Armin B. Cremers, Rainer Manthey,
Peter Martini, Volker Steinhage (Hrsg.)

Sicherheit in komplexen, vernetzten Umgebungen

Workshop im Rahmen der Jahrestagung 2005 der Gesellschaft für Informatik
„Informatik LIVE!“

19.-22. September 2005
in Bonn, Deutschland

Gesellschaft für Informatik 2005

Lecture Notes in Informatics (LNI) – Proceedings
Series of the Gesellschaft für Informatik (GI)

Volume P-68

ISBN 3-88579-397-0
ISSN 1617-5468

Volume Editors
Prof. Dr. Armin B. Cremers
Universität Bonn, Institut für Informatik III
Römerstraße 164, D-53117 Bonn
Email: abc@cs.uni-bonn.de
Prof. Dr. Rainer Manthey
Universität Bonn, Institut für Informatik III
Römerstraße 164, D-53117 Bonn
Email: manthey@cs.uni-bonn.de
Prof. Dr. Peter Martini
Universität Bonn, Institut für Informatik IV
Römerstraße 164, D-53117 Bonn
Email: martini@cs.uni-bonn.de
Privatdozent Dr. Volker Steinhage
Universität Bonn, Institut für Informatik III
Römerstraße 164, D-53117 Bonn
Email: steinhage@cs.uni-bonn.de

printed by Köllen Druck+Verlag GmbH, Bonn

Peer-to-Peer Intrusion Detection Systeme für den Schutz sensibler IT-Infrastrukturen

Hartmut König

Brandenburgische Technische Universität Cottbus
LS Rechnernetze und Kommunikationssysteme
PF 10 13 44
03013 Cottbus
koenig@informatik.tu-cottbus.de

Abstract: Peer-to-Peer (P2P) Systeme haben sich zu einer viel versprechenden Alternative für die Gestaltung von Anwendungen im Internet entwickelt. Die zunehmende Dezentralisierung von Intrusion Detection Systemen sowie der verstärkte Einsatz in mobilen Umgebungen legt die Nutzung des Peer-to-Peer-Prinzips auch für Intrusion Detection Systeme nahe. Erste Ansätze zu P2P Intrusion Detection Systemen wurden vorgeschlagen. Diese Arbeiten nutzen aber bei weitem noch nicht das Potential des P2P-Ansatzes aus. In dem Beitrag werden die Vorteile des Peer-to-Peer-Prinzips für das Intrusion Detection diskutiert. Notwendiger Forschungsbedarf wird aufgezeigt.

1 Einleitung

Peer-to-Peer (P2P) Lösungen haben sich zu einer viel versprechenden Alternative für die Gestaltung von Anwendungen im Internet entwickelt. Ihr wesentlicher Vorteil ist es, Anwendungen zu gestalten, die unabhängig von einem spezifischen Service-Provider aufgesetzt werden können. Viele P2P-Anwendungen sind in der Zwischenzeit entstanden, außerdem eine Reihe von Plattformen, z. B. JXTA [Jxta], die die Entwicklung von P2P-Anwendungen unterstützen. Weltweit wird intensiv über die Gestaltung von P2P-Systemen geforscht. Es ist daher nicht verwunderlich, dass P2P-Systeme auch im Bereich des Intrusion Detection/Intrusion Prevention[1] auftauchen [Ja03], [Hu04], [Vl04].

Aus dem Blickwinkel des Intrusion Detection ist dies ebenfalls nicht überraschend, da es letztlich dem Entwicklungstrend von IDS in den letzten beiden Jahrzehnten entspricht. Waren in den 80er Jahren die meisten IDS-Systemansätze noch stark zentralisiert, d. h. durch die Nutzung einer zentralen Analyse- und Erkennungseinheit gekennzeichnet, so wurde in den 90er Jahren zunehmend über Systeme berichtet, die sowohl die Erfassung als auch die Analyse der Daten dezentralisieren, indem sie einen Teil der Auswertungsfunktionalität in die Nähe der Datenerfassung verlagern [Wi96], [Po97], [Er02], [Ho02]. Daraus entstanden auch erste Ansätze maßgeschneiderte Systemlösungen zu entwickeln

[1] Für die folgende Diskussion ist die Unterscheidung zwischen Intrusion Detection und Prevention Systemen nicht relevant. Der Begriff Intrusion Detection wird hier als Oberbegriff verwendet.

[Ho02], die auf die Erfordernisse ihrer jeweiligen Anwendungsumgebung zugeschnitten werden können. Der Schritt zu P2P-IDS ist daher nur logisch. Diese Entwicklung ist aber nicht allein aus Architektur-Überlegungen zu erklären, sondern resultiert aus einem wesentlich verbreiterten Einsatzfeld von IDS in den letzten Jahren. War das primäre Einsatzgebiet für IDS in den ersten beiden Jahrzehnten vor allem der Festnetzbereich, so sind mit dem Aufkommen der drahtlosen Kommunikation auch Wireless Intrusion Detection Systeme (WIDS) zu einem interessanten Einsatzfall geworden. Hier finden insbesondere die mobilen Ad hoc-Netze (MANETs) gegenwärtig große Aufmerksamkeit, da sie im Vergleich zu den klassischen IDS, die sich vorrangig im schwer zugänglichen (und für die Forschung vergleichsweise weniger spannenden) Systemsoftwarebereich bewegen, eine Menge interessanter Fragestellungen aufwerfen. Einer der Gründe für das Interesse an MANET IDS liegt in der Tatsache begründet, dass sie über keine feste Infrastruktur verfügen und ihre Zusammensetzung sich dynamisch ändert [Hu04]. Die Lösung ist daher, die mobilen Knoten mit einer IDS-Funktionalität zu versehen, die für eine kooperative Erkennung von Attacken genutzt wird. Das entspricht dem P2P-Ansatz. Mit dem Entstehen ubiquitärer IT-Infrastrukturen werden solche Lösungen verstärkt benötigt, um den Sicherheitsanforderungen dieser Umgebungen gerecht zu werden.

Die Sinnfälligkeit von P2P IDS-Infrastrukturen begründet sich nicht allein aus den zuvor genannten Entwicklungen. Die zunehmende Verlagerung systeminterner Kommunikation auf das IP-Protokoll, z. B. in Produktionsprozessen, Fahrzeugen, Flugzeugen, Automatisierungssystemen usw. lässt sensible IT-Infrastrukturen entstehen, die stärker anfällig sind für Störungen als das in früheren proprietären Kommunikationslösungen der Fall war. P2P IDS stellen einen möglichen Ansatz dar, die Sicherheit solcher Infrastrukturen aus reaktiver Sicht zu gewährleisten. Da es sich bei den genannten Systemen um verteilte Systeme handelt, bietet sich schon mal a priori ein verteilter IDS-Ansatz an. Weiterhin sind solche Systeme häufig Veränderungen unterworfen, z. B. durch den Einbau neuer Komponenten, durch reparaturbedingten Austausch, durch Updates oder aber durch generelle Veränderungen der Infrastruktur, z. B. bedingt durch Umstellungen im Produktionsablauf. Solche Änderungen implizieren eine Neuinstallation bzw. Reorganisation der Überwachungsinfrastruktur, was aufwendig sein kann und möglicherweise aus Zeitgründen hinten angestellt wird. Selbstorganisierende P2P-Systeme sind hier flexibler und unterstützen eine dynamische Anpassung der Überwachungsinfrastruktur.

2 Vorteile P2P basierter IDS

Wir nehmen im Folgenden eine IDS-Infrastruktur an, die sich aus gleichberechtigten, kooperierenden IDS-Komponenten, den IDS-Peers, zusammensetzt, die über ein Overlay-Netz miteinander kommunizieren. Die interne Struktur der IDS-Peers ist dabei für diese Diskussion nicht relevant. Was wären die Vorteile solcher P2P IDS-Strukturen? Natürlich leiten sich diese primär aus den typischen Vorteilen von P2P-Systemen ab:

- ***Dezentrale Struktur***
  Die IDS-Peers kommunizieren direkt miteinander. Es gibt (zumindest in reinen P2P-Strukturen) keine zentrale Serverkomponente mehr, die zu einem Engpass in der Kommunikation führen kann und einen *Single Point of Failure* darstellt. Auswer-

tungen können in den IDS-Peers ausgeführt werden. Die IDS-Peers verhalten sich kooperativ, d.h., sie stellen ihr Wissen und ihre Auswertungsfunktionalität anderen IDS-Peers zur Verfügung.

- ***Gleichberechtigung der Partner***
  P2P-Systeme lösen das klassische Client/Server-Paradigma auf. Die IDS-Peers sind aktive und gleichberechtigte Partner, die sowohl als Client und Server agieren können. Sie agieren eigenständig und unterliegen nicht mehr einer zentralen Kontrolle. Entscheidungen werden autonom getroffen. Das bedingt allerdings einen höheren Realisierungsaufwand im Vergleich zu zentralisierten Systemen.
- ***Fehlertoleranz***
  Infolge des Fehlens einer zentralen Auswertungseinheit, wird das System toleranter gegenüber dem Ausfall von Komponenten. Sie müssen nicht zu einem vollständigen Zusammenbruch der Überwachung führen. Die Analyse kann (zumindest partiell) von anderen Knoten übernommen werden.
- ***Selbstorganisation***
  IDS-Peers können sich selbständig ohne Vorgabe einer zentralen Autorität zu einem IDS verbinden. Mobile Komponenten können dem System dynamisch beitreten und es bei Ortsveränderung wieder verlassen. Ausfälle und Veränderungen der Überwachungsstruktur adaptieren sich selbständig.
- ***Skalierbarkeit***
  Intrusion Detection Systeme sind nicht mehr in ihrer Größe beschränkt. Sie können jeweils dem Umfang und der Struktur der zu überwachenden Systeme und Anwendungen dynamisch angepasst werden.
- ***Kostenverteilung***
  In einer P2P-Infrastruktur verteilen sich die Kosten für die Erstellung und Wartung der Analysedatenbestände auf die IDS-Peers. Signaturen und Verhaltensprofile müssen nicht unbedingt zentral gepflegt werden. Die aufwendige Erstellung und Aktualisierung dieser Datenbestände kann an verschiedenen Orten von unterschiedlichen Systemadministratoren vorgenommen werden.

3 Notwendiger Forschungsbedarf

Es gibt erste Ansätze für P2P IDS [Vl04], [Ja03], [Hu04], die einzelne Vorteile des P2P nutzen. IDS, die die Möglichkeiten des P2P bewusst in der vollen Breite ausnutzen, sind bis jetzt noch nicht bekannt. Eine Umsetzung des Konzepts in der oben skizzierten Form erfordert noch erheblichen Forschungsbedarf, da zum einen der P2P-Ansatz generell noch in der Entwicklung ist und zum anderen eine 1:1-Umsetzung dieser Konzepte ohne eine Berücksichtigung der spezifischen Aspekte des Intrusion Detection schwierig ist. Wir diskutieren im Folgenden Probleme, die im Kontext der Anwendung des P2P-Prinzips zu lösen sind. Manche der genannten Probleme sind nicht ausschließlich IDS-spezifisch.

- ***Vertrauen***
  In sich selbst organisierenden IDS-Strukturen müssen sich IDS-Peers zueinander finden und Kontakt aufnehmen. Das setzt Vertrauen voraus. Welchem neuen Peer kann ich trauen bzw. kann der Peer dem IDS trauen, dem er beitreten möchte. Ver-

trauen ist dabei nicht nur während der Beitrittsphase erforderlich, sondern auch bei dem Zugriff auf Datenbestände, bei der Weitergabe von Wissen oder der Delegierung von Analysen. Mechanismen, die Vertrauen zwischen den IDS-Peers herstellen, sind eines der zentralen Probleme der Gestaltung von P2P IDS. Das war bisher in den starren IDS-Strukturen weniger erforderlich.

- ***Selbstorganisation***
  Selbstorganisierende IDS sind bisher kaum bekannt. Es sind Prinzipien zu entwickeln, nach denen sich die IDS-Peers zu einem System zusammenfinden und dieses verwalten. Dabei spielen neben Vertrauen solche Aspekte eine Rolle wie die Analysefähigkeit der IDS-Peers, das eingebrachte Wissen (Signaturen, Verhaltensmuster, Auditdaten), und die Rolle, die ein Peer innerhalb der Organisationsstruktur übernehmen soll (siehe unten). Zu den Aspekten der Selbstorganisation hören u.a.:
  Organisationsformen. Traditionelle IDS verfügen über eine ziemlich fest vorgegebene Struktur, die festlegt, welche Komponenten die Analyse durchführen und welche Wege von der Erfassung bis zur Analyse der Auditdaten durchlaufen werden. Solch feste Strukturen und Rollenzuweisungen sind in P2P-IDS nicht zu finden. Andererseits zeigen P2P-Anwendungen wie Gnutella oder Skype, dass es zweckmäßig ist, Peers mit geringerer Leistungsfähigkeit bzw. schmalbandigerer Anbindung zu entlasten und bestimmte Aufgaben Super-Peers bzw. Super-Nodes [Si04] zuzuordnen. P2P-Plattformen wie JXTA verwenden ein noch differenzierteres Rollenspektrum. Es sind also optimale Organisationsstrukturen für P2P IDS zu untersuchen. Entscheidende Kriterien dabei sind die Selbstorganisationsfähigkeit, die Analysefähigkeit und die (Attacken-)Erkennungsfähigkeit. Dies hängt aber auch von den Einsatzszenarien ab. So muss z.B. in einem MANET bei der Einschätzung der Analysefähigkeit auch der Batterieverbrauch miteinbezogen werden [Hu04].
  Delegierung von Analysen. Da in einem P2P IDS selten von einer homogenen Zusammensetzung ausgegangen werden kann, muss eine unterschiedliche Leistungsfähigkeit der IDS-Peers angenommen werden. Dies kann bei weniger leistungsfähigen Peers dazu führen, dass die notwendigen Analysen in Überlastsituationen nicht mehr lokal in den erforderlichen Zeitschranken durchgeführt werden können. Eine P2P-Umgebung bietet die Möglichkeit, Analysen auf andere Knoten zu verlagern, die weniger ausgelastet sind bzw. über das notwendige Wissen verfügen.
  Austausch von Wissen. In einer heterogenen P2P-Umgebung kann davon ausgegangen werden, dass die lokalen IDS-Komponenten über unterschiedliche Analysefähigkeiten verfügen bedingt durch differierende Bestände an Signaturen, Verhaltenswissen oder Protokollszenarien. Eine P2P-Umgebung bietet die Möglichkeit eigenes Wissen bekannt zu machen und das Wissen zwischen Peers abzugleichen.
- ***Gegenmaßnahmen***
  Auch die Frage von Gegenmaßnahmen stellt sich in einem P2P IDS neu. Es müssen Strategien entwickelt werden, wie Gegenmaßnahmen initiiert und koordiniert werden. Das ist natürlich von dem jeweiligen Angriff abhängig. Aber auch spielt die Problematik Vertrauen hier eine wichtige Rolle, um z. B. festzulegen, welcher Peer das Recht erhält, bestimmte Gegenmaßnahmen zu initiieren, die wiederum auch andere Peers betreffen können.
- ***Selbstschutz***
  IDS sind selber ein häufiges Angriffsziel, um die Systemüberwachung auszuschalten. Deshalb ist der Selbstschutz von IDS immer schon ein wichtiges Thema. In ei-

ner P2P-Umgebung erweitern sich die Angriffsmöglichkeiten wesentlich. Geschützt werden müssen sowohl die einzelnen IDS-Peers als auch die Kommunikationsbeziehungen untereinander. Auch wenn für letztere bereits grundsätzlich eine sichere Übertragung benötigt wird, kommt es darauf an Mechanismen zur Abwehr von Angriffen zu entwickeln, in diese Infrastruktur einzudringen. Eine wichtige Rolle in diesem Kontext spielt wieder die Problematik Vertrauen.

4 Schlussbemerkungen

Die P2P-Technologie hat eine Vielzahl neuer, interessanter Anwendungsmöglichkeiten hervorgebracht. Auch im Bereich des Intrusion Detection ist in den nächsten Jahren mit verstärkt mit ihrem Einsatz zu rechnen. Erste Ansätze liegen bereits vor. Die großen Vorteile des P2P-Ansatzes für das Intrusion Detection bestehen in der Dezentralisierung, der Dynamik, der Selbstorganisation und der Skalierbarkeit. Das erlaubt es, auf die relativ aufwendige Entwicklung starrer, dedizierter Systeme zu verzichten und erforderliche Überwachungsstrukturen dynamisch und auf den Einsatzfall zugeschnitten zu generieren. Das wird langfristig auch Kosten reduzieren, da IDS-Komponenten verteilt von mehreren Partnern entwickelt werden können, die sich dann zu einer kooperierenden Struktur zusammenfinden. Der Weg dahin ist jedoch noch weit. Es liegen bisher nur wenige Intrusion-Detection-spezifische Lösungen für die Kooperation bei der Attackenerkennung, den Wissensaustausch und die Selbstorganisation vor. An unserem Lehrstuhl werden gegenwärtig erste Arbeiten zur Entwicklung von P2P IDS durchgeführt. Aufbauend auf einer Implementierung des Ansatzes aus [Ho02] über JXTA werden insbesondere Prinzipien der Selbstorganisation und des Selbstschutzes von P2P IDS untersucht.

Literaturverzeichnis

[Er02] Erbacher R., Walker, K.; Frincke, D.. Intrusion and Misuse Detection in Large-Scale Systems, IEEE Computer Graphics and Applications, 22(2002)1.

[Ho02] Holz, T.; Meier, M.; König, H.: Bausteine für effiziente Intrusion Detection Systeme. PIK 25(2002)3: 144-157.

[Hu04] Huang, Y.; Lee, W.: Attack analysis and detection for ad hoc routing protocols. In Proc. RAID'04, LNCS, Springer, 2004.

[Ja03] Janakiraman, R.; Waldvogel M., Zhang, Q.: Indra: A peer-to-peer approach to network intrusion detection and prevention. In Proceedings of 2003 IEEE WET ICE Workshop on Enterprise Security, Linz, Austria, June 2003.

[Jxta] JXTA-Webseite; http://www.jxta.org

[Po97] Porras, P.A.; Neumann, P.G.: EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances. In Proc. of the 20th National Information Systems Security Conference, Baltimore, USA, Oct. 1997, NIST Gaithersburg, 1997, pp. 353-365.

[Si04] Singh, K.; Schulzrinne, H.: Peer-to-Peer Internet Telephony using SIP. http://www.cs.columbia.edu/~library/TR-repository/reports/reports-2004/

[Vl04] Vlachos, V.; Androutsellis-Theotokis, S.; Spinellis: D.: Security applications of peer-to-peer networks. Computer Networks 45(2):195–205, June 2004.

[Wi96] White, G. B.; Pooch, U. W.: Cooperating security managers: Distributed intrusion detection systems. In Computers&Security 15(1996)5: 441-450.