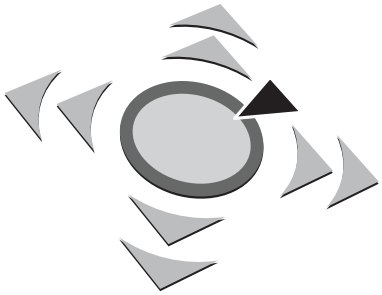
1. GI FG SIDAR Graduierten-Workshop über Reaktive Sicherheit

SPRING

Ulrich Flegel (Hrsg.)
Universität Dortmund, Fachbereich Informatik
D-44221 Dortmund

12. Juli 2006, Berlin



SIDAR-Report SR-2006-01

Vorwort

SPRING ist eine wissenschaftliche Veranstaltung im Bereich der Reaktiven Sicherheit, die Nachwuchswissenschaftlern die Möglichkeit bietet, Ergebnisse eigener Arbeiten zu präsentieren und dabei Kontakte über die eigene Universität hinaus zu knüpfen. SPRING ist eine zentrale Aktivität der GI-Fachgruppe SIDAR, die von der organisatorischen Fachgruppenarbeit getrennt stattfindet. Die Veranstaltung dauert inklusive An- und Abreise einen Tag und es werden keine Gebühren für die Teilnahme erhoben. SPRING findet ein- bis zweimal im Jahr statt. Die Einladungen werden über die Mailingliste der Fachgruppe bekanntgegeben. Interessierte werden gebeten, sich dort einzutragen (`http://www.gi-fg-sidar.de/list.html`). Für Belange der Veranstaltung SPRING ist Ulrich Flegel (Universität Dortmund) Ansprechpartner innerhalb der Fachgruppe SIDAR.

SPRING hatte seine Premiere am 12. Juli 2006 in Berlin und wurde im Zusammenhang mit der internationalen SIDAR-Konferenz *Detection of Intrusions and Malware & Vulnerability Assessment* (DIMVA) in den Räumen der Berlin-Brandenburgischen Akademie der Wissenschaften veranstaltet (siehe Information im Anhang). Die Vorträge deckten ein breites Spektrum ab, von noch laufenden Projekten, die ggf. erstmals einem breiteren Publikum vorgestellt werden, bis zu abgeschlossenen Forschungsarbeiten, die zeitnah auch auf Konferenzen präsentiert wurden bzw. werden sollen oder einen Schwerpunkt der eigenen Diplomarbeit oder Dissertation bilden. Die zugehörigen Abstracts sind in diesem technischen Bericht zusammengefaßt und wurden über die Universitätsbibliothek Dortmund elektronisch, zitierfähig und recherchierbar veröffentlicht. Der Bericht ist ebenfalls über das Internet-Portal der Fachgruppe SIDAR zugänglich (`http://www.gi-fg-sidar.de/`). In dieser Ausgabe finden sich Beiträge zur den folgenden Themen: Verwundbarkeiten und Malware, Incident Management und Forensik, sowie zu verschiedenen Spezialthemen der Intrusion Detection: Realisierungsaspekte, Modellgenerierung und -validierung, sowie neue Technologien.

Besonderer Dank gebührt Konrad Rieck für die lokale Organisation der Veranstaltung, Pavel Laskov für das Hosting durch die Konferenz DIMVA, Michael Meier für seine Anregungen und nicht zuletzt Christopher Wolf für seine Unterstützung mit seinem Erfahrungsschatz bei der Organisation der Kryptotage.

Berlin, Juli 2006 Ulrich Flegel

Contents

Diesen Bericht zitieren als:
Ulrich Flegel, editor. Proceedings of the First GI SIG SIDAR Graduate Workshop on Reactive Security (SPRING). Technical Report SR-2006-01, GI FG SIDAR, Berlin, July 2006, `https://eldorado.uni-dortmund.de/handle/2003/22356`

Beiträge zitieren als:
Autor. Titel. In Ulrich Flegel, editor, Proceedings of the First GI SIG SIDAR Graduate Workshop on Reactive Security (SPRING). Technical Report SR-2006-01, pages xx-yy. GI FG SIDAR, Berlin, July 2006.

Java Security Antipatterns and Refactorings

Marc Schoenefeld*

* University of Bamberg
D-96045 Bamberg, Germany
marc.schoenefeld{at}gmx.org

Over the last years Java has become one of the major programming languages. This is because of the holistic design approach which fulfills the important non- functional requirements needed for enterprise level applications. Security is one of these transparencies that is backed by an embedded security infrastructure framework that allows to provide a safe execution environment for component based software. Every system is as secure as its weakest part. Hackers are equipped with a mind set to find vulnerable spots in the real life projection of system behavior which is the compiled Java bytecode. The quality of products emitted by the software development process is depended of the quality of the embedded prebuilt components. If the base infrastructure and middleware is exploitable by attackers own efforts to harden application security may become useless. The classes of the Java Runtime Environment form the central building block for middleware applications. As part of the trusted computing base they have to be build with security goals in mind. Vulnerable spots may result from constellations in coding or infrastructure. These antipatterns cause rather than solve security problems. This research project is concerned with a classification of programming antipatterns in the implementation of Java middleware systems and their effects on security aspects such as privacy, integrity and availability. The project was started in 2002 and finishes in the end of 2006. By following the practical methodologies of penetration testing the relations between programming antipatterns and vulnerabilities are shown. Practical results have been provided as feedback to software vendors to improve the quality of products such as Sun JDK, and JBoss application server.

The Methodology: To categorize antipatterns and their effects on the different aspects of security a framework was derived from the basic principles of security of Saltzer & Schroeder, common security patterns of Yoder and Barcalow, the vulnerability taxonomy of Lanwehr et al. and the secure programming guidelines of Sun Microsystems. A generic antipattern typically neglects a secure programming guideline and in consequence violates a principle of security. To overcome an antipattern refactorings are applied, which frequently can categorized with a security pattern. The methodology followed typical strategies for white box penetration testing. For possible violations of programming guidelines detectors were written. These detectors work on the Java bytecode and generate candidates such such as methods or fields in classes. The project lead to the detection of a broad catalog of antipatterns violating the secure programming guidelines. The most dangerous were integer overflows, covert channels, harmful serialized object instances and the AllPermission antipattern.

Sicherheit mobiler Endgeräte

Michael Becher

Universität Mannheim
68131 Mannheim
becher@informatik.uni-mannheim.de

Mobiltelefone wurden üblicherweise zur Sprachkommunikation oder zum Austausch kurzer Textnachrichten benutzt. Mit der fortschreitenden Miniaturisierung von Rechenleistung wurden Geräte, die ursprünglich für die Sprachkommunikation entworfen wurden, mit zusätzlichen Funktionen erweitert. Heute verfügbare Mobiltelefone bieten eine Vielzahl an Funktionen und stellen als Pflichtübung noch eine Möglichkeit zur Sprachkommunikation bereit. Mobile Endgeräte sind im Sinne dieser Arbeit sind jegliche Art von Geräten, die mit einem Mobilfunknetz verbunden werden können.

Die Betriebssysteme mobiler Endgeräte haben sich gewandelt von speziell für diesen Zweck entworfenen Betriebssystemen hin zu angepassten Versionen von Betriebssystemen, die auch auf Arbeitsplatzrechnern eingesetzt werden. Diese Entwicklungen bieten eine Vielzahl an Möglichkeiten aus funktionaler Sicht. Aus Sicherheitssicht ist es in vielfältiger Weise möglich, das mobile Endgerät Dinge tun zu lassen, die nicht vom Benutzer erwünscht sind. Durch die ständige Verbindung mit dem Mobilfunknetz können dabei schnell hohe Kosten verursacht werden.

Das Ziel dieser Arbeit ist es, zur Erhöhung der Sicherheit mobiler Endgeräte beizutragen. Die Arbeit beginnt im Juni 2006. Durchgeführt wird sie am ,,Laboratory for Dependable Distributed Systems" in Zusammenarbeit mit der T-Mobile Deutschland GmbH. Die folgenden zwei Schwerpunkte sind für die erste Phase vorgesehen:

- Mit der steigenden Funktionalität der Betriebssysteme steigt auch die Zahl von verfügbarer Malware. An ausgesuchter Malware soll analysiert werden, wie sie das mobile Endgerät infiziert, d.h. welche Schwächen des Betriebssystems sie ausnutzt.
- Unabhängig von den konkreten Ansatzpunkten der Malware sollen prinzipielle Beschränkungen der Betriebssysteme untersucht werden, die für die Erhöhung der Sicherheit relevant sind. Untersuchungsobjekt wird das Betriebssystem ,,Windows Mobile" sein.

Diese beiden Punkte sollen zu Eigenschaften mobiler Endgeräte führen, die die Sicherheit für den Benutzer erhöhen. Es soll also möglich sein, eine Reihe von Anforderungen an die Implementierung der Betriebssysteme von mobilen Endgeräten zu stellen, die aus Sicherheitssicht wichtig sind.

Entropy Based Worm and Anomaly Detection in Fast IP Networks

Arno Wagner*

*ETH Zurich

Detecting massive network events like worm outbreaks in fast IP networks, such as Internet backbones, is hard. One problem is that the amount of traffic data does not allow real-time analysis of details. Another problem is that the specific characteristics of these events are not known in advance. There is a need for analysis methods that are real-time capable and can handle large amounts of traffic data. We have developed an entropy-based approach [WP05], that determines and reports entropy contents of traffic parameters such as IP addresses. Changes in the entropy content indicate a massive network event. We give analyses on two Internet worms as proof-of-concept. While our primary focus is detection of fast worms, our approach should also be able to detect other network events. We discuss implementation alternatives and give benchmark results. We also show that our approach scales very well.

References

[WP05] Arno Wagner and Bernhard Plattner: *Entropy Based Worm and Anomaly Detection in Fast IP Networks*, STCA security workshop, WET ICE 2005 Link"oping, Sweden, 2005, (best paper award)

Transparentes Load-Balancing für Network Intrusion Detection Systeme

Matthias Vallentin* und Robin Sommer†

*TU München
vallentin{at}icsi.berkeley.edu

†ICSI
robin{at}icir.org

Network Intrusion Detection Systeme (NIDS) erkennen Verletzungen der Sicherheitsrichtlinien, indem sie den den Netzwerkverkehr auf bösartige Aktivitäten überwachen. Leistungsstarke Gbps-Netzwerke stellen jedoch neue Herausforderungen an ein NIDS. In Umgebungen mit hohem Datenaufkommen erreichen bisherige Ansätze, deren Architekturen auf Einzelbetrieb ausgelegt sind, häufig ihre Grenzen. Um der unzureichenden Rechenkapazität entgegen zu wirken, bieten Hersteller meist sehr teure, zugeschnitte Spezial-Hardware an. In unserer Arbeit stellen wir Methodiken zum *Clustering* und *Load-Balancing* von NIDS auf Standard-Hardware vor, die wir am Beispiel des Open-Source NIDS Bro [Pax99] in die Praxis umsetzen. Ferner integrieren wir einen Cluster in die Netzwerk-Infrastruktur des Lawrence Berkeley National Laboratory (LBNL, [LBL]), mit dem externe Verbindungen des Netzwerks und die DMZ überwacht werden.

Traditionelle Systeme verwenden zur Erkennung von Angriffen einen Satz Signaturen mit bereits existierenden Angriffen, die sie byteweise mit dem Datenstrom vergleichen. Bro verwaltet darüber hinaus einen genaues Abbild des Netzwerkzustandes, der policy-neutral erfasst wird. Das Konzept des *Independent State* [SoPa05] erlaubt es, diesen Zustand mehreren parallel laufenden Instanzen zugänglich zu machen und untereinander auszutauschen. Während bisherige Herangehensweisen nur aggregierte Informationen (z.B. Logs und Alarme) austauschen, kann Bro seine gesamten angesammelten Zustandsinformationen allen Instanzen bekannt machen. Diese Möglichkeit birgt ein großes Anwendungspotential im Hinblick auf eine verteilte Analyse mit höherer Transparenz [SoPa05].

Darauf aufbauend haben wir Bro um Mechanismen erweitert, mit denen ein skalierbarer NIDS-Cluster geschaffen werden kann. In Gbps-Netzwerken ist es damit möglich, sich nicht nur wie bisher aufgrund knapper Rechenkapazität auf eine Teilmenge des Netzwerkverkehrs zu beschränken, sondern die Analyse auf die vollständige Datenmenge auszuweiten. Insbesonders haben wird Bros Policy-Skripte für den Einsatz in einem Cluster protokollspezifisch angepasst. Die Erweiterungen erlauben eine feine Kontrolle der auszutauschenden Zustandsinformationen und bieten Unterstützung für unterschiedliche Cluster-Topologien.

Literatur

[LBL] Lawrence Berkeley National Laboratory. `http://www.lbl.gov`.

[Pax99] Vern Paxson. *Bro: A System for Detecting Network Intruders in Real-Time*. Computer Networks, 31(23-24):2435-2463, 1999.

[SoPa05] Robin Sommer und Vern Paxson. *Exploiting Independent State For Network Intrusion Detection*. In *Proceedings of the 21st Annual Computer Security Applications Conference*, 2005.

Netzbasierte Angriffs- und Anomalieerkennung mit TOPAS

Lothar Braun und Gerhard Münz
Rechnernetze und Internet, Wilhelm-Schickard-Institut für Informatik, Universität Tübingen
{braunl|muenz}@informatik.uni-tuebingen.de

Die Erkennung von Denial-of-Service(DoS)-Angriffen und Würmern in großen Netzwerken mit hohen Bandbreiten stellt eine besondere Herausforderung dar. Der Einsatz konventioneller Intrusion-Detection-Systeme, wie z.B. Snort [MR99], ist dort problematisch, weil diese Netzwerkverkehr nur punktuell und nur bis zu einer gewissen Paketrate beobachten und untersuchen können. Das hier vorgestellte System *TOPAS* (Traffic flOw and Packet Analysis System) verarbeitet Verkehrsdaten, die von Netzwerkmonitoren über die Standardprotokolle Cisco Netflow [BC04] und IPFIX/PSAMP [BC06a, BC06b] exportiert werden. Die Netzwerkmonitore übernehmen dabei die Selektierung und Vorverarbeitung der Verkehrsdaten durch Paketfilterung, Sampling und Flow-Accounting. Da Netzwerkmonitore auch für andere Aufgaben eingesetzt werden, z.B. zur Abrechnung des geflossenen Datenvolumens, lässt sich das System leicht in bestehende Netze integrieren.

TOPAS ist in der Lage, sowohl Flow-Daten, als auch Paketdaten zu verarbeiten. Dabei beschreiben die Flow-Daten Verkehrsströme, die in letzter Zeit an einem Netzwerkmonitor beobachtet wurden. Sie können verwendet werden, um Angriffe zu entdecken, die Änderungen in der Zusammensetzung der Flows verursachen. Paketdaten dienen dagegen zur Untersuchung einzelner Pakete und deren Inhalte, z.B. durch signaturbasierte Erkennungsverfahren.

Die Verkehrsdaten können von Monitoren stammen, die gleichzeitig verschiedene Stellen des Netzes überwachen. Dadurch können die Verkehrsdaten aus dem gesamten Netz mit einer einzigen Instanz des Systems auf Angriffe und Anomalien hin untersucht werden. In größeren Netzen und bei hohen Bandbreiten kann TOPAS aber auch verteilt betrieben werden, wenn das Verkehrsdatenvolumen die Verarbeitungskapazität einer Instanz übersteigt. TOPAS besteht aus zwei Teilen: Einem Kollektor, der das System mit Verkehrsdaten versorgt, sowie einem Modulsystem, das es erlaubt, in getrennten Modulen verschiedene Analysealgorithmen parallel auf die Verkehrsdaten anzuwenden. Die Module sind dabei auf die Erkennung bestimmter Angriffe oder Anomalien spezialisiert, z.B. auf die Erkennung von DoS-Angriffen, Port-Scans oder gefälschten Absenderadressen. Die Module können dynamisch gestartet werden, was eine ereignisgesteuerte Analyse der vorliegenden Verkehrsdaten ermöglicht. So kann beispielsweise ein permanent aktiviertes Modul eine wenig rechenintensive Erstanalyse der Flow-Daten vornehmen und, sobald ein Verdacht auf einen Anomalie vorliegt, eine genauere Analyse durch ein nachgestartetes Modul veranlassen, um die Anomalie zu klassifizieren, einzelne Pakete aus den verdächtigen Flows zu untersuchen oder die Analyse abzubrechen, wenn sich die Anomalie als ungefährlich herausstellt. TOPAS wird derzeit im Rahmen des EU-Projekts *Diadem Firewall* entwickelt und eingesetzt.

Literatur

[MR99] Martin Roesch: *Snort: Lightweight Intrusion Detection for Networks.* In *13th USENIX Conference on System Administration*, USENIX Association, 1999, Seiten 229–238.

[BC04] Benoit Claise: *Cisco Systems NetFlow Services Export Version 9.* RFC 3954, Okt. 2004.

[BC06a] Benoit Claise: *IPFIX Protocol Specification.* Internet-Draft, draft-ietf-ipfix-protocol-21, April 2006

[BC06b] Benoit Claise: *Packet Sampling (PSAMP) Protocol Specifications*, Internet-Draft, draft-ietf-psamp-protocol-05, März 2006

Kooperative Anomalieanalyse für die Erkennung von Multi-Stage Angriffen

Oliver Petz* und Daniel Hamburg*

* AG Integrierte Informationssysteme, Ruhr Universität Bochum
oliver.petz{at}rub.de, daniel.hamburg{at}iis.rub.de

Intrusion Detection Systeme (IDS) nehmen in Netzwerken Ereignisdaten auf und lösen bei eindeutigen Angriffsindizien Alarme aus. Bei Multi-Stage Angriffen führt häufig erst die Aggregation mehrerer Ereignisse zur Erkennung. Erfolgt die Aggregation auf einer zentralen Instanz, bildet diese einen Single-Point of Failure und ein lohnenswertes Ziel für Angreifer. Für eine dezentrale Erkennung aller Angriffe wäre der Austausch sämtlicher Ereignisse zwischen allen beteiligten IDS notwendig, was jedoch zu einer Überlastung des Netzwerkes führen kann. Es gilt einen Kompromiss zwischen benötigter Bandbreite und Kapazitäten der IDS-Elemente und dem Potenzial der Angriffserkennung zu finden.

Der hier vorgestellte Ansatz zur Erkennung von Multi-Stage Angriffen basiert auf der Kooperation einzelner im Rahmen eines Verbundes miteinander kommunizierender IDS. Ein IDS, das ein lokales Ereignis als potenzielle Gefahr identifiziert, fordert von allen Verbundteilnehmern Informationen zu von ihnen aufgenommenen Ereignissen, die Ähnlichkeiten zum potentiell gefährlichen Ereignis aufweisen, an. Durch Aggregation der ähnlichen Ereignisse wird es dem anfordernden IDS ermöglicht, die Existenz eines Multi-Stage Angriffes zu konstatieren. Die periodische Wiederholung dieses Informationsaustausches erlaubt die Detektion von Angriffen, deren einzelne Schritte über einen längeren Zeitraum verteilt sind. Des Weiteren ist die Detektion robust gegenüber Angriffen auf einzelne Verbundteilnehmer.

Im Rahmen der Kooperation überwachen die IDS einzelne Netzwerkelemente mit Hilfe von Methoden der Anomalieanalyse (Statistik, Neuronale Netze). Hierbei wird ein lokaler Normalzustand ermittelt und neu auftretende Ereignisse einer der drei Klassen *Normalverhalten*, *Soft-Anomalie (S-A)* oder *Hard-Anomalie (H-A)* zugeordnet. Eine *Soft-Anomalie* liegt vor, wenn ein Ereignis signifikant vom Normalverhalten abweicht, jedoch nicht eindeutig als Angriff identifizierbar ist. Auftretende *Soft-* und *Hard-Anomalien* werden in das *Ereignisprotokoll* eingetragen, *Soft-Anomalien* zusätzlich in eine temporäre *S-A* Liste. Protokoll- und Listeneinträge enthalten das auslösende Ereignis und die Bewertung des Gefahrenpotenzials (z.B. Abweichung vom Normalverhalten).

Jedes IDS verschickt periodisch seine *S-A* Liste an alle anderen IDS und löscht diese anschließend lokal. Es muss sichergestellt werden, dass zu einem Zeitpunkt nur ein IDS seine Liste sendet.

Jedes IDS vergleicht die zuletzt erhaltene Liste mit seiner eigenen aktuellen *S-A* Liste. Weist ein lokales Ereignis Ähnlichkeiten zu einem in der erhaltenen *S-A* Liste auf, wird es aus der lokalen Liste gelöscht. Nach Ablauf einer Zeitperiode sendet das IDS seine *S-A* Liste an alle anderen IDS.

Zusätzlich vergleicht jedes IDS eine erhaltene *S-A* Liste mit seinem *Ereignisprotokoll* und sucht nach ähnlichen Ereignissen. Findet es Ähnlichkeiten, sendet es die entsprechenden Einträge (*Soft-* und/oder *Hard-Anomalien*) des Protokolls an das IDS, dessen *S-A* Liste es analysiert hat. Für die Messung der Ähnlichkeit können unterschiedliche Algorithmen eingesetzt werden, wobei der Einsatz von Methoden der Mustererkennung sinnvoll erscheint.

Erhält ein IDS Antworten auf das Versenden seiner *Soft-Anomalien* Liste, so muss es an Hand der darin enthaltenen Ereignisse entscheiden, ob es sich um Teile eines Multi-Stage Angriffes handelt. Als Metrik für die Wahrscheinlichkeit des Vorhandenseins eines Multi-Stage Angriffes dient eine Kombination aus der Anzahl erhaltener Antworten und den Bewertungen des Gefahrenpotenzials der einzelnen Anomalien.

Diploma Thesis - Finding Structures In Internet Traffic With Association Rules

Svenja Wendler and Prof. Norbert Pohlmann

Institute for Internet Security
Fachhochschule Gelsenkirchen, University Of Applied Sciences
D-45877 Gelsenkirchen
svenja.wendler@internet-sicherheit.de
norbert.pohlmann@internet-sicherheit.de

The internet is omnipresent in our normal course of life. It is steadily being extended by new services like Voice over IP. New technologies offer new room for attacks that need to be minimized. At present there is no possibility to observe attacks and failures and to monitor arising technology trends from a global perspective.

Within the scope of the research project Internet Early Warning Systems the Institute for Internet Security in Gelsenkirchen develops the Internet Analysis System (IAS). It analyses local data communication in defined subnetworks of the internet. The system though creates a global view of the internet by combining many local views. An evaluation system interprets the communication-parameters under different aspects and displays these in an intuitive manner.

In the scope of my diplomathesis I develop a user friendly module of analysis to find association rules in internet traffic, that will be integrated into the Internet Analysis System. The user will be able to rate the rules, comment them and use them for further analysis.

The Internet Analysis System retrieves its raw data about the internet traffic by probes. These pick network traffic on communication lines of different subnetworks and count the appearance of communication parameters like protocols or services on the several ISO OSI layers. The counted communication parameters are called descriptors. Association rules illustrate correlations between different descriptors.

The Apriori Algorithm, that is used in market basket analysis, finds association rules of descriptors on certain probes and their counters. Thus the user is able to compare the relation profiles of internet services on different probe locations and the time-based change of a relationship profile on one probe location.

Association rules offer a great approach to find structures in network traffic. They provide a solid base for the development of Early Warning Modules.

References

[WF05] Ian H. Witten and Eibe Frank: book: *Data Mining. Practical Machine Learning Tools and Techniques*, Morgan Kaufmann Publishers, Juli 2005

[PP06] Norbert Pohlmann and Marcus Proest: article: *Messverteilung - Die globale Sicht auf das Internet*, iX - Magazin für professionelle Informationstechnik, Heise Verlag, Ausgabe 2-2006, April 2006,

TAIPAN: A Rule Learner for Positive and Negative Rule generation applied to Security Alarm Filtering

Pascal Baumgartner*

*pascal.baumgartner@swisscom.com

In the last few years rule-learners, traditional and associative ones have evolved towards a powerful and efficient tool for classification of different data sets. Except the algorithm from Antonie *et al.*[AZ04], the research in RIPPER [CW95], SLIPPER [CS99], FOIL [RQ93] and CPAR [YH03] only concentrated on positively correlated features for rule-generation. These algorithms showed good results with respect to the tested data sets, but they did not integrate negative associations into their experiments. Thus, this paper concentrates on the creation of a binary rule-learner, that uses both, positively (presence) and negatively (absence) correlated features to create a compact and accurate rule-set, which is a powerful classifier even for unseen data. TAIPAN adopts a greedy algorithm to create rules directly from the training data. To avoid missing important rules, we used a different approach when choosing the literals for rule-generation than traditional rule-learners. We applied our learner to a real world problem of security alarm filter rule maintenance to support human analysts in our company. Due to the fact that the rule sets generated by TAIPAN are human-readable and -understandable, it is possible for an experienced analyst to cooperate with TAIPAN and modify, add or delete one or more rules to keep the rule-set up-to-date. Human acceptance tests are currently in progress.

Literatur

[AZ04] Marie-Luiza Antonie and Osmar R. Zaïane: An Associative Classifier based on Positive and Negative Rules. Proceedings of the 9th ACM SIGMOD workshop on Research issues in data mining and knowledge discovery (2004), 64 - 69.

[CW95] William W. Cohen: Fast effective Rule Induction. ICML'95, 115 - 123.

[CS99] William W. Cohen and Yoram Singer: A Simple, Fast, and Effective Rule Learner. AAAI/IAAI'99. 335 - 342.

[RQ93] J. Ross Quinlan and R. Mike Cameron-Jones: FOIL : A Midterm Report. ECML'93.

[YH03] Xiaoxin Yin and Jiawei Han: CPAR: Classification based on Predictive Association Rules. SDM'03.

Validierung von Signaturen – Testmethoden zur Feststellung von Korrektheit und Präzision

Sebastian Schmerl[†]
[†]BTU Cottbus
sbs{at}informatik.tu-cottbus.de

Die Wirksamkeit von Signaturanalysesystemen hängt entscheidend von der Genauigkeit der verwendeten Signaturen ab. Ungenaue Signaturen schränken die Erkennungsmächtigkeit von Misuse-Detection-Systemen bzw. die wirtschaftliche Rentabilität dieser stark ein. Demzufolge ist die Test- bzw. Korrekturphase ein essentieller Bestandteil des Entwicklungsprozesses neuer Signaturen. In dieser Phase werden Korrektheit und Präzision einer Signatur überprüft. Dies erfolgt mit dem Ziel eventuelle Entwurfs- oder Spezifikationsfehler zu beseitigen und die Signatur möglichst zu einer idealen Signatur zu entwickeln. Eine *ideale* Signatur beschreibt dabei exakt die Menge M_I aller Manifestationen des zugehörigen Angriffs. Unter einer *Manifestation* eines Angriffs werden die bei der Durchführung einer Sicherheitsverletzung generierten Audit-Ereignisse verstanden. Typischerweise entstehen im Signatur-Entwicklungsprozess keine idealen Signaturen, sondern über- bzw. unterspezifizierte Signaturen.

Unterspezifizierte Signaturen beschreiben neben Aktionsfolgen, die zu einem erfolgreichen Angriff führen, auch Aktionsfolgen, die legitimen Verhalten entsprechen oder keine Ausnutzung einer Schwachstelle zur Folge haben. Unterspezifizierte Signaturen beschreiben somit eine Manifestationsmenge M_U, die eine Übermenge der Manifestationen der idealen Signatur M_I darstellt. Sprich: $M_I \subset M_U$. Um diese Spezifikationsfehler zu erkennen, werden ausgehend von der Signatur Testdaten abgeleitet. Dazu werden Audit-Ereignissen komplementär zur Sensorfunktionalität eines IDS wieder Aktionen zugeordnet. Da die Signatur die Audit-Ereignisse einer Attacke beschreibt, können somit alle beschriebenen Aktionsfolgen, die zu einem erfolgreichen Angriff führen sollten, hergeleitet werden. Die abgeleiteten Aktionsfolgen werden anschließend auf einem dedizierten System auf die erfolgreiche Ausnutzung der Verwundbarkeit getestet. Wird die Verwundbarkeit bei einer Aktionsfolge nicht ausgenutzt, liegt typischerweise ein Spezifikationsfehler vor. Die Schwierigkeiten und die Grenzen dieses Ansatzes liegen neben der Ableitung der Aktionsfolgen hauptsächlich in der Feststellung ob die Verwundbarkeit tatsächlich ausgenutzt wird.

Im Gegensatz dazu erkennen *überspezifizierte* Signaturen nicht alle Ausprägungen einer Attacke, d.h. es existieren Aktionsfolgen für eine erfolgreiche Verwundbarkeitsausnutzung, die nicht durch die Signatur spezifiziert werden. Demzufolge ist die erkannte Manifestationsmenge $M_{\ddot{U}}$ einer überspezifizierten Signatur eine Teilmenge der Manifestationsmenge der idealen Signatur. Sprich: $M_{\ddot{U}} \subset M_I \subset M_U$. Eine Teststrategie für überspezifizierte Signaturen muss sicherstellen, dass die Erkennung des Angriffes auch gewährleistet bleibt, wenn einzelne oder mehrere Aktionen des Angriffs durch semantisch gleichwerte bzw. isomorphe Aktionen ausgetauscht werden. Ziel solcher Transformationen ist, den Angriff so umzuformen, dass sich die Spuren des Angriffs verändern und somit einer Erkennung ausgewichen wird. Die eigentliche Angriffsstrategie zur Ausnutzung der Verwundbarkeit bleibt jedoch erhalten. Dementsprechend muss die Signatur durch die Erkennung von semantisch gleichwertigen Aktionen vervollständigt werden. Allerdings ist durch weitere Tests sicherzustellen, ob die Ausnutzung der Verwundbarkeit auch durch die semantisch gleichwertigen Aktionen gegeben ist.

Der Beitrag beschreibt die skizzierten Teststrategien, deren Grenzen und offene Problemfälle.

Entwicklung eines Intrusion-Detection-Verfahrens zur Erkennung von VoIP-initiierten DoS-Attacken auf Rettungsleitstellen

Christoph Fuchs

Universität Bonn, Institut für Informatik IV
D-53117 Bonn
fuchsc{at}cs.uni-bonn.de

Der Einsatz der Voice-over-IP-Technik als Alternative zum bestehenden Festnetz, dem Public Switched Telephone Network (PSTN), findet bei Endkunden zunehmende Verbreitung. Durch die Kopplung von IP-basierten Netzen mit dem PSTN über VoIP-Gateways werden Telefonverbindungen zwischen VoIP-Anschlüssen und Festnetzanschlüssen ermöglicht. Der Zusammenschluss dieser beiden Netztypen setzt das PSTN einigen bisher nur in IP-Netzen herrschenden Sicherheitsrisiken aus. So entsteht eine neuartige Gefahr von aus VoIP-Netzen initiierten Denial-of-Service (DoS) Angriffen auf Anschlüsse im PSTN. Besondere Brisanz besitzt ein derartiger Angriff in Verbindung mit dem Notrufdienst. Ein Angreifer kann durch gezieltes Absetzen einer großen Anzahl gefälschter Notrufe, sämtliche eingehenden Telefonleitungen der Rettungsleitstelle – auch als Public Safetey Access Point (PSAP) bezeichnet – blockieren und so die Rettungskette bereits frühzeitig unterbrechen. Dies kann im schlimmsten Fall den Verlust von Menschenleben bedeuten [SSTT05].

Eine interessante Frage in diesem Kontext ist, inwiefern einem DoS-Angriff aus den VoIP-Netzen auf einen PSAP begegnet werden kann, um den Totalausfall der Leitstelle zu verhindern. Eine Schwierigkeit besteht dabei in der eigentlichen Erkennung eines Angriffs und in der Abgrenzung von einem hohen Notrufaufkommen bei Unwetterlagen, Großbränden oder Katastrophen [AFM+06]. Weiterhin sind Fehlalarme (false positives) im PSAP nicht tolerierbar, da je nach ergriffenen Gegenmaßnahmen, wie dem Verwerfen von Anrufen, reale Notrufe verloren gehen können.

Im Rahmen einer Diplomarbeit wurde ein Verfahren entwickelt, das es ermöglicht, DoS-Angriffe im PSAP frühzeitig erkennen zu können. Dazu wurde die in einem PSAP eingesetzte Telefonanlage um eine Komponente erweitert, die die aufkommende Last der Notrufe nach Methoden der Intrusion-Detection analysiert. Zur Unterscheidung von Angriffs- und Katastrophenfällen werden, nach dem Ansatz der kooperativen Intrusion-Detection [OvgF05], die Verkehrsprofile der eingehenden Notrufe getrennt nach ihren Ursprungsnetzen – also PSTN, Mobilfunk oder VoIP – betrachtet und korreliert. Die Effektivität der Angriffserkennung wurde durch Emulation unterschiedlicher Szenarien evaluiert und mögliche Gegenmaßnahmen und ihre Einsetzbarkeit im Kontext des Notrufdienstes bewertet.

Literatur

[AFM+06] Aschenbruck, Nils ; Frank, Matthias ; Martini, Peter ; Tölle, Jens ; Legat, Roland ; Richmann, Heinz-Dieter: Present and Future Challenges Concerning DoS-attacks against PSAPs in VoIP Networks. In: *Proceedings of the Fourth IEEE International Workshop on Information Assurance*, April 13 - 14, 2006, S. 103–108

[SSTT05] Schulzrinne, H. ; Shanmugam, M. ; Taylor, P. ; Tschofenig, H.: *Security Threats and Requirements for Emergency Calling.* 2005. – IETF ECRIT Draft draft-taylor-ecrit-security-threats-00.txt

[OvgF05] Otto vor dem gentschen Felde, Nils: *Leistungsfähigkeit von Anomalieerkennungsverfahren in domänenübergreifenden Meta-IDS*, Universität Bonn, Diplomarbeit, 2005

Physical Intrusion Detection Using RFID

Benjamin Fabian

Institute of Information Systems
Humboldt-University Berlin
bfabian@wiwi.hu-berlin.de

Radio Frequency Identification (RFID) is about to be deployed on single items for the mass market, combined with the introduction of an Electronic Product Code (EPC) that (in principle) extends the conventional barcode by a globally unique serial number. Future ubiquity of this technology has the potential to extend intrusion detection systems (IDS) from the virtual to the physical world. A major component of physical IDS could be the use of the EPC Network, a global distributed system of databases that contain object information. Incoming and outgoing items that pass a company perimeter or areas with restricted access could be identified and tracked by RFID. On the other hand, conventional network taps and IDS sensors in future pervasive smart office environments could monitor IP traffic to the EPC Network for suspicious signatures that indicate forbidden or suspect goods have passed individual RFID reader locations. Data aggregation and correlation already in place for classical network or host intrusion detection could be upgraded to cope with these new physical detection methods, though new challenges will arise by the amount of new data collected. With the EPC Network in place, detection errors could be reduced by globally sharing semantic item classification lists that could improve IDS signature generation, event interpretation, and risk evaluation.

Tracking and identification of physical objects could be easily extended to individual persons carrying these objects. Privacy issues need to be addressed and solved *before* physical intrusion detection is to be used in the field.

HostLock - ein automatisches Quarantänesystem für Netzwerke

Adrian Wiedemann*

* Rechenzentrum Universität Karlsruhe (TH)
D-76131 Karlsruhe
adrian.wiedemann{at}rz.uni-karlsruhe.de

Rechnerinfektionen mit Würmern sind mittlerweile an der Tagesordnung, Während bei kleineren Netzwerken dieses Problem noch mit Handarbeit in den Griff zu bekommen ist, skaliert diese Methode bei größeren Netzwerken nicht mehr. Dies tritt insbesondere bei wissenschaftlich genutzten Netzwerken auf, da diese einer hohen Rechnerfluktuation unterworfen sind und eine große Vielfalt von Rechnerplattformen aufweisen, in der keine durchgehende Sicherheitsrichtlinie durchsetzbar ist. Aus diesem Grund muss die Sperrung von Rechnern oder Rechnerzugängen automatisiert erfolgen.

Bei der Entwicklung eines Automatismus müssen verschiedene Bedingungen berücksichtigt werden. Kernpunkt dabei sollte die Unabhängigkeit des Systems bezüglich der Netztopologie sein. Des Weiteren muss die Entwicklung flexibel, leicht anpassbar und erweiterbar sein. Dies führt zu einer modularen Bauweise; die Kommunikation zwischen den verschiedenen Komponenten geschieht dabei über standardisierte Schnittstellen (Webservices [W3C02]) mittels SOAP [W3C03].

Um Rechner zu erkennen, die mit Schadsoftware infiziert sind, müssen innerhalb der Netzwerktopologie verschiedene Mechanismen realisiert werden, um Informationen über den infizierten Rechner zu erhalten. Diese Mechanismen sind Filter im Datenstrom, elektronische Köder und Überwachungs-systeme an gespiegelten Netzanschlüssen. Für diese Maßnahmen müssen die entsprechenden Sensormodule an die spezifischen Systeme angepasst werden.

An der Universität Karlsruhe (TH) sind die grundlegenden Komponenten momentan implementiert. Dies beinhaltet die Komponenten zur Datensammlung, Datenhaltung und Auswertung. Sperrmodule und weitere Sensormodule sind in Planung.

Die Maßnahmen zur Sperrung eines Rechners oder Rechnerzugangs sind aufgrund der im Datenstrom nachgestellen Sensorik nur reaktiv möglich - eine Neuinfektion anfälliger Systeme kann so nicht verhindert werden. Es aber möglich, den Betreuern von großen Netzinstallationen einen effizienten Überblick über die schadhaften Systeme zu geben. Durch die ständige Analyse des Datenstroms können so auch Auffälligkeiten an Systemen erkannt werden, die auf eine Infektion oder ein kompromittiertes System hinweisen und mit herkömmlichen Verfahren nicht erkannt worden wären. Dies ist insbesondere bei einer großen Plattformheterogenität von Vorteil.

Ein ähnlicher Ansatz wird von der Universität Duisburg-Essen [Rie05] verfolgt - dieses System verwendet ein Honeynet für die Detektion von Einbrüchen. Der Aspekt der reaktiven Sperrung von Rechnerzugängen ist dort auf den physikalischen Rechnerzugang beschränkt. Dies setzt eine homogene Netzinfrastruktur im Zugangsbereich, sowie einen dedizierten Zugang für jeden Rechner im Netz voraus.

Literatur

[W3C03] W3C SOAP Specification, http://www.w3.org/TR/soap/, last seen: 30.5.2006

[W3C02] W3C Webservices, http://www.w3.org/2002/ws/, last seen: 30.5.2006

[Rie05] Stephan Riebach, Birger Toedtmann, Erwin Rathgeb, Combining IDS and Honeypot Methods for Improved Detection and Automated Isolation of Compromised Systems, University of Duisburg-Essen, DIMVA 2005

Ein Sicherheitsportal zur Selbstverwaltung und automatischen Bearbeitung von Sicherheitsvorfällen als Schlüsseltechnologie gegen Masseninfektionen

Jochen Kaiser*, Alexander Vitzthum*, Peter Holleczek*, Falko Dressler†

*Regionales Rechenzentrum †Rechnernetze und Kommunikationssysteme, Institut für Informatik, Universtität Erlangen

Die massive Zunahme von Sicherheitsvorfällen sorgt für eine Verschärfung der Bedrohungslage und eine drastische Zunahme der möglichen bzw. tatsächlichen Schäden. Viele Endsysteme sind mit Malware kompromittiert und bleiben es für lange Zeit, da die Kompromittierung durch den Endnutzer nicht erkannt wird und/oder ohne fremde Hilfe auch nicht entfernt werden kann. Oftmals findet von den betroffenen Systemen aus eine Infizierung/Kompromittierung weiterer Systeme statt. Durch eine frühzeitige Erkennung und Auflösung von Sicherheitsvorfällen kann die Situation deutlich verbessert werden. An der Universität Erlangen wurde die PRISM (Portal for Reporting Incidents and Solution Managment) Plattform entwickelt. Es handelt sich hierbei um ein modulares System, welches Sicherheitsvorfälle über mehrere Pfade gemeldet bekommt und Endnutzern dann die Möglichkeit bietet, diese Sicherheitsvorfälle selbst zu beheben. Dadurch kann frühzeitig ein Sicherheitsvorfall behoben werden und der Schaden für den Betroffenen und durch frühzeitige Verhinderung der Weiterverbreitung auch für weitere Nutzer begrenzt werden. PRISM liegt eine modulare Architektur zugrunde, welche sich durch einfache Erweiterbarkeit auszeichnet. Die einzelnen Systemkomponenten können dabei folgende Kategorien aufgeteilt werden: Aufzeichnungseinheiten, welche Sicherheitsvorfälle entgegennehmen, zentrale Auswertelogiken, sowie Frontends, wie z.B. ein Selbstbedienungsterminal für die Nutzer-unterstützte Auflösung von Sicherheitsvorfällen. Die Eingabe von Sicherheitsvorfällen kann hierbei auf mehrere Weisen erfolgen. In der experimentellen Implementierung sind Sensoren integriert, die über das IDMEF (Intrusion Detection Message Exchange Format) Protokoll die Sicherheitsmeldungen an den Systemkern weitergeben. Der Datenverkehr eines Nutzers, welcher mit seinem System in das Internet gelangen will, wird dabei auf das Selbstbedienungsterminal umgeleitet. Daher wird bei Nutzung des Web-Browsers der Nutzers nun automatisch auf eine spezielle Seite umgeleitet, welche neben der Darstellung des Sicherheitsproblems auch Zusatzinformationen zur Behebung des Sicherheitsproblems. Ein möglicher Einsatzzweck sind Universitäten, deren offene Forschungsnetze und anspruchsvolle Nutzergruppen besondere Herausforderungen an das IT-Sicherheitsmanagement stellen. Ein anderer Einsatzzweck ist das Management von Endkunden bei Zugangsprovidern. Endkunden sind üblicherweise nicht in der Lage ihr Endsystem so abzusichern, dass keine Sicherheitsvorfälle entstehen. Ebenso werden auch Sicherheitsvorfälle mit Malware nicht erkannt und behoben. Hier kann nun das Sicherheitsportal Abhilfe leisten und den Endkunden kostengünstig auf den Sicherheitsvorfall hinweisen und ihn interaktiv lösen. Die beschriebene Komponente ist Teil einer in der Entwicklung befindlichen Architektur zur Verbesserung der Sicherheit in Netzwerken. Die wesentlichen Eckpunkte der Untersuchung sind hierbei das Einordnen und das Routing bzw. die Eskalation von Sicherheitsvorfällen. Ein weiterer wichtiger Aspekt ist das Finden von Lösungen für diese kritischen Ereignisse. Hierbei wird auch analysiert, wie diese Lösungen in ein Vorfallsmanagementsystem integriert werden können und welche Anforderungen an Schnittstellen hier existieren. Die Untersuchungen sollen dazu beitragen, den massiven automatischen Infektionen mit Malware durch eine möglichst automatisierte Betreuung von Sicherheitsvorfällen zu begegnen. Der Vorteil, welchen Malware durch den Einsatz automatischer Verbreitungsverfahren hat, soll hierbei wieder wettgemacht werden, was eine manuelle Auflösung von Sicherheitsvorfällen nicht leisten kann.

Wie man Einbrüche mit Experimenten analysiert

Stephan Neuhaus

Universität des Saarlandes

Die Analyse von Einbrüchen ist schwierig, weil sie größtenteils von Hand gemacht werden muss. Die wenigen Werkzeuge, die es gibt (z.B. METAL [LBJ05] oder BackTracker [KC03]), arbeiten, indem sie von den vorhandenen Spuren ausgehend rückwärts auf die Ursache schließen. Das erfordert aber eine Modellbildung und eine genaue Kenntnis des angegriffenen Systems. Ist das Modell fehlerhaft, die Kenntnis des Systems lückenhaft oder sind die vorhandenen Spuren nicht ausreichend oder nicht verlässlich, kommt es zu lückenhaften oder fehlerhaften Analysen.

Wir haben ein Werkzeug namens Malfor entwickelt, dass diese Probleme mit *Experimenten* löst [NZ06]. Dazu zeichnen wir zunächst den Produktivbetrieb auf. Finden wir einen Einbruch, spielen wir Teile der aufgezeichneten Ereignisse wieder ein: Findet der Einbruch auch ohne Ereignis X statt, kann X für den Einbruch nicht relevant gewesen sein. Unter Kontrolle eines Minimierungs-Algorithmus namens Delta Debugging [HZ02] wiederholen wir das Einspielen mit immer anderen Ereignismengen, bis nur noch relevante Ereignisse übrig sind. Wir finden so vollautomatisch die für den Angriff relevanten Prozesse und dehnen das Verfahren gerade auf angriffsverursachende Netzwerkeingaben von Prozessen (Angriffs-Signaturen) aus.

Wir haben dieses Verfahren erfolgreich auf einen Angriff angewandt, der mit herkömmlichen Methoden nur schwer oder gar nicht analysierbar ist. Dieser Angriff lädt über einen fehlerhaft konfigurierten Apache-Webserver ein Kernel-Modul, das einen zusätzlichen root-Account in die Passwortdatei einfügt. Die Passwortdatei wird dabei niemals von einem Prozess geöffnet oder anderweitig modifiziert. Diese erfolgreiche und *vollautomatische* Analyse zeigt die Stärke unseres Ansatzes.

Weitere Vorteile experimenteller Analyse sind: Die so gewonnenen Erkenntnisse sind *evident richtig*: Die Korrektheit der Erkenntnisse beruht nicht auf einer möglicherweise falschen Deduktion sondern ist unmittelbar einem Satz von Experimenten zu entnehmen. Als Ergebnis einer solchen experimentellen Analyse erhält man einen *ausführbaren Testfall*, der beliebig oft wiederholt werden kann, um weitere Erkenntnisse zu gewinnen oder um den Angriff etwa vor Gericht zu demonstrieren.

Literatur

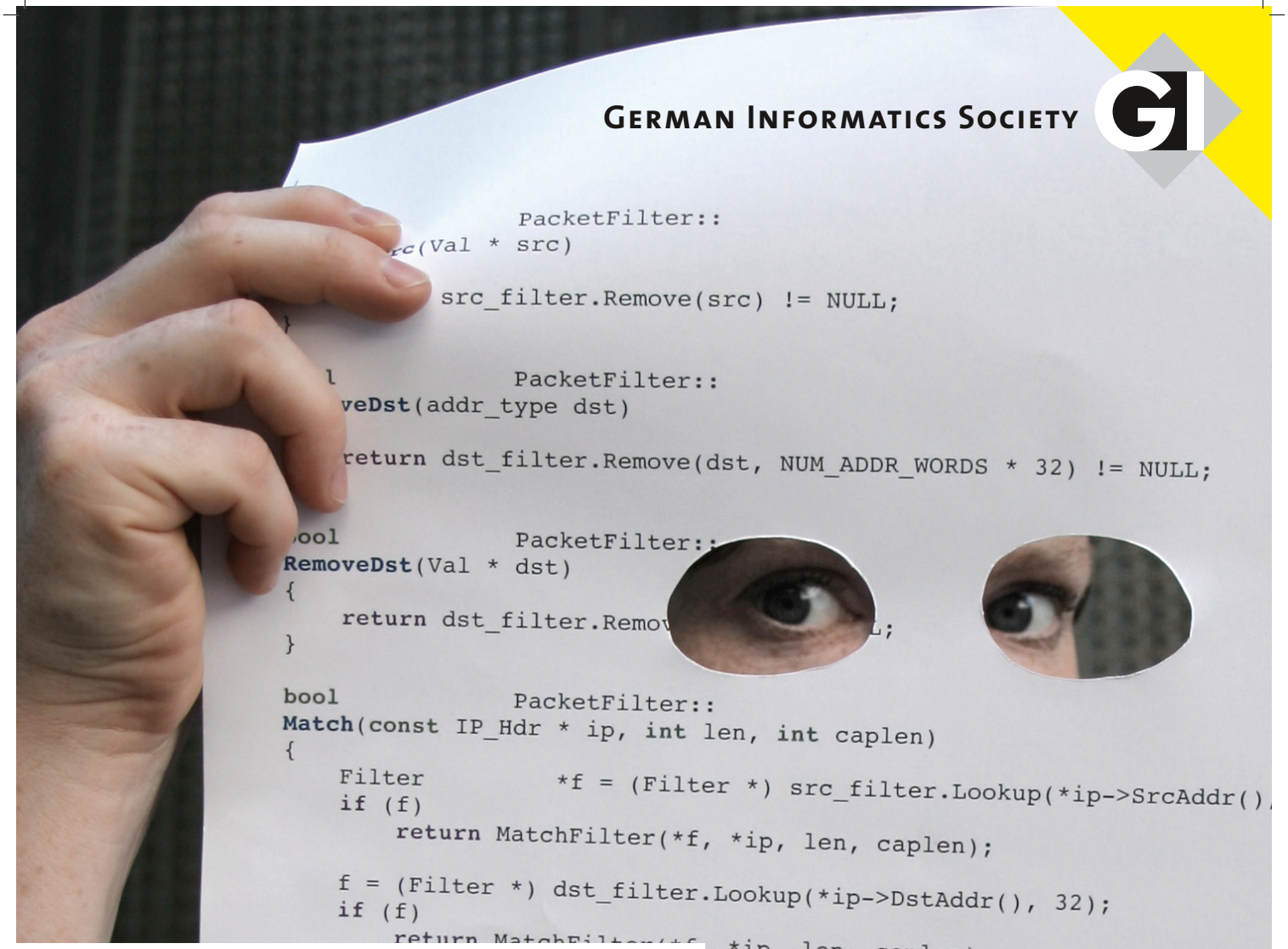
[HZ02] Hildebrandt, Ralf ; Zeller, Andreas: Simplifying and Isolating Failure-Inducing Input. In: *IEEE Transactions on Software Engineering* 26 (2002), Februar, Nr. 2, S. 183–200

[KC03] King, Samuel T. ; Chen, Peter M.: Backtracking intrusions. In: *Proceedings of the Nineteenth ACM Symposium on Operating Systems Principles*. New York, NY, USA : ACM Press, 2003. – ISBN 1–58113–757–5, S. 223–236

[LBJ05] Larson, Ulf ; Barse, Emilie L. ; Jonsson, Erland: METAL: A Tool for Extracting Attack Manifestations. In: Julisch, Klaus (Hrsg.) ; Krügel, Christopher (Hrsg.): *Proceedings of the Second International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, Springer Verlag, Juli 2005 (Lecture Notes in Computer Science 3548). – ISBN 3–540–26613–5, S. 85–102

[NZ06] Neuhaus, Stephan ; Zeller, Andreas: Isolating Intrusions by Automatic Experiments. In: *Proceedings of the 13th Annual Network and Distributed System Security Symposium*. Reston, VA, USA : Internet Society, Februar 2006. – ISBN 1–891562–22–3, S. 71–80

German Informatics Society



DIMVA 2006

Detection of Intrusions and Malware & Vulnerability Assessment

July 13-14, 2006
Berlin, Germany

Location:

Berlin-Brandenburg Academy of Sciences and Humanities

Conference and Event Centre
Markgrafenstraße 38
D -10117 Berlin

In cooperation with IEEE, enisa

Live at DIMVA:
2nd European Capture-The-Flag contest CIPHER on July 14th

Keynotes:
John McHugh, Dalhousie University, Canada
Michael Behringer, Cisco Systems, France

Organizing Committee:
General Chair: Pavel Laskov, Fraunhofer FIRST, Germany
Program Chair: Roland Büschkes, RWE AG, Germany
Sponsoring Chair: Marc Heuse, n.runs GmbH, Germany
Publicity Chair: Ulrich Flegel, University of Dortmund, Germany

You never know what lurks behind the code! Viruses, worms, spyware, and hidden vulnerabilities have become part of an everyday concern of system administrators and ordinary users. To counter an imminent threat of hacker attacks, security mechanisms should be able to adapt to changing environments and promptly react to incidents. By bringing together experts in reactive security from academic, governmental and commercial institutions, DIMVA facilitates development of novel security approaches and their smooth transfer into practice.

McAfee, TSB, symantec., nruns...

Special Interest Group SIDAR

www.dimva.org