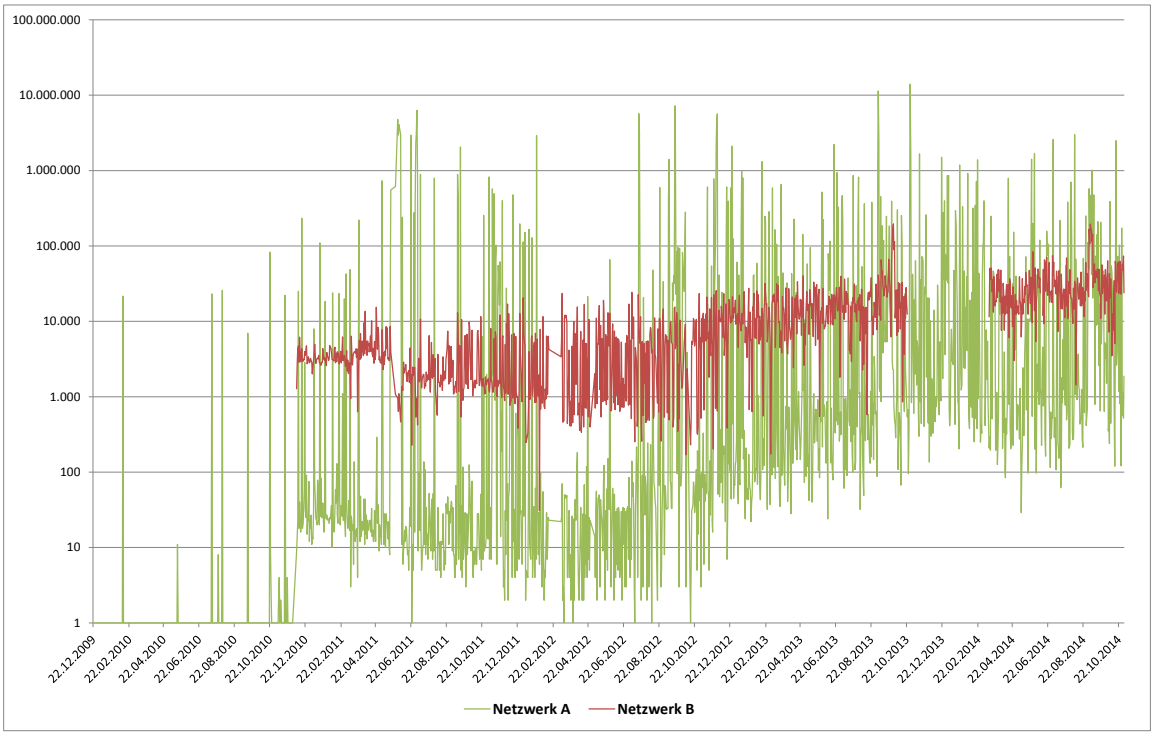


Abbildung 52: Nachrichten pro Tag je Netzwerk

Tabelle 10 zeigt den prozentualen Anteil von drei SIP-Methoden, die in beiden Netzwerken für einen Angriff verwendet wurden. Die Werte unterstützen das zuvor beschriebene Verhalten, da über 92% der Angreifer in Netzwerk A gezielt REGISTER-Pakete für einen Angriff verwendeten. Der geringe Anteil (1,8%) an OPTIONS-Paketen wird sofort deutlich. Nach der erfolgreichen Übernahme einer Nebenstelle ist der Angreifer in der Lage, Toll Fraud-Angriffe auszuführen. Dies zeigt das Vorkommen der SIP-Methoden INVITE, BYE, CANCEL, ACK. Da für den Aufbau einer SIP-Sitzung nur wenige Pakete benötigt werden und die korrekten Zugangsdaten durch vorausgegangene Angriffe mit REGISTER-Paketen bekannt sind, werden vergleichsweise wenige Pakete benötigt. In Netzwerk B liegt der Server Scan-Anteil bei fast 100%, wenn berücksichtigt wird, dass Angreifer die Server Scans mit OPTIONS- und INVITE-Paketen ausführen.

6.2.2 Analyse des grundsätzlichen Angreiferverhaltens

Nachfolgend werden die gesammelten Messdaten in Hinblick auf die vier bekannten Angriffsstufen analysiert.

6.2.2.1 Server Scan

Die Honeynet-Analysen zeigen, dass die Angreifer verschiedene Scan-Verhalten anwenden. Zu Beginn wurden ausschließlich recht einfache Scans, die Charakteristika von „for“-Schleifen aufwiesen, verwendet. Dadurch wurde ein Subnetz aufsteigend getestet, indem ein OPTIONS-Paket pro IP-Adresse versendet wurde. Nach einigen Monaten wurde das Scan-Verhalten optimiert, da die IP-Adressen im Honeynet-Subnetz nicht mehr sequenziell,

Tabelle 10: Anteil der SIP-Methoden pro Netzwerk

SIP-Methode	Netzwerk A	Netzwerk B
REGISTER	92,0339%	0,1430%
OPTIONS	1,8124%	98,8546%
INVITE,ACK,BYE,CANCEL	6,1537%	1,0024%

sondern durch eine Zufallsauswahl getestet wurden. In der Laborumgebung wurde im Rahmen dieser Dissertation das White-Hacking Tool SIPvicious [31] überprüft und das Angreiferverhalten konnte exakt nachgestellt werden. Auch der Eintrag im SIP-Header User Agent stimmte überein. Neben SIPvicious wurden weitere Tools identifiziert, die fast ausschließlich Server Scans durchführen und nicht für weitere Angriffsstufen verwendet werden, wie z.B. „sipsscuser“ (User Agent: sundayddr) [39]. Dieses Tool hat über Jahre hinweg den meisten Server Scan-Verkehr verursacht. Betrachtet man die Paketstruktur und das Verhalten, so erhärtet sich der Verdacht, dass es sich um eine modifizierte Version von SIPvicious handelt [63].

Ein weiteres Scan-Verhalten konnte bis zum Ende des Feldversuchs nachgewiesen werden: Ein Angreifer sendet typischerweise 32 OPTIONS-Pakete an eine IP-Adresse und zeigt anschließend für eine relativ lange Zeitperiode (einige Stunden) keine Aktivität mehr, bis der Scan an einem anderen Zielhost wieder aufgenommen wird. Hier ist anzunehmen, dass der Angreifer die Angriffe verschleiern möchte, indem dieser nur wenige Pakete sendet und so durch Monitoringsysteme nicht ausgefiltert wird. Zum Anderen werden große Netzwerkbereiche überprüft, so dass bedingt durch die Zufallsauswahl der IP-Adressen eine gewisse Zeit vergeht, bis der Angreifer die Scans bei den Lehrstuhl-Honeypots fortsetzt. Bei den Analysen wurde deutlich, dass viele Quell-IP-Adressen wiederholt auftraten, zum Teil mit erheblichem zeitlichen Abstand.

Abbildung 53 zeigt für den Messzeitraum, wie viele Angreifer (Quell-IP-Adressen) welche Anzahl an OPTIONS-Nachrichten an die Honeypots sendeten. Die x-Achse zeigt die Anzahl der OPTIONS-Pakete pro Quell-IP-Adresse und die y-Achse zeigt die Anzahl der Quell-IP-Adressen, die die gleiche Anzahl an Paketen gesendet haben. Aus Darstellungsgründen ist der Wertebereich der x-Achse auf 100.000 SIP-Pakete begrenzt (Maximalwert: ca. 1,5 Millionen)

Auffällig ist der Peak bei 32. Eine detaillierte Analyse zeigt, dass die 32 Pakete (sowie Vielfache von 32 Paketen) direkt an eine einzelne Honeypot-IP-Adresse gesendet wurden. Die relativ hohen Werte um 32 treten durch Wiederholungen in der Paketübertragung auf, falls kein Antwortpaket empfangen wurde. Dieses Scan-Verhalten kann in der Implementierung der Toolsuite SIPvicious nachgewiesen werden. Im rechten Bereich des Diagramms (größer 100 SIP-Pakete) ist das vielfach verwendete „normale“ Scan-Verhalten

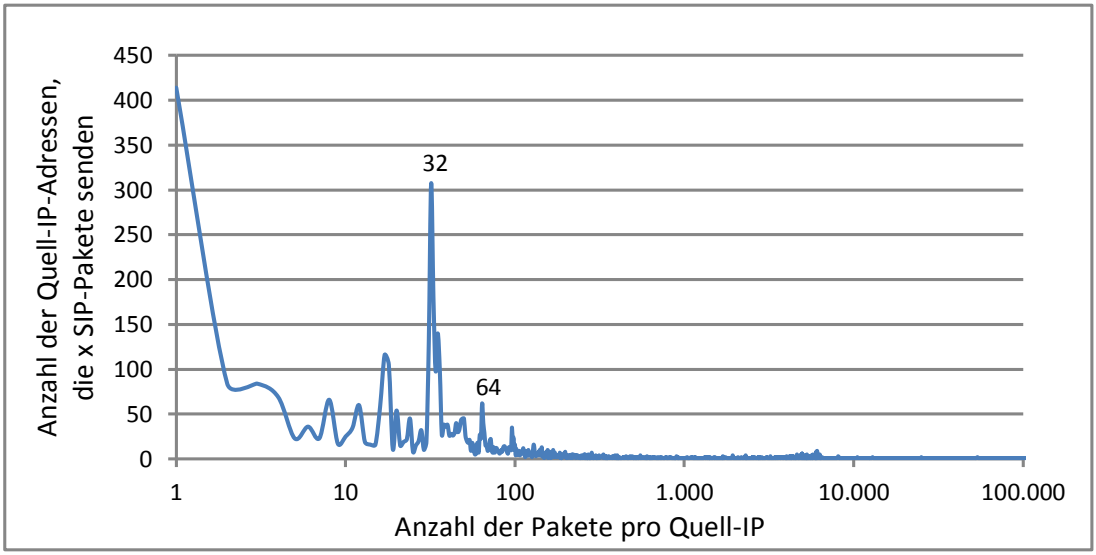


Abbildung 53: Häufigkeit verschiedener Server Scans

sichtbar. In diesem Fall senden die Angreifer bis zu 1,5 Millionen Pakete zu unterschiedlichen Ziel-IP-Adressen um SIP-Server in dem Honeynet auffinden zu können.

Ca. 10% der Angreifer sendet nur 10 oder wenige SIP-Pakete. Dies ist auf Softphones zurückzuführen, die vor einer Registrierung ein OPTIONS-Paket senden, um die Funktionalität des Servers abzufragen. Darüber hinaus testen Angreifer vor einem Toll Fraud-Anruf, ob die zuvor ermittelten Honeypots noch existieren.

Diese Auswertung zeigt deutlich die Vorteile des STR-Monitorings, da nur so große Subnetzbereiche überwacht und analysiert werden können und verschiedene Angriffsmuster bei einzelnen Hosts sonst nicht erkannt werden könnten. Darüber hinaus ist eine weitergehende, globalere Analyse der Angriffe notwendig, um diese Fragestellungen zu beantworten. Dazu wurde in Kapitel 5.3 das verteilte Angriffserkennungssystem beschrieben, das theoretisch eine weltweite Angriffsanalyse in verschiedenen Netzwerken erlaubt.

6.2.2.2 Extension Scan

Nach dem Auffinden der SIP-Server im Honeynet beginnen die Angreifer typischerweise mit der nächsten Angriffsstufe, indem REGISTER-Pakete an einen einzelnen Honeypot gesendet werden. Für die Identifizierung von aktiven Nebenstellen konnten zwei Herangehensweisen beobachtet werden: Auf der einen Seite werden Zahlenbereiche mit einer Schleife durchlaufen (z.B. von 100 bis 9999) oder es wird ein Zufallsgenerator verwendet, der einen identischen Wertebereich verwendet. Auf der anderen Seite werden Wörterbücher für diese Angriffsstufe verwendet, die gängige Vornamen, numerische Werte oder bestimmte String-Werte (z.B. „default“) beinhalten.

Das Honeynet für die forensischen Analysen am Lehrstuhl besteht aus vier Honeypots mit den Nebenstellen 201, 302, 333 und 400. Ein weiterer Honeypot hat zusätzlich Nebenstellen aus dem Bereich 1000 bis 9999 sowie einfache Zeichenketten (z.B. „test“ oder Vornamen), so dass auch das Verhalten bei höheren Nebenstellenwerten und alphanumerischen Zeichen überprüft werden kann.

Zu Beginn der Honeynet-Analysen wurden ausschließlich Nebenstellen im Bereich von 100 bis 999 sowie einige alphanumerische Zeichenketten durch die Angreifer getestet. Im Laufe der Analysen wurde jedoch verstärkt der Bereich oberhalb von 1.000 überprüft (z.B. Nebenstelle 7415), aber nur sporadisch die Nebenstellen mit alphanumerischen Zeichenketten. Daher ist davon auszugehen, dass die Angreifer verstärkt größere TK-Anlagen mit entsprechendem Nebenstellenbereich (und üblicherweise ohne alphanumerische Nebenstellenbezeichnungen) als Opfersystem erwarten und das Angriffsverhalten entsprechend anpassen.

Da jedoch für die Angriffsstufen Extension Scan und Registration Hijacking die gleiche SIP-Methode REGISTER verwendet wird, muss dies bei den Analysen berücksichtigt werden. Dies wird mit der Clustering-Analyse möglich (siehe auch Kapitel 4.3 und 6.2.3). Werden die Ergebnisse getrennt nach Angriffsstufen betrachtet, zeigt sich, dass Nebenstellen mit einem geringeren Zahlenwert häufiger angegriffen werden als Nebenstellen mit einem höheren Zahlenwert.

Zwei verschiedene Verhaltensweisen der Angreifer konnten identifiziert werden: Entweder beginnt der Registration Hijacking-Angriff, sobald eine Nebenstelle gefunden wurde oder die weiteren Angriffsstufen erfolgen erst, wenn der Extension Scan abgeschlossen ist. Die Fragestellungen in diesem Kapitel machen auch deutlich, dass eine rein chronologische, paketbasierte Auswertung nicht ausreicht und eine detaillierte Clustering-Analyse getrennt nach den Angriffsstufen notwendig ist.

6.2.2.3 Registration Hijacking

Nachdem ein Angreifer aktive Nebenstellen identifiziert hat, versucht typischerweise der gleiche Angreifer (identische Quell-IP-Adresse) die Passwörter mit einer Brute-Force-Attacke zu knacken und auf diese Art und Weise die Nebenstelle für spätere Toll Fraud-Angriffe zu übernehmen. Die Peaks in Abbildung 52 des Netzwerkes A werden durch Registration Hijacking-Angriffe verursacht. Diese Angriffsstufe wird im Vergleich zum Server Scan und Extension Scan nicht mit möglichst wenigen SIP-Nachrichten getarnt oder verschleiert, da hier eine enorme Anzahl an Paketen verwendet wird, um das Passwort zu erraten. Werden die am häufigsten eingesetzten Angriffswerkzeuge betrachtet, so zeigt sich, dass das Tool sundayddr ausschließlich für Server Scans eingesetzt wird, jedoch bei den nachfolgenden Angriffsstufen nicht in Erscheinung tritt.

Das Werkzeug „VaxSipUserAgent“ hingegen wird nicht für Server Scans, sondern ausschließlich für die weiteren Angriffsstufen (inkl. Toll Fraud) eingesetzt und wurde erstmals im Jahr 2011 identifiziert [6] [45]. Ab September 2013 konnten Folgeversionen mit einer höheren Angriffsintensität nachgewiesen werden. Angriffe in den ersten drei Stufen erfolgen überwiegend mit SIPvicious, jedoch niemals Toll Fraud-Anrufe. Die Entwicklung der Nutzung der Angriffswerkzeuge an drei verschiedenen Messstandorten wird in Kapitel 6.3 beschrieben.

6.2.2.4 Toll Fraud

Sobald sich ein Angreifer an einer Nebenstelle erfolgreich registriert hat, sind Toll Fraud-Anrufe möglich. Das Verhalten unterscheidet sich dann nicht von einem regulären Anwender. Die missbräuchliche Nutzung ist nur anfänglich feststellbar, wenn ein Angreifer verschiedene Amtskennzahlen zum Verlassen der Nebenstellenanlage ausprobiert. Bei den vorgestellten Angriffsstufen handelt es sich um Angriffe auf einen echtzeit-kritischen Dienst mit dem Ziel, für das Opfer kostenpflichtige Telefonate zu Premium- oder Auslandsrufnummern führen zu können. Da für die Kommunikationsverbindung schon während der Signalisierung über das SIP-Protokoll dynamisch Ports für die Medienverbindung (Sprachdaten) festgelegt werden, kann davon ausgegangen werden, dass es sich bei der Quell-IP-Adresse um die Adresse des Angreifers handelt. Betrachtet man nun die gewählten Rufnummern und gleicht die Quell-IP-Adressen mit Hilfe eines Geolocation-Dienstes [57] ab, so lassen sich weitere Zusammenhänge analysieren. Um die Herkunft der Angreifer-IP-Adressen im Lehrstuhl-Honeynet klären zu können, erfolgt im STR in Verbindung mit einem Geolocation-Dienst automatisch eine Zuordnung zwischen IP-Adresse und Ursprungsland.

Abbildung 54 zeigt die 110 Länder, von denen mit Hilfe des STRs Toll Fraud-Angriffe bis Oktober 2014 detektiert wurden. Die Abbildung wurde mit „Google Geo Charts“ [64] erzeugt. Je dunkler grün die Einfärbung eines Landes ist, desto mehr Toll Fraud-Anrufe wurden von diesem Land aus initiiert. Überdurchschnittlich viele Toll Fraud-Versuche kamen aus Frankreich, Großbritannien, Deutschland, USA, Russland und Ägypten. Bei zahlreichen Anrufen, die ihren Ursprung in einem westlichen Land (Analyse mit Geolocation-Dienst) und als Zielrufnummer den Nahen Osten haben, wird vermutet, dass die Angreifer Sprachdienste für die Kommunikation auf Kosten Dritter zur Verfügung stellen. Darüber hinaus konnte beobachtet werden, dass auch Anrufe innerhalb einer Region (Naher Osten, asiatischer Raum) durchgeführt wurden, da Quell-IP-Adresse und die gewählte Zielrufnummer auf das gleiche oder das Nachbarland hinweisen.

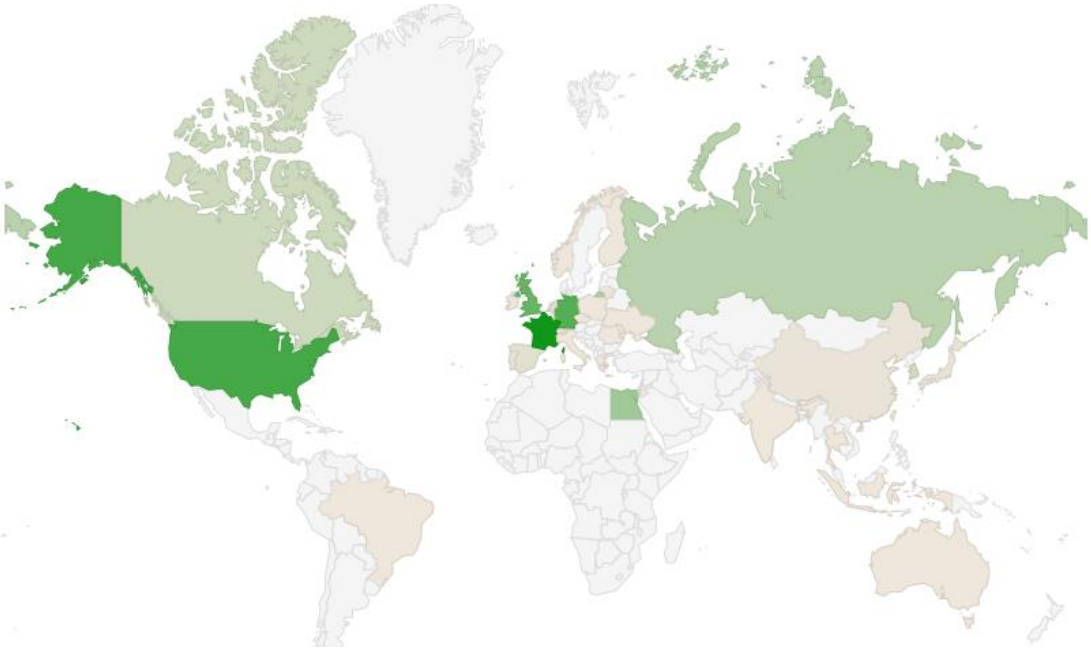


Abbildung 54: Herkunft der Toll Fraud-Angriffe [46]

Tabelle 11 zeigt die fünf am häufigsten detektierten Zielrufnummern der Toll Fraud-Angriffe. Die Angreifer versuchen, durch Variierung der Amtskennzahlen die Nebenstellenanlage zu verlassen und eine Amtsleitung für den eigentlichen Anruf zu erhalten. Die letzten fünf Zeilen in Tabelle 11 zeigen deutlich, wie die Angreifer für eine identische Zielrufnummer die Amtsvorwahlen verändern (z.B. keine Amtskennzahl, 8, 9, 0, +). Die Anrufe erfolgen überwiegend zu Rufnummern in den Ländern Großbritannien (+44), Israel (+972), Palästina (+970), USA (+1) sowie zu internationalen Premium Rufnummern (0900, +979). Während sich die Ortsvorwahlen hinter den Ländervorwahlen typischerweise nicht verändern, wird oft die Durchwahl am Ende der Rufnummer verändert. Auf Grund der auffällig hohen Anrufhäufigkeit bestimmter Rufnummern, die von unterschiedlichen Angreifern angerufen werden, muss davon ausgegangen werden, dass es sich hier um Testrufnummern zur Bestimmung des Angriffserfolges handelt. Aus rechtlichen Gründen war die Vermittlung der Anrufe über das deutsche Festnetz nicht

Tabelle 11: Toll Fraud-Zielrufnummern

Rufnummer	Anzahl der Anrufe
00442034113985	24.144
9**0044**2034113985	24.141
00972597524662	5.342
0**00972**597524662	5.342
000**0044**1604901033	3.213
…	…
00972597459073	722
8**00972**597459073	721
+**972**597459073	721
9**00972**597459073	719
0**00972**597459073	712

möglich. Die Annahme der Existenz der genannten Testrufnummern konnte jedoch mit Hilfe eines Kooperationspartners bestätigt werden. Mitschnitte der Anrufe zu diesen Rufnummern haben gezeigt, dass dort Sprachinformationen mit dem Inhalt „It works“ und ähnlichen Informationen ausgetauscht wurden. Darüber hinaus gab es im Messzeitraum Anrufversuche zu über 82.000 verschiedenen Zielrufnummern von unterschiedlichen Angreifern. Die Wählversuche pro Rufnummer für die nicht in Tabelle 11 aufgeführten Rufnummern lagen zwischen einem und 3096.

6.2.3 Ergebnisse der Clustering-Analyse

Die vorausgegangenen Analysen basieren nur auf einzelnen SIP-Nachrichten. Da z.B. für die Angriffsstufen Extension Scan und Registration Hijacking die SIP-Methode REGISTER verwendet wird, ist eine umfassendere Auswertung notwendig, die nicht nur auf einzelnen SIP-Paketen basieren darf. Darüber hinaus wird für verschiedene Angriffe innerhalb einer Angriffsstufe eine unterschiedliche Anzahl an SIP-Nachrichten benutzt. So benötigt typischerweise ein Wörterbuchangriff mehr SIP-Pakete als eine numerische, iterative Brute-Force-Attacke. Bei beiden Angriffen handelt es sich jedoch um Registration Hijacking. Für die automatische Identifizierung der Angriffsstufen werden die zugehörigen Nachrichten zu einem Attack-Cluster kombiniert, indem die Quell-IP-Adresse, die Angriffsstufe sowie das Zeitverhalten berücksichtigt werden. Um die auftretenden Angriffsversuche besser verstehen zu können, wurden auf Grundlage der gesammelten Messdaten die in Tabelle 12 dargestellten vier Attack-Cluster definiert. Für jede Angriffsstufe werden die definierten Bedingungen für die Korrelierung der SIP-Pakete anhand der Parameter Ziel-IP-Adresse, SIP-Methode, Nebenstelle und Anmeldedaten gezeigt.

Da der Clustering-Ansatz das Attribut Quell-IP-Adresse berücksichtigt, würde ein Angriff zweimal gezählt werden, wenn sich die Angreifer-IP-Adresse während einer Angriffsstufe ändern sollte. Manuelle Überprüfungen haben jedoch gezeigt, dass keine Änderung der IP-Adresse während eines einzelnen Angriffs erfolgt. Die vollständige Angriffskette (Angriffsstufen eins bis vier) trat ausschließlich in Netzwerk A (Netzwerk mit SIP-Komponenten) auf. Durch die Zuordnung der SIP-Nachrichten zu den Angriffsclustern nach dem zuvor vorgestellten Schema und der Abwendung von der reinen Nachrichtenanzahl ergibt sich nun eine deutlich bessere Übersicht über die Angriffsversuche in Netzwerk A und B (Netzwerk ohne SIP-Komponeten).

Tabelle 13 zeigt die Anzahl der Angriffe pro Angriffsstufe und Monat sowie die zugehörige Anzahl der SIP-Nachrichten im Messzeitraum Februar 2011 bis Oktober 2014. Zur besseren Visualisierung der Messergebnisse wird ein Farbverlauf verwendet, der niedrige Werte in weiß und hohe Werte in rot einfärbt. Je intensiver die rötliche Einfärbung der Werte ist, desto höher ist die Anzahl der Angriffe bzw. die Anzahl der SIP-Pakete. Messwerte von vier

Tabelle 12: Übersicht über Attack-Cluster

Parameter	Server Scan	Extension Scan	Registration Hijacking	Toll Fraud
Ziel-IP-Adresse	variiert	identisch	identisch	identisch
SIP-Methode	OPTIONS	REGISTER	REGISTER	INVITE
Nebenstelle	nicht definiert	variiert	identisch	bekannt*, identisch
Anmeldedaten	nicht definiert	nicht definiert	variiert	bekannt*, identisch

** Nebenstelle und Anmeldedaten sind aus vorherigen Angriffsstufen bekannt*

Tabelle 13: Angriffe und SIP-Nachrichten nach Clustering-Ansatz

Monat	Server Scan		Extension Scan		Registration Hijacking		Toll Fraud (Call)	
	Angriffe	Pakete	Angriffe	Pakete	Angriffe	Pakete	Angriffe	Pakete
2011-02	274	96.648	9	16.379	6	45.954	1	116
2011-03	241	103.666	127	92.740	25	125	3	64
2011-05	238	79.243	10	35.280	7	9.603.316	1	1.032
2011-06	171	50.623	9	14.541	8	13.963.419	1	10
2011-07	70	71.078	6	27.482	40	10.483.106	8	684
2011-08	56	72.889	1	12.890	20	772.207	1	542
2011-09	35	93.441	10	108.247	148	3.243.164	13	10.506
2011-10	56	70.773	2	16.487	7	228.572	12	19.571
2011-11	55	85.012	42	196.356	146	2.259.409	31	9.195
2011-12	45	118.823	9	70.223	43	588.468	21	6.613
2012-01	32	102.274	36	301.494	31	3.031.381	6	358
2012-04	26	84.407	6	7.029	3	12.050	6	4.548
2012-05	38	154.031	16	30.531	5	2.066	4	7.667
2012-07	54	168.021	11	1.255.628	19	5.218.975	12	3.862
2012-08	96	140.554	14	77.280	20	431.304	12	372
2012-09	52	173.766	23	114.433	48	11.502.498	15	599
2012-10	34	147.061	17	43.933	31	303.338	6	244
2012-11	55	259.407	28	239.221	71	1.173.970	22	15.982
2012-12	67	327.065	38	280.903	77	2.838.915	26	5.880
2013-01	63	326.325	32	353.790	62	1.264.838	33	2.357
2013-02	61	340.074	29	405.220	79	1.448.105	40	9.575
2013-03	71	401.766	35	229.032	95	1.010.044	36	8.147
2013-04	76	399.748	18	96.897	30	229.133	63	9.048
2013-05	71	518.875	33	272.611	47	359.673	71	4.581
2013-06	65	476.572	36	1.146.364	72	1.217.579	77	54.508
2013-07	82	519.025	55	407.307	137	1.942.613	70	4.804
2013-08	72	473.526	12	58.609	56	672.059	64	3.506
2013-09	101	1.363.486	46	137.618	120	16.582.314	72	54.325
2013-10	88	495.908	48	175.525	69	16.336.390	51	4.217
2013-11	95	2.787	88	389.343	145	1.755.900	84	10.261
2013-12	95	2.668	100	367.111	309	2.439.267	79	19.090
2014-01	74	2.368	78	1.260.718	156	1.176.640	78	7.696
2014-02	92	2.286	67	735.618	206	2.286.968	91	9.969
2014-03	121	606.569	69	253.150	761	370.317	93	108.348
2014-04	91	590.864	38	564.770	192	336.339	82	1.767
2014-05	143	823.787	58	215.947	876	3.286.420	89	6.344
2014-06	184	935.373	32	144.609	281	266.612	88	60.594
2014-07	275	896.983	47	561.748	146	2.593.655	87	19.847
2014-08	142	752.715	39	512.415	283	3.303.769	82	7.302
2014-09	205	1.857.279	56	629.122	258	1.800.312	117	75.821
2014-10	287	1.032.430	49	734.364	261	1.994.403	123	24.470

Farbverlauf zeigt Intensität der Anzahl der Angriffe bzw. Anzahl der Pakete
(je ausgeprägter die Einfärbung, desto höher die Werte)

Monaten wurden im gesamten Messzeitraum durch Hardwareausfälle beeinträchtigt und daher aus der Ergebnistabelle entfernt. Für die Angriffsstufe Server Scan wurden die Messwerte auf beiden Netzwerken (A+B) berücksichtigt.

Zu Beginn der Messungen im Jahr 2011 gab es eine große Anzahl von Server Scan-Angriffen, die jedoch mit einer geringen Anzahl an OPTIONS-Paketen durchgeführt wurden. Nach einem Rückgang der Angriffe bis Anfang 2012 stieg anschließend die Anzahl der SIP-Nachrichten und die Anzahl der Angriffe, die der Angriffsstufe Server Scan zugeordnet wurden, über den Messzeitraum deutlich an.

Bis zum Ende des Analysezeitraums hat sich das Scan-Verhalten dahingehend geändert, dass die ursprüngliche Angriffsanzahl zum Ende der Messungen im Oktober 2014 wieder erreicht wurde, jedoch mit deutlich höherer Intensität nach aktiven SIP-Komponenten gesucht wurde. Abbildung 55 stellt für den Analysezeitraum die Anzahl der Server Scan-Angriffe mit der Anzahl der verwendeten SIP-Pakete gegenüber. Das soeben beschriebene

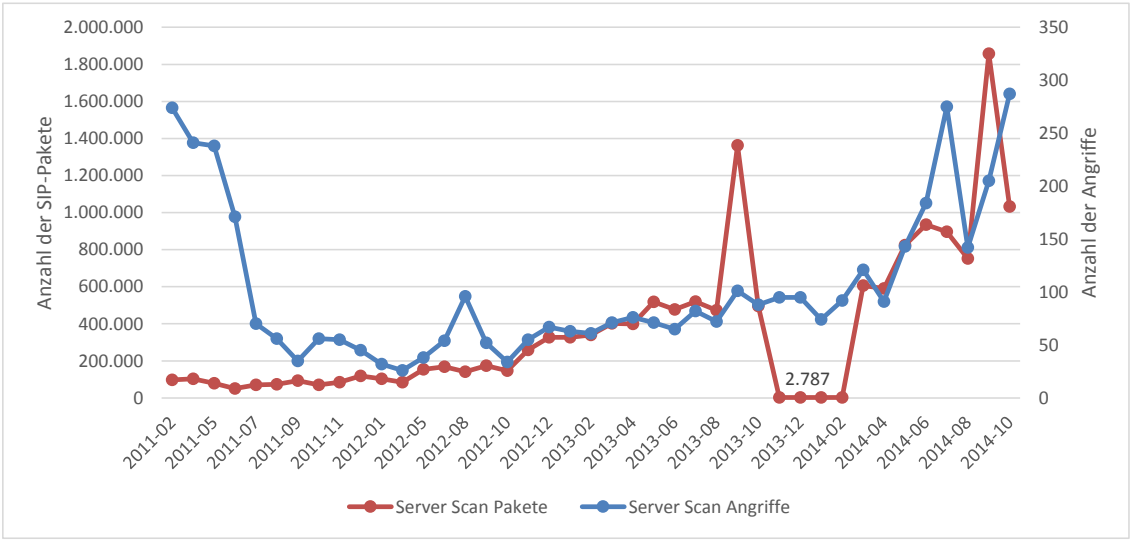


Abbildung 55: Clustering für die Angriffsstufe Server Scan

Verhalten ist gut erkennbar. In den Monaten September 2013 und September 2014 werden zwei Peaks in der Nachrichtenanzahl deutlich. Diese sind auf sehr massive Scanversuche von zwei Angreifern zurückzuführen. In dem Zeitraum von November 2013 bis Februar 2014 gab es vereinzelt Routingausfälle in dem Netzwerk B (Netzwerk ohne SIP-Komponenten), wodurch sich die niedrigen Paketanzahlen (z.B. Nov 2013: 2.787 SIP-Pakete) für die Angriffsstufe Server Scan ergeben. Dennoch blieb die Anzahl der Angriffe auf einem konstant hohen Niveau.

Für die Angriffsstufe Extension Scan fallen die Anzahl der Angriffe und die zugehörige Paketanzahl in dem Zeitraum bis Ende 2012 vergleichsweise gering aus. Nur im Juli 2012 gibt es einen Peak bei der Anzahl der SIP-Nachrichten. Hier hat ein einzelner Angreifer alle Honeypots mit jeweils identischen Angriffen attackiert und für diesen Scan 1,2 Millionen Pakete versendet. Ein vergleichbares Verhalten, jedoch mit zwei ursächlichen Angreifern, konnte in den Monaten Juni 2013 und Januar 2014 festgestellt werden. Die Abbildung 56 zeigt, dass im Jahreswechsel 2012/2013 die Extension Scans für einen kurzen Zeitraum intensiver wurden. In den Folgemonaten stieg zwar die Anzahl der Angriffe, jedoch erfolgten diese besonders in der zweiten Jahreshälfte 2013 mit geringerer Intensität, wenn die zwei beschriebenen Peaks als Sonderfälle betrachtet werden.

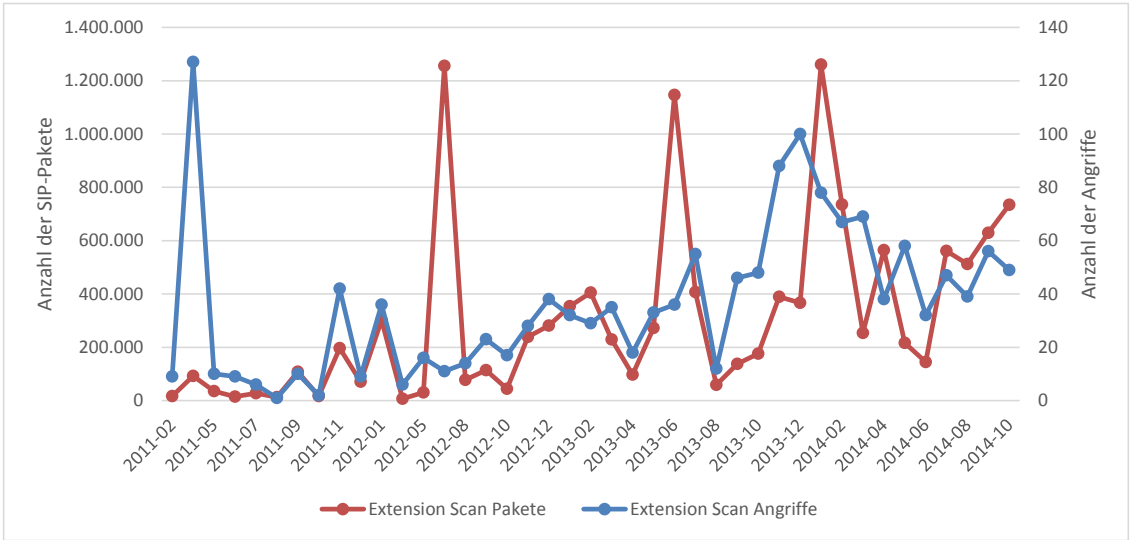


Abbildung 56: Clustering für die Angriffsstufe Extension Scan

Bei den Werten für die Angriffsstufe Registration Hijacking werden die Vorteile der Clustering-Analyse besonders deutlich: So zeigt sich, dass eine extrem hohe Anzahl an SIP-Nachrichten (13,9 Millionen) im Juni 2011 nur durch acht Angriffe bedingt wurde. Im März 2014 hingegen wurden 762 Angriffe mit nur 370.420 SIP-Paketen durchgeführt. Dies zeigt, dass eine ausschließliche Betrachtung der Anzahl der SIP-Nachrichten keine umfassende Aussage über das Angreiferverhalten erlaubt.

Abbildung 57 zeigt, dass über den gesamten Messzeitraum zwei verschiedene Verhaltensweisen detektiert wurden: Wird für einen Angriff eine hohe Anzahl an SIP-Nachrichten (größer 1.000) verwendet, handelt es sich um verschieden umfangreiche Wörterbuchattacken. Ist die Anzahl der SIP-Pakete hingegen gering, werden üblicherweise zufällige oder iterative Zahlenkombinationen zum Übernehmen der Nebenstelle verwendet. Gerade in den letzten Monaten der Messungen zeigte sich, dass die Anzahl der Angriffe zunahm, diese aber in Hinblick auf die Paketanzahl und somit für ein normales Netzwerk-Monitoring vergleichsweise unauffällig waren. Um einen möglichen Schaden von den Anwendern bzw. den Unternehmen abwenden zu können, ist es unerlässlich, ein echtzeit-basiertes Erkennungssystem auf SIP-Ebene zu installieren. Diese Verhaltensänderung bei den Angriffen deutet auf veränderte oder neue Angriffswerkzeuge hin, die in Kapitel 6.2.4 und Kapitel 6.3 erläutert werden.

Die absoluten Werte in Tabelle 13 sowie die grafische Darstellung in Abbildung 58 zeigen deutlich, dass die Toll Fraud-Angriffe stark zugenommen haben. Im Vergleich zu den übrigen Angriffsstufen erfolgen diese mit einer deutlich geringeren Paketanzahl pro Angriff. Im letzten Jahr zeigten sich jedoch verstärkt Toll Fraud- Angriffe, die mit deutlich höherer Intensität durchgeführt wurden. Dies macht deutlich, dass die Toll Fraud-Problematik bei der Erkennung und der Abwehr von Angriffen dringend berücksichtigt werden muss, damit für den Betreiber und den Anwender von VoIP-Diensten kein Schaden entsteht.

Die Honeypot-Systeme simulieren zwar den Gesprächsaufbau, so dass eine Analyse des Angreiferverhaltens möglich ist, erlauben jedoch keine externe Gesprächsvermittlung in das klassische Telefonnetz. Die Angreifer testen systematisch verschiedene Zahlenkombinationen zum Verlassen der Nebenstellenanlage, gefolgt von unterschiedlichen internationalen Vorwahlen und Rufnummern. Nur wenige Angriffsversuche betreffen Premiumdienste wie z.B. 0900. Da keine echte Vermittlung der

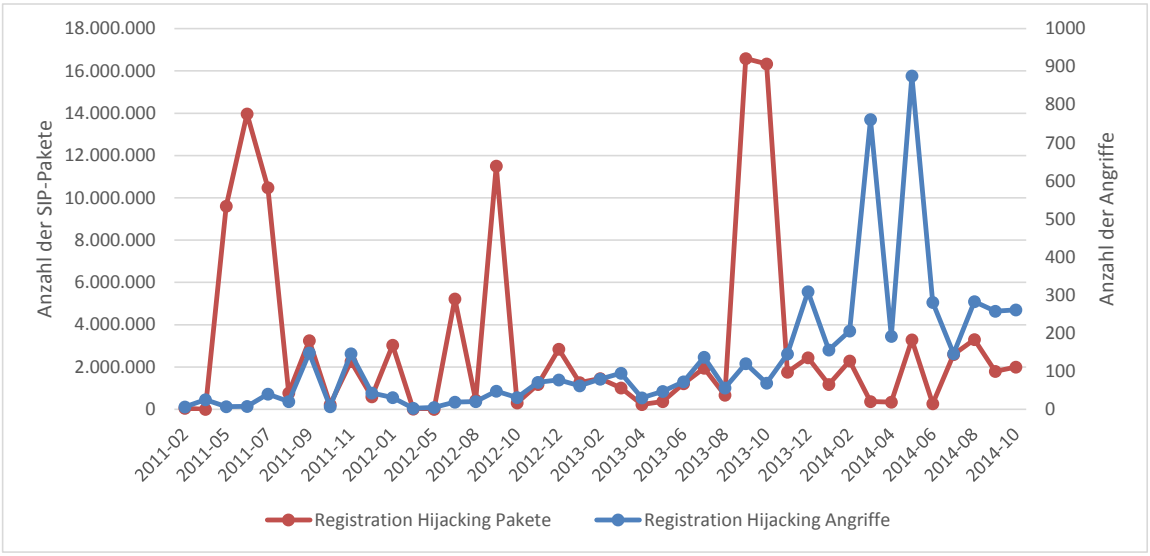


Abbildung 57: Clustering für die Angriffsstufe Registration Hijacking

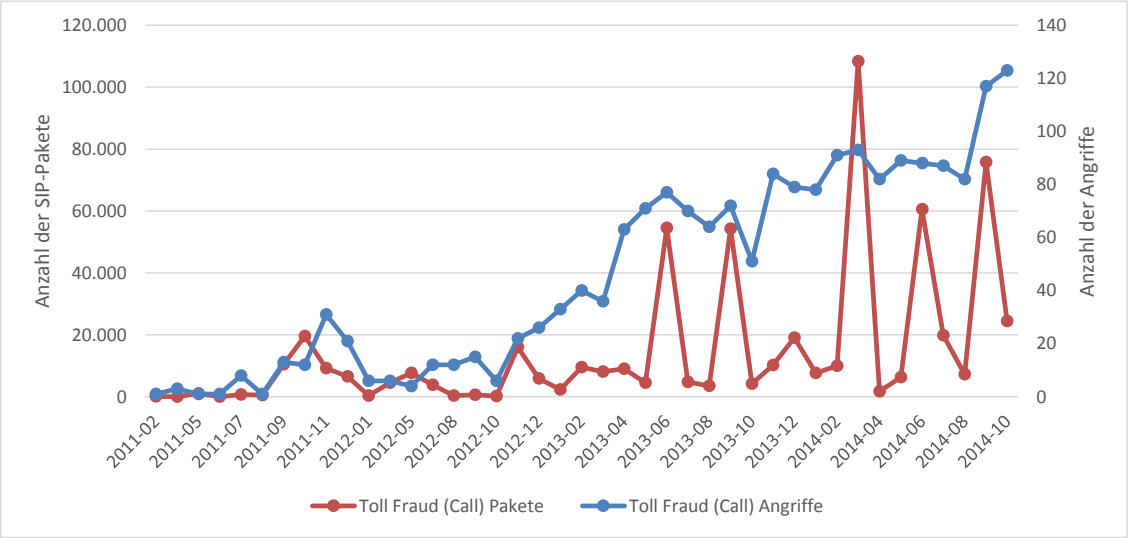


Abbildung 58: Clustering für die Angriffsstufe Toll Fraud

Anrufe erfolgt, muss davon ausgegangen werden, dass die Angriffe vorzeitig aufhören, da der „Nicht-Erfolg“ von den Angreifern bemerkt wird.

6.2.4 Kumulative Verteilung der Angriffe über den Messzeitraum

Der Clustering-Ansatz ermöglicht eine Analyse basierend auf der Anzahl der Nachrichten pro einzelnem Angriff, um neue Angriffsverhalten in den gesammelten Daten zu erkennen. Um die Änderungen im Angriffsverhalten während des Messzeitraums erkennen zu können, wurden für jede Angriffsstufe auf Basis der kumulativen Verteilungsfunktion Auswertungen über 12 Monate (im Jahr 2014: 10 Monate) für den Zeitraum vom 01.01.2011 bis 31.10.2014 erstellt. Die nachfolgenden Diagramme zeigen pro Jahr auf der X-Achse die Anzahl der SIP-Nachrichten und auf der Y-Achse den prozentualen Anteil der Angriffe, die bis zu x SIP-Pakete pro Angriff verwendet haben.

6.2.4.1 Server Scan

Abbildung 59 zeigt für die Angriffsstufe Server Scan, dass in den Jahren 2011 und 2012 diese Angriffsart bei 32 SIP-Paketen startete und im Jahr 2011 50% der Angreifer bis zu 64 Pakete pro Angriff nutzten. Dieses Verhalten kann durch die Verwendung des Tools SIPvicious begründet werden, da es sich um Vielfache von 32 Paketen handelt.

Ab dem Jahr 2013 nutzten 20% der Angreifer weniger als 32 Pakete. Hier wird deutlich, dass bedingt durch neue Angriffswerkzeuge veränderte Verhaltensweisen erkennbar sind. Eine Analyse der Angriffstools (User Agents) in Kapitel 6.3 hat gezeigt, dass das Angriffstool SIPvicious über den Messzeitraum einen konstant hohen Anteil von bis zu 87% aufweist, sich jedoch die Art des Angriffs verändert. Im Jahr 2011 hatte SIPvicious einen Gesamtpaketanteil von 39%. Dieser stieg in den Folgejahren auf bis zu 90% an. Zeitgleich reduzierte sich der Paketanteil des Tools sundayddr auf ein Sechstel von 60% im Jahr 2011 auf 11% im Jahr 2012. Da die Anzahl der Angriffe in diesem Zeitraum jedoch sogar leicht anstieg, zeigt sich eine Änderung in der Durchführung der Angriffe.

Es muss davon ausgegangen werden, dass die Anzahl der Pakete pro Angriff reduziert wurde, um die Angriffe auf SIP-Server weniger auffällig zu gestalten. In Hinblick auf die gesendeten SIP-Pakete reduzierte sich der Anteil von sundayddr bis zum Jahr 2014 sogar auf nur noch 1,6% (Angriffsanteil 3%). Die Änderungen der Verhaltensweisen der Tools SIPvicious und sundayddr sind eine Erklärung für die unterschiedlichen Kurven für 2011 und die übrigen Jahre. Für die Jahre 2012 bis 2014 zeigt Abbildung 59, dass sich die Kurven im

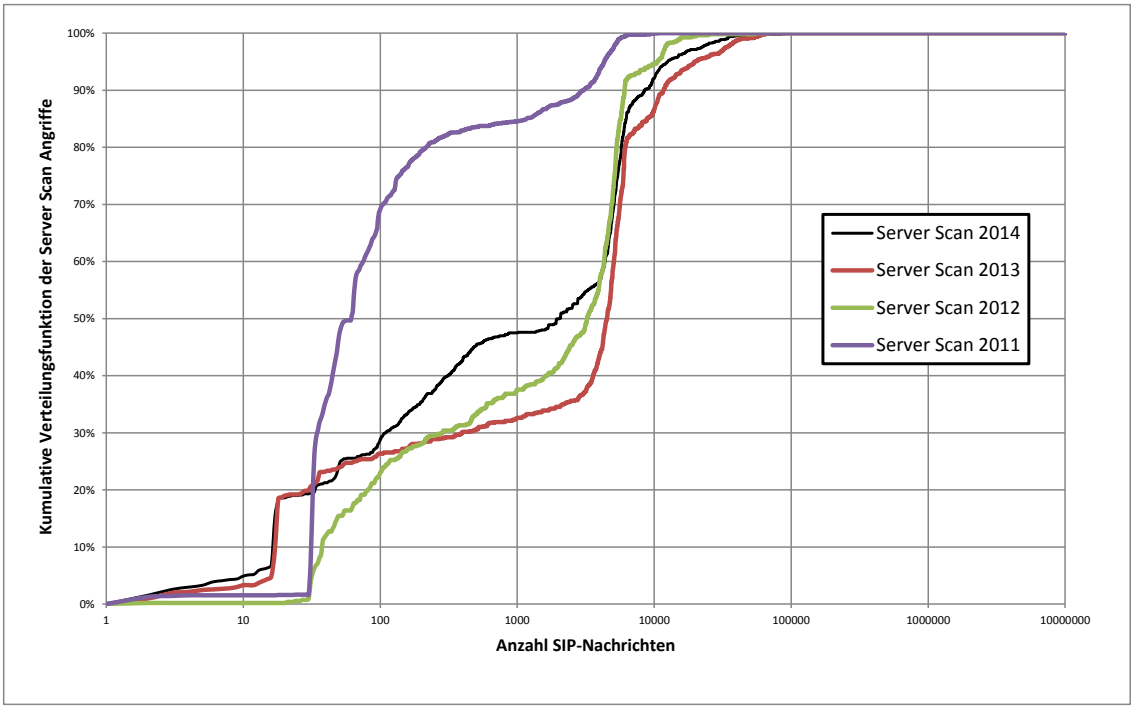


Abbildung 59: Kumulative Verteilungsfunktion der Server Scan-Angriffe

oberen Bereich annähern und 20% der Angreifer über 5.300 SIP-Pakete für einen Server Scan benutzten.

Eine weitere Bestätigung für die Anpassung des Angriffsverhaltens ist ein Angriffswerkzeug, das erst seit Mai 2014 auftrat. Bei diesem Tool ist auffällig, dass das User Agent-Feld acht zufällige Zeichen enthält. Diese werden bei einem Server Scan-Angriff pro Ziel-IP-Adresse verändert. Typischerweise werden nicht mehr als 2.000 Pakete pro Angriff versendet.

6.2.4.2 Extension Scan

In Abbildung 60 zeigt sich, dass im Gegensatz zu den Server Scans nur eine moderate Anpassung des Angriffsverhaltens bei Extension Scans im Messzeitraum stattgefunden hat. Darüber hinaus können zwei Verhaltensweisen erkannt werden: 47% bis 50% der Angreifer verwendeten für einen Angriff maximal 100 SIP-Pakete (z.B. zum Prüfen einiger zufälliger Nebenstellennummern), während der übrige Teil der Angriffe mit über 100 SIP-Paketen ausgeführt wurde.

In den Jahren 2011 und 2012 wurde das Tool SIPvicious für fast 90% der Extension Scan-Angriffe verwendet. Daher ergeben sich sehr ähnliche Kurven für diese Jahre. Im Jahr 2012 wurde vereinzelt ein neues Angriffswerkzeug mit der Bezeichnung VaxSipUserAgent erkannt, das jedoch erst im Jahr 2013 7% der Extension Scan-Angriffe verursacht hat. Bis Juli 2014 stieg der Anteil auf fast 30%, währenddessen die Anzahl der Angriffe von SIPvicious im gleichen Umfang zurückging. Dabei muss berücksichtigt werden, dass sich das Angriffsverhalten der beiden Tools signifikant unterscheidet. Während dem Tool SIPvicious im Messzeitraum über 90% der empfangenen SIP-Pakete zugeordnet werden konnten, stieg die maximale Paketanzahl bei dem Tool VaxSipUserAgent nie über 6% der Gesamtpakete pro Jahr. Die Verbreitung dieses Angriffswerkzeuges konnte an mehreren Standorten nachgewiesen werden (siehe Kapitel 6.3).

Im Bereich von 100 bis 10.000 Nachrichten zeichnete sich für die Jahre 2013 und 2014 eine Änderung - bedingt durch das neue Angriffswerkzeug - ab. So wurden vermutlich auf Telefonanlagen der Unternehmen ausgerichtete Angriffe mit möglichst unauffälligem Verhalten durchgeführt. Dafür wurden Nebenstellen im Bereich von 100 bis 9.999 zufällig

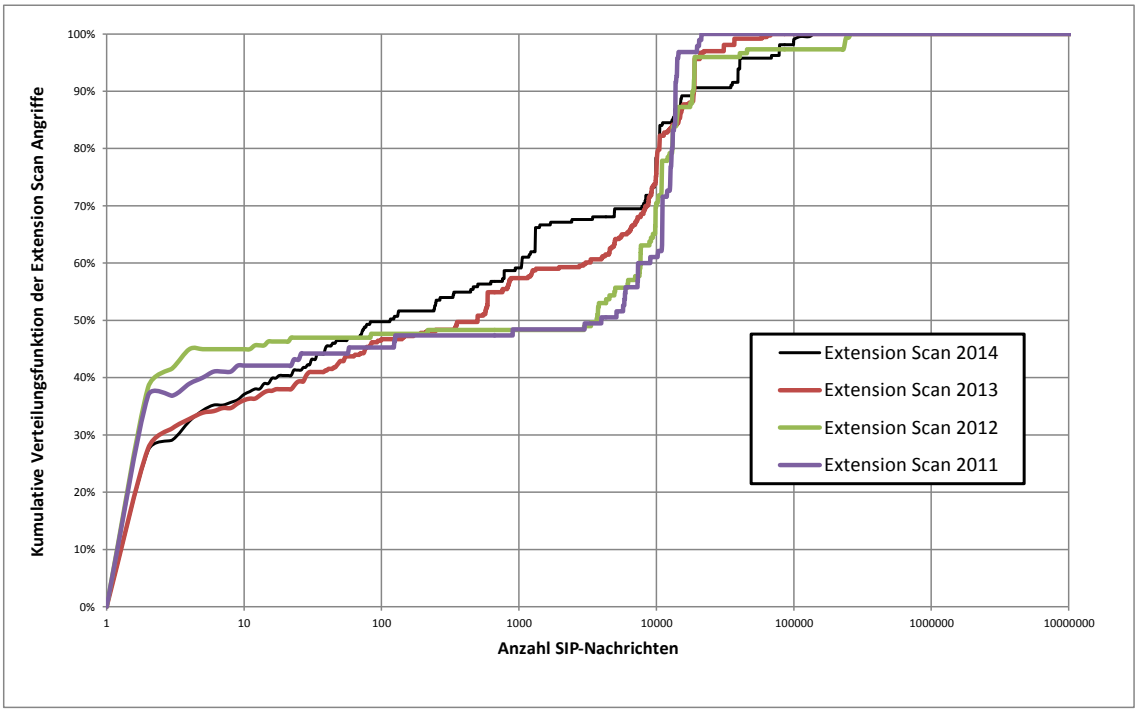


Abbildung 60: Kumulative Verteilungsfunktion der Extension Scan-Angriffe

mit einer geringeren Paketanzahl als bisher überprüft. Oberhalb von 10.000 Nachrichten ist für jedes Jahr zu erkennen, dass 20% der Angreifer auch sehr massive Angriffe mit vordefinierten Listen bzw. Wörterbüchern für die Nebenstellenbezeichnungen durchführten (Treppenbildung in den Kurven).

6.2.4.3 Registration Hijacking

Für die Angriffsstufe Registration Hijacking ist ebenfalls eine Veränderung im Angriffsverhalten während der Honeynet-Analysen zu erkennen. Abbildung 61 zeigt für das Jahr 2011, dass 40% der Angreifer bis zu 51 Pakete für einen Angriff auf eine Nebenstelle verwendeten (Raten einzelner Kennwörter), 20% benutzten bis zu 10.000 SIP-Pakete (Raten von numerischen Kennwörtern) und 40% der Angreifer verwendeten verschieden große Wörterbücher, um das Kennwort einer Nebenstelle mittels Brute-Force-Attacke zu erraten.

Die unterschiedlichen Wörterbücher können in der violetten Kurve anhand der Treppenbildung erkannt werden. Für das Jahr 2012 zeigt sich, dass im unteren Bereich 25% der Angreifer bis zu 500 SIP-Pakete für einen Angriff verwendeten und dass die Angriffe mit über 100.000 Paketen angestiegen sind (von 2% auf 8%). Die Honeynet-Analyse zeigt, dass 98% der SIP-Nachrichten auf das Tool SIPvicious zurückzuführen sind, woraus eine Anpassung des Angriffsverhaltens im Vergleich zum Jahr 2011 resultiert. Die Folgejahre 2013 und 2014 zeigen jedoch, dass sich gerade die massiven Angriffe abschwächten. So gingen die Angriffe mit mehr als 1.000 Paketen von 59% auf 15% zurück und Attacken mit mehr als 10.000 Paketen erreichten im Jahr 2014 nur noch einen Anteil von 9% statt ursprünglich 39%.

Es muss davon ausgegangen werden, dass die Angreifer das Vorgehen optimieren, um eine Erkennung durch Messung der Netzwerklast für das SIP-Protokoll zu verhindern. Da die Anzahl der Angriffe nicht rückläufig ist, sondern die Art der Angriffe verändert wird, wäre eine Verteilung der Angriffe durch Bot-Netze oder der Einsatz anderer Angriffswerkzeuge denkbar. Dies kann in Hinblick auf das neu erkannte Tool VaxSipUserAgent belegt werden: In den Jahren 2013 und 2014 erreichte dieses Angriffswerkzeug einen Anteil von bis zu 90%

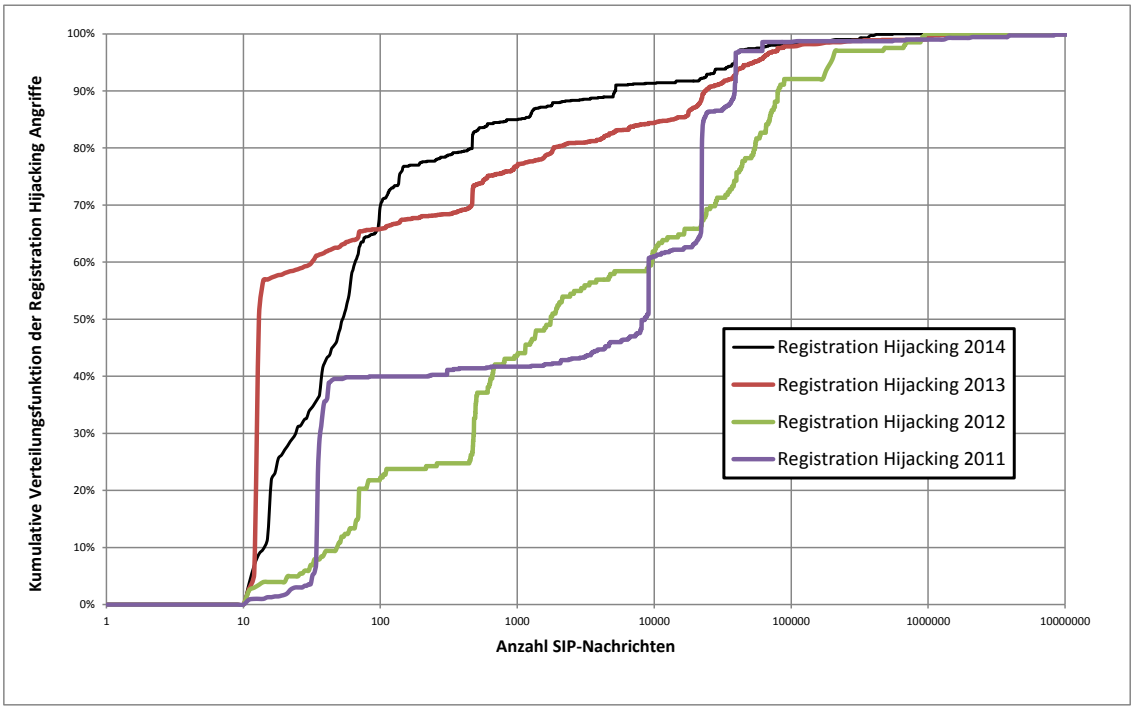


Abbildung 61: Kumulative Verteilungsfunktion der Registration Hijacking-Angriffe

an den Registration Hijacking-Angriffen. Jedoch machten diese Angriffe nur bis zu 5% der gesamten SIP-Nachrichten dieser Angriffsstufe aus.

6.2.4.4 Toll Fraud

Wie in Kapitel 6.2.2.4 beschrieben, zeigt sich auch in Abbildung 62 über den Messzeitraum eine Optimierung der Toll Fraud-Versuche. Zu Beginn der Aufzeichnungen im Jahr 2011 wurden bei 20% der Angriffe über 1.000 SIP-Pakete verwendet, währenddessen die Folgejahre sehr ähnliche Kurven zeigen und weniger Pakete pro Angriff benutzt wurden (maximal 7% der Angriffe wiesen mehr als 1.000 Pakete auf). So werden vordefinierte Rufnummern mit unterschiedlichen Amtsrufnummern gezielt ausprobiert bzw. vom Angreifer eingerichtete Testrufnummern angerufen, um den Erfolg des Angriffes testen zu können.

Diese optimierten Angriffe wurden fast ausschließlich mit dem Tool „SipCLI“ [65] in der Version 1.8 ausgeführt. Dabei handelt es sich um einen SIP-Client für Linux, der Shell-basiert genutzt und somit durch Skripte automatisiert eingesetzt werden kann. Dieses Tool hat bei Toll Fraud-Angriffen einen Anteil von bis zu 80% in den Jahren 2012 bis 2014. 40% der Angriffe erfolgten mit weniger als 15 SIP-Nachrichten. Bei diesen Angriffen wurden bekannte Softphones wie z.B. Eyebeam [66], X-Lite [67] oder Zoiper [68] eingesetzt, so dass von manuellen Angriffen ausgegangen werden kann.

Da das Honeynet aus rechtlichen Gründen keine Anrufe in das klassische Telefonnetz weitervermittelt, wird zwar das optimierte Verhalten der Angreifer sichtbar, jedoch sind aus diesem Grund nur wenige manuelle Toll Fraud-Versuche erkennbar. Kann ein Angreifer eine Nebenstellenanlage erfolgreich kompromittieren (Bestätigung durch Anwahl von Testrufnummern), so ist davon auszugehen, dass nach kurzer Zeit zahlreiche Anrufe von Softphones zu verschiedenen Zielrufnummern feststellbar sein werden.

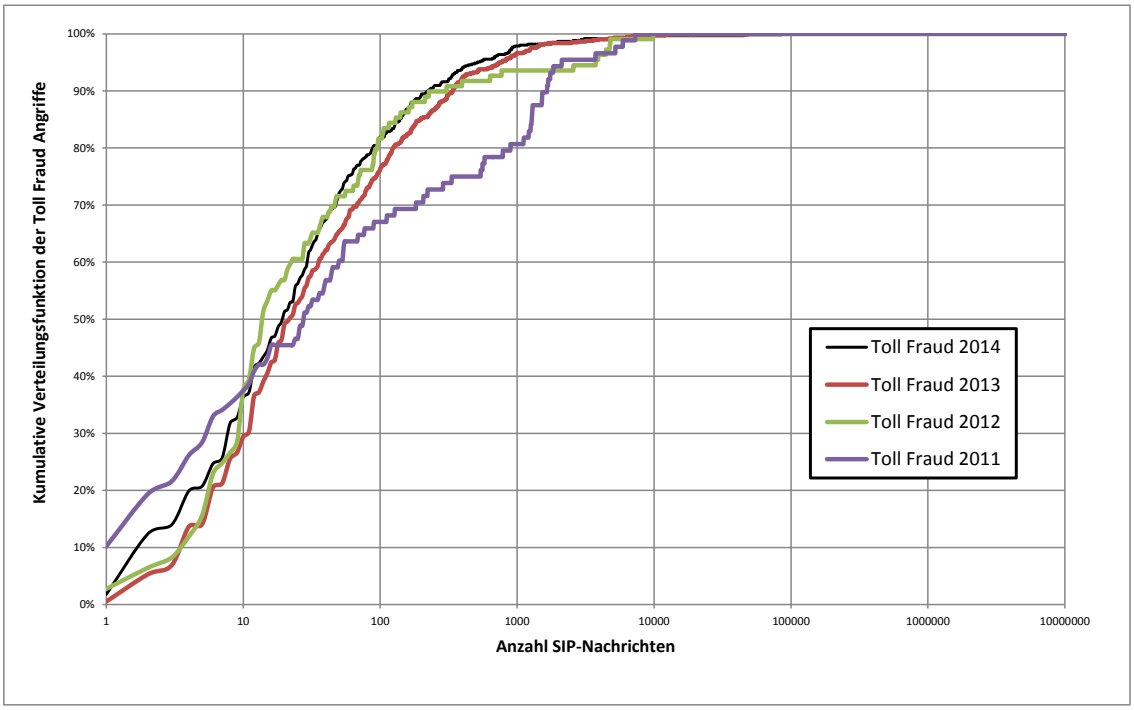


Abbildung 62: Kumulative Verteilungsfunktion der Toll Fraud-Angriffe

6.3 Forensischer Vergleich verschiedener Messstellen

Die forensischen Analysen am Standort Essen haben die Angriffsaktivitäten auf SIP-basierte Netzwerke verdeutlicht. In diesem Kapitel soll geklärt werden, ob in anderen Netzwerkbereichen des Internets identische Verhaltensweisen bei den Angriffen feststellbar sind. Da auf Grund der bisherigen Analysen davon auszugehen ist, dass die Angriffe über sehr große Netzbereiche durchgeführt werden, müssten die gleichen Angreifer auch an anderen Standorten sichtbar sein.

Für den Zeitraum Oktober 2013 bis Oktober 2014 stehen im STR die gesammelten SIP-Daten von drei Netzwerken in Essen, Wien und dem Forschungsnetz NorNet [8] (Standorte in Norwegen, Deutschland und China) zur Verfügung, so dass eine vergleichende Analyse möglich ist. Tabelle 14 gibt einen Überblick über die untersuchten Netzwerke. Am Standort Essen wurden die meisten SIP-Pakete aufgezeichnet, obwohl hier die geringste Anzahl an Honeypots im Einsatz ist. Dies lässt sich mit dem überwachten Bereich von zwei Class-C-Netzen (508 IP-Adressen) im Vergleich zu acht (Wien) bzw. 30 überwachten IP-Adressen (NorNet) erklären. Auffällig ist die doppelt so hohe Anzahl an Angreifer-IP-Adressen im NorNet-Testbed im Vergleich zum Essener Standort. Durch die überregionale und länderübergreifende Verteilung der NorNet-Honeypots in 30 verschiedenen Subnetzen wurden diese Systeme, im Gegensatz zu den lokalen Installationen in Essen und Wien, von zusätzlichen Angreifern erkannt.

6.3.1 Identische Angreifer

In dem Messzeitraum wurden 876 IP-Adressen aus 67 Ländern erkannt, die in allen drei Netzwerken Angriffe durchgeführt haben. Abbildung 63 zeigt die Schnittmengen der identischen IP-Adressen für die drei Standorte. Somit haben ca. ein Drittel der Angreifer aus Essen und Wien auch Systeme an den anderen Standorten angegriffen.

Die Schlussfolgerung aus den Ergebnissen der forensischen Analysen, dass es sich um sehr großflächige Angriffe handelt, wird dadurch bestätigt.

Tabelle 14: Statistische Daten zu den analysierten Netzwerken

Information	Essen	Wien	NorNet
Anzahl der SIP-Pakete	60.006.802	20.785.111	19.986.357
Identifizierte IP-Adressen	2.635	2.854	5.335
Anzahl der Honeypots	5	8	30
Anzahl der überwachten IP-Adressen	508	8	30
Anzahl der Subnetze	2	1	30

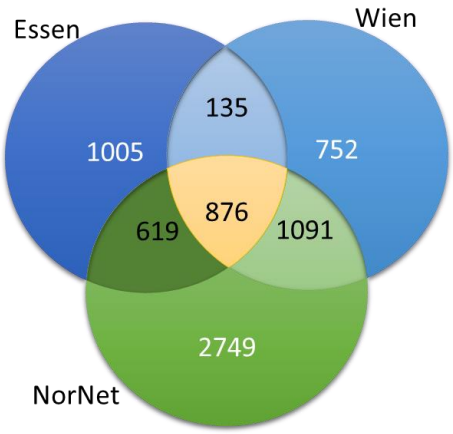


Abbildung 63: Identische IP-Adressen in verschiedenen Netzwerken

Dies macht deutlich, dass für eine zuverlässige Angriffsabwehr in Echtzeit eine verteilte Angriffserkennung hilfreich ist, damit im Internet bekannte Angreifer an allen Standorten sofort blockiert werden können. Besonders bei wiederkehrenden Angreifern würde der Schutz mit Hilfe von Real-time-Blacklists sehr gut funktionieren. Daher betrachtet die nachfolgende Auswertung die Fragestellung, wie lange die Angreifer an den verschiedenen Standorten aktiv waren und ob es eine Übereinstimmung der in Abbildung 63 gezeigten Teilmenge von 876 identischen Angreifern in den drei Netzwerken gibt.

6.3.2 Wiederkehrende Angreifer

Auf Grund der hohen Anzahl von Angreifer-IP-Adressen in den unterschiedlichen Netzwerken wurde zunächst von temporären Angriffsaktivitäten ausgegangen. Daher wurde für den Vergleichszeitraum eine Analyse zur Identifizierung von wiederkehrenden Quell-IP-Adressen durchgeführt. Dabei sollte die Fragestellung geklärt werden, von wie vielen der gesamten Angreifer-IP-Adressen über welchen Zeitraum in den Netzwerken wiederkehrende Angriffe durchführt wurden. Die Zielsetzungen für diese Auswertung waren die Erkennung von Angriffen, die von Langzeit-Scannern ausgehen, und der Schutz vor diesen.

Abbildung 64 zeigt auf Basis der kumulativen Verteilungsfunktion die Dauer der Angriffe. Auf der X-Achse wird die Anzahl der Tage abgebildet. Die Y-Achse zeigt den prozentualen Anteil der Angreifer, die bis zu x Tage im Honeynet erkannt wurden. Die eingezeichneten Kurven geben die Werte für jedes der drei Vergleichsnetzwerke an. Es konnten Langzeit-Angreifer identifiziert werden, die an bis zu 390 Tagen in den Netzwerken aktiv waren. In Essen wurden 36,7% und in Wien 41,3% der Angreifer mit mehr als 24 Stunden Angriffsaktivität erkannt. Im NorNet liegt dieser Wert bei ca. der Hälfte der Angreifer (49,7%). Die Kurven für die Honeynets in Wien und im NorNet liegen sehr nah beieinander

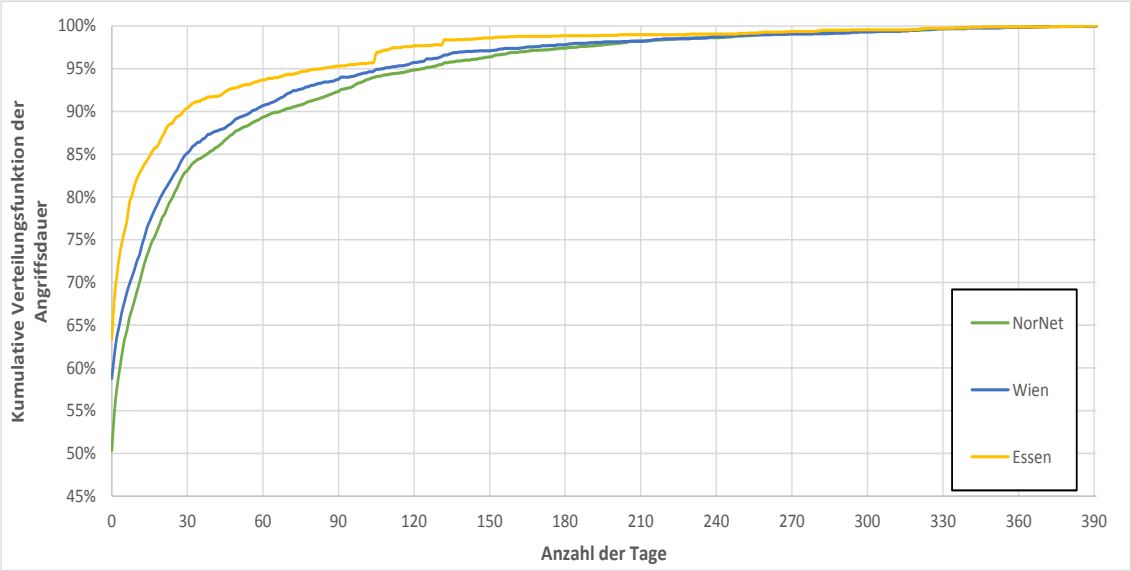


Abbildung 64: Wiederkehrende Quell-IP-Adressen

und nähern sich bei 150 Tagen Angriffsaktivität an. Die Kurve für das Honeynet in Essen liegt dauerhaft oberhalb der Kurven der anderen Netzwerke. Daraus ergibt sich, dass ein geringer Anteil der Angreifer in Essen Langzeit-Scans durchgeführt hat. Im Umkehrschluss verdeutlicht die Kurve für das NorNet, dass dort im Vergleich zu den anderen Standorten die meisten Langzeit-Scanner aktiv waren. Am Standort Essen wurden 10% der Angreifer an mehr als 30 Tagen im Messzeitraum identifiziert, währenddessen der Anteil in Wien und NorNet bei 15% bzw. 17% lag.

Speziell der höhere Wert für das NorNet-Testbed lässt sich mit der größeren Verteilung der NorNet-Honeypots in entfernten Subnetzen erklären, da hier der Erfassungsbereich größer ist. Sobald ein Angreifer einen großen Teil des Internets scannt und angreift, ist die Wahrscheinlichkeit im Vergleich zu den lokalen Honeynets höher, dass dieser von den NorNet-Messstellen erfasst wird.

An allen drei Standorten wurden, wie in Abbildung 63 gezeigt, 876 identische IP-Adressen identifiziert. 14% dieser Angreifer-IP-Adressen zeigten im Messzeitraum mindestens 30 Tage Aktivität. Bei mindestens 60 Tagen Aktivität liegt der Anteil der Langzeit-Scanner bei 10%. Dies widerlegt die mögliche Vermutung, dass es sich bei den 876 identischen IP-Adressen überwiegend um Langzeit-Angreifer handelt. Vielmehr wird deutlich, dass die Angreifer über einen kurzen Zeitraum breitflächige Angriffe durchführen.

Bei den bekannten IP-Adressen, die über mehrere Monate identifiziert wurden, zeigte sich ein spezielles Angriffsverhalten: Im Gegensatz zu Angreifern, die die verschiedenen Stufen eines Toll Fraud-Angriffs durchführten und nur wenige Tage Aktivität zeigten, führten die Langzeit-Angreifer kontinuierliche Server Scans aus. Es muss davon ausgegangen werden, dass diese Scans die Aufgabe haben, zu prüfen, ob die bereits erkannten SIP-Server auch weiterhin zur Verfügung stehen bzw. ob neue SIP-Server in einem den Angreifern bereits bekannten Netzwerk installiert wurden. Dies würde auch die vorausgegangenen Untersuchungsergebnisse bestätigen, dass neue SIP-Server in nur wenigen Stunden nach der Inbetriebnahme massiv angegriffen werden.

Außerdem wird die Annahme bestätigt, dass ein verteiltes Erkennungssystem Schutz bieten kann, da eine Schnittmenge der Angreifer an allen Standorten nachgewiesen werden konnte. Davon wurden 14% als Langzeit-Scanner identifiziert, die über einen Zeitraum von bis zu 360 Tagen wiederkehrende Angriffsaktivitäten gezeigt haben.

6.3.3 Entwicklung der Angriffswerkzeuge

In Kapitel 6.2.4 wurde gezeigt, dass sich das Angriffsverhalten im Messzeitraum verändert hat und dass modifizierte bzw. neue Angriffswerkzeuge identifiziert wurden, die für die Verhaltensänderung ursächlich sind. Diese Änderungen haben das Ziel, dass die Angriffe möglichst unauffällig und für Netzwerk-Monitoring-Komponenten unsichtbar erfolgen sollen.

Zu Beginn der Analysen für diese Dissertation im Dezember 2010 wurden überwiegend nur Tools wie SIPvicious, sundayddr und gängige Softphones für Angriffe eingesetzt. Die nachfolgende vergleichende Analyse für die drei Netzwerkstandorte im Messzeitraum von Oktober 2013 bis Oktober 2014 zeigt jeweils die Entwicklung der Anteile der Angriffswerkzeuge (siehe Abbildung 65) und verdeutlicht, dass die analysierten Veränderungen auch an anderen Standorten nachgewiesen werden können.

Abbildung 65 zeigt den prozentualen Anteil der Angreifer-Werkzeuge pro Standort. Die Identifizierung wird über den SIP-Header „UserAgent“ vorgenommen, soweit dieser Wert gesetzt ist. Bei einer fehlenden Header-Information erfolgt die Einordnung in den User Agent „leer“. Da die Angreifer-Werkzeuge mit unterschiedlichen Paketanzahlen pro Angriff arbeiten, basiert diese Auswertung auf der Anzahl der Angreifer (Quell-IP-Adresse), um mögliche Verfälschungen bei den prozentualen Anteilen zu vermeiden.

Der Anteil des weitverbreiteten Tools SIPvicious bleibt unverändert hoch, währenddessen das Werkzeug sundayddr ab September 2014 nicht mehr nachweisbar ist. An allen Standorten ist der Rückgang von sundayddr zu beobachten. Vor dem in Abbildung 65 betrachteten Vergleichszeitraum kann mit Hilfe der STR-Auswertungen festgestellt werden, dass der Anteil von sundayddr kontinuierlich abnahm, währenddessen im Jahr 2012 zunächst sporadisch, im Jahr 2013 jedoch kontinuierlich der Anteil des neuen Angriffswerkzeuges VaxSipUserAgent anstieg [6]. Auch in der Analyse in Abbildung 65 ist das Werkzeug VaxSipUserAgent standortübergreifend und kontinuierlich zu beobachten, so dass davon ausgegangen werden muss, dass einzelne Werkzeuge wie sundayddr durch neue Angriffswerkzeuge ersetzt und die Angriffe in Zukunft optimiert werden.

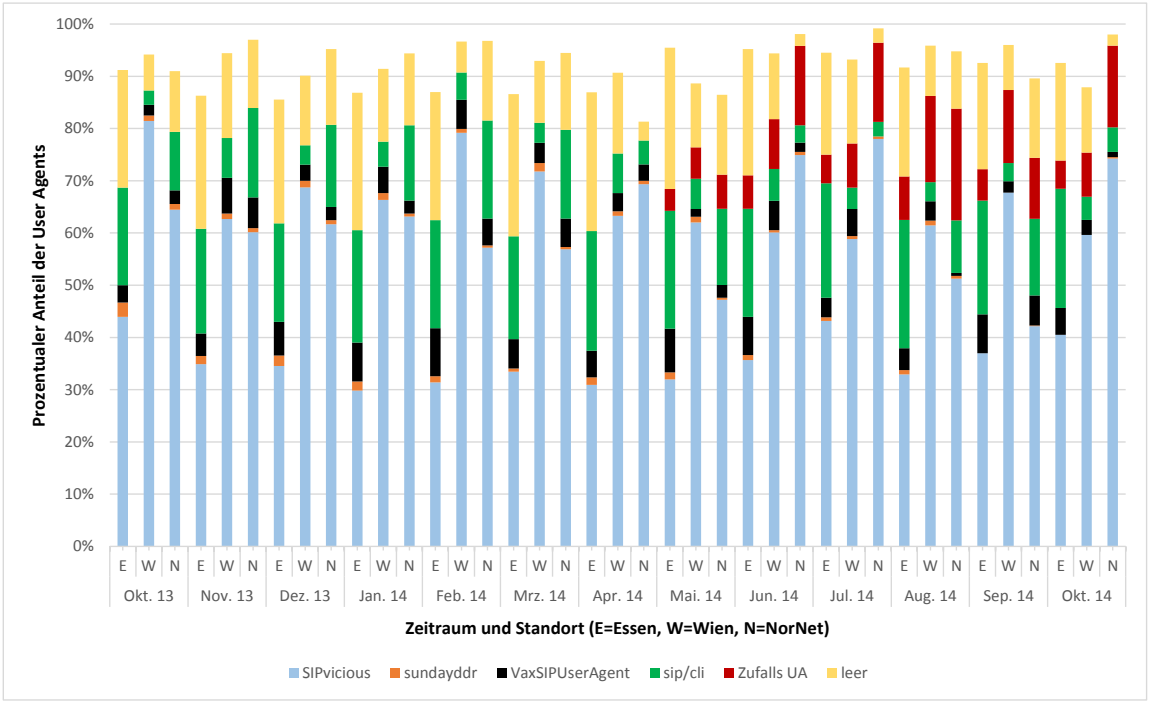


Abbildung 65: Entwicklung der Anteile der User Agents (10/2013 bis 10/2014)

Die Untersuchungen im Rahmen dieser Dissertation haben darüber hinaus gezeigt, dass das Programm VaxSipUserAgent deutlich weniger SIP-Pakete für einen Angriff verwendet als beispielsweise SIPvicious und somit unauffälliger agieren kann. Aus diesem Grund ist es unerlässlich, dass eine verteilte Angriffserkennung die SIP-Pakete korreliert und die durchgeführten Angriffsstufen erkennt, so dass böswillige Anrufe sofort unterbunden werden können.

Das Werkzeug sip/cli arbeitet Shell-basiert und ist über den Vergleichszeitraum kontinuierlich an allen Standorten nachweisbar. Der Anteil des User Agents ist jedoch am Standort Essen vergleichsweise hoch. Mit diesem Werkzeug werden nach bisherigen Auswertungen die unterschiedlichen Amtsrufnummern gezielt ausprobiert (siehe auch Kapitel 6.2.4.4). Da am Standort Essen im Gegensatz zum Standort Wien das Verlassen der Nebenstellenanlage nicht möglich ist, ist ein anhaltendes Ausprobieren der Amtskennzahlen wahrscheinlich.

Bisher konnten die Angriffswerkzeuge an der Kennung im SIP-Header-Feld User Agent identifiziert werden. Seit Mai 2014 wurde ein neues Programm erkannt, das pro attackierter Ziel-IP-Adresse einen neuen, zufälligen aus acht Zeichen bestehenden Wert für das User Agent-Feld im SIP-Header generiert. Für die Erkennung müssen komplexere Regeln eingesetzt werden, die das User Agent-Feld mit regulären Ausdrücken überprüfen bzw. weitere SIP-Header-Felder für die Erkennung berücksichtigen. Abbildung 65 zeigt deutlich, dass dieses Angriffswerkzeug in keinem Netzwerk bis einschließlich April 2014 auftrat, ab Mai 2014 jedoch kontinuierlich nachgewiesen wurde. Nach den durchgeführten Untersuchungen beschränkt sich dieses Werkzeug bisher auf Server Scan-Angriffe.

6.3.4 Herkunft der Angreifer

Unabhängig von den identischen IP-Adressen an den analysierten Standorten wurde für jedes Netzwerk die Herkunft der Angreifer anhand der Quell-IP-Adresse mit einer GeoIP-Datenbank [57] überprüft. Abbildung 66 zeigt die TOP 10 der Herkunftsländer pro Netzwerk. Die Länder, von denen die meisten Angriffe ausgehen, sind in allen Netzwerken identisch, jedoch mit einer unterschiedlichen Verteilung. Aus den USA, Deutschland und

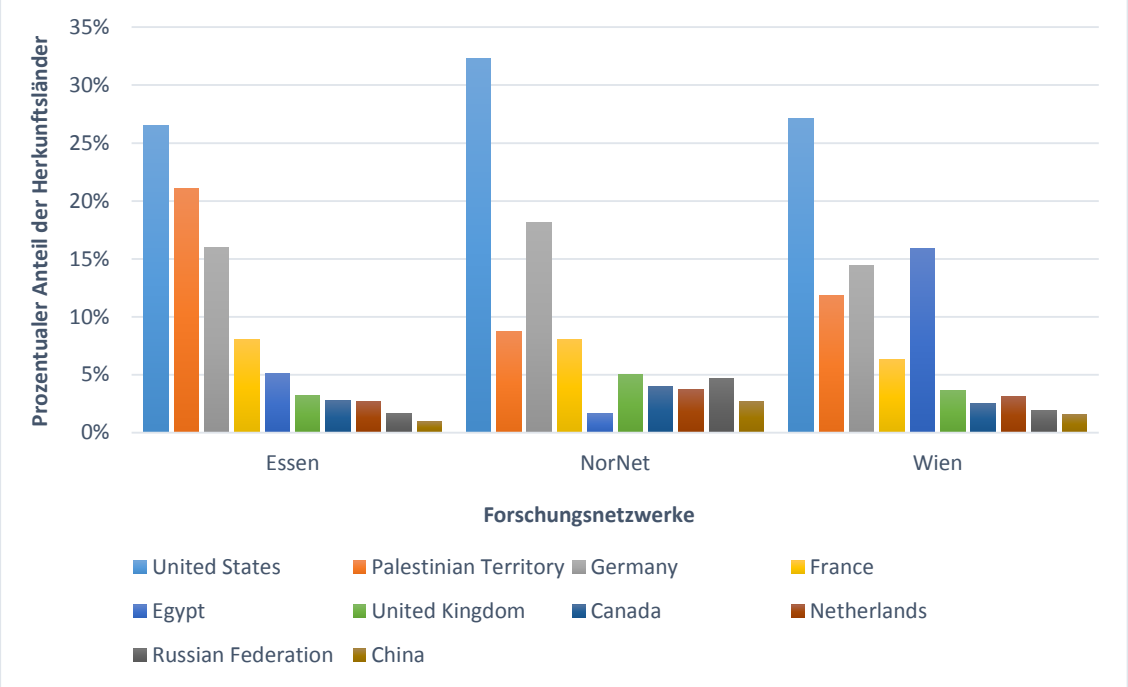


Abbildung 66: Herkunft der Angreifer auf Basis der Quell-IP-Adresse

den Palästinenser-Gebieten erfolgen im NorNet-Testbed und in Essen die meisten Angriffe. In Wien zeigt sich eine ähnliche Verteilung, jedoch kommen hier auffällig viele Angriffe aus Ägypten. Die forensischen Analysen haben überwiegend Toll Fraud-Anrufe in den arabischen Raum und nach Israel gezeigt. Da das Honeynet in Wien zeitweise auch Gespräche in das klassische Telefonnetz vermittelt hat, könnte diese Funktionalität auf Grund der instabilen politischen Lage in Ägypten im Versuchszeitraum von Interesse gewesen sein.

Der Vergleich der drei Netzwerke hat gezeigt, dass die analysierten Effekte im Essener Honeynet auch an den anderen Standorten zutreffend sind: Die Entwicklung der Angriffswerkzeuge konnte zeitnah in allen Netzwerken nachgewiesen werden. Die TOP 10 der Herkunftsländer stimmt ebenfalls überein. Darüber hinaus konnten die gleichen Angreifer an unterschiedlichen Standorten identifiziert werden, die auch nachweislich Langzeit-Scans über mehrere Monate durchgeführt haben. Für die Abwehr von Angriffen ist das Wissen über die Existenz von diesen breiten und langen Scan-Versuchen essentiell, damit SIP-Server bzw. Firewalls rechtzeitig über potentielle Angreifer informiert werden können.

6.4 Evaluierung und Feldversuch des Security Sensor Systems

Mit der ersten stabilen Implementierung des Security Sensor Systems wurde von September 2013 bis März 2014 ein Feldversuch durchgeführt. In dem Unterkapitel 6.4.1 werden zunächst die eingesetzten Signaturen diskutiert. Der Feldversuch diente der Evaluierung der Funktionsweise des neuen Systems (Kapitel 6.4.2) sowie der Beurteilung von Angriffen in SIP-basierten Netzwerken an verteilten Standorten (Kapitel 6.4.3).

6.4.1 Signaturen des Feldversuchs

Für die Definition der Sensor-Signaturen wurden in der Laborumgebung verschiedene SIP-Softphones (z.B. X-Lite, Zoiper, Eyebeam, Apps für das iPhone) und die SIP-Telefonanlage Asterisk in Hinblick auf das Verhalten bei Registrierungen von Nebenstellen und das Aufbauen von Anrufen untersucht. Auf Grundlage dieser Untersuchungen wurden Schwellenwerte für die Erkennungssignaturen festgelegt. Die Regelsätze wurden bewusst einfach gehalten, damit die Angriffserkennung an den einzelnen Standorten möglichst wenig Last und False Negatives verursacht. Ein wichtiger Aspekt war die Funktionsweise in produktiven Umgebungen. Hier sollte sichergestellt sein, dass durch den normalen SIP-Verkehr möglichst keine False Positives generiert werden.

Für die Angriffsstufen Server Scan, Extension Scan und Registration Hijacking wurde jeweils eine Signatur für den Feldversuch aktiviert. Da jeder Anrufversuch und somit jedes INVITE-Paket in einer Honeynet-Umgebung als Angriff gilt, wurde auf eine spezielle Toll Fraud-Regel verzichtet. Die definierten Schwellenwerte pro Angriffsstufe werden in Tabelle 15 gezeigt.

Da ein SIP-Client zur Abfrage der von dem Server unterstützten Funktionen typischerweise ein OPTIONS-Paket sendet, sollte der Schwellenwert für die Server Scan-Signatur bei mindestens zwei OPTIONS-Paketen liegen. Darüber hinaus versendet ein Angreifer bei einem Server Scan im Gegensatz zu produktiven SIP-Clients mehrere OPTIONS-Pakete pro Sekunde an unterschiedliche IP-Adressen. Zur Vermeidung von False Positives und zur Berücksichtigung des typischen Angriffsverhaltens bei Server Scans müssen innerhalb von drei Sekunden drei OPTIONS-Pakete an unterschiedliche Ziel-IP-Adressen gesendet werden. Sollten sich die Zeitabstände zwischen den einzelnen SIP-Paketen in Zukunft vergrößern, so kann das Zeitverhalten der Regel entsprechend angepasst werden.

Tabelle 15: Signaturbedingungen für den Feldversuch

Angriffsstufe	Bedingungen	Zeitverhalten
Server Scan	• SIP-Methode: OPTIONS • 3 SIP-Pakete an verschiedene Ziel-Hosts	3 Sekunden
Extension Scan	• SIP-Methode: REGISTER • 4 SIP-Pakete an unterschiedliche Nebenstellen eines SIP-Servers	4 Sekunden
Registration Hijacking	• SIP-Methode: REGISTER • 100 SIP-Pakete an eine identische Nebenstelle eines SIP-Servers	60 Sekunden

Bei den Server Scan-Angriffen ergeben sich im Vergleich zu den nachfolgenden Angriffsstufen Besonderheiten: Ein Server Scan kann nur erfolgreich erkannt werden, wenn mehrere Hosts bzw. Subnetze überwacht werden. Nur so kann beurteilt werden, ob der Angreifer OPTIONS-Pakete an unterschiedliche Systeme sendet.

Steht hingegen nur ein einzelner Honeypot zur Verfügung, so wird auf diesem System nur eine einzelne OPTIONS-Nachricht sichtbar. Der Server Scan kann nur erkannt werden, wenn davon ausgegangen wird, dass in einer Honeypot-Umgebung sämtliche SIP-Nachrichten als Angriff gewertet werden müssen. Bei dieser Annahme können jedoch False Positives auftreten, wenn bei einem Toll Fraud-Angriff ein Softphone verwendet wird, das zu Beginn des Angriffs ebenfalls ein OPTIONS-Paket versendet. In produktiven Umgebungen generieren zahlreiche SIP-Clients OPTIONS-Nachrichten, so dass ein Server Scan in diesem Fall nicht erkannt werden kann.

Eine weitere Besonderheit in Hinblick auf die Server Scans ergibt sich auch in Honeynet-Umgebungen mit einer Subnetz-Überwachung, wenn der Angreifer die einzelnen SIP-Pakete von unterschiedlichen Systemen aus sendet. In diesem Fall würde die Angriffserkennung nicht funktionieren, da die Erkennung auf Basis der Quell-IP-Adresse erfolgt. Dieses Verhalten ist denkbar, wenn der Angreifer über ein Bot-Netz verfügen würde und die Angriffe somit auf mehrere Systeme verteilen könnte. In diesem Fall müssten von zahlreichen Quell-IP-Adressen einzelne OPTIONS-Pakete im STR sichtbar sein. Während des Feldversuches konnten jedoch nur sehr wenige IP-Adressen mit nur einem OPTIONS-Paket nachgewiesen werden (weniger als 10 Stück/Monat), so dass dieses Verhalten für die Definition von Angriffssignaturen nicht berücksichtigt werden musste.

Bei der Extension Scan-Signatur musste berücksichtigt werden, dass gängige VoIP-Anschlüsse der großen Provider üblicherweise drei Rufnummern (in Sonderfällen maximal 10 Rufnummern) beinhalten, die von einem Endgerät (z.B. Heimrouter) in einem sehr kurzen Zeitraum registriert werden. Das Angriffsverhalten ist in diesem Fall dem Vorgehen in der produktiven Umgebung sehr ähnlich, da mehrere REGISTER-Pakete an unterschiedliche Nebenstellen eines SIP-Servers gesendet werden. Damit durch das Standardverhalten keine False Positives ausgelöst werden, müssen für das Zutreffen dieser Regel vier REGISTER-Pakete an unterschiedliche Nebenstellen eines Servers gesendet werden. Da die forensischen Analysen gezeigt haben, dass bei einem Extension Scan mehrere SIP-Pakete pro Sekunde gesendet werden, wurde für diese Regel ein Zeitlimit von vier Sekunden für vier SIP-Pakete gesetzt.

Die Honeynet-Auswertungen haben gezeigt, dass die Registration Hijacking-Angriffe typischerweise sehr massiv ausfallen (bis zu mehreren Millionen Paketen in wenigen Minuten bzw. Stunden). Wird hingegen das Verhalten von SIP-Clients in produktiven Umgebungen berücksichtigt, so werden nur wenige REGISTER-Pakete (ca. 10 Stück) mit verschiedenen Anmeldedaten an dieselbe Nebenstelle versendet. Dies ist der Fall, wenn ein Anwender das falsche Passwort verwendet (z.B. Tippfehler bzw. Fehlversuche). Darüber hinaus muss berücksichtigt werden, dass die gängigen SIP-Clients nach drei erfolglosen Anmeldeversuchen eine Anwenderinteraktion zur Eingabe des Passwortes erfordern, so dass nicht mehr als 10 SIP-Pakete innerhalb von 10 Sekunden versendet werden.

Für die Honeynet-Umgebung wurde eine Regel definiert, die innerhalb von 60 Sekunden 100 SIP-Pakete pro Nebenstelle voraussetzt, damit die Last der Sensoren an den verschiedenen Standorten gering gehalten wird. Der Wert von 100 REGISTER-Nachrichten wurde als Schwellenwert zur Reduzierung der Reports gewählt. So würde z.B. bei einem niedrigeren Schwellenwert von beispielsweise 10 Fehlversuchen nach 10 REGISTER-Paketen an eine Nebenstelle jeweils ein Report generiert werden. Daraus würde für einen umfangreichen Registration Hijacking-Angriff mit z.B. einer Millionen SIP-Paketen ein Versand von 100.000 Reports resultieren. In der aktuellen Sensorimplementierung können die Schwellenwerte feingranularer gewählt werden. Außerdem wird das Problem der zahlreichen Reports durch die Funktion RepCount eingeschränkt. Zu Beginn des Feldversuches war diese Funktion jedoch noch nicht verfügbar. Um eine Vergleichbarkeit der Ergebnisse zu gewährleisten, wurden die bestehenden Regeln nicht geändert.

False Positives sind bei der verwendeten Signatur nicht zu erwarten, da der Schwellenwert deutlich über den gescheiterten Anmeldeversuchen von Endanwendern liegt. Im nachfolgenden Kapitel werden die beschriebenen Regeln in einem Feldversuch eingesetzt und in Hinblick auf die Angriffserkennung analysiert (False Negatives).

6.4.2 Ergebnisse des Feldversuchs am Standort Essen

Für die Evaluierung der Sensorfunktionalität wurden die Ergebnisse der Angriffserkennung des STRs (siehe Kapitel 5.2) und des Sensor Central Service (SCS) (siehe Kapitel 5.3.3) miteinander verglichen. Es wurden die Daten des Feldversuches von September 2013 bis März 2014 am Standort Essen verwendet. Da bei abweichenden Ergebnissen eine manuelle Analyse der Messdaten erforderlich war, wurden drei Messzeiträume (siehe Tabelle 16) mit einer Dauer von sieben Tagen ausgewählt, die unterschiedlich starke Angriffsintensitäten aufwiesen.

Das Ziel dieser Evaluierung ist die Beurteilung der Angriffserkennung auf Basis der definierten Signaturen für die Angriffsstufen Server Scan, Extension Scan und Registration Hijacking. Dabei liegt der Fokus auf der Fragestellung, welche Angriffe nicht erkannt wurden (False Negatives) und inwieweit diese nicht von dem Regelsatz erfasst wurden. Damit die Erkennung der Angriffsstufen möglichst feingranular erfolgt, wurden für die STR-Analysen folgende Annahmen getroffen:

- Server Scan: mindestens zwei OPTIONS-Pakete an mindestens zwei Hosts
- Extension Scan: mindestens zwei REGISTER-Pakete an mindestens zwei unterschiedliche Extensions einer Ziel-IP-Adresse
- Registration Hijacking: mindestens zwei REGISTER-Pakete mit unterschiedlichen Zugangsdaten an die gleiche Nebenstelle eines SIP-Servers

Die Schwellenwerte für die zu vergleichenden Signaturen des Security Sensor Systems entsprechen jenen in Tabelle 15. Darüber hinaus stellt eine manuelle Analyse für die ausgewerteten Zeiträume sicher, dass die automatischen Angriffsauswertungen korrekt

Tabelle 16: Vergleichende Überprüfung der SCS-Angriffserkennung mit STR-Messdaten

Nr	Zeitraum	Server Scan			Extension Scan			Registration Hijacking		
		STR	SCS	%	STR	SCS	%	STR	SCS	%
1	21.-27.10.2013	32	29	91%	6	6	100%	9	9	100%
2	11.-17.11.2013	28	24	86%	18	17	94%	15	14	93%
3	17.-23.02.2014	30	27	90%	22	20	91%	51	43	84%

arbeiten. Tabelle 16 zeigt für drei Zeiträume die Ergebnisse der Angriffsanalysen für STR und SCS getrennt für die drei Angriffsstufen. Die Spalte „%“ gibt an, wie viel Prozent der vom STR erkannten Angriffe auch durch die Sensorsignaturen erkannt wurden.

Die Angriffserkennung erfolgt auf Basis der Quell-IP-Adresse. Zur Sicherstellung der Vergleichbarkeit wird in den aufgeführten Analysezeiträumen nur ein Angriff pro Angreifer und Angriffsstufe gezählt. Führt ein Angreifer z.B. innerhalb des Vergleichszeitraumes am ersten und am letzten Tag einen Server Scan durch, so werden diese beiden Angriffe als ein Angriff gezählt, da die Quell-IP-Adresse und der Angriffstyp identisch sind.

Die manuellen Analysen haben gezeigt, dass die Anzahl der erkannten Angriffe im STR-System für die angegebenen Zeiträume korrekt sind, wenn bei den Server Scans von einzeln auftretenden OPTIONS-Paketen abgesehen wird. Diese einzelnen OPTIONS-Pakete werden weder durch die Sensorsignaturen noch durch den STR als Angriff erfasst, da es sich dabei um reguläre OPTIONS-Anfragen von Softphones handeln kann. Besonders in produktiven Umgebungen ist dieser Effekt daher zunächst unauffällig, jedoch besteht theoretisch die Gefahr, dass ein Botnet für Server Scans eingestetzt wird.

Für die Angriffsstufe Server Scan werden ca. 90% der Angriffe durch die signaturbasierte Erkennung identifiziert. Die False Negatives können durch die manuelle Analyse der SIP-Verkehrsdaten wie folgt begründet werden:

- Es wurden nur zwei OPTIONS-Pakete empfangen, so dass die Mindestpaketanzahl der Signatur nicht erreicht wurde.
- Im Messzeitraum Februar 2014 wurden Angreifer identifiziert, die OPTIONS-Pakete mit einem zeitlichen Abstand von mehr als drei Sekunden sendeten. Hier besteht ein Zusammenhang mit der Weiterentwicklung der Angriffstools (siehe Kapitel 6.3).

Durch eine Anpassung der Mindestpaketanzahl (z.B. >= 2) und der Zeitbedingungen (z.B. zwei SIP-Pakete in 10 Sekunden) in der Signatur Server Scan können die False Negatives weiter minimiert werden.

Bei der Stufe Extension Scan werden über 90% der Angreifer erkannt. Im ersten Messzeitraum sogar 100%. Die False Negatives wurden wie folgt verursacht:

- Bei einem einzelnen Extension Scan-Angriff wurden nur drei Nebenstellen gescannt.
- Die übrigen nicht erkannten Angriffe wurden auf Grund der zeitlichen Bedingungen nicht berücksichtigt, da hier zwischen zwei und 10 Sekunden zwischen den SIP-Paketen lagen.

Da die Signaturen auch in produktiven Umgebungen eingesetzt werden und False Positives vermieden werden sollen, macht eine Senkung der Mindestpaketanzahl auf Grund eines False Negatives für diese Regel keinen Sinn. Eine Erhöhung des zeitlichen Timeouts wäre hingegen folgerichtig, so dass auch die Extension Scan-Angriffe erkannt würden, die bedingt durch neue Werkzeuge (z.B. VaxSipUserAgent) mehr Zeit zwischen den einzelnen SIP-Paketen vergehen lassen.

Die Registration Hijacking-Angriffe wurden in den ersten beiden Zeiträumen zu 100% bzw. 93% erkannt. Bei der dritten Evaluierung fallen hingegen acht False Negatives auf.

Die manuelle Analyse hat gezeigt, dass gegen Ende des Feldversuches durchaus Registration Hijacking-Angriffe mit deutlich geringerer Intensität durchgeführt werden. So wurden Registration Hijacking-Angriffe mit weniger als 100 SIP-Nachrichten in 60 Sekunden durchgeführt. Der niedrigste Wert lag bei 51 REGISTER-Paketen.

Während die bekannten Angriffswerkzeuge wie z.B. SIPvicious weiterhin massive Angriffe mit sehr hohen Paketanzahlen (zwischen 1.000 und 13 Millionen) durchführen, zeigen neue Werkzeuge u.a. ein verändertes Angriffsverhalten unterhalb von 100 REGISTER-Paketen bzw. mit deutlich größeren Zeitabständen zwischen den einzelnen Angriffspaketen.

Da sich gegen Ende des Feldversuches eine Verhaltensänderung bei den Angriffen andeutete und auch die Analysen zu den Angriffswerkzeugen (siehe auch Kapitel 6.3) eine Weiterentwicklung der Angriffe zeigen, sollten die Schwellenwerte der Signaturen in Hinblick auf die Paketanzahl und das Zeitverhalten angepasst werden.

Die Ergebnisse haben gezeigt, dass die Angriffserkennung mit den einfach gehaltenen Regelsätzen gut funktioniert hat (zwischen 84% und 100% Erkennungsrate). Soll die Erkennungsleistung noch weiter optimiert werden, so ist es sinnvoll, zwischen Honeynet- und Produktivumgebungen zu unterscheiden und möglichst feingranulare Schwellenwerte zu wählen, damit eine effektive Erkennung gewährleistet ist und möglichst wenig False Positives / False Negatives generiert werden. Dazu können weitere SIP-Header-Felder berücksichtigt und komplexere Bedingungen in den Signaturen für die Angriffserkennung genutzt werden.

6.4.3 Angriffserkennung an verschiedenen Standorten

Die Ergebnisse der vorausgegangenen Analysen zeigen, dass die SIP-spezifischen Bedrohungen ein globales Problem darstellen. So erfolgen die Angriffe nicht nur regional bei einzelnen SIP-Servern, sondern großflächig und international in den unterschiedlichsten Netzwerken. Durch die Verteilung der Sensoren an verschiedenen Standorten im Internet konnten die Angriffe im SCS korreliert werden. Außerdem konnte erstmalig die Vorgehensweise der Angreifer über Netzwerkgrenzen hinweg beurteilt werden. Mit der nachfolgenden Analyse soll gezeigt werden, dass die Erkennung von Angriffen an verschiedenen Standorten einen Mehrwert für die Abwehr von SIP-basierten Angriffen bietet.

Um die verteilten Angriffe zu visualisieren und die zeitlichen Zusammenhänge darzustellen, wurde beispielhaft für den Monat Januar 2014 eine standortübergreifende Analyse auf Basis der Daten des Security Sensor Systems angefertigt. Von allen Sensorstandorten in Deutschland, Norwegen und China wurden die empfangenen Sensorreports in dem SCS korreliert und bezüglich des Zeitpunktes des Angriffs, des Ortes und des Angriffstyps sortiert. Abbildung 67 zeigt die Auswertung für die sechs Angreifer, die im Januar 2014 die meisten Angriffe durchgeführt haben. Die Balken in der Abbildung geben an, an welchen Tagen des Monats der Angreifer an welchen Standorten identifiziert und welcher Angriffstyp benutzt wurde (orange: Server Scan, blau: Extension Scan, grün: Registration Hijacking). Für die Beurteilung des Scan-Bereiches wird pro Standort auch das Class-A-Netzwerk angegeben. Dadurch kann geklärt werden, ob die Angreifer große Netzbereiche auf- bzw. absteigend oder zufällig überprüfen. Wenn ein Angreifer zu Beginn des Angriffs an einem Tag an mehreren Standorten Aktivität zeigte, so wird die Reihenfolge der angegriffenen Standorte mit einer Ziffer verdeutlicht.

Die Abbildung 67 zeigt, dass nur zwei Angreifer (A1 und A6) die Angriffsstufen eins bis drei durchgeführt haben. Die übrigen Angreifer (A2 bis A5) führten ausschließlich Server Scans durch.

Von dem Angreifer A1 wurden bereits im Dezember 2013 an den norwegischen Standorten Server Scans und Extension Scans erkannt. Am 03.01.2014 begannen die gleichen Angriffsmuster in München und ab dem 14.01.2014 auch in Essen. Während die verschiedenen Angriffsstufen in Essen in einem Zeitraum von zwei Tagen abliefen, lagen diese an norwegischen Standorten über Wochen auseinander. Bei den Registration Hijacking-Angriffen am 20.01.2014 orientierte sich die Angriffsreihenfolge nicht an den Class-A-Netzen. Der Angreifer wurde somit an 11 Standorten in Europa identifiziert, obwohl die Netzbereiche in Hinblick auf das Class-A-Netz weit auseinander liegen (62 bis 217). Der Angreifer zeigte über einen Zeitraum von 32 Tagen Aktivität. Aktuell kann bei den Angriffsversuchen kein einheitliches Schema bezüglich der Reihenfolge der Class-A-Netzwerke erkannt werden.

Auch Angreifer A6 führte an drei Standorten alle drei Angriffsstufen durch, währenddessen an den anderen beiden Standorten nur ein Server Scan erkannt wurde. Bei der Betrachtung

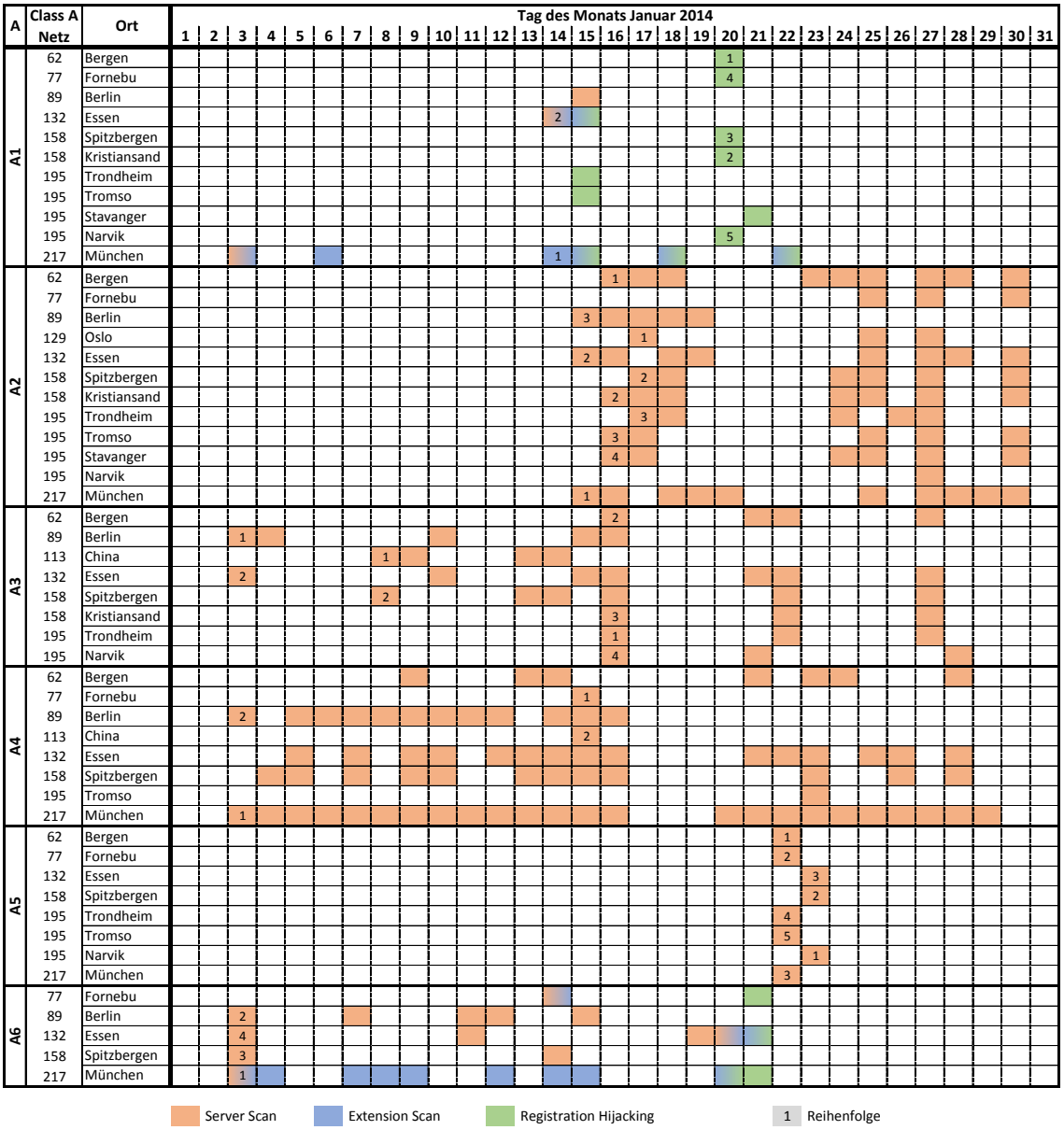


Abbildung 67: Korrelierung der Angriffe mehrerer Standorte im Monat Januar 2014

der Class-A-Netzwerke wird deutlich, dass der Angreifer von hohen zu niedrigen Netzwerken sprang und nicht kontinuierlich auf- bzw. absteigend angriff. Dieser Angreifer war über einen Zeitraum von 17 Tagen aktiv.

Im Gegensatz zu den beschriebenen Angreifern, die alle Angriffsstufen durchführten, deuten die Ergebnisse der forensischen Analysen bereits auf die Existenz von Langzeit-Scannern hin, die das Internet für einen Zeitraum von wenigen Wochen bis zu über einem Jahr nur nach aktiven SIP-Servern durchsuchen (Server Scans).

Von dem Angreifer A2 wurden in der zweiten Monatshälfte umfangreiche Server Scans über 12 Standorte durchgeführt, die zeitlich sehr nah beieinander lagen. So begann der Server Scan an den Standorten München, Essen und Berlin mit einem Abstand von einigen Stunden am 15.01.2014, währenddessen die Angriffe an den norwegischen Standorten einen Tag später begannen. Am ersten Tag scannte der Angreifer die Netzbereiche absteigend und am Folgetag aufsteigend. Die Ergebnisse zeigen jedoch auch, dass nicht das gesamte Internet kontinuierlich systematisch gescannt wurde, da der Angriff an einigen Standorten erst mehrere Tage versetzt stattgefunden hat.

Bei den Angreifern A3 und A4 werden besonders die Langzeit-Scans deutlich, die über den gesamten Monat verteilt an unterschiedlichen Standorten erkannt wurden. Dabei muss hervorgehoben werden, dass die Angreifer viele Netzwerke in Europa sowie ein Netzwerk in China angegriffen haben. Bei der Betrachtung der Reihenfolge der Scan-Versuche zeigt sich, dass diese auf- bzw. absteigend sowie nach einem zufälligen Muster (A3: 16.01.2014) durchgeführt wurden.

Im Gegensatz zu diesen langanhaltenden Scans zeigt sich für den Angreifer A5, dass acht Standorte innerhalb von zwei Tagen angegriffen wurden. Die Reihenfolge der Scans wurde an den beiden Tagen entsprechend variiert.

Diese detaillierte zeitliche Auswertung zeigt deutlich, dass die Angriffe in SIP-Netzwerken ein globales Problem sind und die Angreifer nicht nur einzelne Honeynets angreifen. Weitere Analysen der SCS-Daten haben gezeigt, dass zahlreiche Angreifer pro Monat bis zu 20 verschiedene Honeypots weltweit angriffen und von wenigen Tagen bis hin zu mehreren Monaten aktiv waren. In zukünftigen Analysen sollten die Langzeit-Scanner schwerpunktmäßig beobachtet werden, um eine optimierte Erkennung zu gewährleisten.

Da die Angreifer verschiedene Standorte attackieren, kann durch die zweistufige Echtzeit-Erkennung des Security Sensor Systems sichergestellt werden, dass SIP-Server durch entsprechende Gegenmaßnahmen geschützt werden, sobald von einem oder mehreren Standorten ein potenzieller Angreifer gemeldet wird. Dies wird möglich, da die Angriffe nicht zeitgleich stattfinden und somit der Zeitraum von wenigen Minuten bis zu einigen Stunden genutzt werden kann, um Abwehrkomponenten an anderen Standorten zu benachrichtigen.

Der Fokus dieser Dissertation liegt auf der Analyse und der Erkennung von Angriffen. Die möglichen Ansätze zur Abwehr von Angriffen werden in Kapitel 5.3.7 und in [7] thematisiert.

6.5 Fazit und Empfehlungen

In diesem Kapitel werden die Ergebnisse der Auswertungen zusammengefasst. Außerdem wird das in den Analysen ermittelte Potential der umfangreichen Konzepte aufgezeigt. Das Kapitel schließt mit Empfehlungen für die Nutzung der entwickelten Komponenten für die Analyse und Angriffserkennung in SIP-basierten Netzwerken.

6.5.1 Zusammenfassung der Ergebnisse

Mit der Weiterentwicklung der Single Honeypots zu dem STR-Honeynet mit einer großflächigen, passiven Überwachung wurden Server Scan-Angriffe sichtbar, deren Existenz mit einem einzelnen Honeypot nicht nachweisbar gewesen wären. Die zentrale Datensammlung erlaubt komfortable SQL-basierte Auswertungsmöglichkeiten. Diese haben gezeigt, dass die SIP-spezifischen Bedrohungen zunehmen und dass bereits Weiterentwicklungen bei den Angriffswerkzeugen (z.B. VaxSipUserAgent, Zufalls-UA) zu beobachten sind. Die Angriffe sollen für gängige Netzwerk-Monitoring-Komponenten möglichst verschleiert werden, indem z.B. das User Agent-Feld im SIP-Header mit Zufallswerten belegt wird. Neben den großflächigen IP- und Nebenstellen-Scans sowie umfangreichen Wörterbuchangriffen wird durch die Auswertungen deutlich, dass die gefährlichen Toll Fraud-Angriffe bereits existieren und weiter zunehmen. So werden die kompromittierten Nebenstellen systematisch mit verschiedenen Amtskennzahlen überprüft, um im Anschluss internationale Telefonnummern (z.B. Naher Osten) und Premium-Rufnummern auf Kosten des Serverbetreibers anzurufen.

Bei den Analysetechniken ist das Konzept des Clusterings besonders hervorzuheben, da es für die Erkennung der Angriffsstufen unzureichend ist, SIP-Pakete zu zählen oder einen Mustervergleich bezogen auf ein einzelnes Paket durchzuführen. Nur die Korrelierung der Pakete und die Analyse der SIP-Session erlaubt eine ausreichende Erkennung. Die Anzahl der SIP-Pakete ermöglicht keine Aussage über den Angriffstyp oder über den Erfolg oder Misserfolg eines Angriffs.

Die Weiterentwicklung der Angriffswerkzeuge und die Änderung des Angriffsverhaltens kann durch die Analysen dieser Dissertation belegt werden. So hat sich z.B. die Anzahl der Pakete pro Angriff über den Messzeitraum verändert. Aus den Analysen resultiert, dass eine detaillierte Clustering-Analyse unabhängig von der reinen Paketanzahl unerlässlich ist, da die Paketanzahl keine Auskünfte über die Gefährdungslage gibt. So können z.B. wenige SIP-Pakete zu einem vergleichsweise harmlosen Server Scan gehören oder Toll Fraud-Angriffe bedeuten, die eine bereits kompromittierte Nebenstelle ausnutzen und finanziellen Schaden anrichten.

Die vorherigen Analysen basieren auf der Quell-IP-Adresse. Um auch wechselnde IP-Adressen einem Angreifer zuordnen zu können, wurde das Konzept des dynamischen Honeypots entwickelt. Die Ergebnisse des ersten Feldversuches haben gezeigt, dass die Angreifer-IP-Adresse aktuell während der ersten drei Angriffsstufen jedoch nicht wechselt. Für zukünftige Analysen bietet dieses System neue Möglichkeiten, so dass der Angreifer unabhängig von der Quell-IP-Adresse erkannt werden kann.

Der Vergleich von wenigen STR-Standorten hat gezeigt, dass die identischen Angreifer-IP-Adressen an unterschiedlichen Standorten weltweit identifiziert werden konnten und Langzeit-Scanner in sehr großen Netzbereichen weltweit aktiv waren (wenige Wochen bis hin zu über einem Jahr). Daher ist eine großflächige Überwachung der Angriffsaktivitäten notwendig. Es hat sich gezeigt, dass es sich bei den Honeynet-Ergebnissen nicht nur um lokale Effekte eines einzelnen Netzwerks handelt, sondern dass die Veränderungen im Angriffsverhalten (z.B. neue Angriffswerkzeuge) im zeitlichen Zusammenhang auch an anderen Standorten nachgewiesen werden konnten.

Ein erster Feldversuch des Security Sensor Systems hat die Funktionsweise des Systems bestätigt und eine ressourcenschonende Erkennung an verschiedenen Messstellen ermöglicht. Die bewusst einfach gehaltenen Regelsätze hatten eine gute Erkennungsrate (84% bis 100%). Auf Grund der Konflikte bei der Regeldefinition für Honeynet- und

Produktivumgebungen müssen für eine Optimierung der Erkennungsleistung differenzierte Signaturen erstellt und an zukünftige Angriffsmuster angepasst werden.

Weiterhin konnten die Ergebnisse der forensischen Untersuchungen in Hinblick auf die weltweit verteilten Angriffe bestätigt werden. Es konnte gezeigt werden, dass die verschiedenen Angriffsstufen parallel bzw. innerhalb von wenigen Tagen bis hin zu einem Zeitraum von einem Monat an bis zu 12 Messstellen durchgeführt wurden, obwohl diese bezogen auf die Class-A-Netzwerke nicht immer benachbart lagen. Die verteilte Angriffserkennung in Echtzeit zeigte in dem Feldversuch ein großes Potential für Schutzmaßnahmen, da Angriffe frühzeitig erkannt und noch nicht betroffene Systeme rechtzeitig benachrichtigt werden können.

Die vorgestellten Ergebnisse bestätigen, dass die für diese Dissertation entwickelten Komponenten in einem Feldversuch erfolgreich getestet und dass schon während der ersten Versuchsreihe wichtige Erkenntnisse gewonnen werden konnten.

6.5.2 Empfehlungen

In dieser Dissertation liegt der Fokus auf den Konzepten und den Werkzeugen für die Analyse und die Erkennung von Angriffen. Daher wurden auf Grundlage der forensischen Analysen die entwickelten Komponenten in einem ersten Feldversuch getestet. In Abhängigkeit von dem Einsatzzweck muss das richtige Werkzeug gewählt werden. So wird zwischen der Analyse bzw. dem Verstehen der Angriffe und der automatisierten verteilten Angriffserkennung unterschieden. Für zukünftige Arbeiten können die einzelnen Werkzeuge je nach gewünschtem Ziel verwendet werden.

Da gezeigt wurde, dass sich die Angriffe stetig weiterentwickeln, ist eine kontinuierliche Analyse des Angriffsverhaltens mit einem STR-Honeynet zur Optimierung von Erkennungssignaturen unerlässlich. Die Analyse darf dabei nicht auf einen einzelnen Host beschränkt sein, damit möglichst alle Effekte der Angriffe sichtbar werden (ausreichend großer Überwachungsbereich). Besonders in produktiven Umgebungen müssen die Schwellenwerte präzise zwischen Normal- und Angriffsverkehr gewählt werden, so dass die Überwachungskomponenten keine Fehlalarme generieren (False Positives). Auf Basis der für diese Dissertation bereitgestellten Regelsätze müssen diese kontinuierlich optimiert werden, indem die aktuelle Bedrohungslage weiterhin detailliert beobachtet wird und die Schwellenwerte angepasst bzw. weitere Parameter hinzugefügt werden.

Durch die detaillierte Analyse des Angriffsverhaltens können, wie in [69] beschrieben, Muster abgeleitet werden, die z.B. für bestimmte Angriffswerkzeuge gültig sind. Darüber hinaus können weitere Header-Felder in die Regelsätze miteinbezogen werden, damit eine höhere Erkennungsrate gewährleistet wird. Zusätzlich können verstärkt die SIP-Responses der SIP-Server bei der Angriffserkennung berücksichtigt werden. Dadurch kann z.B. der Erfolg der Extension Scan- und Registration Hijacking-Angriffe festgestellt werden.

Trotz der Weiterentwicklung der Angriffswerkzeuge bleibt die Anzahl aktuell noch überschaubar, so dass Regelsätze für einzelne Angriffstools aufgestellt werden können, die auf Basis von regulären Ausdrücken das User Agent-Feld im SIP-Header auswerten (z.B. Zufalls-User Agent mit acht wechselnden großen und kleinen Buchstaben). Für die Erkennung von Bot-Netzen hingegen kann eine Signatur sinnvoll sein, die einzelne OPTIONS-Nachrichten von unterschiedlichen Quell-IP-Adressen zu verschiedenen Ziel-IP-Adressen in einem ausreichend großen Zeitraum berücksichtigt.

Von den Angriffsstufen geht eine unterschiedlich starke Gefährdung aus. So ist z.B. die Bedrohung durch einen Server Scan-Angriff geringer als durch einen Registration Hijacking-Angriff mit nachfolgendem Toll Fraud-Anruf. Daher sollte bei der verteilten

Angriffserkennung das Potential der zweistufigen Analyse im SCS genutzt werden. Zusätzlich sollten die Angriffsmeldungen von unterschiedlichen Standorten korreliert werden. Diese übergeordnete Analyse ermöglicht das Anlegen einer Wissensdatenbank über die erkannten Angreifer und somit eine Einschätzung des Risikos, wenn ein Angreifer bereits an anderen Standorten systematische Scans durchgeführt hat.

Um die Vorteile einer verteilten, zweistufigen Angriffserkennung nutzen zu können, sollten möglichst viele Messstellen im Internet verteilt werden. Die verteilte Angriffserkennung kann optimal für den Schutz von SIP-Servern genutzt werden, indem eine Benachrichtigung durch den SCS erfolgt, sobald ein oder mehrere Standorte von einem Angreifer attackiert wurden. Dabei kann berücksichtigt werden, bei welcher Gefährdungsstufe eine Alarmmeldung versendet wird.

Der Schutz von VoIP-Servern und der Austausch von Alarmmeldungen kann zum Beispiel durch eine Real-time-Blacklist (z.B. eRBL [7]) erfolgen, die potenzielle Angreifer beinhaltet und bei einem Zugriff auf die VoIP-Infrastruktur durch eine Firewall oder einen SIP-Server abgefragt wird. Sobald ein Angreifer eine SIP-Nachricht an ein geschütztes Netzwerk sendet, erfolgt eine Abfrage der Blacklist, ob die anfragende Quell-IP-Adresse bereits als verdächtig gemeldet wurde. Falls ein Eintrag in der Blacklist vorhanden ist, kann in Abhängigkeit von der Gefahreneinstufung eine entsprechende Reaktion erfolgen:

- Verwerfen der OPTIONS-Nachricht und „Verstecken“ des SIP-Servers durch die Nicht-Beantwortung weiterer Nachrichten
- Verändertes Verhalten auf REGISTER-Anfragen, indem nicht existierende Nebenstellen und fehlerhafte Anmeldeversuche mit nur einem SIP-Status-Code beantwortet werden (z.B. „404 NOT FOUND“)
- Verwerfen von mehr als drei REGISTER-Anfragen und Benachrichtigung des Anwenders über einen anderen Kommunikationskanal

7 Zusammenfassung und Ausblick

In diesem Kapitel werden die Arbeiten dieser Dissertation zusammengefasst. Darüber hinaus wird ein Ausblick auf mögliche zukünftige Arbeiten auf diesem Forschungsgebiet gegeben.

7.1 Zusammenfassung

Für diese Dissertation wurden Angriffe auf SIP-basierte Netzwerke analysiert und Konzepte für geeignete Erkennungsmechanismen entwickelt. Dafür wurde der Ansatz der Analyse mit Ködersystemen aufgegriffen. Die in der Literatur vorgefundenen VoIP-Honeypots auf Basis des klassischen Honeynet-Prinzips wurden erweitert, so dass eine zentrale Überwachung und Analyse von größeren Netzwerkbereichen möglich wurde. Durch die passive Anbindung der Monitoring-Komponenten konnten diese auch in produktiven Umgebungen eingesetzt werden, ohne im Fehlerfall Einfluss auf bestehende SIP-Server zu nehmen. Die Datenschutzbestimmungen wurden mit Hilfe der optionalen Anonymisierungsfunktion eingehalten. Die Vorverarbeitung des aufgezeichneten SIP-Verkehrs und die direkte Speicherung in einer SQL-Datenbank ermöglichte automatische Analysen, die über eine Management-Website sofort abrufbar sind.

Ein weiterer wichtiger Schritt war die Abkehr von einfachen statistischen Analysen auf Basis einzelner SIP-Pakete. Der neue Clustering-Ansatz korreliert die SIP-Pakete und berücksichtigt somit die Kommunikationsverbindung (SIP-Session). Dies ermöglichte eine Auswertung nach den einzelnen Angriffsstufen (Server Scan, Extension Scan, Registration Hijacking und Toll Fraud) unabhängig von der Paketanzahl.

Während der mehrjährigen Untersuchungen war zu beobachten, dass Angreifer die ersten drei Angriffsstufen von der gleichen Quell-IP-Adresse ausführten, die eigentlichen Toll Fraud-Angriffe jedoch oftmals von einer anderen IP-Adresse ohne vorausgegangene Scans erfolgten. Durch das entwickelte Konzept des dynamischen Honeypots konnte nachvollzogen werden, dass Daten über kompromittierte Nebenstellen zwischen den Angreifern weitergegeben wurden. Die Neuerung bestand darin, dass die Angreifer in diesem Honeypot-System unabhängig von der Quell-IP-Adresse erkannt werden konnten. Über die Zuordnung einer Nebenstelle zu einem Angreifer und die Berücksichtigung der von dem Angreifer verwendeten Zugangsdaten wurde somit eine spätere Identifizierung möglich.

Auf Grund der vollständigen SIP-Datenaufzeichnung mit hohem Ressourcenaufwand war es äußerst schwer, Kooperationspartner von dem Einsatz des STR-Monitoring-Systems inkl. Honeynet zu überzeugen und somit Messdaten von unterschiedlichen Standorten zu erhalten. Da es sich bei den Angriffen in SIP-basierten Netzwerken jedoch um ein globales Problem im gesamten Internet handelt, war eine Erkennung an verschiedenen Standorten notwendig.

Daher wurde für diese Dissertation das Konzept des Security Sensor Systems entwickelt, das eine verteilte, signaturbasierte Angriffserkennung in Echtzeit ermöglicht. Leichtgewichtige Sensoren konnten somit in unterschiedlichsten Umgebungen unter Berücksichtigung des Datenschutzes verteilt und in Betrieb genommen werden. Die Erkennung der Angriffe basierte auf vordefinierten Signaturen, die aus den forensischen Analysen abgeleitet und in eine XML-basierte Beschreibungssprache überführt wurden.

Dabei wurde der SIP-Normalverkehr in produktiven Umgebungen beachtet, so dass False Positives minimiert werden konnten. Die erkannten Angriffe (Zutreffen der Signatur) wurden automatisch an den Zentraldienst am Standort Essen gemeldet und konnten daher untereinander korreliert und im Angriffsfall für die Benachrichtigungen der Abwehrkomponenten genutzt werden. Dieser Lösungsansatz ist auch im Rahmen des BMBF-Projektes SUNSHINE [7] gefördert worden.

Für die vorgestellten Konzepte wurde eine umfangreiche Werkzeugsammlung entwickelt, die die Basis für die durchgeführten Analysen darstellte. Für die forensischen Offline-Untersuchungen kam der SIP Trace Recorder mit den entwickelten High Interaction Honeypots zum Einsatz. Das Security Sensor System wurde in einem ersten Feldtest für die Echtzeit-Erkennung von SIP-basierten Angriffen bei verschiedenen Kooperationspartnern verwendet.

Die Ergebnisse des Feldversuches in dieser Dissertation zeigen, dass die Bedrohungen für die SIP-Infrastruktur ansteigen und dass bereits eine Weiterentwicklung und Optimierung der Angriffswerkzeuge nachzuweisen ist. Die zunehmende Anzahl der Toll Fraud-Versuche mit internationalen Anrufzielen (und auch zu Premium-Rufnummern) verdeutlicht, dass bei einem unzureichenden Schutz der SIP-Server für die Nutzer und Betreiber sehr schnell ein erheblicher finanzieller Schaden entstehen kann. Es ist daher unerlässlich, die vorgeschalteten, systematischen Angriffsstufen frühzeitig zu erkennen und Abwehrkomponenten zu benachrichtigen.

Die aufgezeigten Änderungen im Angriffsverhalten während des Feldtests zeigen, dass die Angriffsmuster weiterhin analysiert und die Regelsätze für die Sensoren bei Bedarf aktualisiert und verfeinert werden müssen. Weiterhin muss beachtet werden, dass das alleinige Zählen von SIP-Paketen nicht ausreichend ist, da so keine Aussage zu den Angriffen und der Gefährdungslage getroffen werden kann. Es hat sich gezeigt, dass die Korrelierung der SIP-Pakete mit Hilfe der Sensor-Signaturen nur eine geringe False Negative-Rate aufweist und somit sehr gut für die Erkennung von SIP-spezifischen Angriffen geeignet ist.

Der Vergleich der verschiedenen Messstellen belegt, dass die analysierten Angriffsmuster nicht nur im Netzwerk der Universität Duisburg-Essen, sondern zeitlich zusammenhängend auch an anderen Standorten auftraten. Dadurch wird deutlich, dass die ermittelten Ergebnisse auch für andere Netzwerke gültig sind und dass die Toll Fraud-Problematik bereits für alle Betreiber von SIP-Servern relevant ist. Da die im Sensor Central Service eingegangenen Sensorreports auf Basis der SCS-Regelsätze korreliert werden, kann ein SIP-Server frühzeitig vor einem Angriff geschützt werden, wenn z.B. an einem anderen Standort bereits Scans auf die VoIP-Infrastruktur ablaufen. Die erfolgreiche Interaktion mit Abwehrkomponenten konnte während des BMBF-Projektes SUNSHINE demonstriert werden.

7.2 Ausblick

Der Fokus dieser Dissertation lag auf der Entwicklung von Konzepten und Werkzeugen für die Analyse und Erkennung von Angriffen. Nachfolgend soll ein Ausblick auf weitere mögliche Forschungsarbeiten gegeben werden, die die entwickelten Werkzeuge und Konzepte aufgreifen.

In einem Feldversuch für diese Dissertation wurde das Sensor-System mit vergleichsweise einfachen Regelsätzen erfolgreich evaluiert und gezeigt, dass das System für die verteilte Angriffserkennung geeignet ist. Zum Ende des Feldversuches konnten monatlich einzelne OPTIONS-Pakete von unterschiedlichen Quell-IP-Adressen beobachtet werden. Dies kann ein Hinweis auf Angriffe mit einem Bot-Netz sein, jedoch war ein Nachweis im Rahmen

dieser Dissertation auf Grund des sporadischen Auftretens nicht möglich. Bei zukünftigen Arbeiten auf diesem Forschungsgebiet sollte dieser Aspekt weiterhin verfolgt werden. Außerdem sollten entsprechende Regelsätze definiert werden, da sich das Angriffsverhalten nachweislich über den Beobachtungszeitraum verändert hat. Mit Hilfe des entwickelten STR-Honeynets kann das Angreiferverhalten weiterhin beobachtet und zu einem späteren Zeitpunkt, neben den automatischen Auswertungen, detailliert analysiert werden. Anhand der Ergebnisse können neue Signaturen entwickelt werden, die weitere SIP-Header-Werte (z.B. User Agent, Call-ID) und Bedingungen (z.B. verschiedene Quell-IP-Adressen für die Bot-Netz-Erkennung) beinhalten, um eine optimale Erkennung zu gewährleisten.

Die in dieser Dissertation entwickelten Mechanismen für die verteilte Angriffserkennung können für einen zukünftigen groß angelegten Feldversuch mit möglichst vielen verteilten Messstellen im Internet genutzt werden. Dabei sollten speziell die Zusammenhänge zwischen den Angriffen weltweit analysiert und die SCS-Regeln zur Korrelierung der verteilten Angriffe genutzt und weiterentwickelt werden. Dadurch kann geprüft werden, welche Angreifer welche Angriffsstufen an welchen Standorten durchgeführt haben. In Abhängigkeit von der Bedrohungslage kann dann eine entsprechende Reaktion veranlasst werden.

Ein weiterer wichtiger Schritt zum Schutz vor SIP-basierten Angriffen ist die Entwicklung geeigneter Abwehrkomponenten, die über die vorhandene und getestete Schnittstelle an den SCS angebunden werden können. Da die Angriffe in Echtzeit erkannt werden, müssen die Schutzkomponenten entsprechend schnell benachrichtigt werden. Dabei ist eine dynamische und individuelle Abwehr essentiell, da das dauerhafte Blockieren einer Angreifer-IP-Adresse wegen wechselnder Quell-IP-Adressen (z.B. DHCP-Adresszuweisung durch den Provider bzw. NAT-Router mit mehreren Anwendern) keinen Sinn machen würde. Die Abwehrkomponenten können dem VoIP-Server vorgeschaltet sein (z.B. eine gesteuerte Firewall) oder alternativ bei einem erkannten Angreifer intern ein anderes Verhalten des SIP-Servers auslösen (z.B. temporär keine Reaktion auf eingehende Registrierungsanfragen von einer bestimmten IP-Adresse oder für eine bestimmte Nebenstelle). An dieser Stelle sind feingranulare Techniken notwendig, die die SIP-Kommunikation berücksichtigen und zum Beispiel einzelne Nebenstellen temporär schützen bzw. über andere Kommunikationswege den Endanwender informieren (z.B. SMS, E-Mail).

Literatur

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley und E. Schooler, *RFC 3261-SIP: Session initiation protocol,* 2002.

[2] D. Hoffstadt, A. Marold und E. Rathgeb, „Analysis of SIP-Based Threats Using a VoIP Honeynet System," in *Conference proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-2012)*, Liverpool, 2012.

[3] Digium, „Asterisk.org," [Online]. Available: http://www.asterisk.org. [Zugriff am 10 2014].

[4] D. Hoffstadt, S. Monhof und E. P. Rathgeb, „SIP Trace Recorder: Monitor and Analysis Tool for threats in SIP-based networks," in *TRaffic Analysis and Classification Workshop (IWCMC2012-TRAC)*, Limassol, 2012.

[5] D. Hoffstadt, N. Wolff, S. Monhof und E. Rathgeb, „Improved detection and correlation of multi-stage VoIP attack patterns by using a Dynamic Honeynet System," in *IEEE International Conference on Communications (ICC)*, Budapest, Hungary, 2013.

[6] A. Aziz, D. Hoffstadt, E. Rathgeb und T. Dreibholz, „A Distributed Infrastructure to Analyse SIP Attacks in the Internet," in *IFIP Networking 2014 Conference*, Trondheim, Norway, 2014.

[7] D. Hoffstadt, E. Rathgeb, M. Liebig, R. Meister, Y. Rebahi und T. Q. Thanh, „A comprehensive framework for detecting and preventing VoIP fraud and misuse," in *International Conference on Computing, Networking and Communications (ICNC)*, Honolulu, HI, USA, 2014.

[8] „NorNet - A Real-World, Large-Scale Multi-Homing Testbed," [Online]. Available: https://www.nntb.no/. [Zugriff am 10 2014].

[9] E. T. S. I. (ETSI), „Next Generation Networks," [Online]. Available: http://www.etsi.org/technologies-clusters/technologies/next-generation-networks. [Zugriff am 10 2014].

[10] 3GPP, „UMTS," [Online]. Available: http://www.3gpp.org/technologies/keywords-acronyms/103-umts. [Zugriff am 10 2014].

[11] 3GPP, „LTE," [Online]. Available: http://www.3gpp.org/technologies/keywords-acronyms/98-lte. [Zugriff am 10 2014].

[12] ITU-T, „H.323 : Packet-based multimedia communications systems," [Online]. Available: https://www.itu.int/rec/T-REC-H.323/e. [Zugriff am 10 2014].

[13] ITU-T, „H.320 : Narrow-band visual telephone systems and terminal equipment," [Online]. Available: https://www.itu.int/rec/T-REC-H.320/en. [Zugriff am 10 2014].

[14] IETF, „RFC2616: Hypertext Transfer Protocol," [Online]. Available: https://www.ietf.org/rfc/rfc2616.txt. [Zugriff am 10 2014].

[15] IETF, „RFC3550: RTP: A Transport Protocol for Real-Time Applications," [Online]. Available: http://tools.ietf.org/html/rfc3550. [Zugriff am 10 2014].

[16] J. Rosenberg und H. Schulzrinne, „RFC 3262: Reliability of Provisional Responses in the Session Initiation Protocol (SIP),“ [Online]. Available: https://www.ietf.org/rfc/rfc3262.txt. [Zugriff am 10 2014].

[17] J. Rosenberg und H. Schulzrinne, „RFC 3263: Session Initiation Protocol (SIP): Locating SIP Servers,“ [Online]. Available: https://www.ietf.org/rfc/rfc3263.txt. [Zugriff am 10 2014].

[18] J. Rosenberg und H. Schulzrinne, „RFC 3264: An Offer/Answer Model with the Session Description Protocol (SDP),“ [Online]. Available: https://www.ietf.org/rfc/rfc3264.txt. [Zugriff am 10 2014].

[19] A. B. Roach, „RFC 3265: Session Initiation Protocol (SIP)-Specific Event Notification,“ [Online]. Available: https://www.ietf.org/rfc/rfc3265.txt. [Zugriff am 10 2014].

[20] M. Handley, E. Schooler, J. Rosenberg und H. Schulzrinne, „RFC 2543: SIP: Session Initiation Protocol,“ [Online]. Available: https://www.ietf.org/rfc/rfc2543.txt. [Zugriff am 10 2014].

[21] IETF, „RFC4566: SDP: Session Description Protocol,“ [Online]. Available: http://tools.ietf.org/html/rfc4566. [Zugriff am 10 2014].

[22] „The Honeynet Project: Know Your Enemy,“ [Online]. Available: https://www.honeynet.org/papers. [Zugriff am 10 2014].

[23] I. Mokube und M. Adams, „Honeypots: Concepts, Approaches and Challenges,“ in *AVM-SE 45 Proceedings of the 45th annual southeast regional conference*, Winston-Salem, USA, 2007.

[24] N. Provos, „Developments of the Honeyd Virtual Honeypot,“ [Online]. Available: http://www.honeyd.org/. [Zugriff am 10 2014].

[25] „Dionaea Honeypot,“ [Online]. Available: http://dionaea.carnivore.it/. [Zugriff am 10 2014].

[26] P. S. Foundation, „Python,“ [Online]. Available: http://www.python.org/. [Zugriff am 10 2014].

[27] F. Audet, „RFC 5630: The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP),“ [Online]. Available: http://tools.ietf.org/html/rfc5630. [Zugriff am 10 2014].

[28] M. Spencer, B. Capouch, E. Guy, Ed., F. Miller und K. Shumard, „IAX: Inter-Asterisk eXchange Version 2,“ [Online]. Available: https://tools.ietf.org/html/rfc5456. [Zugriff am 10 2014].

[29] freeswitch.org, „Cross-Platform Scalable FREE Multi-Protocol Soft Switch,“ [Online]. Available: https://freeswitch.org/. [Zugriff am 10 2014].

[30] Yate, „Yet Another Telephony Engine,“ [Online]. Available: http://www.yate.ro. [Zugriff am 10 2014].

[31] „Sipvicious,“ [Online]. Available: http://blog.sipvicious.org. [Zugriff am 10 2014].

[32] „VMware vSphere Hypervisor (Bare-Metal-Hypervisor),“ VMware, [Online]. Available: http://www.vmware.com/de/products/vsphere-hypervisor. [Zugriff am 10 2014].

[33] A. Adelsbach, A. Alkassar, K.-H. Garbe, M. Luzaic, M. Manulis, E. Scherer, J. Schwenk und E. Siemens, VoIPSEC - Studie zur Sicherheit von Voice over Internet Protocol, Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2005.

[34] ITU-T, „Call detail recording, ITU-T Recommendation Q.825," [Online]. Available: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=Q.825. [Zugriff am 10 2014].

[35] Cisco, „Session Border Controller," [Online]. Available: http://www.cisco.com/c/en/us/td/docs/net_mgmt/active_network_abstraction/3-7/reference/guide/ANARefGuide37/sbc.html. [Zugriff am 10 2014].

[36] S. Ehlert, Denial-of-Service Detection and Mitigation for SIP Communication Networks, PhD Thesis, 2009.

[37] M. Nassar, S. Niccolini, R. State und T. Ewald, „Holistic VoIP Intrusion Detection and Prevention System," in *Proceedings of the 1st international conference on Principles, systems & applications of IP telecommunications*, New York, 2007.

[38] M. Nassar, R. State und O. Festor, „VoIP Honeypot Architecture," in *10th IFIP/IEEE International Symposium on Integrated Network Management*, Munich, 2007.

[39] C. Valli, „An Analysis of Malfeasant Activity Directed at a VoIP Honeypot," in *Proceedings of the 8th Australian Digital Forensics Conference*, Perth, 2010.

[40] Y.-S. Wu, S. Bagchi, S. Garg, N. Singh und T. Tsai, „SCIDIVE: A Stateful and Cross Protocol Intrusion Detection Architecture for Voice-over-IP Environments," in *Proceedings of the 2004 International Conference on Dependable Systems and Networks*, Washington, DC, USA, 2004.

[41] „Snort," Sourcefire, [Online]. Available: http://www.snort.org/. [Zugriff am 10 2014].

[42] „Bro Network Security Monitor," [Online]. Available: http://www.bro-ids.org. [Zugriff am 12 2011].

[43] M. Gruber, F. Fankhauser, S. Taber, C. Schanes und T. Grechenig, „Trapping and analyzing malicious VoIP traffic using a honeynet approach," in *Internet Technology and Secured Transactions (ICITST)*, Abu Dhabi, UAE, 2011.

[44] M. Gruber, F. Fankhauser, S. Taber, C. Schanes und T. Grechenig, „Security Status of VoIP Based on the Observation of Real-World Attacks on a Honeynet," in *Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Inernational Conference on Social Computing (SocialCom)*, Boston, USA, 2011.

[45] M. Gruber, C. Schanes, F. Fankhauser und T. Grechenig, „Voice calls for free: How the black market establishes free phone calls - Trapped and uncovered by a VoIP honeynet," in *Eleventh Annual Conference on Privacy, Security and Trust (PST)*, Tarragona, Spain, 2013.

[46] J. Safarik, M. Voznak, F. Rezac, P. Partilal und K. Tomala, „Automatic analysis of attack data from distributed honeypot network," in *Proceedings of the SPIE*, 2013.

[47] A. Dainotti, A. King, K. Claffy, F. Papale und A. Pescapè, „Analysis of a "/0" Stealth Scan from a Botnet," in *ACM SIGCOMM Internet Measurement Conference 2012*, Boston, Massachusetts, USA, 2012.

[48] IETF, „Cisco Systems NetFlow Services Export Version 9," [Online]. Available: http://www.ietf.org/rfc/rfc3954.txt. [Zugriff am 10 2014].

[49] „Tcpdump,“ [Online]. Available: http://www.tcpdump.org. [Zugriff am 12 2011].

[50] „WinPcap,“ [Online]. Available: http://www.winpcap.org. [Zugriff am 12 2011].

[51] „Wireshark,“ [Online]. Available: https://www.wireshark.org/. [Zugriff am 10 2014].

[52] „PHP: Hypertext Preprocessor,“ [Online]. Available: http://www.php.net. [Zugriff am 12 2011].

[53] „Extensible Markup Language (XML),“ [Online]. Available: http://www.w3.org/XML/. [Zugriff am 10 2014].

[54] „Java,“ Oracle, [Online]. Available: http://java.com. [Zugriff am 12 2011].

[55] „JNetPcap,“ [Online]. Available: http://jnetpcap.com/. [Zugriff am 10 2014].

[56] „MySQL,“ [Online]. Available: http://www.mysql.com. [Zugriff am 12 2011].

[57] „MaxMind - IP Geolocation and Online Fraud Prevention,“ [Online]. Available: http://www.maxmind.com/app/python. [Zugriff am 10 2014].

[58] I. Free Software Foundation, „GCC, the GNU Compiler Collection,“ [Online]. Available: https://gcc.gnu.org/. [Zugriff am 10 2014].

[59] B. Dawes, D. Abrahams und R. Rivera , „Portable C++ source libraries,“ [Online]. Available: http://www.boost.org/. [Zugriff am 10 2014].

[60] „LibCurl,“ [Online]. Available: http://libcurl.org/. [Zugriff am 10 2014].

[61] R. T. Fielding und R. N. Taylor, „Principled Design of the Modern Web Architecture,“ in *ACM Transactions on Internet Technology (TOIT)*, NY, USA, 2002.

[62] DFN-Verein, „Das Deutsche Forschungsnetz (DFN),“ [Online]. Available: https://www.dfn.de/. [Zugriff am 10 2014].

[63] „Sundayddr,“ [Online]. Available: http://honeynet.org.au/?q=sunday_scanner. [Zugriff am 08 2011].

[64] „Google Charts,“ Google, [Online]. Available: https://developers.google.com/chart/interactive/docs/gallery/geochart. [Zugriff am 10 2014].

[65] „SipCLI,“ Kaplan Bilisim Teknolojileri Yazilim ve Ticaret Ltd., [Online]. Available: http://www.kaplansoft.com/sipcli/.

[66] Counterpath, „Eyebeam VoIP Calling Software,“ [Online]. Available: http://www.counterpath.com/eyebeam/. [Zugriff am 10 2014].

[67] Counterpath, „X-Lite,“ [Online]. Available: http://www.counterpath.com/x-lite/. [Zugriff am 10 2014].

[68] Zoiper.com, „ZoiPer: Free VoIP SIP Softphone,“ [Online]. Available: http://www.zoiper.com/en. [Zugriff am 10 2014].

[69] A. Aziz, D. Hoffstadt, S. Ganz und E. Rathgeb, „Development and Analysis of Generic VoIP Attack Sequences Based on Analysis of Real Attack Traffic,“ in *Trust, Security and Privacy in Computing and Communications (TrustCom)*, Melbourne, VIC, 2013.