Selbstschützende mobile Systeme

Stephan Groß
Technische Universität Dresden
01062 Dresden
Email: st.gross@inf.tu-dresden.de

Abstract: Die meisten in herkömmlichen Netzen eingesetzten Sicherheitsmaßnahmen gehen von einer fixen Netzwerktopologie aus und untersuchen an zentralen Positionen die übertragenen Datenflüsse auf potentiell gefährliche Inhalte. Hierbei greift ihre Konfiguration implizit auf ein Modell der Netzwerkstruktur zurück. Die Anwendung dieser Maßnahmen in einem mobilen Umfeld ist daher schwierig, da dessen dynamische Struktur die permanente Anpassung dieses Netzmodells erfordert. Zudem erlaubt die eingeschränkte Leistungsfähigkeit mobiler Geräte keine aufwendigen Analysen der übertragenen Datenflüsse. Wir schlagen daher vor, mobile Netze nicht als Ganzes zu schützen sondern jedes einzelne System abzusichern. Anstelle einer globalen Sicht auf das Netzwerk setzen wir damit eine Vielzahl lokaler Modelle. Wir stellen ein erstes Architekturmodell für ein selbstschützendes mobiles System vor und diskutieren dadurch aufgeworfene Fragen.

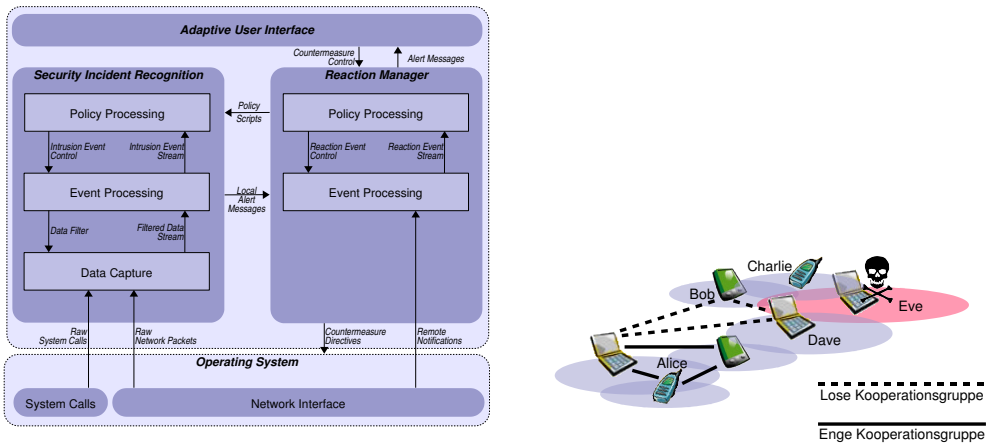
1 Motivation

Mobile Geräte werden in unterschiedlichen und oft nur wenig vertrauenswürdigen Umgebungen betrieben. Sie sind daher ebenso wie herkömmliche Computer einer Vielzahl von Bedrohungen ausgesetzt. Schlimmer noch, kompromitierte Geräte bieten Angreifern eine Möglichkeit zur Umgehung zentraler Verteidigungslinien wie Firewalls oder VPN Gateways und stellen damit eine Bedrohung für bestehende Intranets dar [ZLH03]. Es scheint also geboten, die Anstrengungen für die Entwicklung sicherer mobiler Geräte zu verstärken [BH03]. Heutige Sicherheitsmaßnahmen zum Schutz von Rechnernetzen können unterteilt werden in präventive und überwachende Maßnahmen. Präventive Maßnahmen versuchen Sicherheitsbedrohungen zu verhindern, indem potentiell gefährliche Aktionen unterbunden werden. Dies erfolgt durch vergleichsweise „einfache“ Techniken zur Kontrolle des Zugriffs auf Systemressourcen (z.B. Firewalls oder Anti-Viren Software) oder aber durch technisch ausgefeiltere Methoden wie zum Beispiel Virtuelle Private Netze, die mittels kryptographischer Verfahren das Abhören von Kommunikationsverbindungen verhindern. Auf der anderen Seite dienen überwachende Maßnahmen der Entdeckung anomalen Systemverhaltens. So durchsuchen Log-Monitore die Protokolldaten eines Systems nach unerwünschten Aktionen in der Vergangenheit. Intrusion Detection Systeme (IDS) sind darüber hinaus in der Lage potentiell gefährliche Operationen bereits zur Laufzeit zu erkennen oder sogar zu unterbinden (Intrusion Detection and Response oder Intrusion Prevention Systeme). Die Installation, Konfiguration und Kontrolle solcher Systeme erfordert jedoch ein profundes Sicherheitswissen über das der durchschnittliche Anwender eines mobilen Endgeräts in aller Regel nicht verfügt. In der mobilen Welt benötigen wir daher autonom agierende Systeme, die in der Lage sind sich weitgehend selbst zu schützen und in ihrer Bedienung den Anwender nicht überfordern. Ein weiterer Nachteil bei der Anwendung herkömmlicher Netzsicherheitstechniken im mobilen Umfeld stellt die gängige Praxis dar, das Netz von zentralen Punkten aus zu überwachen und als Ganzes zu schützen. Damit fließt die vorhandene Netztopologie zumindest implizit in die Konfiguration der eingesetzten Sicherheitsmaßnahmen ein. Dieses Vorgehen ist für die sich häufig ändernden mobilen Umgebungen nicht praktikabel. Stattdessen sollte jedes einzelne Gerät bestmöglich geschützt werden.
Im folgenden beschreiben wir unsere Vision von selbstschützenden mobilen Systemen und diskutieren wesentliche Herausforderungen für deren Umsetzung. Kapitel 2 behandelt die grundlegenden Komponenten einer initialen Systemarchitektur. Darüber hinaus stellen wir ein Konzept vor, mit dem vertrauenswürdi-

ge Systeme gemeinsam ihren individuellen Schutz verbessern können. Kapitel 3 vergleicht unsere Ideen mit vorhandenen Arbeiten, fasst erste Ergebnisse zusammen und gibt einen Ausblick auf weitere geplante Schritte.

2 Kernkomponenten selbstschützender mobiler Systeme

Das fehlende Know-How eines gewöhnlichen Anwenders und die Dynamik ihres Umfelds machen neue Strategien zum Schutz mobiler Netze notwendig. Ein mobiles System muss sich möglichst gut selbst schützen können. Dazu sollte es sich nicht nur selbständig gegen Angriffe verteidigen sondern diese auch frühzeitig vorhersehen. Abbildung 1(a) zeigt eine erste Systemarchitektur für ein solches System, die in den folgenden Abschnitten ebenso erläutert wird, wie der in Abbildung 1(b) dargestellte Ansatz für die Zusammenarbeit einander vertrauender Systeme, mit dem Ziel besser und schneller auf Bedrohungen zu reagieren.



(a) Basisarchitektur

(b) Kooperationsstrategien

Abbildung 1: Selbstschützende mobile Systeme

Adaptive Benutzerschnittstelle. Die wachsende Komplexität bleibt eine der größten Herausforderungen bei der Entwicklung von IT-Systemen. Gerade Sicherheitslösungen stehen in dem Ruf, nur schwer bedienbar zu sein und den normalen Arbeitsablauf zu behindern [WT]. Adaptive Benuzterschnittstellen [WP00, Whi04] helfen das Risiko von Fehlkonfigurationen zu minimieren und machen die Bedienung für unerfahrene Nutzer einfacher. Die Interaktion mit dem Nutzer sollte dabei kontinuierlich an dessen Wissensstand angepasst werden.

Erkennen und Bekämpfen von Sicherheitsverletzungen. Die Komponenten zur Erkennung möglicher Sicherheitsverstöße fassen wir unter dem Namen *Security Incident Recognition (SIR)* zusammen. Es handelt sich hierbei um ein host-basiertes IDS zur Überwachung des Systems und seiner Umgebung. Wir erweitern hierfür Bro [Pax99] und REMUS [BGM02] um sowohl den lokalen Netzverkehr als auch das lokale Systemverhalten zu überwachen. Sobald die SIR eine schädliche Aktion entdeckt, informiert sie den *Reaction Manager*, der über das weitere Vorgehen entscheidet. Beide Komponenten ähneln sich im Aufbau, der aus den Entwurfsanforderungen *Trennung von Sicherheitsmechanismen und -politik* sowie *Effizente Verarbeitung* resultiert. Sicherheitspolitiken sind typischerweise untrennbar mit der Umgebung verbunden, für die sie aufgestellt wurden. Verändert sich die Umgebung, muss auch die Sicherheitspolitik an die geänderten Voraussetzungen angepasst werden. Eine klare Trennung von Spezifikation und Implementierung hilft, das System einfach und flexibel zu halten. Das mehrstufige Filtern der verarbeiteten Daten in den einzelnen Schichten unseres Architekturentwurfs soll den Ressourcenbedarf minimieren und damit einen reibungs-

losen Betrieb des Gesamtsystems auch auf ressourcenschwachen Geräten sicherstellen. Der Reaction Manager als zentrale Kontrollinstanz für das Eindämmen schädlicher Aktivitäten initiiert lokale Gegenmaßnahmen indem er durch entsprechende Anweisungen an das Betriebssystem die Ausführung bestimmter Systembefehle oder die weitere Kommunikation mit einer bestimmten Netzwerkadresse unterbindet. Darüberhinaus reagiert er auf eingehende Warnungen von benachbarten Systemen und koordiniert gemeinsame Reaktionen.

Kooperationsstrategien. Die Fokussierung auf den Schutz des einzelnen Systems birgt auch Probleme. So wird das mobile Netz als Gesamtsystem nur noch eingeschränkt wahrgenommen, da jedes Einzelsystem nur die Systeme in seiner Funkreichweite kennt. Dies und die eingeschränkten Systemressourcen mobiler Geräte behindert die Erkennung von Angriffen. In Analogie zur nachbarschaftlichen Hilfe in der realen Welt streben wir eine koordinierte Zusammenarbeit zur Überwindung dieser Einschränkungen an. Wir definieren hierzu eine sogenannte *Kooperationsgruppe* als Menge gemeinsam agierender Systeme. Dabei teilen die Systeme in einer *engen Kooperationsgruppe* sowohl ihr Wissen als auch ihre Systemressourcen während in einer *losen Kooperationsgruppe* lediglich Informationen ausgetauscht werden. Die Mitgliedschaft in einer Kooperationsgruppe wird durch den Reaction Manager verwaltet. In Abbildung 1(b) hat Alice ihre Geräte in einer engen Kooperationsgruppe zusammengefasst, so dass ihr Handy beispielsweise rechenintensive Analyseaufgaben an ihren Laptop delegieren kann. Darüber hinaus ist sie Mitglied einer losen Kooperationsgruppe mit Bob und Dave. Diese warnen Alice vor der Angreiferin Eve bevor sie überhaupt in deren Funkreichweite ist. Der Unterschied zwischen beiden Arten von Kooperationsgruppen lässt sich vor allem am Grad des Vertrauens festmachen, den die beteiligten Geräte einander entgegenbringen. In Informationssystemen werden Vertrauensbeziehungen meist durch kryptographische Verfahren wie asymmetrische Verschlüsselungs- oder Signatursysteme realisiert. Die Bereitstellung der hierfür notwendigen öffentlichen Schlüssel ist in unserem Szenario jedoch nur schwer zu realisieren, da die Verfügbarkeit einer Public Key Infrastructure nicht garantiert werden kann. Für enge Kooperationsgruppen können stattdessen Pairing-Mechanismen verwendet werden wie sie aus dem Bluetooth-Protokoll bekannt sind. Hiermit kann eine gesicherte Verbindung zwischen zwei Geräten aufgebaut werden indem auf jedem Gerät ein gemeinsamer Code eingegeben wird aus dem im weiteren Verlauf des Verfahrens ein sicherer symmetrischer Schlüssel zur Verschlüsselung des Datenverkehrs generiert wird. Für lose Kooperationsgruppen sind peer-basierte Lösungen wie das von PGP bekannte Web-of-Trust eine Lösung. Die Verwendung von Empfehlungssystemen, um eigene Erfahrungen mit denen anderer zu kombinieren und so die Vertrauenswürdigkeit eines Partners einzuschätzen, ermöglicht darüber hinaus die Zusammenarbeit für den Fall, dass kein kryptographisch gesicherter Kommunikationskanal zur Verfügung steht [MG05].

3 Diskussion und Ausblick

Unser Ansatz wurde durch eine Vielzahl von Arbeiten aus unterschiedlichen Bereichen inspiriert. Ganger und Nagle propagieren in ihrem eher informellen Papier [GN01] die Errichtung von Schutzwällen um die einzelnen Systeme eines Netzwerkes und vergleichen diese Taktik mit dem Schutz mittelalterlicher Festungen vor Belagerungen. Die Idee kooperierender IDS wurde erstmals 1996 von White, Fisch und Pooch vorgestellt [WFP96]. Seitdem griffen mehrere Implementierungen diesen Gedanken auf ohne jedoch die besonderen Anforderungen im mobilen Umfeld zu berücksichtigen [PN97, SZ00, KTK01, JWZ03]. Aktuelle Arbeiten zu Wireless IDS gehen die Probleme von unterschiedlichen Seiten an, weisen durch ihre eingeschränkte Sichtweise aber immer wieder Defizite auf. Entweder wird wie in [LSLO03, SLO04, BJDS04] stillschweigend die Existenz einer zentralen Infrastruktur vorausgesetzt oder man konzentriert sich auf einen eng begrenzten Aspekt des Gesamtsystems wie zum Beispiel das Routing in Ad-hoc Netzen [PMdSJ03,PPM$^+$03,ZLH03]. Allen Ansätzen gemein ist ihre Fokussierung auf technische Fragen. Prozess- und Bedienbarkeitsaspekte werden weitgehend außer Acht gelassen. Gerade in diesem Bereich haben wir Anleihen bei den Self-X Konzepten aus dem noch recht jungen Gebiet des Autonomic Computing genommen, das sich die einfache Nutzung komplexer Systeme auf die Fahnen schreibt [KC03, GC03, BBC$^+$03].

Unser Prototyp befindet sich zur Zeit noch im Aufbau. Eine erste Version der Security Incident Recognition Komponente wurde gerade fertiggestellt. Hierfür wurden der Event-Handler und die Policy-Engine von Bro erweitert. Im Rahmen dieser Arbeiten wurde auch eine umfangreiche Klassifikation in der Literatur beschriebener Angriffe erstellt. Sie bildet die Grundlage für erweiterte Bro-Policies, um Angriffe auf IEEE 802.11 WLAN-Verbindungen aufzudecken. Darüber hinaus haben wir mit den technischen Grundlagen für den Aufbau von Kooperationsgruppen begonnen. Diese ergänzen die bereits in Bro vorhandenen Mechanismen zum Nachrichtenaustausch mit anderen Systemen. Unser Hauptaugenmerk liegt dabei auf der Evaluation aus der Literatur bekannter Verfahren für die Realisierung von Vertrauensbeziehungen wie zum Beispiel Trust Management Systeme. Auch wenn uns momentan noch praktische Erfahrungen fehlen, so sind wir dennoch überzeugt, dass unser Ansatz eine vielversprechende Lösung für den Schutz mobiler Netze darstellt. Die Fertigstellung eines ersten Prototypen ist für Mitte 2006 geplant.

Literatur

[BBC+03] D. F. Bantz, C. Bisdikian, D. Challener, J. P. Karidis, S. Mastrianni, A. Mohindra, D. G. Shea und M. Vanover. Autonomic personal computing. *IBM Systems Journal*, 42(1):165–176, 2003.

[BGM02] Massimo Bernaschi, Emanuelle Gabrielli und Luigi V. Mancini. REMUS: A Security-Enhanced Operating System. *ACM Transactions on Information and System Security*, 5(1):36–61, Februar 2002.

[BH03] Levente Buttyán und Jean-Pierre Hubaux. Report on a Working Session on Security in Wireless Ad Hoc Networks. *ACM SIGMOBILE Mobile Computing and Communications Review*, 7(1):74–94, Januar 2003.

[BJDS04] Joel W. Branch, Nick L. Petroni Jr., Leendert Van Doorn und David Safford. Autonomic 802.11 Wireless LAN Security Auditing. *IEEE Security & Privacy*, 2(3):56–65, Mai 2004.

[GC03] A. G. Ganek und T. A. Corbi. The dawning of the autonomic computing era. *IBM Systems Journal*, 42(1):5–18, 2003.

[GN01] Gregory R. Ganger und David F. Nagle. Better Security via Smarter Devices. In *Proceedings of the 8th Workshop on Hot Topics in Operating Systems (HotOS-VIII)*, Elmau, Germany, Mai 2001. IEEE.

[JWZ03] R. Janakiraman, M. Waldvogel und Q. Zhang. Indra: A peer-to-peer approach to network intrusion detection and prevention. In *12th IEEE International Workshop on Enabling Technologies (WETICE 2003), Infrastructure for Collaborative Enterprises*, Linz, Austria, Juni 2003.

[KC03] Jeffrey O. Kephart und David M. Chess. The Vision of Autonomic Computing. *IEEE Computer*, 36(1):41–50, Januar 2003.

[KTK01] Christopher Krügel, Thomas Toth und Engin Kirda. Sparta – a mobile agent based intrusion detection system. In *IFIP Conference on Network Security*, Belgium, 2001. Kluwer Academic Publishers.

[LSLO03] Yu-Xi Lim, Tim Schmoyer, John Levine und Henry L. Owen. Wireless Intrusion Detection and Response. In *Proceedings of the 2003 IEEE Workshop on Information Assurance*, Seiten 68–75, United States Military Academy, West Point, NY, USA, Juni 2003. IEEE.

[MG05] Seamus Moloney und Philip Ginzboorg. Security for Interactions in Pervasive Networks: Applicability of Recommendation Systems. In C. Castelluccia et al., Hrsg., *ESACS 2004*, number 3313 in LNCS, Seiten 95–106, Berlin Heidelberg, 2005. Springer-Verlag.

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

[PMdSJ03] Ricardo Staciarini Puttini, Ludovic Mé und Rafael Timóteo de Sousa Jr. Preventive and Corrective Protection for Mobile Ad Hoc Network Routing Protocols. In *Wireless On-Demand Network Systems*, Jgg. 2928 of *LNCS*, Seiten 213–226. Springer-Verlag Heideberg, Dezember 2003.

[PN97] P. A. Porras und P. G. Neumann. Emerald: Event monitoring enabling responses to anomalous live disturbances. In *20th National Information Systems Security Conference*, Seiten 353–365, Oktober 1997.

[PPM+03] Ricardo S. Puttini, Jean-Marc Percher, Ludovic Mé, Olivier Camp, Rafael de Sousa Jr., Cláudia J. Barenco Abbas und L. Javier García-Villalba. A Modular Architecture for Distributed IDS in MANET. In Vipin Kumar, Marina L. Gavrilova, Chih Jeng Kenneth Tan und Pierre L'Ecuyer, Hrsg., *Computational Science and Its Applications – ICCSA 2003*, Jgg. 2669 of *LNCS*, Seiten 91–113, Montreal, Canada, August 2003. Springer-Verlag Heidelberg.

[SLO04] Timothy R. Schmoyer, Yu Xi Lim und Henry L. Owen. Wireless Intrusion Detection and Response – A case study using the classic man-in-the-middle attack. In *Proceedings of the 2004 IEEE Wireless Communications and Networks Conference*, Atlanta, Georgia, USA, Marz 2004.

[SZ00] Eugene H. Spafford und Diego Zamboni. Intrusion detection using autonomous agents4. *Computer Networks*, (34):547–570, 2000.

[WFP96] Gregory B. White, Eric A. Fisch und Udo W. Pooch. Cooperating Security Managers: A Peer-Based Intrusion Detection System. *IEEE Network*, 10(1):20–23, January/February 1996.

[Whi04] Alma Whitten. *Making Security Usable*. Dissertation, Carnegie Mellon University, Mai 2004. CMU-CS-04-135.

[WP00] G. Wolf und A. Pfitzmann. Properties of Protection Goals and their Integration into a User Interface. *Computer Networks, Special Issue on Electronic Commerce*, 32, 2000.

[WT] A. Whitten und J. D. Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. Carnegie Mellon University, Pittsburgh, PA. Retrieved April, 12 2005 from http://www.gaudior.net/alma/johnny.pdf.

[ZLH03] Yongguang Zhang, Wenke Lee und Yi-An Huang. Intrusion Detection Techniques for Mobile Wireless Networks. *Wireless Networks*, 9(5):545–556, September 2003.