ISSN 1861-0641

IT-Sicherheit & Datenschutz

Ausgabe 04/06
21.04. – 19.05.2006

Zeitschrift für rechts- und prüfungssicheres Datenmanagement

Praxis – Anwendungen – Lösungen

Sicherheits- und Datenschutz-Management

Grundlagen – Technik und Methoden

Markt-Nachrichten

EXTRA

Vorschriften – Gesetze – Urteile

Online-Service
www.it-sd.com

VOGEL

Der Informationsdienst für IT-Manager,
IT-Sicherheits- und Datenschutzverantwortliche.

Prof. Dr. Stephen D. Wolthusen

Risikomanagement, Sicherheitspolitiken und technische Verfahren zu deren Durchsetzung (II)

Die Umsetzung einer unternehmensweiten Sicherheitspolitik stößt in der Praxis häufig schnell an ihre Grenzen: Schwächen in der Architektur von Betriebssystemen und mangelndes Verständnis der Anwender konterkarieren die notwendigen Verbesserungsschritte häufig schon im Ansatz. Einen Ausweg bietet die Automatisierung der entsprechenden Prozesse, an der das Projekt COSEDA des *Fraunhofer-Instituts für Graphische Datenverarbeitung* (IGD) arbeitet.

Die im Projekt COSEDA entwickelten Software-Module ergänzen den Betriebssystemkern um wichtige Sicherheitsfunktionen

Die Sicherheitspolitiken steuern hierbei eine Reihe von Modulen, welche jene Teilaspekte der Politik realisieren, die sich nicht mit den Mitteln des Betriebssystems selbst durchsetzen lassen. So ermöglicht z. B. ein Modul zur Absicherung von Dateisystemen die vollständig transparente, selektive Verschlüsselung bis auf Ebene einzelner Dateien ungeachtet des verwendeten Dateisystems. Gleichzeitig lassen sich auf diesem Weg Regeln für die Verschlüsselung gemeinsam genutzter Netzlaufwerke oder Wechseldatenträger (z.B. USB-Sticks oder auch CD-/DVD-RW) auf Arbeitsgruppenebene vorgeben, wobei sogar die Interoperabilität zwischen verschiedenen Betriebssystemplattformen und Datensicherungssystemen gewährleistet wird. Autorisierte Nutzer werden durch diese Vorgänge nicht belastet oder beeinträchtigt, Dritte sind jedoch mit verschlüsselten Dateiinhalten konfrontiert.

Erzwungene Verschlüsselung und automatische Signatur

Mit ihrer Hilfe lassen sich z. B. Übergriffe auf Synchronisationsprogramme von PDAs verhindern

Neben mobilen Datenträgern sind jedoch auch andere Schnittstellen und Geräte von besonderer Bedeutung für die Umsetzung von Sicherheitspolitiken, da hier vielfältige Bedrohungen z. B. durch den Anschluss an Netzwerkhardware oder auch das Einspielen von *keystroke loggern* bestehen. Ein weiteres Angriffsziel sind auf Anwendungsebene unzureichend gesicherte Schnittstellen wie z. B. Synchronisationsprogramme von PDAs, auf die Unbefugte mit Leichtigkeit zugreifen können, um Daten zu entwenden oder auch Malware einzuspielen. Eine Ergänzung des Betriebssystemkerns sorgt hier nach Maßgabe der Sicherheitspolitik für die dynamische Anpassung der Zugriffsbefugnisse, so dass ein Mitarbeiter bestimmte Geräte beispielsweise nur dann als Speichermedien verwenden kann, wenn diese die zuvor genannten Verschlüsselungsmechanismen nutzen. Analoge Mechanismen existieren für den Datenverkehr im Netz-

Ein weiteres Software-Modul erzwingt das Verschlüsseln und Signieren von E-Mails

werk und insbesondere für E-Mail. Im letzteren Fall wird ein Filtermechanismus für eingehende und ausgehende Mails in den Betriebssystemkern integriert, so dass der Nachrichtenverkehr diesen zunächst immer passieren muss. Auf diese Weise werden ausgehende Mails automatisch gemäß den Vorgaben der Sicherheitspolitik signiert und verschlüsselt, wobei der Client zum Versand Standards wie OpenPGP und S/MIME nutzt. Dies stellt sicher, dass auch Empfänger, die nicht über COSEDA bzw. das *Distributed Mail Guard* (DMG)-Modul verfügen, die Mails mit anderen Sicherheitswerkzeugen bearbeiten können. Anwender müssen dann nur noch wählen, wie streng sie diesen Mechanismus handhaben wollen. Dabei reicht die Variationsbreite vom „opportunistischen" Vorgehen – die Verschlüsselung erfolgt automatisch, sofern der Schlüssel des Adressaten bekannt oder öffentlich zugänglich ist – bis zur rigiden Variante, die den Versand bestimmter Mitteilungen nur dann zulässt, wenn der Schlüssel explizit in einer Whitelist erfasst ist. Ebenso automatisch läuft dann auch die Annahme und Entschlüsselung von Nachrichten ab. Dies hat den entscheidenden Vorteil, dass die Vorgaben zur sicheren Handhabung von E-Mail automatisch umgesetzt werden, ohne dass ein manueller Eingriff erforderlich wäre. Bedienungsfehlern oder der Umgehung einer Sicherheitspolitik durch die Anwender wird somit ein Riegel vorgeschoben – eine entscheidende Verbesserung gegenüber der Standardsituation.

Da alle Module auf dem lokalen PC ablaufen, entfallen die Nachteile zentralisierter Lösungen

Gegenüber zentralisierten Vorgehensweisen, wie z.B. virtuellen Poststellen, bietet der lokalisierte Ansatz zudem weitere wesentliche Vorteile in Bezug auf die Handhabung von Schlüsselmaterial. Während zentrale Instanzen notwendig über die Schlüssel aller Nutzer verfügen und so selbst zu einem lohnenden Ziel werden, hält DMG diese dezentral und unter der Kontrolle der Nutzer vor, etwa auf Smartcards oder Token. Dabei können diese jedoch nie direkt auf ihre Schlüssel zugreifen; vielmehr führt das Schutzprogramm die entsprechenden Operationen im Betriebssystemkern im Namen des Nutzers aus. Auch im Fall einer Kompromittierung des Nutzerkontos (z. B. durch einen Virus) verhindert diese Vorgehensweise, dass die Schadsoftware Zugriff auf das Schlüsselmaterial erlangt und im Namen des Nutzers beliebige Nachrichten lesen oder verfassen kann. Ausgeschlossen ist somit auch, dass sensible Daten nach außen gelangen oder Prozesse zum Nachteil des Anwenders ohne dessen Einwilligung angestoßen werden – zumal die im DMG implementierten COSEDA-Sicherheitspolitiken in jedem dieser Fälle eines ausdrückliche Willenserklärung des jeweiligen Nutzers erzwingen und dabei sowohl dessen physische Präsenz als auch die Befugnis etwa zum Versenden einer Nachricht oder Aufgeben einer Bestellung überprüfen.
Da in allen Schritten das Prinzip einer möglichst interaktionsfreien und unsichtbaren Integration der Sicherheitsmechanismen zugrunde gelegt wird, sind auch ungeschulte Nutzer in der Lage,

derartige Systeme zu bedienen, ohne dass die Sicherheit des Netzwerks gefährdet ist.
Seine besondere Flexibilität und Mächtigkeit erlangt das COSEDA-System vor allem durch Möglichkeit zur Integration der vorgenannten Module, die als Aktuatoren ebenso wie als Sensoren für die Bewertung und Durchsetzung von Sicherheitspolitiken agieren und die Sicherheitsmechanismen dynamisch an den erkannten Kontext anpassen. So lassen sich präzise Regeln festlegen, nach denen ein Mitarbeiter – abhängig von vorher durchlaufenen Prüfungen – zwar öffentliche Präsentationen auf einen USB-Stick kopieren kann, nicht jedoch vertrauliche Dokumente. Damit werden auch komplexe Sicherheitspolitiken mit minimalem Zusatzaufwand umsetzbar.

Durch Integration aller COSEDA-Module entsteht ein besonders mächtiges System, mit dessen Hilfe sich auch komplexe Sicherheitspoilitiken umsetzen lassen

Mathematische Grundlagen

Kernelement zur Erzielung dieser Flexibilität ist ein automatischer Mechanismus zur Herleitung weiter Teile von Sicherheitsaspekten, den das COSEDA-Projekt im Rahmen seiner Forschungen entwickelt hat und beständig verfeinert. Im Zentrum steht dabei ein mathematisches Modell, das die dynamische Ableitung nachgeordneter technischer Sicherheitspolitiken aus abstrakten Vorgaben zur Laufzeit ermöglicht.

Mit Hilfe formaler Begriffsanalyse wurden hierfür sicherheitsrelevante Kernfunktionen und Abhängigkeiten von Standardbetriebssystemen erfasst und in formaler Logik erster Ordnung formuliert sowie eine formale Semantik dieser Prädikate erstellt. Dies ermöglichte zunächst die Modellierung der Komponenten und Abläufe innerhalb des Betriebssystems selbst. Dabei lassen sich Subjekte und Objekte der Systeme als Konstanten der formalen Theorie darstellen und Operationen, Mengenzugehörigkeiten sowie funktionale Abhängigkeiten in Form von Funktions- und Prädikatssymbolen. Für alle Plattformen (Rechnersysteme, Betriebssysteme, Anwendungsprogramme etc.), auf die das Modell anzuwenden ist, bedarf es einer formalen Interpretation des Modells. Wurden jedoch die zugrunde liegenden Systeme ihrerseits nicht mit Hilfe formaler Logik modelliert und spezifiziert, ist es nicht möglich, die Korrespondenz der Interpretation mit der Semantik des Zielsystems formal zu beweisen.
Innerhalb des vorgenannten Modells können nun insbesondere auch Sicherheitspolitiken unmittelbar durch Symbole und eigentliche Axiome modelliert werden. Die Existenz eines formalen Beweises für ein n-äres Prädikat wird hierbei semantisch als eine erlaubte bzw. erforderliche Operation betrachtet. Gegeben eine formale Theorie T, ein Modell M und eine Politik oder Menge von Politiken Ψ, kann die Menge der erlaubten (erforderlichen) Operationen dabei unter Verwendung des Lindenbaum'schen Erweiterungslemmas als $Ln(\Psi)$ beschrieben werden.

Im Zentrum der Forschungsarbeiten von COSEDA steht die Entwicklung und Verfeinerung eines mathematischen Modells zur Ableitung von Sicherheitspolitiken aus abstrakten Vorgaben

Für jede Instanz eines modellierten Systems liefert eine Interpretation der formalen Theorie die Semantik dieser Plattform. Da diese Abbildungen aufgrund der unterschiedlichen Strukturen der modellierten Systeme in der Regel nonepimorph sind, handelt es sich bei den Interpretationen jeweils um Bijektionen auf einen Homomorphismus des formalen Modells.

Ein besonderes Problem besteht dabei in der Implementierung der Sicherheitsfunktionen zur Laufzeit, die eine starke Strukturierung sowohl der Politiken als auch des abstrakten Modells notwendig macht

Da jedoch die zulässigen und geforderten Operationen in Echtzeit erfolgen müssen und eine direkte Formulierung der Politik aufgrund des dann erforderlichen Umfangs nicht praktikabel ist, sind weitere Strukturierungsmaßnahmen erforderlich. Durch die Einbettung von algebraischen Verbandsstrukturen in die formale Theorie lassen sich diese sowohl für das zugrunde liegende abstrakte Modell als auch für die Sicherheitspolitiken selbst vornehmen. Entsprechende algebraische Strukturen können zudem zur Strukturierung der Sicherheitspolitiken selbst dienen. So lassen sich z. B. in Anlehnung an die Organisationsstruktur des Anwenderunternehmens hierarchische Politiken konstruieren und bereichsspezifische Regelungen in Abhängigkeit von Relationen innerhalb der Verbandsstruktur anwenden. Hierzu können einerseits die axiomatischen Strukturen des zugrunde liegenden Modells und andererseits spezifische Strukturen konstruiert werden, etwa für rollenbasierte Sicherheitspolitiken, die effizient durch rekursive Mengenbeschreibungen für Subjekte und Objekte unter Verwendung separater Prädikatssymbole dargestellt sind. Der Politikmechanismus ist dabei jedoch vollständig neutral und aufgrund seiner Darstellung in Form einer Theorie erster Ordnung in der Lage, sämtliche maschinell darstellbaren Sicherheitspolitiken wiederzugeben. Dies ermöglicht nicht nur wesentliche Beschleunigungen bei der automatischen Herleitung, sondern auch die Formulierung abstrakter Sicherheitspolitiken, die sich automatisch auf Elemente niedrigerer Ebenen auswirken. So lässt sich z. B. beim Zugriff eines Prozesses auf eine bestimmte Datei sicherstellen, dass dieser einem Nutzer zugeordnet ist, der über bestimmte Befugnisse verfügt, während die fragliche Datei einerseits für den Geschäftsprozess notwendig und andererseits einem Projekt zugeordnet ist, für das der Nutzer die erforderlichen Berechtigungen aufweist.

Die Automatisierung der Sicherheitsfunktionen minimiert die Fehlerquote und erleichtert notwendige Software-Anpassungen

Die Automatisierung und Abstraktion minimiert somit die Risiken durch Fehler bei der Umsetzung einer Sicherheitspolitik und reduziert den Anpassungsaufwand bei deren Ergänzung oder Änderung. Zudem erlaubt sie, dynamisch auf Bedrohungen zu reagieren, z. B. indem aufgrund einer erkannten Anomalie im überwachten Teilbereich eines Netzes andere Knoten und Systeme angewiesen werden, schärfere Sicherheitsmechanismen zu nutzen und risikoreiche Dienste temporär zu deaktivieren.

Zum Autor:
Prof. Dr. Stephen D. Wolthusen ist Lecturer am *Department of Mathematics* der Universität London und Associate Professor am *Norwegian Information Security Laboratory* in Gjøvik. E-Mail-Kontakt: stephen.wolthusen@rhul.ac.uk