

Herausforderungen für eine effektive, effiziente und datenschutzgerechte IT-Frühwarnung

Ulrich Flegel und Michael Meier
Universität Dortmund
Fachbereich Informatik, Lehrstuhl 6, Informationssysteme und Sicherheit
44221 Dortmund
Germany

Tel./Fax: +49-231-755-6481/2405
email:{ulrich.flegel, michael.meier}@udo.edu

1 Einleitung

Mit der wachsenden Abhängigkeit unserer Gesellschaft von der Zuverlässigkeit informationstechnischer Systeme (IT) gewinnen Fragen der IT-Sicherheit an Bedeutung. Während bisher vorrangig präventive Maßnahmen und Mechanismen im Vordergrund standen, wird zunehmend deutlich, dass IT-Sicherheit nicht allein durch Prävention erreichbar ist. Vielmehr stellt Prävention einen Grundpfeiler dar, neben dem ergänzend die reaktiven Aspekte der IT-Sicherheit stehen. Voraussetzung für die Reaktion auf Sicherheitsvorfälle ist dabei eine zuverlässige und rechtzeitige Erkennung entsprechender Situationen. Dazu ist ein kooperativer Informationsaustausch zwischen verschiedenen Institutionen nicht nur von Vorteil sondern zur Erkennung koordinierter verteilter Angriffe zwingend erforderlich. Die hierbei ausgetauschten Informationen umfassen Beobachtungen von Aktivitäten, auf deren Grundlage eine Erkennung von IT-Sicherheitsverletzungen erfolgen kann, sowie Erkennungsergebnisse und Informationen zur Reaktion auf erkannte Vorfälle.

Für die Erkennung von Sicherheitsverletzungen (Intrusion Detection) existieren zwei grundlegende Strategien, die *Missbrauchserkennung* bzw. *Signaturanalyse (Misuse Detection)* und die *Anomalieerkennung (Anomaly Detection)*. Erstere untersucht Protokoll- bzw. Audit-Daten nach Mustern bekannter Sicherheitsverletzungen, den Signaturen. Anomalieerkennung untersucht Nutzer- oder Systemaktivitäten auf Abweichungen von vordefinierten oder ermittelten Aktivitätsprofilen und kennzeichnet diese Abweichungen als Sicherheitsverletzungen. Der Vorteil signaturbasierter Verfahren liegt in ihrer höheren Erkennungsgenauigkeit. Anomalieerkennung bietet den Vorteil, unbekannte Sicherheitsverletzungen erkennen zu können, führt aber aufgrund geringer Erkennungsgenauigkeit häufig zu unakzeptablen Fehlalarmraten. Darüber hinaus signalisieren diese Systeme lediglich Anomalien, von denen häufig nicht ohne weiteres auf eine konkrete Sicherheitsverletzung geschlossen werden kann. Daher werden im folgenden Verfahren zur Missbrauchserkennung fokussiert.

Ein großflächiger kooperativer Einsatz von Intrusion-Detection-Technologie zur umfassenden und frühzeitigen Information über aufgetretene Sicherheitsverletzungen führt zu der Idee eines IT-Frühwarnsystems. In den folgenden Abschnitten geben wir einen Überblick zu bisherigen eigenen Arbeiten in diesem Themenkreis und zeigen Fragestellungen auf, die sich im Zusammenhang mit der Entwicklung eines IT-Frühwarnsystems ergeben.

2 Bisherige Arbeiten und Fragestellungen

Der praktische Einsatz von derzeit verfügbaren Systemen zur Missbrauchserkennung ist mit einer Reihe von Problemen verbunden. Eines der Hauptprobleme ist die Vielzahl der von den Systemen erzeugten Alarme. Häufig werden tausende von Alarmen pro Tag erzeugt, wobei 99% Fehlalarme sind [1, 2]. Unter der Voraussetzung einer korrekten Spezifikation von Signaturen, können Fehlalarme durch Missbrauchserkennungssysteme ausgeschlossen werden. Derartige Systeme erkennen genau die Muster, die in den Signaturen beschrieben sind. Die Ursache für hohe Fehlalarmraten ist dementsprechend auf der Ebene der Signaturspezifikation zu suchen. Zum einen ist eine systematische

Betrachtung der relevanten Aspekte von komplexen Angriffssignaturen erforderlich. Mit verschiedenen existierenden Sprachen zur Beschreibung von Signaturen sind unterschiedliche Mengen von Signaturen beschreibbar. Vielfach können Signaturen mit den zur Verfügung stehenden Sprachmitteln nicht exakt spezifiziert werden. Zum anderen birgt die Entwicklung komplexer Angriffssignaturen ein inhärentes Fehlerpotential. In existierenden Sprachen fehlen geeignete Mittel, die den Signaturentwickler bei der Beherrschung dieser komplexen Aufgabe unterstützen. Es ist notwendig, ausdrucksstarke Spezifikationssprachen zu entwickeln, die dennoch eine effiziente Auswertung erlauben.

Die steigende Leistungsfähigkeit von IT-Systemen führt zu einem weiteren Problem für die Missbrauchserkennung. Der damit einhergehende Anstieg des Datenaufkommens führt existierende Missbrauchserkennungssysteme an die Grenzen ihrer Leistungsfähigkeit. Dieses Problem wird zusätzlich dadurch verschärft, dass aus der zunehmenden Komplexität der IT-Systeme ein Zuwachs an zu analysierenden Signaturen resultiert. Aktuelle Systeme zur Missbrauchserkennung setzen verschiedene Standardverfahren zur Analyse ein, die an ihre Leistungsgrenzen stoßen, so dass eine zeitnahe Erkennung von Angriffen schwieriger wird. Daher besteht dringender Bedarf an der Entwicklung effizienter Analyseverfahren zur Missbrauchserkennung.

Grundlage für die Erkennung von Sicherheitsverletzungen ist die Erhebung und Verarbeitung von Protokoll- bzw. Audit-Daten, die in der Regel dazu geeignet sind, die involvierten Nutzerkennungen zu ermitteln, um bei Missbrauch Zurechenbarkeit herstellen zu können. Problematisch ist, dass dies einerseits im Interesse der Betreiber und der Nutzer ist, die einem Missbrauch zum Opfer gefallen sind, andererseits jedoch im Konflikt mit dem Recht der Nutzer auf informationelle Selbstbestimmung steht. Dieses Spannungsfeld zwischen Datenschutz und Zurechenbarkeit beeinflusst die Akzeptanz und Rechtmäßigkeit von Technologien zur automatischen Erkennung von Sicherheitsvorfällen und erfordert geeignete Maßnahmen, um den in Konflikt stehenden Interessen verschiedener Parteien gerecht zu werden. Gesellschaftlich relevante IT-Systeme haben sowohl reaktiven Sicherheitsaspekten als auch dem Recht und Interesse der Nutzer auf informationelle Selbstbestimmung Rechnung zu tragen, indem möglichst wenig personenbezogene Daten herangezogen und nachgehalten werden. Es ist erforderlich Verfahren zu entwickeln, die Personenbezüge vermeiden und mit dem Gesetz in Einklang stehen.

Innerhalb dieser Problemkreise wurden in bisherigen Arbeiten die folgenden Fragestellungen untersucht und entsprechende Lösungen erarbeitet:

Was sind die charakteristischen Eigenschaften von Signaturen und was muss in Signaturen spezifiziert werden, um eine exakte Erkennung zu ermöglichen?

Zur Systematisierung der semantischen Aspekte von Angriffssignaturen wurde ein Modell der Semantik von Signaturen [3] entwickelt, aus dem Anforderungen an Sprachen zur Beschreibung von Signaturen resultieren.

Wie können die relevanten Aspekte von Signaturen erfasst, modelliert und beschrieben werden?

Es wurde ein petrinetzbasierter Ansatz zur Modellierung von Signaturen und Simulation von Analyseabläufen entwickelt [4, 5]. Des Weiteren wurden Sprachwerkzeuge entwickelt, die eine intuitive und ausdrucksstarke Beschreibung von Signaturen erlauben [6, 7].

Wie kann die Analyseeffizienz von Missbrauchserkennungsverfahren optimiert werden?

Ausgehend von der Modellierung und Simulation mittels Signaturnetzen wurden charakteristische Strukturen von Signaturen sowie Eigenschaften der Missbrauchserkennung identifiziert, die zur Optimierung der Analyseeffizienz herangezogen werden können. Entsprechende Optimierungsstrategien wurden entwickelt und implementiert [7]. Anhand einer vergleichenden Evaluierung wurden erhebliche Verbesserungen der Analyseeffizienz nachgewiesen [8].

Wie können bestehende Konflikte hinsichtlich der Interessen Zurechenbarkeit bzw. Nachweisbarkeit und informationeller Selbstbestimmung fair gelöst werden?

Es wurden Verfahren entwickelt, die unter Verwendung maßgeschneiderter Pseudonyme, die Verkettbarkeit und damit die Analysierbarkeit von Audit-Daten gewährleisten und gleichzeitig die

Aufdeckbarkeit der Pseudonyme auf Angriffsszenarien begrenzen [9, 10, 11, 12, 13]. Dabei werden Signaturen als Missbrauchsmodelle für die Pseudonymerstellung verwendet. Durch die Verfahren werden mittels kryptographischer Mechanismen erstmals Pseudonym-Verkettbarkeit und –Aufdeckbarkeit technisch zweckgebunden und unumgebar durchgesetzt [9].

3 Aktuelle Fragestellungen im Kontext IT-Frühwarnung

Im Kontext der Entwicklung eines inter-/nationalen IT-Frühwarnsystems ergeben sich folgende Fragestellungen:

Wie kann in kooperierenden Allianzen trotz organisatorischer Vertraulichkeitsanforderungen ein Informationsaustausch zur Steigerung der Erkennungseffektivität realisiert werden?

Zur Verbesserung der Informationslage sind großflächige Kooperationen erforderlich. Außerdem sind Informationen über Erkenntnisse aus gesellschaftlich-sozialen Kontexten einzubeziehen (z.B. Hersteller, Sicherheitsbehörden, Strafverfolgungsbehörden) [14]. Ein entsprechender Informationsaustausch wird jedoch nur zustande kommen, wenn Sicherheitsbedenken (z.B. bzgl. der Vertraulichkeit von Informationen in den Audit-Daten) und daraus resultierendes Misstrauen der Kooperationspartner durch geeignete Ansätze ausgeräumt werden können. Hierfür sind Verfahren zur Reduktion, Kontrolle und Steuerung von Informationsflüssen in kooperierenden Allianzen erforderlich. Basierend auf Erfahrungen aus Arbeiten zur Informationsreduktion mittels Pseudonymen wurden bereits Anforderungen an derartige Verfahren untersucht [15].

Wie können effizient und effektiv qualitätsgesicherte Signaturen für neue Angriffe entwickelt werden?

Für Verfahren zur Missbrauchserkennung ist auch die Entwicklung von (qualitätsgesicherten) Signaturen zur Erkennung neuer Angriffe ein Zeitfaktor. Zur effektiven und effizienten Signaturentwicklung sind jedoch auch geeignete Verfahren zur Ermittlung der charakteristischen Kriterien zur Erkennung eines Angriffs erforderlich. Es sind derzeit weder manuelle noch automatische Verfahren bekannt, die für eine systematische Ableitung von Signaturen aus Exploits verwendet werden können. Ihre Ableitung erfolgt zumeist empirisch auf der Grundlage jahrelanger Erfahrungen von Sicherheitsexperten. Entsprechend besteht weiterer Forschungsbedarf, um den empirischen Anteil in der Signaturentwicklung durch Entwicklung systematischer Vorgehensweisen zu reduzieren, so dass exakte Signaturen in kürzeren Entwicklungszeiten erstellt werden können. In diesem Zusammenhang sind außerdem Methoden zur Validierung von Signaturen von Interesse. Erste Ansätze für Ableitungsmethoden wurden bereits erarbeitet [16, 17].

4 Zusammenfassung

Im Kontext der IT-Frühwarnung spielen die Aspekte der Signaturentwicklung, der Handhabung von Fehlalarmen, hohem Datenaufkommen und Angriffsvielfalt eine ebenso herausragende Rolle wie die Anforderungen hinsichtlich Vertraulichkeit und Datenschutz von erhobenen Daten. Unsere bisherigen Lösungen bilden Grundlagen durch eine systematische Betrachtung, Modellierung und Spezifikation von Signaturen. Auf diesem Fundament wurden domänenspezifische, hocheffiziente Analysemethoden sowie sichere und effiziente Pseudonymisierungsverfahren entwickelt.

Darauf aufbauend sind für den Einsatz in IT-Frühwarnsystemen geeignete Methoden für die zeitnahe und qualitätsgesicherte Entwicklung von Signaturen zu entwerfen. Die durch den kooperativen Charakter eines IT-Frühwarnsystems verschärften Anforderungen bzgl. Vertraulichkeit und Datenschutz wurden bereits untersucht und legen den Grundstein für die Entwicklung angemessener Verfahren zur Informationsreduktion.

5 Literatur

- [1] Julisch, K.: Dealing with False Positives in Intrusion Detection. Präsentation auf dem Symposium on Recent Advances in Intrusion Detection (RAID 2000), 2000, http://www.raid-symposium.org/raid2000/Materials/Abstracts/50/Julisch_foils_RAID2000.pdf
<http://www.raid-symposium.org/raid2000/Materials/Abstracts/50/50.pdf>
- [2] Julisch, K.: Using Root Cause Analysis to Handle Intrusion Detection Alarms. Dissertation, Fachbereich Informatik, Universität Dortmund, 2003.
- [3] Meier, M.: A Model for the Semantics of Attack Signatures in Misuse Detection Systems. In: Proc. of the 7th Information Security Conference, S. 158-169, LNCS 3225, Springer, 2004.
- [4] Flegel, U.; Meier, M.: Towards a Scalable Approach to Tailoring the Disclosure of Pseudonymous Audit Data to Misuse Detection Signatures. Internes Diskussionspapier, 2002.
- [5] Meier, M.: Missbrauchserkennung in IT-Systemen – Modellierung, Beschreibung und Optimierung. Dissertation (eingereicht), Fakultät Mathematik, Naturwissenschaften und Informatik, Brandenburgische Technische Universität Cottbus, 2005.
- [6] Meier, M.; Bischof, N.; Holz, T.: SHEDEL - A Simple Hierarchical Event Description Language for Specifying Attack Signatures. In: Proc. of the 17th International Conference on Information Security. S. 559-571, Kluwer, 2002.
- [7] Meier, M.; Schmerl, S.: Effiziente Analyseverfahren für Intrusion-Detection-Systeme. In: Proc. of the Second GI Conference on "Sicherheit - Schutz und Zuverlässigkeit", LNI P-62, S. 209-220, Köllen Verlag, 2005.
- [8] Meier, M.; Schmerl, S.; Koenig, H.: Improving the Efficiency of Misuse Detection. In: Proc. of the Second Conference on "Detection of Intrusions & Malware and Vulnerability Assessment" (DIMVA 2005), LNCS 3548, S. 188-205, Springer, 2005.
- [9] Pseudonymizing Audit Data for Privacy Respecting Misuse Detection. Dissertation, Fachbereich Informatik, Universität Dortmund, Januar 2006.
- [10] Flegel, U.: Ein Architektur-Modell für anonyme Autorisierungen und Überwachungsdaten. In: Proc. of the First GI Conference on "Sicherheit - Schutz und Zuverlässigkeit", Mit Sicherheit Informatik, LNI P-36, S. 293-304, Frankfurt, Köllen Verlag, 2003.
- [11] Flegel, U.: Praktikabler Datenschutz für Log-Daten. In: Proc. of the 10th Workshop on "Sicherheit in vernetzten Systemen", S. F1-F20, Hamburg, Books on Demand, 2003.
- [12] Flegel, U.: Pseudonymizing Unix Log Files. In: Proc. of the Infrastructure Security Conference (InfraSec2002), LNCS 2437, S. 162-179, Bristol, Springer, 2002.
- [13] Biskup, J.; Flegel, U.: Threshold-based Identity Recovery for Privacy Enhanced Applications. In: Proc. of the 7th ACM Conference on Computer and Communications Security (CCS 2000), S. 71-79, Athens, ACM Press, 2000.
- [14] Welsch, G.; Frießem, P.: Ein IT-Frühwarnsystem für Deutschland – Vorschlag für einen politischen Ansatz. Datenschutz und Datensicherheit, Vol. 29 (2005), Nr. 11, S. 651-656, Vieweg, 2005.
- [15] Flegel, U.; Biskup, J.: Requirements of Information Reductions for Cooperating Intrusion Detection Agents. In: Proc. of the International Conference on Emerging Trends in Information and Communication Security (ETRICS 2006), LNCS 3995, S. 466-480, Freiburg, Springer, 2006, to appear.
- [16] Schmerl, S.; König, H.; Flegel, U.; Meier, M.: Simplifying Signature Engineering by Reuse. In: Proc. of the International Conference on Emerging Trends in Information and Communication Security (ETRICS 2006), LNCS 3995, S. 436-450, Freiburg, Springer, 2006, to appear.
- [17] Schmerl, S.; Flegel, U.; Meier, M.: Vereinfachung der Signarentwicklung durch Wiederverwendung. In Dittmann, J.(ed.): Proc. of the Third GI Conference on "Sicherheit - Schutz und Zuverlässigkeit", LNI P-77, S. 201-212, Magdeburg,, Köllen Verlag, 2006.