

# Modellierung von Netzsicherheitssystemen umfangreicher vernetzter IT-Infrastrukturen

João Porto de Albuquerque<sup>1,2</sup>, Heiko Krumm<sup>2</sup>, and Paulo Lício de Geus<sup>1</sup>

<sup>1</sup>Institute of Computing , State University of Campinas , 13083-970 Campinas/SP Brazil

<sup>2</sup>FB Informatik , University of Dortmund , 44221 Dortmund Germany

**Abstract:** Angesichts zunehmend komplexer werdender vernetzter IT-Infrastrukturen sind das integrierte Design und das automatisierte Management der unterschiedlichen Sicherheitstechniken und Mechanismen von großem Interesse. Besonders in umfangreichen Systemen, sollte das Sicherheitsmanagement durch Ansätze mit einem geeigneten Abstraktionsniveau so unterstützt werden, dass das System unter Verdeckung der Konfigurationsdetails der eingesetzten Mechanismen betrachtet werden kann. Dieses Papier stellt einen skalierbaren Ansatz zur Modellierung von Netzsicherheitssystemen vor, der auf den Konzepten des Policy-basierten Managements und des modellbasierten Managements aufbaut.

## 1 Einleitung

Die gegenwärtigen vernetzten IT-Infrastrukturen enthalten eine zunehmende Vielzahl von Sicherheitsmechanismen, um die bestehenden Schutzanforderungen gegen netzbasierete Angriffe zu erfüllen. In diesem komplexen Anwendungsfeld steigen die Kosten des Sicherheitsmanagements sehr schnell, dessen Aufgaben die Installation und initiale Konfiguration der Sicherheitsdienste, sowie danach, während des Systembetriebes, ihre Überwachung, Prüfung, Anpassung und Rekonfiguration umfassen. Dieses breite Aufgabenfeld ist schwer überschaubar, so dass Möglichkeiten zur korrekten Abstraktion und zur qualitätsgesicherten Tool-gestützten Planung und Konfiguration als Schlüsselfaktoren zum Erleichtern der Managementaufgaben gesehen werden können.

Um das Problem zu lösen, verwenden wir eine Kombination der Ansätze des modellbasierten Managements (MBM) [LVK02] und der Policy-Hierarchien [MS93]. Wir setzen uns mit der Behandlung umfangreicher Systeme auseinander, da in vorherigen Arbeiten das Modell wegen seiner großen Anzahl von Bestandteilen sehr unübersichtlich wird. Als Lösung führen wir das Diagramm abstrakter Subsysteme (DAS) ein. Das DAS erweitert die Modellierungstechnik von MBM und führt eine neue Abstraktionsschicht ein, in welcher ein Gesamtsystem als Zusammensetzung abstrakter Subsysteme (AS) dargestellt wird. Im DAS, werden die Details versteckt. Sie werden nur noch in der internen Spezifikation jedes Subsystems behandelt. Diese Modularisierung ermöglicht eine Dekomposition von Systemanalyse und -entwurf, so dass Verständlichkeit und Skalierbarkeit der Modelle deutlich verbessert werden.

Im Folgenden führen wir die Modellierungstechnik ein, um anschließend ihre praktische Nutzung an Hand eines Anwendungsbeispiels zu verdeutlichen (Abschnitt 3). Ein Fazit in Abschnitt 4 schließt das Papier ab.

## 2 Modellierungstechnik

Die Struktur des Modells wird in Abb. 1 gezeigt. Sie wird durch drei Abstraktionsniveaus geprägt: *Roles & Objects* (RO), *Subjects & Resources* (SR), und *Diagram von Abstrakten Subsystemen* (DAS). Jedes Niveau ist eine Verfeinerung des übergeordneten im Sinne einer Policy-Hierarchie [MS93]. Das oberste Niveau (RO) bietet eine anwendungsbezogene Ansicht des Netzes an, während das niedrigste eine technische Sicht darstellt. Die vertikalen Unterteilungen unterscheiden zwischen dem Modell des tatsächlichen zu verwaltenden Systems und den Policies, die dieses System regulieren und sich jeweils auf die Modellkomponenten des gleichen Niveaus beziehen.

Da die zwei obersten Niveaus (RO und SR) von vorherigen Arbeiten über modellbasiertes Management [LVK02] übernommen wurden, werden sie anschließend kurz beschrieben. Das dritte Niveau (DAS) ist dann das Hauptthema dieses Papiers und wird im folgenden Abschnitt erläutert.

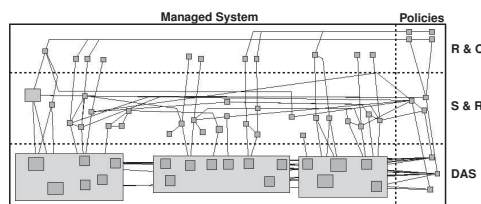


Abbildung 1: Modellübersicht

Das oberste Niveau (RO) basiert auf den Konzepten der Rollenbasierten Zugriffskontrolle (RBAC) [Sea00]. Die Hauptklassen in diesem Niveau sind: Rollen nach denen Personen, die im modellierten Anwendungsfeld arbeiten, handeln (*Roles*); Objekte des Anwendungsfeldes, auf welche die Zugriffe reglementiert werden (*Objects*); und *AccessModes*; d.h. die unterschiedlichen Zugriffsarten auf die Objekte. Die Klasse *AccessPermission* erlaubt dem Nutzer einer Rolle, auf ein bestimmtes Objekt gemäß eines *AccessModes* zuzugreifen.

Das zweite Niveau (SR in Abb. 1) bietet eine Systemansicht an, die im Hinblick auf die im System angebotenen Dienste definiert wird, und es besteht folglich aus einer umfassenderen Menge von Klassen. Die Objekte dieses Niveaus stellen dar: (a) Personen, die im Anwendungsfeld arbeiten (*User*); (b) Subjekte, die im Interesse des Nutzers agieren (*SubjectTypes*); (c) Services im Netz, die verwendet werden, um auf Ressourcen zuzugreifen (*Services*); (d) die Abhängigkeit eines Services von anderen Services (*ServiceDependency*); und zuletzt (e) logische Ressourcen im Netz (*Resources*).

## 2.1 Diagram von abstrakten Subsystemen

Ein DAS soll die Gesamtstruktur des zu verwaltenden Systems in modularer Art und Weise beschreiben, d.h. das System als Zerlegung in Subsysteme (AS'e) zusammen mit ihrer Kopplung darstellen. Folglich ist das DAS in formaler Definition ein Graph, der aus AS'en als Knoten und aus Kanten besteht, welche die möglichen Kommunikationswege zwischen den AS'en darstellen. Ein abstraktes Subsystem (AS) ist eine abstrakte Ansicht eines Systemsegments; d.h. eine vereinfachte Darstellung einer gegebenen Gruppe zusammenhängender Systembestandteile. Als solches ist ein AS ein Subgraph des DAS und kann folgende Komponententypen enthalten:

**Akteure** stehen für Gruppen von Elementen eines Systems, die ein aktives Verhalten haben; d.h. sie leiten Kommunikation ein und führen von Obligations-Policies vorgeschriebene Operationen durch.

**Mediatoren** unterstützen die Kommunikation im System. Sie leiten Aufträge weiter, kontrollieren den Netzverkehr, und filtern und/oder wandeln den Datenfluss in Entsprechung zu Autorisierungspolicies um. Darüber hinaus können sie durch Obligations-Policies vorgeschriebene Operationen ausführen, z.B. das Registrieren von Informationen über Datenflüsse.

**Targets** sind passive Elemente; sie enthalten Informationen, die von den Akteuren zugegriffen werden.

**Connectors** schließlich stehen für Schnittstellen eines AS; d.h. sie stellen eingehende und abgehende Kommunikationsmöglichkeiten eines AS dar.

Jede dieser Elementarten stellt eine Gruppe von Mechanismen des tatsächlichen Systems (z.B. Hosts, Prozesse, Protokolle, Netzschnittstellen) dar. Die Objekte eines DAS stellen folglich Aggregationen solcher Mechanismen dar, die in einer Policy-orientierten Ansicht des Systems gruppiert werden, um nur die relevanten Aspekte für eine globale Ansicht der Systemstruktur sichtbar werden zu lassen (für eine ausführliche Erklärung des Modellierens von abstrakten Subsystemen sei auf [PKdG05a] verwiesen).

## 3 Anwendungsbeispiel

Ein Beispiel-Modell ist in Abb. 2 gezeigt, welche das DAS eines Beispielsystems (unten) zusammen mit den Niveaus RO und SR darstellt. Dieses Modell gibt ein typisches Netz-szenario wieder, für das auf dem obersten Niveau (RO) fünf *AccessPermissions* definiert werden, um die Zugriffsrechte der Benutzer im internen Netz zu regulieren, und um Benutzern aus dem Internet zu erlauben, die Firmen-Internet-Präsenz abzurufen. In der untersten Schicht verdeutlicht das DAS des Beispielszenarios die Konzepte, die in dem vorherigen Abschnitt erklärt wurden. Das AS „Internal Network“ etwa (rechts unten) enthält die *Akteure* „internal mail clients“ und „internal web clients“, den *Mediator* „Web proxy“ sowie auch das *Target* „Internal mail server“ und einen *Connector* (das Rechteck).

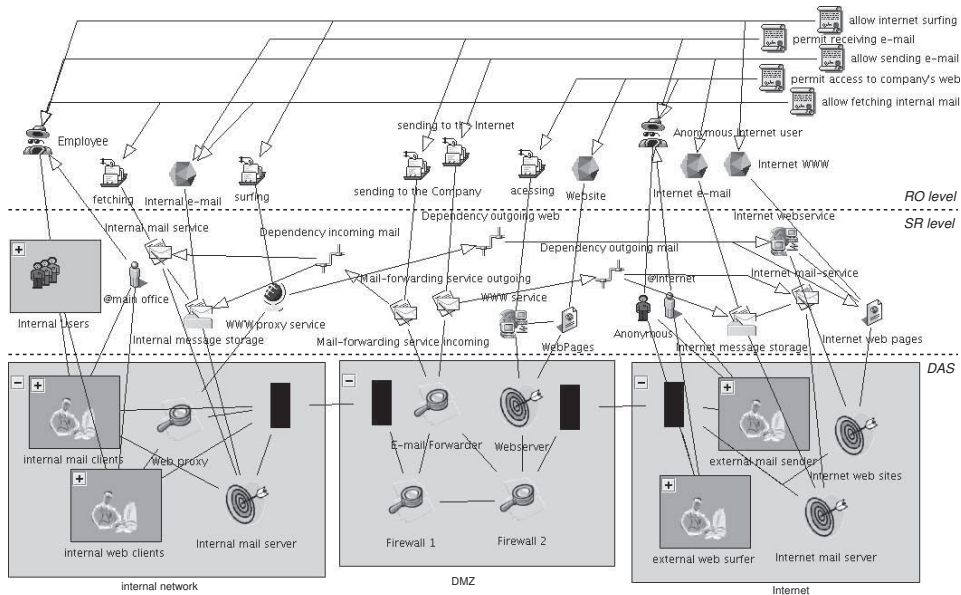


Abbildung 2: Dreischichtiges Modell

Um ein Modell zu vervollständigen, wird schließlich jedes AS eines DAS in eine ausführliche Ansicht der tatsächlichen System-Elemente expandiert. Abb. 3 zeigt als Beispiel die expandierte Repräsentation der ASE „Internal Network“ (links) und „DMZ“ (rechts). Beim Vergleich der vereinfachten Ansichten (im DAS von Abb. 2) mit den ausführlichen (Abb. 3), kann man ersehen, dass das Modellieren mit abstrakten Subsystemen deutliche Vorteile hinsichtlich Prägnanz und Verständlichkeit des Modells bietet, und zugleich eine umfassende Ansicht der Gesamtsystemarchitektur zur Verfügung stellt. Folglich ist diese Modellierungstechnik besonders geeignet zur Darstellung und Behandlung sehr umfangreicher Modelle.

## 4 Fazit

Dieses Papier hat eine skalierbare Modellierungstechnik vorgestellt, die den Ansatz des modellbasierten Managements erweitert, um die Behandlung von sehr umfangreichen vernetzten Systemen zu unterstützen. Diese Modellierungstechnik wendet das Prinzip „Teile und herrsche“ an, um Skalierbarkeit zu erzielen; d.h. die Teilung des Systems in kleinere Segmente ermöglicht, jedes Segment im Detail separat zu behandeln, und das vollständige System nur in einer abstrakteren Ansicht der Interaktion der Segmente zu betrachten.

Wir haben auch ein Software-Werkzeug entwickelt, das den Benutzer im Modellieren des Systems mittels graphischer Editorfunktionen unterstützt sowie zusätzliche Funktionen für die Überprüfung von Modell-Einschränkungen und Konsistenzbedingungen enthält (die

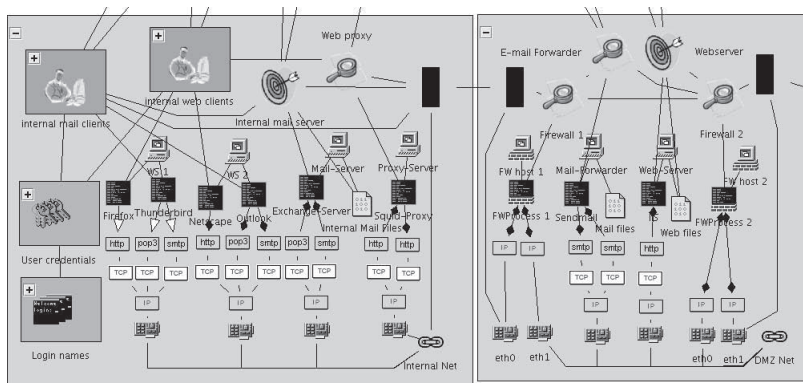


Abbildung 3: Expandierte ASE

Abbildungen dieses Papiers wurden mit diesem Werkzeug hergestellt). Sobald das Systemmodellieren abgeschlossen ist, führt das Werkzeug eine automatische Verfeinerung der abstrakten Sicherheitspolicy (d.h. die *AccessPermissions* im RO-Niveau – siehe Abschnitt 2) durch die Zwischenniveaus (SR und DAS) bis hin zur Erzeugung von Konfigurationsdateien für die benutzten Sichermechanismen durch.

Das begleitende Papier [PKdG05a] vertieft die Modellierungstechnik, während eine Formalisierung der Methodologie in [PKdG05b] erläutert wird. Derzeit beschäftigen wir uns damit, die begonnene Formalisierung weiter zu entwickeln.

## Literatur

- [LVK02] I. Lück, S. Vögel und H. Krumm. Model-based configuration of VPNs. In R. Stadler und M. Ulema, Hrsg., *Proc. 8th IEEE/IFIP Network Operations and Management Symposium NOMS 2002*, Seiten 589–602, Florence, Italy, 2002. IEEE.
- [MS93] J. D. Moffett und M. S. Sloman. Policy Hierarchies for Distributed System Management. *IEEE JSAC Special Issue on Network Management*, 11(9), 11 1993.
- [PKdG05a] J. Porto de Albuquerque, H. Krumm und P. L. de Geus. On Scalability and Modularisation in the Modelling of Security Systems. In *To Appear in the 10th European Symposium On Research In Computer Security (ESORICS 2005)*, Milan, Italy, September 2005.
- [PKdG05b] J. Porto de Albuquerque, H. Krumm und P. L. de Geus. Policy Modeling and Refinement for Network Security Systems. In *Sixth IEEE International Workshop on Policies for Distributed Systems and Networks*, Seiten 24–33, Stockholm, Sweden, June 2005.
- [Sea00] R. Sandhu und D. Ferraiolo et. al. The NIST Model for Role-Based Access Control: Towards a Unified Standard. In *5th ACM Workshop on Role-Based Access Control*, Berlin, Germany, 2000.