Ulrich Flegel, Michael Meier (Eds.)

Detection of Intrusions and Malware & Vulnerability Assessment

GI Special Interest Group SIDAR Workshop, DIMVA 2004
Dortmund, Germany, July 6-7, 2004
Proceedings

Gesellschaft für Informatik 2004

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

Volume P-46

ISBN 3-88579-375-X
ISSN 1617-5468

Volume Editors
Ulrich Flegel
University of Dortmund,
Computer Science Department, Chair VI, ISSI
D-44221 Dortmund, Germany
ulrich.flegel@udo.edu
Michael Meier
Brandenburg University of Technology Cottbus,
Computer Science Department, Chair Computer Networks
P.O. Box 10 13 44, D-03013 Cottbus, Germany
mm@informatik.tu-cottbus.de

printed by Köllen Druck+Verlag GmbH, Bonn

Aktive Strategien zur Schutzzielverletzungerkennung durch eine kontrollierte Machtteilung in der Zugriffskontrollarchitektur

Joerg Abendroth*
Distributed Systems Group
Trinity College, Dublin
Joerg@Abendroth.info

Abstract: Zugangskontrolle und Intrusion Detection werden oft separat behandelt. Zur Erkennung von Schutzzielverletzungen wird hauptsächlich der Datenverkehr eines Netzwerkes ausgewertet - dies geschieht in einer passiven Weise.
Aktive Strategien zum Erkennen von Angriffen sind nur durch neue Zugriffskontrollsysteme und kontrollierte Machtteilung möglich.
In dem vorliegenden Beitrag wird eine neue Kategorisierung von Zugriffskontrollsysteme vorgestellt und insbesondere auf die kontrollierte Machtteilung eingegangen. Es wird gezeigt wie neue aktive Strategien zur Schutzzielverletzungserkennung möglich werden. Diese Strategien erlauben auch den Missbrauch berechtigter Benutzer, die ihre Befugnisse missbrauchen, zu erkennen. Ebenso können nun bekannte Ideen aus der SPAM Bekämpfung in die Zugangskontrolle übernommen werden. Ein Prototyp wurde mittels der ASCap Architektur implementiert und zeigt, dass die vorgestellten Techniken einsetzbar sind.

1 Zugangskontrollsysteme und Schutzzielverletzungserkennung

Auf dem Gebiet der Zugangskontrollsysteme werden oft Neuerungen vorgestellt, welche die Verwaltung oder Anpassung an bestimmte Anwendungen erleichtern. Als Beispiel mag RBAC[1] [FK92] dienen, das die Verwaltung durch die Einführung einer Abstraktionsschicht, den sogenannten Rollen, erleichtert. Doch wenige Ansätze berücksichtigen ein Hauptproblem der Praxis - nämlich, dass fast jede Anwendung ein Einzelsystem darstellt und applikations- oder verwaltungsbereichübergreifende Zugangsregeln nur schwer realisiert werden können. Wenn dieses Problem auf der Ebene der Zugangskontrolle gelöst ist, dann eröffnen sich interessante Möglichkeiten auf der Ebene der Intrusion Detection Systeme (IDS). Verknüpfte Systeme, die es dem IDS erlauben in Zugriffskontrollmechanismen einzugreifen, ermöglichen nicht nur passive, sondern aktive Strategien zur Angriffserkennung.

*Der Author ist durch ein Forschungsstipendium der IONA Technologies PLC unterstützt.
[1] Role Based Access Control

Traditionell gibt es auf dem Gebiet der IDS zwei Hauptrichtungen: Schutzzielverletzungen werden entweder anhand ihrer Angriffssignaturen erkannt [ER88, De87] oder durch eine Abweichung von dem historisch bekannten, angriffsfreien Datenverkehr [LJ88]. Bei beiden Ansätzen wird der Datenverkehr passiv beobachtet. Intrusion Prevention Systeme (IPS) erweitern die bekannten IDS Systeme um ein aktives Element. Diese Systeme können in den Datenverkehr aktiv eingreifen. So kann ein als Gateway eingesetzes IPS System den Datenverkehr von OSI Schicht 7 auswerten und sogar verändern. Ein wichtiger Anwendungsfall sind große Firmennetze, die Softwarepatches nicht zeitnah einspielen können. IPS Systeme können etwaige Sicherheitslücken am Netzübergang stopfen.

Analysiert man die Strategien mit denen die Intrusion Prevention Systeme entscheiden ob ein Angriff vorliegt, dann findet man wieder die gleichen zwei *passiven* Techniken. *Aktive* Systeme hingegen würden nicht nur beobachten, sondern bei Alarmzeichen oder als "routinemäßigen Rundgang" das System so verändern, dass Eindringlinge bemerkt werden. Strategien aktiver IDS befassen sich nicht mit den Anwendungen und deren Schwachstellen, sondern dem Angreifer und dessen Eigenschaften. Für diese aktiven Strategien ist eine Verknüpfung der Zugriffskontrollarchitektur (ZKA) und IDA nötig. Diese verknüpften Systeme müssen Zugriffspolitiken haben, die eine kontrollierte Machtteilung erlauben.

Die in [AJ03] vorgestellte ZKA ist universell in Anwendungen einsetzbar. Ziel dieses Entwurfes war eine flexible und bei Bedarf dynamisch umkonfigurierbare ZKA. Die Zugangsentscheidungsfunktion ist aus Unterelementen, den Regelmodulen, zusammengesetzt und wird durch einen lokalen Vermittleragenten dem jeweiligen Anwendungsdienst zugänglich gemacht. Diese Objektorientierung erlaubt eine kontrollierte, teilweise Machtteilung auf dem Gebiet der Verwaltung. Weitere Elemente der Architektur sind externe Sicherheitsserver, deren Verhalten verschiedenen Nutzungsebenen zugeordnet sein kann. So ist es beispielweise möglich, dass ein externer Sicherheitsserver ein Bindeglied zum IDS darstellt oder sein Verhalten durch deren Einflussnahme ändert.

Ist eine Verknüpfung von IDS und ZKA möglich, können grundlegend neue Strategien in dem IDS eingesetzt werden. Passives Erkennen von auftretenden Alarmzeichen kann durch ein aktives Provozieren derselben ersetzt werden. Strategien können beispielweise in Verdachtsmomenten das Zugangssystem so umkonfigurieren, dass Angriffe deutlicher sichtbar werden. Eine solche Alarmzustandskonfiguration kann jedoch einen Mehraufwand für legitime Systembenutzer bedeuten (zusätzliche Passwortabfragen z.B. per SMS, etc.).

Einen weiteren Vorteil der Verknüpfung von ZKA und IDS stellt das Auslagern der letzteren dar. Ein Security Audit in heutigen Praxis erfolgt überwigend durch einer einmaligen Zustandsüberprüfung. Schwachstellen werden zu dem Zeitpunkt der Prüfung erkannt, doch ein dauerhafter Überwachen wäre nur durch das Installieren schwer überprüfbarer Programme möglich, so dass der Kunde der externen Firma vollständig vertrauen muss. Die vorgestellte Architektur ermöglicht es jedoch, im Rahmen der ZKA die benötigten Daten an den externen Dienstleister zu liefern oder diesem teilweise Einfluss zu gewähren. Diese kontrollierte Abgabe von Verwaltungsmacht stellt eine Neuerung auf dem Gebiet der ZKA dar und ermöglicht auch die bereits erwähnte Verknüpfung mit einem IDS.

In dem vorliegenden Beitrag wird zuerst der Stand der Technik diskutiert. Danach wird in Abschnitt 3 die ASCap Architektur vorgestellt. Abschnitt 4 erörtert eine Kategorisierung der geteilten Zugriffsverwaltung. Diese ist die Grundlage um beispielweise externe Dienstleister teilweise an der Zugriffskontrolle zu beteiligen. Dann stellt Abschnitt 5 Strategiebeispiele vor, die mit der ASCap Architektur möglich werden. Zuletzt fasst Abschnitt 6 die Ergebnisse zusammen und diskutiert weiterführende Forschungsansätze.

2 Verwandte Ansätze

Auf dem Gebiet der Access Control Mechanism wurde die ASCap Architektur von den “active capabilities” [QL96] und dem “proxy principle” [Sh86] beeinflusst. Entgegen den ersten Capability basierten Betriebssystemen [Le84] geht die ASCap Architektur von keinem Referenzmonitorbereich auf dem Clientrechner aus.

Außerdem haben Forschungsergebnisse von Kühnhauser auf dem Gebiet der Metapolitiken [Kü95] die Frage aufgeworfen, wie eine kontrollierte Machtteilung in der Zugangskontrolle möglich wird. Kühnhauser stellt mit [Kü99] gezielt eine Lösung für überschneidende Verwaltungsgebiete vor, in der durch etwaige Konfliktsituationen aufgelöst werden können. Eine Erweiterung um aktive Elemente wäre möglichen, auch wenn dies nicht in den vorliegenden Forschungsbeiträgen behandelt wird.

Aktuelle IDS Systeme sind meist passiver Natur; es werden Datenströme beobachtet und Anzeichen für Verstöße gesucht (z.B. snort [We04d]). Die IPS können aktive in den Datenverkehr eingreifen (z.B. um weitere Einbruchsaktivitäten zu verhindern), doch verwenden auch nur passive Datenauswertungskomponenten. Bei IPS systemen wird die IDS mit der firewall verknüpft. Im Gegensatz dazu verknüpft die ASCap Architektur das IDS System mit der ZKA, was auch proaktives Handeln zulässt.

Die Forschung auf dem Gebiet der aktiven Netzwerke versucht nicht nur die Konfiguration und Wartung von Netzwerken zu vereinfachen, sondern stellt auch systemübergreifende Schnittstellen zur Verfügung. Hess, Jung und Schäfer [JS03] stellen mit FIRDAN eine Architektur vor, die IDS und Reaktion auf Angriffe kombiniert. Sie binden z.B. Honeypots [2] in die Verteidigung ein, indem sie Netzwerkverkehr dorthin umleiten, um mehr Informationen über den Eindringling zu sammeln. Die Komponent von FIRDAN, die Alarme auswertet, kann das System Verändern, falls ein Angreifer den eigentlichen Angriff unter einer hohe Anzahl von Falschalarmen verstecken will. So wird es möglich, einen echten Angriff trotz Täuschungsmanöver zu erkennen. Es bleibt jedoch offen, ob FIRDAN es erlaubt, mittels “Wachrundgänge” noch unentdeckte Eindringlinge zu finden.

[2] Designierte Dummyrechner, die Angreifer anlocken sollen und dann einen Alarm auslösen.

Die IDA Architektur[3] [AOTG99] sucht Anzeichen eines erfolgreichen Einbruchs und entsendet dann einen Agenten, der den Vorfall genauer untersucht. Da die Befugnisse des Agenten weitreichend sein können, wäre eine Interaktion mit der lokalen Zugriffskontrolle denkbar. In dem Fall, in dem die IDA von einem externen Dienstleister betrieben wird, erhält dieser weitreichende Kontrolle über das interne Firmennetz. Die ASCap Architektur erlaubt hier durch Einsatz der kontrollierten Machtteilung ein differenzierteres Vorgehen.

3 Die ASCap Zugriffkontrollarchitektur

Als Basis der vorgestellten Intrusion Detection Strategien dient die ASCap[4] ZKA. In diesem Abschnitt stellen wir die Hauptmerkmale vor, die für ein Verständnis zwingend notwendig sind. Für eine umfassende Beschreibung sei auf [AJ03] verwiesen.

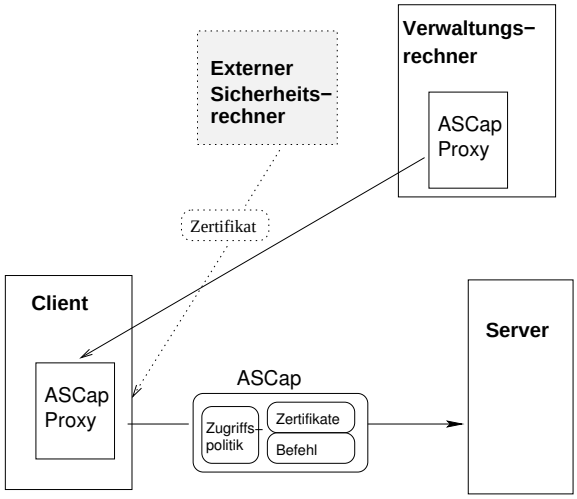

Abbildung 1: Überblick über die ASCap Zugriffskontrollarchitektur

Abbildung 1 zeigt die Komponenten der ASCap Architektur. Die vier rechteckigen Kästen symbolisieren jeweils einen eigenständigen und vernetzten Rechner. Der *Verwaltungsrechner* ist die Administrationskomponente. Sie stellt den *ASCap Proxy* zur Verfügung, der wiederum das Verhalten des Zugriffskontrollsystems bestimmt. Da es möglich ist, dass der ASCap Proxy erst kurz vor dem Versenden konfiguriert wird, ist ein dynamisches Anpassen an verschiedene Szenarien der IDS denkbar. Der *Client* stellt den Benutzerrechner da, der auf den *Server* zugreifen will. Vor Zugriffen kann eine Kommunikation mit einem externen Sicherheitsrechner vorgeschrieben sein. Der externe Sicherheitsrechner kann das Verhalten des Zugriffskontrollsystems erweitern, beispielweise ein Auswerten von Daten

[3] Intrusion Detection Agent System
[4] Active Software Capabilities

(IDS).
In fast allen Fällen liefert der externe Sicherheitsrechner ein Zertifikat zurück. Der ASCap Proxy sammelt die Zertifikate externer Sicherheitsrechner und interner Clientquellen und fasst diese mit der *Zugriffspolitik*[5] zur ASCap zusammen. Interne Clientquellen sind der genaue Zugriffswunsch (aufgeführt als *Befehl* in der Abbildung) und z.B. ein Passwort des Benutzers. Die ASCap beinhaltet somit alle Informationen des Clients, die zum Entscheiden der Zugriffsanfrage nötig sind.
Benötigt ein System beispielweise einen zeitnahen Revokation Service, können weitere externe Sicherheitsanfragen von Serverseite erfolgen. Der Server wertet die Zertifikate mit der angegebenen Zugriffspolitik aus. Diese kann entweder in ausführbarer Form (kryptographisch mittels Signatur geschützt) in der ASCap vorliegen oder per Referenz von einer gesicherten Datenbank auf dem Server geladen werden.

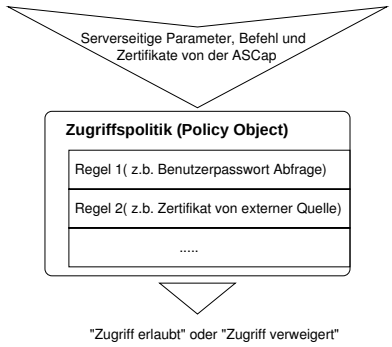

Abbildung 2: Die Zugriffspolitik stellt die Zugriffsentscheidungsfunktion dar.

Die Abbildung 2 zeigt zwei Dinge: Wie die Zugriffsentscheidung durch die Zugriffspolitik erreicht wird und den inneren Aufbau der Zugriffspolitik.
Die Zugriffspolitik stellt quasi die Zugriffsentscheidungsfunktion dar: sie erhält Parameter vom Server, sowie die Zertifikate der ASCap als Eingabeparameter. Die Ausgabe der Zugriffspolitik ist ein “Zugriff erlaubt” oder “Zugriff verweigert”. Auf der Abstraktionsebene der Zugriffspolitikimplementierung besteht eine Zugriffspolitik aus verschiedenen Zugriffsregeln. Jede Regel liefert ein Einzelergebnis, das ähnlich wie bei Kühnhausers Metapolitiken unterschiedlichen Einfluss auf die endgültige Zugriffsentscheidung haben. Ein negatives Ergebnis einer Regel, kann, einen positiven Einfluss auf die Zugriffsentscheidung haben.
Um eine Vielzahl von Zugriffsmodellen zu unterstützen, kann die ASCap Architektur in zwei Modi betrieben werden. Der erste Modus (Referenz-Modus) erlaubt eine erhöhte Sicherheitseinstufung und Bearbeitungsgeschwindigkeit. In der ASCap wird anstelle der vollen Zugriffspolitikimplementierung nur eine Referenz zu einer schon auf dem Server vorhandenen Zugriffspolitik gegeben. Dies schützt nicht nur vor Angriffen auf den kryptographischen Schutz (Signatur) der Zugriffspolitik, sondern erlaubt auch auf dem Server

[5] im engl. policy object

die verwendbaren Zugriffspolitiken zu limitieren. Der zweite Modus, “active capability policy” genannt, erlaubt es, die gesamte Zugriffspolitikimplementierung mittels der ASCap dem Server zu liefern. Dies bietet eine erhöhte Flexibilität und ermöglicht dynamische Zugriffsmodelle. Die Sicherheit des zweiten Modus ist durch die Verwendung kryptographischer Verfahren zur Integritätswahrung der Zugriffspolitik gewährleistet. Jedoch muss der Server der Quelle der Zugriffspolitik vertrauen, falls Quelle und Server keine Verwaltungseinheit bilden. Die Problematik wird in Abschnitt 4 genauer diskutiert.
Die ASCap Architektur wurde ursprünglich konzipiert, um verschiedene Zugriffsmodelle mit derselben Zugriffskontrollarchitektur und Andwendungsschnittstelle darstellen zu können. Dies bedeutet, dass sowohl hoch sichere als auch sehr flexibele Modelle dargestellt werden können. Um die allgemeine Sicherheit und Flexibilität zu zeigen, wurde ein Verhaltensmodell mittels eines Prozesskalkulus modelliert. Der π-Kalkulus erlaubt mittels Verhaltenskongruenzen sowohl verschiedene Zugriffsmodellimplementierung zu vergleichen, als auch zu zeigen, dass die von der ASCap Architektur eingeführten Zusatzelemente (z.B. der ASCap Proxy oder die externen Sicherheitsrechner) nicht die Zugriffsmodelle beeinflussen. Der formale Beweis ist in [Ab03] zu finden.

4 Geteilte Zugriffsverwaltung

In den aktuellen Anwendungen wird die Zugriffsverwaltung meist zentral nach dem Referenzmonitorprinzip mittels eines Domaincontrollers implementiert. Ansätze dezentraler Verwaltungsstrukturen bedienen sich meist der PKI[6] [Va02]. Diese Ansätze können jedoch nur drei der von uns identifizierten Kategorien der geteilten Zugriffsverwaltung darstellen. Die vierte Kategorie, die kontrollierte Machtteilung[7], ist nicht darstellbar. Nachfolgend werden die Kategorien der geteilten Zugriffsverwaltung anhand von Beispielen der ASCap Architektur vorgestellt.

4.1 Kategorie α: Einfache Verwaltung, Intern

Diese Kategorie kann als Basisklasse angesehen werden; es findet keine Machtteilung statt und beide Rechner (Verwaltungsrechner und Server) gehören der gleichen Verwaltungseinheit an. Abbildung 3 zeigt diese Situation. Der Kreis um den Server deutet die Verwaltungseinheit einer Firma an. Es wird davon ausgegangen, dass in einer Verwaltungseinheit die einzelnen Teilkomponenten dem Ziel der Verwaltungseinheit wohlgesonnen sind, d.h. keine Angriffe gegen andere Mitglieder derselben Verwaltungseinheit stattfinden. Nachdem der Client den *ASCap Proxy* erhalten hat, wird angenommen, dass er den Regeln der Verwaltungseinheit folge leistet (dargestellt durch die gestrichelte Linie). Doch auch im

[6] public key infrastructure
[7] im engl. ’partial outsourcing’ genannt

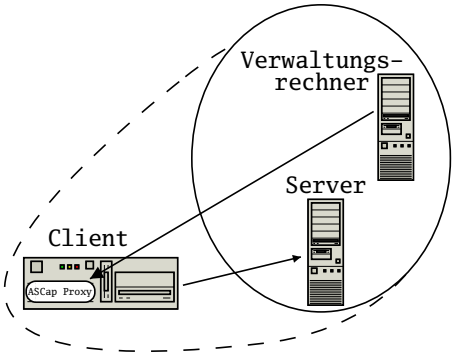

Abbildung 3: Kategorie α: Keine Machtteilung, einfache Verwaltung

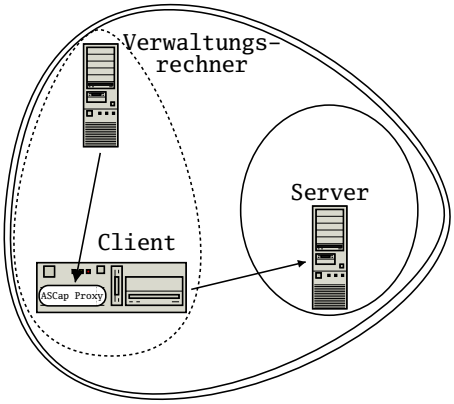

Abbildung 4: Kategorie β: Volle Machtabgabe, beispielweise zu einem externen Dienstleister

Falle eines Verstoßes (z.B. bei Manipulation eines Zertifikates) kann dieser immer noch durch die verwendeten kryptographischen Signaturen erkannt werden.
Sicherheitstechnisch ist diese Kategorie einfach zu analysieren, da es nur eine Verwaltungseinheit gibt. Sowohl Authentifizierung als auch Zugriffsbefugnisse werden von einem einzigen (firmeninternen) Verwaltungsrechner kontrolliert.

Vorteile sind die, die eine zentrale Verwaltung heutzutage bietet.

Nachteile beinhalten die Tatsache, dass die volle Verwaltung von der firmeneigenen IT Abteilung getragen werden muss. Ein externer Dienstleister kann die firmeneigenen Abteilungen beraten, ist jedoch in den Prozess der Zugriffsverwaltung in keiner Weise eingebunden.

Anwendungsbeispiel: Zugangskontrollarchitekturen der heutigen Anwendungen, z.B. ein *Windows Domain Controller*, dessen Passwort nur Angehörigen der eigenen Firma bekannt ist.

Möglichkeiten für die Schutzzielverletzungserkennung: Die interne Firma kann eigene Erkennungsanwendungen einsetzen, die aber separat von der ZKA operieren. Eine externe Firma kann Überwachungsanwendungen im Verwaltungsbereich der internen Firma installieren, doch dies stellt eine zusätzliche Sicherheitsschwachstelle dar.

4.2 Kategorie β: Einfache Verwaltung, Extern

Abbildung 4 zeigt das Gegenbeispiel zu Kategorie α - die Verwaltung wird vollständig von einer externen Verwaltungseinheit betreut. Wiederum stellt der durchgezogene Kreis um den Server die Verwaltungseinheit dar, der ein natürliches Vertrauen zugeordnet ist. Diesmal deutet die gestrichelte Linie an, dass der Client den Regeln des Verwaltungsrechners folgen muss und somit beide eine eigene Verwaltungseinheit darstellen. Der doppelte Kreis weist darauf hin, dass für einen funktionierenden Zugriff der Verwaltungsrechner und Server ein Vertrauensverhältnis haben müssen.
Die Sicherheit hängt vollständig von dem Verhalten des extern administrierten Verwaltungsrechner ab. Dies erlaubt einer Firma, voll von dem Wissen und Möglichkeiten eines externen Dienstleisters zu profitieren, erfordert jedoch, dass diesem Dienstleister auch voll vertraut wird. Zudem muss die auf Erkennen von Schutzzielverletzungen spezialisierte externe Firma alltägliche Arbeiten wie das Zurücksetzen von Passwörtern übernehmen.

Vorteil ist die vollständig ausgelagerte Arbeit.

Nachteil ist die Tatsache, dass der externen Firma vertraut werden muss.

Anwendungsbeispiel: Ähnlich wie in Kategorie α, doch diesmal installiert und beaufsichtigt von der externen Firma.

Möglichkeiten für die Schutzzielverletzungserkennung: Die externe Firma kann ähnlich der internen Firma Dienste zur IDS betreiben. Die extern installierte Überwachungssoftware stellt nun nicht mehr eine so große Sicherheitsschwachstelle dar. Dennoch können auch in dieser Kategorie nur passive Strategien zur Angriffserkennung eingesetzt werden.

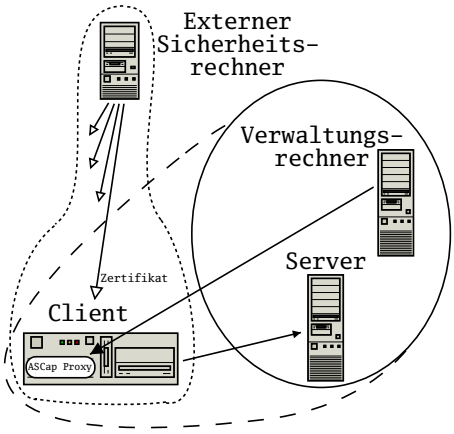

Abbildung 5: Kategorie γ: Machtteilung durch externe Sicherheitsrechner

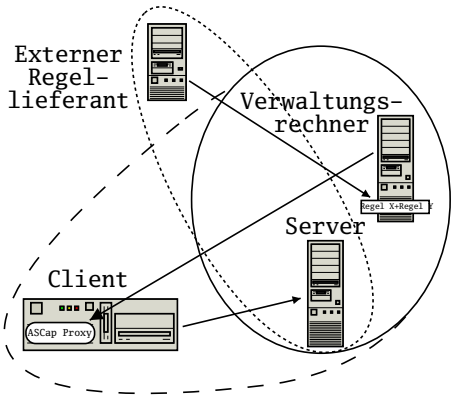

Abbildung 6: Kategorie δ: Kontrollierte Machtteilung durch externe Regellieferanten

4.3 Kategorie γ: Machtteilung durch externe Sicherheitsrechner

In dieser Kategorie wird, wie der Kreis in Abbildung 5 zeigt, die Zugriffsverwaltung von der Firma selbst erledigt. Die Zugriffspolitik erfordert jedoch, dass der Benutzerrechner ein Zertifikat von einem externen Sicherheitsrechner anfordert. Dieser externe Sicherheitsrechner wird von einem externen Dienstleister betrieben und kann Anfragen von einer Vielzahl von Firmen bearbeiten. Da der Benutzerrechner sich ggf. bei dem externen Sicherheitsrechner authentifizieren muss, besteht ein gewisses Vertrauensverhältnis, das durch den gepunkteten Ellipse angedeutet ist. Der erweiterte Kreis zeigt wiederum an, dass der Benutzerrechner den Regeln der Zugriffspolitik folge leisten muss. Es ist kein großer Kreis um den externen Sicherheitsrechner und Server gezogen, da kein zwingendes Vertrauensverhältnis zwischen den Beiden besteht. Dies bedeutet, dass der externe Sicherheitsrechner nicht wahlfrei Zugänge zu dem Server vergeben kann.

Wertet man die Sicherheit dieser Kategorie aus, zeigt sich, dass die interne Firma die endgültige Kontrolle über die Zugangsentscheidungen hat. Dies schließt die Entscheidung ein, welche externen Sicherheitsrechner kontaktiert werden müssen und welchen Einfluss deren Zertifikate erhalten. Aus der Perspektive der Sicherheit kann ein feindlich gesonnener externer Sicherheitsrechner maximal eine zeitweise Dienstverweigerung bewirken.

Schwachstelle dieses Szenarios ist der externe Sicherheitsrechner, der ständig erreichbar sein muss.

Vorteil dieser Kategorie ist die Möglichkeit, dass das Zertifikat der externen Firma erst nach verschiedenen Sicherheitstests ausgehändigt werden kann. Somit kann die Expertise des externen Dienstleisters genutzt werden, ohne ihm Kontrolle über das firmeneigene Netzwerk zu geben.

Anwendungsbeispiel: Diese Kategorie kann durch die externen Sicherheitsrechner der ASCap Architektur implementiert werden. Der Benutzerrechner muss ein oder mehrere Zertifikate abrufen und diese in der ASCap zu dem Server senden.

Möglichkeiten für die Schutzzielverletzungserkennung: Die externe Firma ist so in die Zugriffskontrolle eingebunden, dass sie nur die notwendigen Informationen erhält. Im Vergleich zu einem installierten Überwachungsprogramm kann der Kunde mittels der eingesetzten Zugriffspolitik das zu übermittelte Wissen selbst selektieren. Das IDS kann nun auch übergeordnete Muster erkennen, wie beispielweise einen Benutzer, der eine Vielzahl Zugriffsrechte ansammelt. In einem anderen Szenario händigt ein externer Sicherheitsrechner nur dann ein Zertifikat aus, wenn der Client die volle Transaktionssequenz vorab mitteilt, so dass auch anwendungsspezifische Schutzzielverletzungen erkannt werden, deren Einzelschritte jeweils unbedenklich sind.

Diese Kategorie bietet mit den externen Sicherheitsrechnern ein nützliches Bindeglied zwischen ZKA und IDS.

4.4 Kategorie δ: Kontrollierte Machtteilung durch externe Regellieferanten

Abbildung 6 zeigt die letzte Kategorie. Der externe Regellieferant stellt dem Verwaltungsrechner Einzelregeln zur Verfügung. Der Verwaltungsrechner fügt die verschiedenen Regeln (hier Regel X und Regel Y) zuerst zur vollständigen Zugriffspolitik und dann dem *ASCap Proxy* zusammen. Die gestrichelte Linie um den externen Regellieferanten und den Server zeigt eine natürliche Vertrauensbeziehung an, da der Server nun auch Regeln von dem externen Regellieferanten ausführt.

Schwachstelle: Das System scheint nun eine sicherheitstechnische Schwachstelle mit diesen extern erzeugten ausgeführten Regeln zu haben. Diese ist jedoch minimiert indem die Regelimplementierungen nicht direkt zu dem Server gesendet werden, sondern zuerst den Verwaltungsrechner passieren. Dort können mittels Techniken des Programmbeweises [HR02] und Sandkastentestsystemen ein unbedenkliches Verhalten nachgewiesen werden, bevor die Regel zum Einsatz kommt. Wie bei Kategorie γ kann vom Verwaltungsrechner der Einfluß der extern bereitgestellten Regel kontrolliert werden, so dass keine vollständige Machtabgabe stattfindet.

Vorteil Im Gegensatz zu der vorherigen Kategorie bedient die externe Firma nicht die Clientrechner, sondern die wesentlich kleinere Gruppe der Verwaltungsrechner - dies erlaubt eine bessere Skalierbarkeit.
Die Flexibilität dieser Kategorie kann gezeigt werden, indem der Regellieferant eine Regel bereitstellt, die verlangt einen externen Sicherheitsserver zu kontaktieren - so können alle Kategorie γ Systeme implementiert werden.

Anwendungsbeispiel: Eine Firma betreibt ihren eigenen Verwaltungsrechner, der eine Regelimplementierung von externen Beraterfirmen bezieht. Diese Regeln werden zu einer Zugriffspolitik in einem ASCap Proxy zusammengefasst. Die ASCap ZKA ermöglicht mittels des *active capability* Modus die zeitliche Einführung des neuen ASCap Proxy.

Möglichkeiten für die Schutzzielverletzungserkennung: Ein externer Dienstleister verfolgt die bekannten security Mailing Listen (z.B. CERT[We04a],bugtraq[We04c]). Wird eine neue Sicherheitslücke bekannt, generiert er eine Regel, die etwaige Zugriffsanforderungen auf Angriffsanzeichen prüft. Diese Regel kann den Angriff abwehren ohne einen Informationsfluß zu dem externen Dienstleister zu zulassen.

Weitere Beispiele insbesondere der aktiven Intrusion Detection werden im nachfolgenden Abschnitt besprochen.

4.5 Aktive Intrusion Detection durch eine neue Zugriffskontrollarchitektur

Durch die neu entwickelte *kontrollierte Machtteilung* auf dem Gebiet der ZKA, sowie die nun mögliche Verknüpfung von Zugriffskontrolle und IDS werden neue *aktive* Strategien

möglich. Die aktiven SZVE-Strategien werden Eigenschaften des Benutzers überprüfen, die ihn leichter zuortbar machen, die aber nicht in normalen Arbeitsabläufen auftreten. Ein Beispiel ist ein reguläre Angestellter, der eine Abrechnung eines Projektes erstellen will. Wird ihm mitgeteilt, dass die Daten dieses Projektes zeitweise nicht verfügbar sind, wird er wahrscheinlich andere, nicht onlinegestützte Arbeiten des gleichen Projektes erledigen. Ein Eindringling wird eher dazu übergehen, andere noch verfügbare Projekte auszuspionieren.
Erst eine kontrollierte Machtteilung erlaubt es, externe Expertisefirmen in solchen aktiven IDS-Strategien einzusetzen. Ihnen ist es jedoch nicht möglich, ihre Macht für eigene Einbrüche zu missbrauchen. Dieser Vorteil wird wichtig für große Dienstleister, die zentral Daten sammeln. *Dshield* [We04b] ist ein beliebter Logbuch Auswertungsdienst, der von der hohen Datenmenge profitiert, um unbekannte und schwer erkennbare Angriffssignaturen zu erlernen. Dieser Dienst konnte sich etablieren, da er keine aktiven Elemente in den teilnehmenden Netzen zwingend benötigt. Ebenso erlaubt die Kategorie δ das Einbeziehen externer Dienstleister in die Zugriffskontrolle, ohne ihnen eine pauschale Machtfreiheit über die Systeme zu geben.

5 Strategiebeispiele

Erlaubt die ZKA eine Verknüpfung mit dem IDS wird es möglich, eine neue Klasse von Erkennungsstrategien zu verwenden. In diesem Abschnitt werden drei Gruppen von neuen Erkennungsstrategien zusammen mit der Umsetzung in der ASCap Architektur besprochen:

1. Passives Erkennen kombiniert mit aktivem Eingreifen
2. Aktive Erkennungsstrategien
3. Aktive automatisierte Eindringling Suchstrategien

5.1 Passives Erkennen kombiniert mit aktivem Eingreifen

Diese Gruppe entspricht den heutigen Intrusion Prevention Systemen. Eine kontrollierte Machtteilung erlaubt darüber hinaus den Überblicksvorteil einer globalen Zentrale zur Intrusion Detection auszunutzen. Bei der SPAM Bekämpfung ermöglicht ein Überblick über eine große Anzahl von Mailkonten, SPAM leicht zu identifizieren. So kann ähnlich dem Dshield Projekt [We04b] in einer verknüpften Zugriffskontrolle ein externer Anbieter die erreichten Zugriffsrechte der Benutzer überwachen und beim Auftreten einer Anomalie (z.B. ein Benutzer hat ungewöhnlich viele Zugangsrechte) einen Alarm oder eine Reaktion auslösen.
Umsetzung durch die ASCap Architektur: Mittels des Mechanismus der externen Sicherheitsrechner von Kategorie γ ist es möglich, einer übergeordneten Datenauswertung die notwendigen Informationen zu liefern.

5.2 Aktive Erkennungsstrategien

Geht man von einer Monokultur im Bereich der Zugriffskontrolle aus, so ist es dem einfachen Angreifer möglich, eine einmal entdeckte Nachlässigkeit beliebig auszunutzen. Wenn man, um die Sicherheit zu erhöhen, als Schutzmassnahme alle bekannten Techniken gleichzeitig anwendet, würde dies normale Arbeitsabläufe unnötig erschweren. Als Lösung bietet sich an, periodisch die verwendeten Techniken zu ändern, um Eindringlingen das Leben zu erschweren. Aktive Erkennungsstrategien erweitern dies, indem sie das Verhalten der einzelnen Anwender überwachen. Für jedes Zugriffskontrollszenario werden die Statistiken getrennt geführt. Es wird angenommen, dass rechtmäßige Benutzer in allen Szenarien vollen Zugang haben und dass die Verhaltensmuster gleich sind. Fällt ein Benutzer durch Inaktivität in einem Szenario auf, kann ein Eindringling gefunden worden sein. Die aktiven Erkennungsstrategien rufen nun die Zugriffstechnikwechsel gezielt hervor, um erkannte Muster zu bestätigen und Falschalarme zu vermeiden.
Umsetzung mittels der ASCap Architektur: Verschiedene Zugriffspolitiken mit Regelbausteinen wie verschiedene Sicherheitsabfragen (Passwort, Geburtsdatum etc.) oder der Zuhilfenahme von externen Hilfsmitteln (z.B. SMS die beantwortet werden muss) sind von der internen Firma in Abstimmung mit dem Dienstleister vordefiniert. Die externe Firma kann mittels einer dynamisch änderbaren Regel (Kategorie δ) die verwendete Zugriffspolitik im Einzelfall wählen. Werden Alarmzeichen erkannt, kann die Wahl der Zugriffspolitik so beeinflusst werden, dass Eindringlinge leichter erkannt werden.

5.3 Aktives Suchen

Nach dem Beispiel der manuellen Einzelfallanalyse kann das aktive Suchen aus dem Überprüfen von Annahmen über den Angreifer bestehen. Angreifer verbinden sich oft über Zwischenrechner, die sie beliebig auswählen können. Die Annahme, dass ein normaler Benutzer nur über einen Einzelplatzrechner und begrenzte Einwahlmöglichkeiten verfügt, können zu der Erkennungsstrategie führen, dem verdächtigen Benutzer mitzuteilen, dass die von ihm genutze IP Region zeitweise gesperrt werden muss. Ein hartnäckiger Angreifer wechselt nun leicht den Zwischenrechner und wird so enttarnt.
Eine weitere Eigenschaft eines Spiones kann sein, dass er Daten beliebiger Quelle sammeln will. Arbeitet ein Benutzer außerordentlich lange an einem Projekt und erregt damit aufsehen, so ist es möglich, diesen Bereich zeitweise für ihn zu schließen. Ändert er sein Interessengebiet und arbeitet ebenso intensive an anderen Projekten, so kann ein fleißiger Angreifer gefunden worden sein.
Aktive Strategien zur Angriffserkennung der Gruppe “Aktives Suchen” werden einzelne Eigenschaften des Angreifers annehmen und dann das System zeitweise so verändern, dass diese Eigenschaften deutlicher testbar werden. Damit sind diese Strategien der passiven Datenauswertung deutlich überlegen.
Umsetzung mittels der ASCap Architektur: Nachdem die vermuteten Eigenschaften der Angreifer spezifiziert sind, können Tests entwickelt werden, die diese Eigenschaften überprüfen. Dann ist es möglich an den erforderlichen Stellen in dem System Einstellpunkte

anzubringen, die je einen Test darstellen. In der ZKA werden externe Sicherheitsrechner (Kategorie γ) und dynamisch änderbare Regeln (Kategorie δ) zum Einsatz kommen.

6 Zusammenfassung und Ausblick

In diesem Beitrag wurden aktive Strategien zur Intrusion Detection vorgestellt, die es erlauben, nicht nur nach bekannten Angriffsignaturen im auftretendem Datenverkehr zu suchen, sondern im Falle von allgemeineren Alarmsignalen gezielt Benutzer auf verdächtige Eigenschaften zu prüfen. Diese Tests werden möglich, wenn die IDS enger mit der Zugriffskontrollarchitektur zusammenarbeiten. Hierzu wurden zuerst verschiedene Kategorien der Zugriffskontrollverwaltung vorgestellt. Eine bisher unbekannte Kategorie der kontrollierten Machtteilung wurde aufgezeigt und die ASCap Architektur vorgestellt. Die ASCap Architektur implementiert die kontrollierte Machtteilung und erlaubt so, IDS mit der ZKA zu verknüpfen. Verschiedene Beispiele von Angriffserkennung wurden diskutiert, die mit den verknüpften Systemen angewendet werden können. Es wurde aufgezeigt wie bekannte Techniken der SPAM-Bekämpfung auf die Zugriffskontrolle und Schutzzielverletzungserkennung übertragen werden können.

Das Aufzeigen der Möglichkeit aktiven Strategien zu verwenden wird als Ergebniss unserer Forschung angesehen. Ein passives auf bekannte Angriffssignaturen warten kann durch ein aktives Provozieren von verdächtigem Verhalten erweitert werden. Dabei wechselt der Fokus vom Angriff zum Angreifer. Die Strategie des “Aktives Suchen” erlaubt es einen fleissigen Arbeiter von einem Industriespion zu unterscheiden. Die in diesem Beitrag beschriebenen Strategiebeispiele beruhen auf einfache Annahmen und Teil der weiterführenden Forschung wird es sein, die hier vorgestellten information-technische Infrastruktur zu nutzen um weitere Eigenschaften und Strategien zu finden. Hier sehen wir Chancen auch interdizplinär beispielweise von verhaltenspsychologische Ergebnisse wie [Tu99](Kapitel 25) zu profitieren.

Literatur

[Ab03] Abendroth, J.: Applying π-calculus to practice: An example of a unified security mechanism. Technical Report RS-03-39. Basic Research In Computer Science, University of Aarhus. 2003. 35 pp.

[AJ03] Abendroth, J. und Jensen, C. D.: A unified security mechanism for networked applications. In: *Proceedings of 18th Symposium on Applied Computing (SAC2003)*. S. 351–357. ACM. March 2003.

[AOTG99] Asaka, M., Okazawa, S., Taguchi, A., und Goto, S.: A method of tracing intruders by use of mobile agents. In: *INET’99*. 1999.

[De87] Denning, D. E.: An intrusion-detection model. *IEEE Trans. Softw. Eng.* 13(2):222–232. 1987.

[ER88] E, S. M. S. E. H. und R., W.: Expert system in intrusion detection: A case study. In: *Proceedings of the 11th National Computer Security Conference*. S. 85–91. October 1988.

[FK92] Ferraiolo und Kuhn: Role based access control. In: *Proceedings of 15th National Computer Security Conference*. S. 554–563. October 1992.

[HR02] Huth, M. R. A. und Ryan, M. D.: *Logic in Computer Science*. Cambridge University Press. The Edinburgh Building, Cambridge, DB2 2RU, UK. 2002.

[JS03] Jung, A. H. M. und Schaefer, G.: Combining multiple intrusion detection and response technologies in an active networking based architecture. In: *DFN-Arbeitstagung ueber Kommunikationsnetze, Duesseldorf, Germany*. June 2003.

[Kü95] Kühnhauser, W. E.: On paradigms for security policies in multipolicy environments. In: *Proceedgins of 11th International Information Security Conference (IFIP/SEC'95), Cape Town, South Africa*. 1995.

[Kü99] Kühnhauser, W. E.: Metapolitiken (german). Technical Report RS-AiS-1999-13,ISBN3-88457-362-4. Informationstechnik GmbH. Sankt Augustin. 1999.

[Le84] Levy, H. M.: *Capability-Based Computer Systems*. Digital Press. Bedford, Massachusetts. 1984.

[LJ88] Lunt, T. F. und Jagannathan, R.: A prototype real-time intrusion-detection expert system. In: *IEEE Symposium on Security and Privacy*. S. 59–66. October 1988.

[QL96] Qian, T. und Liao, W.: Active capability: An application specific security and protection model. Technical report. University of Illinois at Urbana-Champaign. 1996.

[Sh86] Shapiro, M.: Structure and encapsulation in distributed systems: The proxy principle. In: *Proceedings of the 6th International Conference on Distributed Computer Systems*. S. 198–204. Cambridge, Massachusetts, U.S.A. 1986.

[Tu99] Turvey, B.: *Criminal Profiling: An Introduction To Behavioral Evidence Analysis*. Academic Press. 24-28 Oval Road, London NW1 7DX,UK. 1999.

[Va02] Various. Open source pki book, http://opensourcepkibook.sourceforge.net. 1.12.2002.

[We04a] Website. http://www.cert.org. 31.1.04.

[We04b] Website. http://www.dshield.org. 31.1.04.

[We04c] Website. http://www.securityfocus.com/archive/1. 31.1.04.

[We04d] Website. http://www.snort.org. 31.1.04.