11-30-2010

New Approaches to Mitigation of Malicious Traffic in VoIP Networks

Tobi Wulff
University of Canterbury

Ray Hunt
University of Canterbury

Recommended Citation

Wulff, T., & Hunt, R. (2010). New Approaches to Mitigation of Malicious Traffic in VoIP Networks. DOI: https://doi.org/10.4225/75/57b52563cd8b0

DOI: 10.4225/75/57b52563cd8b0
8th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 30th November 2010

New Approaches to Mitigation of Malicious Traffic in VoIP Networks

Tobi Wulff and Ray Hunt
Computer Security and Forensics Group
Department of Computer Science and Software Engineering
University of Canterbury
Christchurch, New Zealand
tobi.wulff@canterbury.ac.nz
ray.hunt@canterbury.ac.nz

Abstract

Voice over IP (VoIP) telephony is becoming widespread in use, and is often integrated into computer networks. Because of this, malicious software threatens VoIP systems in the same way that traditional computer systems have been attacked by viruses, worms, and other automated agents. VoIP networks are a challenge to secure against such malware as much of the network intelligence is focused on the edge devices and access environment. This paper describes the design and implementation of a novel VoIP security architecture in which evaluation of, and mitigation against, malicious traffic is demonstrated by the use of virtual machines to emulate vulnerable clients and servers through the use of apparent attack vectors. This new architecture, which is part of an ongoing research project, establishes interaction between the VoIP backend and the end users, thus providing information about ongoing and unknown attacks to users.

Keywords

Voice over IP (VoIP), Session Initiation Protocol (SIP), Denial of Service (DoS), malware, Intrusion Detection System (IDS), event correlation, security architecture

INTRODUCTION

With the increasing availability of affordable broadband Internet and flatrate plans it is possible to use more applications over the Internet by using IP packet-based communication. In particular use of Internet telephony by way of VoIP and other multimedia applications have evolved rapidly in recent times. However, such new Internet applications have seen parallel developments in the evolution of malware previously not know in analogue telephony. It is therefore important that measures and controls are in place to protect both customers as well as the Internet and telephony service providers from malicious hackers and financially-driven attackers. Internet security reports show that VoIP will become a more interesting target to criminals and malicious hackers. [Center, 2008] states that "Cyber criminals will be drawn to the VoIP medium to engage in voice fraud, data theft and other scams — similar to the problems email has experienced". Recent VoIP security surveys show that flooding and DoS (Denial of Service) attacks are the main threats to telephony systems [Geneiatakis et al., 2005] [Keromytis, 2010] [McGann et al., 2005]. However, manipulation of sessions such as hijacking as well as passive attacks such as eavesdropping can have a significant impact on a person's privacy or a company's trade secrets.

Traditional security architectures often consist of several firewalls and other security mechanisms to prevent attackers from eavesdropping on or penetrating the network. However, TCP/IP packet filtering firewalls have limitations on what they can detect and filter. Stateful inspection and some application level firewalls have the ability to detect attacks from the outside or information leaks from the inside. For example, [Snort, 2010] in combination with an adaptive firewall is one example of an intrusion detection system that can detect and block suspicious patterns in application level network data.

Technologies for securing the VoIP connection from one endpoint to the other are often not feasible because a network of trust has to be established before the communication takes place. Also, certain parts of SIP (Session Initiation Protocol) messages have to remain unencrypted (from an end-to-end perspective, they can always be encrypted between single hops) to enable SIP proxies to carry out relying and redirection. A hop-to-hop encryption can be established using the SSL/TLS protocol [Rescarlo, 2000]. However, it has been shown that man-in-the-middle attacks can be conducted against SSL connections [Soghoian et al., 2010].

Although the use of conventional security measures such as the use of protocol-independent end-to-end encryption or secure protocols such as SRTP (Secure Real Time Protocol) may assist, there are several reasons why such simple and obvious solutions often do not work on large scale networks with many users. These include:

- limitations in processing power at end-devices (hardware phones)
- missing trust model for certificates and keys
- protocol incompatibility resulting from different protocol implementations

This paper proposes a novel security architecture that uses well-known network and computer security methods to detect an attack in one part of the VoIP network and thus improve the protection for clients in the entire network.

Section 2 provides an introduction to VoIP technology. Section 3 of this paper discusses attacks and countermeasures and related work currently used in VoIP networks. Section 4 describes a novel VoIP security architecture and associated tools including the implementation of a VoIP honeypot which is used to retrieve data about the usage and attack rate of VoIP systems. Section 5 discusses expected evaluation and results in terms of performance and improvements in security. Section 6 concludes the paper.

VoIP ARCHITECTURE AND SECURITY

VoIP Architecture

VoIP is based upon an end-to-end system architecture where the intelligence of the network is focused at the edges, thus taking load off the VoIP servers in the core. This has advantages in performance and availability but it can also introduce problems, particularly with respect to the security of the system. In such cases the security is potentially decreased by not having an intelligent network core.

For example where no end-to-end IP layer encryption is in place then:

b. end systems have no knowledge of malicious rerouting that introduces vulnerabilities such as man-in-the-middle attacks
c. where malware attacks the end-user's system, this can result in an entire compromise of the VoIP network and anti-virus and firewall software might well be rendered useless. This is particularly true for root kit infections where a more intelligent network core might provide more security to the network user.

VoIP sessions usually involve several different protocol categories that are all necessary to transport multimedia data from one end of the conversation to the other as shown in Figure 1. These include:

vi. low-level utility protocols that are not specific to VoIP, for example ARP, DHCP, or DNS.
vii. call processing and signaling protocols such as SIP which is used for creating, modifying and terminating sessions with one or more participants. These sessions include multimedia telephone calls and conferences.
viii. media protocols which carry the actual data of the conversation such as audio (voice) and video. The most common example is RTP/UDP.
ix. support protocols for session maintenance. These include RTCP, SDP and NTP

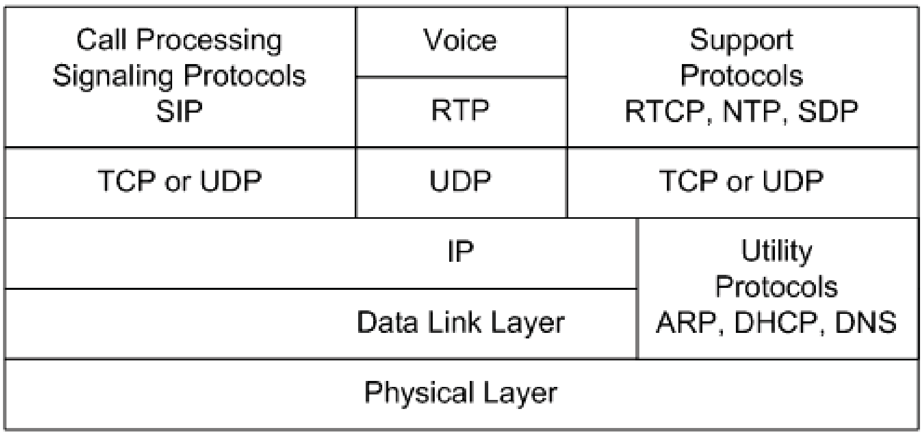

Figure 1: VoIP protocol architecture

Security of VoIP Networks and Applications

VoIP packets are routed in the same manner as other IP-based application traffic on the Internet. For malicious hackers it is easier to intercept or reroute VoIP packets than to tap a traditional phone line because such an attack can be carried out remotely. Because of these security concerns, VoIP traffic should always be encrypted.

Possible attacks and ways to misuse VoIP are [Geneiatakis et al., 2006] [Keromytis, 2010] [McGann et al., 2005]:

- Spit (Spam over Internet telephony)
- Eavesdropping
- Denial of service (DoS) and flooding
- Toll fraud
- Noise injection and malicious traffic

While many approaches to the threat of flooding and DoS attacks have been proposed [Lee et al., 2008], other threats still create significant problems for both consumers as well as service providers. Possible attack vectors at different parts of the VoIP infrastructure are shown in Figure 2.

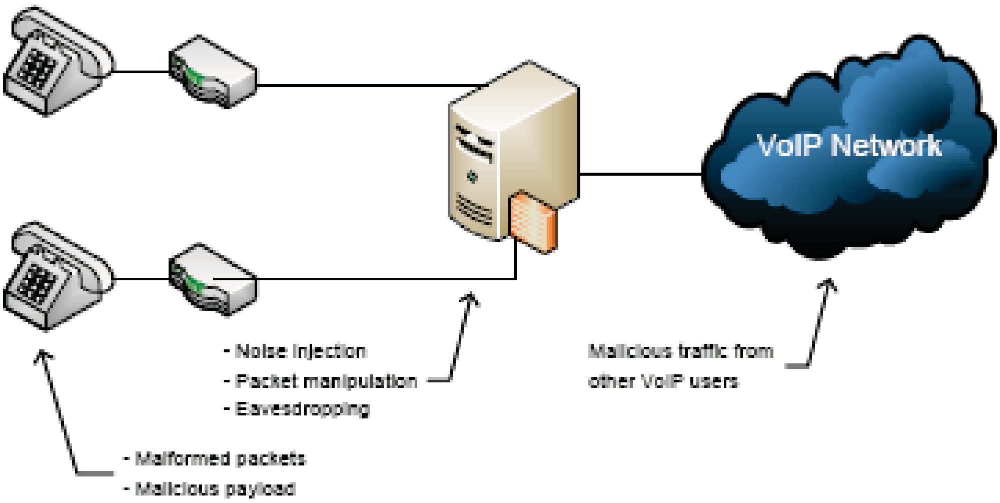

Figure 2: VoIP attack vectors

VoIP networks present significant security challenges since much of the network intelligence is pushed to the edges of the network and thus resides in the end-points, called user agents (UAs). VoIP servers only redirect sessions and assist users to find each other. Often, an established VoIP session does not even have to use these servers and end-users can communicate directly with each other. SIP provides *authentication, integrity, and confidentiality* by relying on existing security mechanisms such as S/MIME (Secure Multipurpose Internet Mail Extensions) which provides public-key encryption and digital signatures [Ramsdell et al., 2010].

To *authenticate* a VoIP user and ensure that the SIP message is generated by a valid UA, a challenge/response dialogue is commonly used. An attacker is still able to change parts of the message without any of the UAs involved noticing. The only part they cannot simply change is the challenge/response. In order to prevent such attacks, further measures are necessary.

Integrity and *confidentiality* can both be achieved using S/MIME. A user can sign a message with their private key so that other users can verify the integrity of the message with the sender's public key. In a very similar way, a user can encrypt a message to other users by using their public keys. It is clear that not all headers of a SIP message can be end-to-end encrypted since proxy servers on the route from one UA to the other may have to analyse and modify certain parts of the SIP header, particularly the first line that contains the address of the next destination.

ATTACKS AND CONTERMEASURES

This section describes several techniques used to exploit flaws in the SIP protocol, the VoIP server software, or the UA software. Additionally, mitigation techniques against these flaws or the resulting attacks are described. Thus the purpose of this section is to provide an overview of what is possible in a SIP-based VoIP environment whether viewed from the attacker's, network administrator's or security expert's perspective.

Common VoIP attacks

Recent Internet security and threat reports [Center, 2008] show that the VoIP attack surface is growing. This is both due to more people using VoIP services as well as more malicious hackers and criminals focusing on attacking these systems.

The Australian chapter of the Honeynet Project deployed VoIP honeypot sensors (called phoneynet) to look for scans and attacks in the Australian address space in 2009 [Reardon, 2009]. Although far less frequent than traditional computer virus and DDoS attacks in the same address space, VoIP scans were detected and results were indicative of the importance of security countermeasures in this area.

Password authentication

Circumventing password authentication using dictionary or brute force attacks will always be possible given a large user base combined with poor security practice. Thus, authenticating clients and servers before the communication commences is not, on its own, a strong method to ensure that only legitimate end-points communicate with each other. It can only provide a basic first step toward a secure architecture.

VoIP Phishing (Vishing)

As with all new technologies it will not take long until criminals discover the potential monetary benefits of social engineering attacks as exemplified by e-mail spam. Even though phishing is not an attack on a computer system itself, it gives the attacker access to it by using social engineering techniques on legitimate users of the VoIP system.

Denial of Service

A Denial of Service (DoS) attack renders the target system useless. This can be achieved in a variety of ways, for example flooding the VoIP network with SIP messages or changing the registration of VoIP phones on the registrar server. The latter can also be used to redirect VoIP traffic to non-legitimate users.

Rogue SIP devices

[Endler and Collier, 2007] demonstrated several ways to insert a rogue SIP UA or server into a VoIP network. To establish these, VoIP UAs have to be tricked into registering to a rogue registrar or redirecting all traffic through a rogue proxy.

Fuzzing

Fuzzing - also known as robustness testing or functional protocol testing [Stallings, 2007]) is a technique used to find software and protocol vulnerabilities. Instead of sending predefined input to a service like a SIP server, traffic is generated according to rules. For example, the Codenomicon SIP test tool [Codenomicon, 2010] comes with 35,000 test cases including INVITE, OPTIONS, and REGISTER SIP messages.

Malicious traffic in the SIP message body

The SIP protocol specification [Rosenberg et al., 2002] only specifies the content of the SIP message line and the SIP headers. The message body on the other hand can contain any arbitrary data. This data can even be encrypted since the SIP message body is only used by the end points of a session. Considering the many different VoIP clients and the variety of features (like sending an image with an INVITE request), it is quite feasible that software bugs enable a malicious hacker to crash the UA or introduce malicious software.

VoIP attack countermeasures

Protocol Improvements
Several protocols exist that are aimed at making VoIP communication secure. The Secure Real-time Transport Protocol (SRTP) uses modern encryption standards to provide "confidentiality, message authentication, and replay protection to the RTP traffic and to the control traffic for RTP" [Baugher et al., 2004].

Attack Countermeasures
[Lee and Hunt, 2008].proposed "a novel method to address the protection necessary to mitigate flooding attacks in VoIP networks" by extending the SIP authentication method and introducing a firewall nonce checking mechanism

Apart from the VoIP protocol improvements mentioned above, mechanisms that protect the users' confidentiality can be installed in other layers of the network stack. For example IPSec can be used as a basic packet transmission infrastructure.

[Thames et al., 2008] outlines a general purpose distributed firewall and response architecture using open-source software. It is a fundamental principle that "once a source IP address has been classified with an anomaly detection mechanism as being untrustworthy, [the architecture has to] deny all access to or from the anomalous host for all members of the trusted domain of administration." We follow this principle and apply it to the special case of a VoIP network.

[Rieck et al., 2008] describes a self-learning intrusion detection system for VoIP systems that can detect SIP traffic such as session setups and tear down messages that deviate from the normal. Another approach to detect whether a stream of data contains telephone voice has been suggested by [Zissman, 1996]. Also, rules to detect some SIP attacks have been published for open-source intrusion detection software such as Snort [Gauci, 2008].

DESIGN OF THE PROPOSED SECURITY ARCHITECTURE

The goal of the VoIP security architecture[12] is to make each user more secure even if attacks and virus infections are in progress. The main idea behind this architecture is collaboration, i.e. servers and clients communicating with each other to increase detection rates of malicious activities. On the end-user side of communication this collaboration can be active or passive. An active collaboration involves specific software that the end-user has to run close to their VoIP equipment in order to collect additional information about malicious activities that the service provider cannot see from their position. In a passive collaboration the user does not have to change the VoIP and network setup and configuration. As shown in Figure 3, reports from end-users are collected in the core of the VoIP network. Then, event correlation provides data for countermeasures that can happen in the core or be pushed back to the users. The Session Border Controller (SBC) is a VoIP application firewall that is installed on the perimeter of the VoIP network. It can be used to deliver additional security features to network users.

Compared to other general purpose architectures that focus mainly on computer systems and attack vectors such as websites or email attachments, our VoIP security architecture examines the use of specific characteristics of VoIP traffic such as SIP and RTP packets. Also, the IDSs and event correlation rules have to be specifically tailored to recognise specific threats as well as the general classes of attacks discussed in Section 2.2.

Active collaboration security software is deployed at the end-user to improve security related communication with the service provider. For example, an IDS is installed at the user's residential gateway to collect accurate information about malicious packets directed at the user or leaving the user's broadband connection.

While all of the inputs from the end-user side shown in Figure 3 can be generated automatically, cases exist where users need to be able to report suspicious activities and VoIP anomalies to the service provider. However, it is crucial that users are not able to alter the VoIP network's behaviour by introducing malicious data.

[12] This architecture is part of an ongoing research project of the Internet Security Research Group at the University of Canterbury, New Zealand.

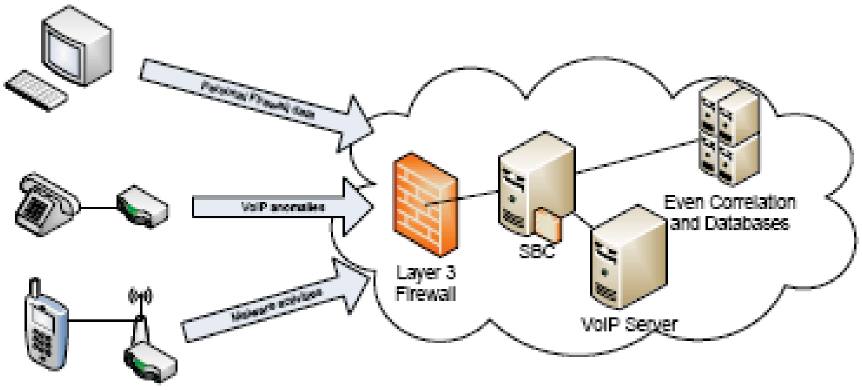

Figure 3: Proposed security architecture

A reporting option for VoIP users can be as simple as pressing a certain number pad key or combination of keys to indicate an incoming malicious call they want to be automatically blocked on the provider side in the future. As soon as enough reports from different users about one particular kind of call are transmitted to the provider, an anomaly detection/event correlation engine can be used to decide whether the VoIP network is in need of protection from this attack. By deploying a host-based private firewall or proxy at the end-user side of the VoIP communication, information about the state of the network and ongoing or previous attacks can be sent back to the service provider. This information can then be used to inform other customers and to improve the security of the system, for example by adding new rules to a firewall.

An effective way to inform users of attacks and vulnerabilities is to use the same communication channel as the threat itself. The reason for this is that no additional form of communication has to be established which can save costs and makes deployment of VoIP much simpler, particularly where many UAs are implemented. SIP can be extended with instant messaging capabilities using the MESSAGE method [Campbell et al., 2002]. On the other hand, a DoS or flooding attack will not only render the VoIP service useless; it can also potentially block the user notification channel.

The key events that are collected by the customer-side IDS in VoIP networks and that are correlated at the service provider side are:

- simultaneous SIP scans against a certain number of users
- brute-force attacks against SIP authentication of several users
- connections from blacklisted IPs/domains
- known malformed packets (Snort rules)
- crashes of UAs or residential gateways and
- other patterns that can be compared to results from the honeypot.

An event correlation engine such as the open-source software SEC can take several of these events and put them in a temporal context [SEC, 2010]. If a certain number of events during a predefined time interval occur, an alarm or a reacting action is triggered as shown in Figure 4.

The following list gives examples of actions taken after certain events affecting several users have been detected. The variable x denotes the number of end-users on the network. This can be changed to adjust the algorithms to the specific network.

1. More than x end-users report a malicious traffic event from the same origin: add origin to blacklist and notify all users.
2. More than x end-users report a crash of their phone's software: add signature to IDS of all users.
3. End-user reports connection attempt from blacklisted IP: "upvote" IP on central blacklist.
4. End-user reports blacklisted malicious data signature: "upvote" signature on central blacklist.
5. More than x end-users manually report a SIP session (a conversation) as spam or malicious: add origin or extracted signature to blacklist and notify all users.

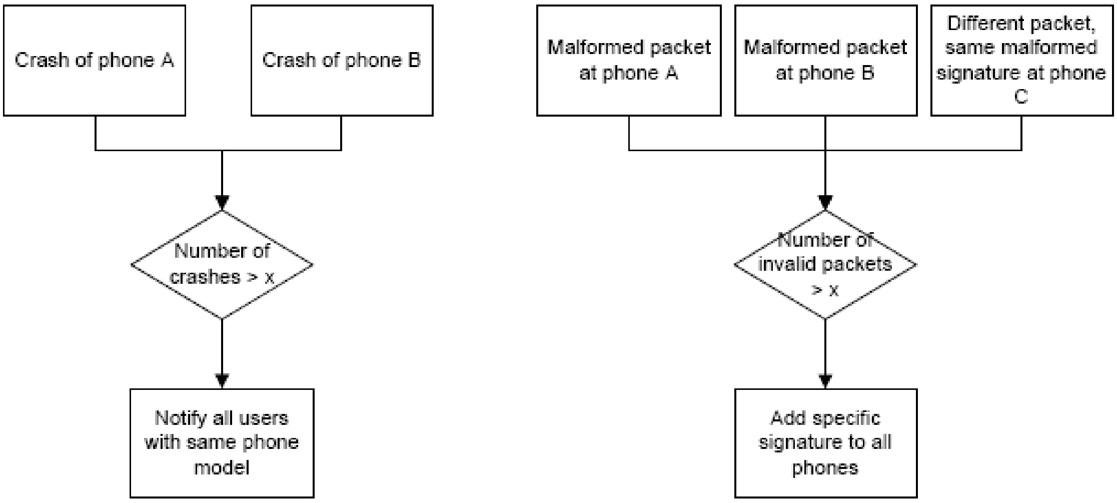
Crash of phone A
Crash of phone B
Number of crashes > x
Notify all users with same phone model
Malformed packet at phone A
Malformed packet at phone B
Different packet, same malformed signature at phone C
Number of invalid packets > x
Add specific signature to all phones

Figure 4: Two event correlation examples

Distribution of new rules and blacklists has to happen in a secure and authenticated way. One way to establish a secure channel from one host to another is the protocol Secure Shell (SSH). OpenSSH is a collection of open-source tools that conduct encrypted and authenticated file transfer.

EXPECTED EXPERIMENTAL RESULTS

In order to determine the usefulness and effectiveness of our implementation of the new architecture, measurements of the security improvements have to be taken in a statistically sound manner. The variables that are being observed and measured are called response variables. The qualitative and quantitative measurements we are going to undertake in the experiments that are part of the ongoing research are described in the following paragraphs.

The propagation time of a worm using a zero-day exploit as well as the percentage of infected systems are good metrics for the effectiveness of the defensive systems and health of a large network. Other useful metrics include the subjective perceived security of each user and the number of malicious connections and data from end-users back to the service provider where it can be measured in a centralised way. Sudden changes in user behaviour [Wang, 2009]) could indicate newly infected VoIP software as regular VoIP data tends to be relatively predictable compared to general network traffic.

Many existing programs and security mechanisms have proven to be suitable for improving network security in VoIP environments. In particular, open-source software is very flexible when it comes to supporting new protocols or implementing new communication paths between several different programs. Snort is able to detect all known attacks as soon as signatures are available. Statistically, it is more likely that another user falls victim to a zero-day exploit in a large network first. As soon as the victim of the attack triggers the distribution of new Snort signature files, all the other users on the network will be safe from this particular attack. SEC has proven to be a solution that is easy to deploy in small networks. However, large enterprise networks often demand additional features such as load-balancing. SEC does not provide these features out-of-the-box but it is feasible to adept it to the requirements of the specific environment.

In order to obtain statistics on the amount of VoIP traffic, both legitimate and malicious, a VoIP module for the low-interaction honeypot Dionaea [Koetter, 2010] has been developed. The intention behind Dionaea is to trap malware exploiting vulnerabilities exposed by services offered to a network, the ultimate goal being to retrieve a copy of the malware.

The VoIP module for Dionaea exposes a SIP server (by default on port 5060) to the network. The module is written in the scripting language Python in order to achieve flexibility and quick development cycles. Dionaea offers a variety of ways to log the actions taken by an attacker: traditional text file logs, logging to an SQLite database which allows flexible and easy querying, and logging to a remote XMPP server. The latter is also used to exchange information and downloaded malware with other honeypots.

The exposed SIP server responds to REGISTER and OPTIONS requests and is able to establish multimedia sessions in response to INVITE requests. Since sophisticated and targeted attacks on VoIP users are not very common yet, the main goal of Dionaea's VoIP module is to analyse the activity of scans and DoS attacks on large networks such as the Internet.

SUMMARY

VoIP communication is an important aspect of many people's and businesses' daily lives and routines. We have described some of the research being carried out on VoIP networks as well as associated Internet threats. Further, we have shown that the amount and quality of attacks against telephony systems is increasing.

We have described the concept of a novel VoIP-specific security architecture. In order to obtain a maximum gain in security while maintaining good performance results, we looked at several methods to implement end-user VoIP IDS and centralised event-correlation engines. Furthermore, we have shown that a combination of end-user (distributed) and centralised systems can achieve better results than stand-alone systems. Due to its use of open-source software, the architecture allows for individual customisation and quick changes.

We still have to test our architecture against VoIP data obtained from real world networks to demonstrate the improvement in security and performance. Also, the results are still preliminary and subject to more measurements and evaluation based on a stronger statistical foundation.

REFERENCES

Baugher M. et al., RFC3711: The Secure Real-Time Transport Protocol (SRTP), 2004. http://tools.ietf.org/html/rfc3711 [Accessed August 2010]

Campbell B. et al., RFC3428: Session Initiation Protocol (SIP) Extension for Instant Messaging, 2002. http://tools.ietf.org/html/rfc3428. [Accessed August 2010]

Center Georgia Tech Information Security, Emerging Cyber Threats Report for 2009 [Journal], 2008.

Codenomicon Test Tools, 2010. http://www.codenomicon.com. [Accessed August 2010]

Endler D. and Collier M., Hacking Exposed VoIP, Cpt 6, McGraw-Hill, 2007.

Gauci S., SIPVicious: Detecting SIP attacks with Snort, 2008. http://webcache.googleusercontent.com/search?q=cache:5QIMR6SyiDQJ:sipvicious.org/blog/2008/02/detecting-sip-attacks-with-snort.html+snort+voip+sip&hl=en&strip=1. [Accessed August 2010]

Geneiatakis D. et al., SIP Security Mechanisms: A state-of-the-art review, Proceedings of the 5th International Network Conference (INC 2005), Samos, Greece, 2005, pp147–155

Geneiatakis D. et al., Survey of Security Vulnerabilities in Session Initiation Protocol, IEEE Communications Surveys & Tutorials, 2006. Vol. 8 No 3, pp.68-81.

Keromytis A. D., Voice-over-IP Security: Research and Practice, IEEE Security & Privacy, Vol. 8 No 2, 2010.

Lee I. and Hunt R., A novel design of a VoIP firewall proxy to mitigate SIP-based flooding attacks, International Journal of Internet Protocol Technology. Vol. 3. No 2, 2008, pp. 128-135.

McGann S and Sicker D., An Analysis of Security Threats and Tools in SIP-Based VoIP Systems, Proceedings of the 2nd Workshop on Securing Voice over IP. - Washington DC, USA , 2005.

Ramsdell B. and Turner S., RFC5751: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2, 2010. http://tools.ietf.org/html/rfc5751. [Accessed August 2010]

Reardon B., VoIP phoneynet: Observations of the VoIP Pilot Thus Far, 2009, http://honeynet.org.au/?q=phoneynet_part2. [Accessed August 2010]

Rescarlo E., SSL and TLS: Designing and Building Secure Systems , Addison Wesley, 2000.

Rieck K et al., A Self-Learning System for Detection of Anomalous SIP Messages, Second International Conference on Principles, Systems and Applications of IP Telecommunications. Services and Security for Next Generation Networks. 2008. pp. 90-106.

Rosenberg J. et al., RFC3261: SIP: Session Initiation Protocol, 2002, http://tools.ietf.org/html/rfc3261. [Accessed August 2010]

SEC SEC - Simple Event Correlator, 2010. http://simple-evcorr.sourceforge.net. [Accessed August 2010]

Snort Home Page Snort, 2010. - http://www.snort.org. [Accessed August 2010]

Soghoian C. and Stamm S., Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL, 2010 [http://papers.ssrn.com]. [Accessed August 2010]

Stallings W., Data and Computer Communications, Chapter 11, Pearson Education Inc., 2007. Vol. 8.

Thames J.L., Abler R. and Keeling D., A distributed firewall and active response architecture providing preemptive protection, ACM-SE '08, 2008. pp220-225.

Wang Yun., Statistical Techniques for Network Security, Chapter 8, Information Science Reference, 2009.

Zissman M., Comparison of four approaches to automatic language identification of telephone speech, IEEE Transactions on Speech and Audio Processing, 1996, Vol. 4. pp31-44.