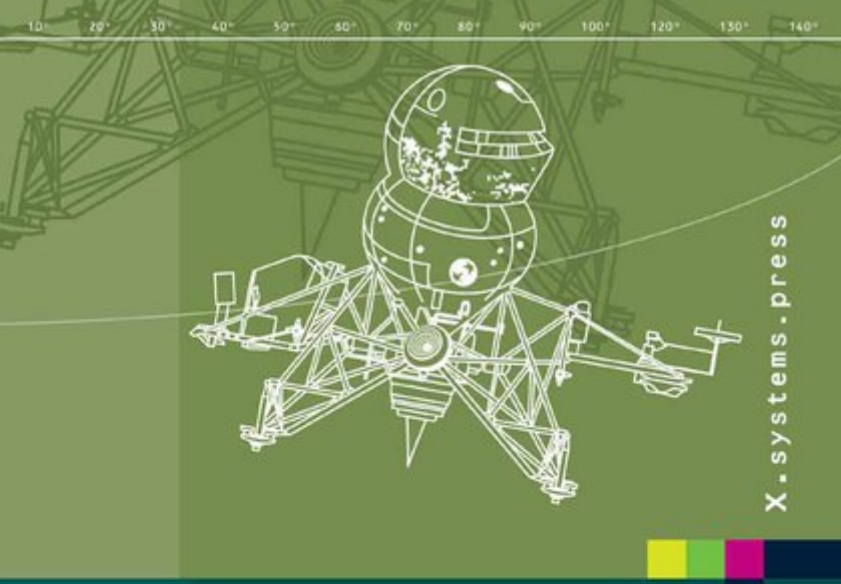


X.systems.press

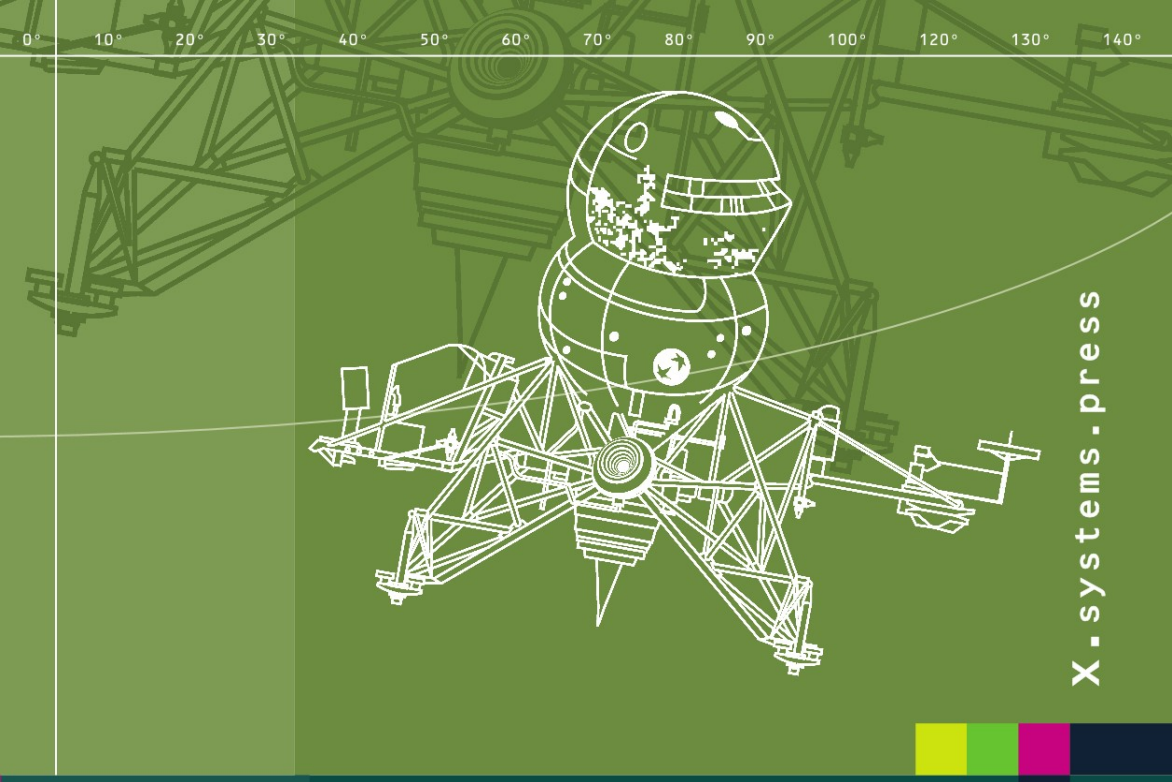
Michael Meier

Intrusion Detection effektiv!

Modellierung und Analyse von Angriffsmustern

CD-ROM

Springer



Michael Meier

Intrusion Detection effektiv!

Modellierung und Analyse von Angriffsmustern

CD-ROM

Springer

X.systems.press

X.systems.press ist eine praxisorientierte Reihe zur Entwicklung und Administration von Betriebssystemen, Netzwerken und Datenbanken.

Michael Meier

Intrusion Detection effektiv!

Modellierung und Analyse von Angriffsmustern

Mit 104 Abbildungen, 16 Tabellen
und CD-ROM

Springer

Dr. Michael Meier
Fachbereich Informatik
Universität Dortmund
44221 Dortmund
michael.meier@udo.edu

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISSN 1611-8618
ISBN-13 978-3-540-48251-2 Springer Berlin Heidelberg New York

Springer ist ein Unternehmen von Springer Science+Business Media
springer.de

Satz: Druckfertige Daten des Autors
Herstellung: LE-TEX, Jelonek, Schmidt & Vöckler GbR, Leipzig
Umschlaggestaltung: KünkelLopka Werbeagentur, Heidelberg
Gedruckt auf säurefreiem Papier 33/3100 YL – 5 4 3 2 1 0

Widmung

Meinen Eltern.

Vorwort

In dem Forschungsgebiet *Intrusion Detection* wird seit Mitte der 80er Jahre gearbeitet. Seit einigen Jahren sind kommerzielle *Intrusion-Detection-Systeme (IDS)* verfügbar, die ergänzend zu präventiven Sicherheitsmechanismen zum Schutz von informationstechnischen Systemen eingesetzt werden können. Die Wirksamkeit zurzeit verfügbarer Systeme bleibt jedoch weit hinter den Erwartungen der Nutzer zurück. Ursache dafür ist eine große Zahl von Fehlalarmen sowie eine schwer zu beziffernde Zahl von unerkannten Sicherheitsverletzungen, durch die der tägliche Einsatz von IDS geprägt ist. Darüber hinaus wird es aufgrund der anfallenden Datenvolumen zunehmend schwieriger in modernen leistungsfähigen Systemen zeitnah Sicherheitsverletzungen zu erkennen.

Dieses Buch betrachtet diese Problemfelder. Dabei werden systematisch fundiert die folgenden Fragestellungen diskutiert und entsprechende Lösungen dargestellt:

- Was sind die relevanten Charakteristika von Sicherheitsverletzungen, die in Angriffsmustern spezifiziert werden müssen, um eine exakte Erkennung zu ermöglichen?
- Wie können komplexe Angriffsmuster geeignet modelliert und beschrieben werden?
- Wie kann die Erkennung der Angriffsmuster effizient(er) realisiert werden?

Dem Leser werden dabei Werkzeuge zur Bewertung existierender und Konstruktion neuer IDS vorgestellt. Schwerpunkte sind dabei die systematische Betrachtung sowie exakte Modellierung und Beschreibung von Angriffsmustern. Darüber hinaus werden existierende Analyseverfahren zur Erkennung von Angriffsmustern beschrieben und ein hinsichtlich Effizienz optimiertes Verfahren vorgestellt.

Dieses Buch ist zum größten Teil während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Lehrstuhl Rechnernetze und Kommunikationssysteme der Brandenburgischen Technischen Universität Cottbus entstanden. Für die wissenschaftliche Betreuung meiner Arbeiten, die eingeräum-

ten Freiräume sowie die in vielerlei Hinsicht angenehme Arbeitsatmosphäre an seinem Lehrstuhl danke ich Hartmut König. Meine Arbeiten zu diesem Buch profitierten unter anderem von der fruchtbaren Zusammenarbeit mit Ulrich Flegel. Während zahlloser Treffen auf Workshops und Konferenzen sowie Besuchen in Dortmund und Cottbus diskutierten wir die Ausdrucksstärke von Modellierungsansätzen für Angriffssignaturen. Als Ergebnis unserer Zusammenarbeit entstand ein allgemeiner Ansatz zur Modellierung von Angriffssignaturen. Mario Schölzel gilt besonderer Dank für seine Unterstützung bei der formalen Definition von Signaturnetzen. Niels Bischof, Christian Rohr und Sebastian Schmerl danke ich für ihre Arbeiten und ihre konstruktiven Ideen zu den Sprachen SHEDEL und EDL sowie den Werkzeugen SAM und SEG, die auf beiliegender CD-ROM enthalten sind.

Dortmund, im November 2006

Inhaltsverzeichnis

Abkürzungsverzeichnis

AID	Adaptive Intrusion Detection system
ANIDA	Aachen Network Intrusion Detection Architecture
ASAX	Advanced Security audit trail Analyzer on uniX
BSM	Basic Security Module
CC	Coordination Center
CERT	Computer Emergence Response Team
CIDF	Common Intrusion Detection Framework
CLIPS	C Language Integrated Production System
CMDS	Computer Misuse Detection System
CPA	Coloured Petri Net Automaton
DARPA	Defense Advanced Research Projects Agency
DPEM	Distributed Program Execution Monitor
ECA	Event Condition Action
EDL	Event Description Language
EGID	Effektive Gruppen-ID
EMERALD	Event Monitoring Enabling Responses to Anomalous Live Disturbances
ET	Ereignis-Token
EUID	Effektive User-ID
FL	Failed Login
FRT	Fire Ready Tokens
GID	Gruppen-ID
GUI	Graphical User Interface
ID	Identifikator
IDIOT	Intrusion Detection In Our Time
IDMEF	Intrusion Detection Message Exchange Format
IDRS	Intrusion Detection and Response System
IDS	Intrusion-Detection-System
IDWG	Intrusion Detection Working Group
IETF	Internet Engineering Task Force
Inter-EB	Inter-Ereignis-Bedingung
Intra-EB	Intra-Ereignis-Bedingung
IP	Internet Protokoll
IPS	Intrusion-Prevention-System

IT-	Informationstechnisch (im Zusammenhang)
MIDAS	Multics Intrusion Detection and Alerting System
MuSig	Misuse Signature
OID	Objekt-ID
P-BEST	Production-Based Expert System Toolset
PID	Reale Prozess-ID
RGID	Reale Gruppen-ID
RUID	Reale User-ID
RUSSEL	RUle-baSed Sequence Evaluation Language
SAM	Signature Analysis Module
SEG	Snoopy-based EDL GUI
SHEDEL	Simple Hierarchical Event DEscription Language
STAT	State Transition Analysis Technique
StraFER	Straight Forward Event Recognition
SUID	Set-User-ID
TT	Token-Token
UID	User-ID

1 Einleitung

Die moderne Informationsgesellschaft basiert auf komplexen informationstechnischen Infrastrukturen, die einen zunehmenden Grad an Vernetzung aufweisen. Immer mehr private und öffentliche Institutionen verwenden *informationstechnische Systeme (IT-Systeme)*, um ihre Dienste effektiver und effizienter anbieten und abwickeln zu können. Durch die globale Vernetzung wird der Zugang zu Diensten in Zukunft für jedermann, zu jederzeit und von jedem Ort möglich sein. Die Vorteile dieser Entwicklungen sind unbestritten. Sie bringen jedoch auch Nachteile mit sich. Aus der Verlagerung vieler gesellschaftlicher Prozesse auf IT-Systeme resultiert eine direkte Abhängigkeit unserer Gesellschaft von diesen Systemen. Dadurch gewinnt der Schutz von IT-Systemen zunehmend an Bedeutung.

Klassische Sicherheitsmechanismen, z. B. kryptographische Verfahren und Zugangskontrollsysteme, wie beispielsweise Firewalls, sind notwendige Komponenten zum Schutz von IT-Infrastrukturen und heute weit verbreitet. Während bisher vorrangig präventive Maßnahmen und Mechanismen im Vordergrund standen, wird zunehmend deutlich, dass die Sicherheit von IT-Systemen nicht allein durch Prävention erreichbar ist. Vielmehr stellt Prävention einen Grundpfeiler dar, neben dem reaktive Aspekte der Sicherheit von IT-Systemen stehen.

Um in der Lage zu sein, auf Sicherheitsverletzungen reagieren zu können, sind Mechanismen zur Erkennung von Sicherheitsverletzungen erforderlich. Seit Mitte der 80er Jahre hat sich daher das Forschungsgebiet der *Angriffserkennung (Intrusion Detection)* entwickelt. Seit einiger Zeit sind kommerzielle *Intrusion-Detection-Systeme (IDS)* verfügbar, die ergänzend zu präventiven Sicherheitsmechanismen zum Schutz von IT-Systemen eingesetzt werden können.

Die in diesem Gebiet entwickelten Verfahren zur Erkennung von Sicherheitsverletzungen können grob in Anomalieerkennung und Missbrauchserkennung unterteilt werden. Verfahren zur *Anomalieerkennung* basieren auf der expliziten Definition von normalem Verhalten und erkennen Abweichungen von dieser Norm. Problematisch bei diesen Verfahren sind die inhärente Unschärfe der gelieferten Ergebnisse sowie die Frage, ob jede Anomalie eine Sicherheitsverletzung darstellt.

Zur *Missbrauchserkennung* ist das Vorliegen expliziter Definitionen von Angriffsmustern in Form von Signaturen erforderlich. Beobachtete Aktionen werden auf Übereinstimmung mit den Signaturen überprüft. Prinzipiell sind Verfahren zur Missbrauchserkennung bezüglich der Erkennungsgenauigkeit sehr robust und liefern scharfe Ergebnisse, auf deren Grundlage Reaktionen auf Angriffe veranlasst werden können. Die Missbrauchserkennung stellt daher ein unverzichtbares Basisauswertungsverfahren von IDS dar, das um Anomalieerkennung ergänzt werden kann. Naturgemäß sind Verfahren zur Missbrauchserkennung jedoch auf die Erkennung von bekannten, durch Signaturen repräsentierten Angriffen beschränkt.

Obwohl die Notwendigkeit von Systemen zur Missbrauchserkennung unwidersprochen bleibt, ist der Einsatz derzeit verfügbarer Systeme mit einer Reihe von Problemen verbunden. Eines der Hauptprobleme ist die Vielzahl der von den Systemen erzeugten Alarme. Häufig werden tausende von Alarmen pro Tag erzeugt, von denen 99% Fehlalarme sind. Aufgrund dieser Alarmflut ist es schwierig die Alarme zu identifizieren, die tatsächlich Sicherheitsverletzungen anzeigen. Dadurch wird der Nutzen von IDS infrage gestellt.

Unter der Vorraussetzung einer korrekten Spezifikation von Signaturen, können Fehlalarme durch Missbrauchserkennungssysteme ausgeschlossen werden. Missbrauchserkennungssysteme erkennen genau die Muster, die in den Signaturen beschrieben sind. Die Ursache für hohe Fehlalarmraten ist dementsprechend auf der Ebene der Spezifikation der Signaturen zu suchen. Zum einen fehlt eine Systematik zur Betrachtung der relevanten Aspekte von Angriffssignaturen. Mit verschiedenen existierenden Sprachen zur Beschreibung von Signaturen sind unterschiedliche Mengen von Signaturen beschreibbar. Vielfach können Signaturen mit den zur Verfügung stehenden Sprachmitteln nicht exakt spezifiziert werden. Zum anderen führt die Komplexität von Angriffssignaturen zu einem Fehlerpotential bei ihrer Entwicklung. In existierenden Sprachen fehlen geeignete Mittel, um den Signaturentwickler bei der Beherrschung dieser Komplexität zu unterstützen.

Die steigende Leistungsfähigkeit von IT-Systemen führt zu einem weiteren Problem für die Missbrauchserkennung. Der damit einhergehende Anstieg des Datenaufkommens führt existierende Missbrauchserkennungssysteme an die Grenzen ihrer Leistungsfähigkeit. Die aus der zunehmenden Komplexität der IT-Systeme resultierende Steigerung der Anzahl zu analysierender Angriffsmuster verschärft dieses Problem zusätzlich. Aktuelle Systeme zur Missbrauchserkennung setzen verschiedene Standardverfahren zur Analyse ein. Der Entwicklung und Untersuchung optimierter Analyseverfahren zur Missbrauchserkennung wurde bisher kaum Auf-