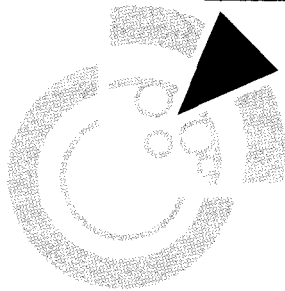


Ulrich Flegel, Michael Meier (Eds.)

Detection of Intrusions and Malware & Vulnerability Assessment

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

TECHNISCHE
INFORMATIONSBIBLIOTHEK
UNIVERSITÄTSBIBLIOTHEK
HANNOVER



DIMVA 2004

Contents

Intrusion Detection

Alarm Reduction and Correlation in Intrusion Detection Systems	9
---	----------

*Tobias Chyssler, Stefan Burschka, Michael Semling, Tomas Lingvall,
Kalle Burbeck*

Alert Verification Determining the Success of Intrusion Attempts	25
---	-----------

Christopher Kruegel and William Robertson

Komponenten für kooperative Intrusion-Detection in dynamischen Koalitions-umgebungen	39
---	-----------

Marko Jahnke, Martin Lies, Sven Henkel, Michael Bussmann and Jens Tölle

Vertrauensbasierte Laufzeitüberwachung verteilter komponenten- strukturierter E-Commerce-Software	55
--	-----------

Peter Herrmann, Lars Wiebusch and Heiko Krumm

Intrusion detection in unlabeled data with quarter-sphere Support Vector Machines	71
--	-----------

Pavel Laskov, Christin Schäfer and Igor Kotenko

Sensors for Detection of Misbehaving Nodes in MANETs	83
---	-----------

Frank Kargl, Andreas Klenk, Michael Weber, Stefan Schlott

Aktive Strategien zur Schutzzielverletzungserkennung durch eine kontrollierte Machtteilung in der Zugriffskontrollarchitektur	99
--	-----------

Joerg Abendroth

Honeypots

A Honeynet within the German Research Network – Experiences and Results . .	113
--	------------

Helmut Reiser and Gereon Volker

Ermittlung von Verwundbarkeiten mit elektronischen Ködern	129
--	------------

Maximillian Dornseif, Felix C. Gärtner and Thorsten Holz

Vulnerabilities

Foundations for Intrusion Prevention	143
---	------------

Shai Rubin, Ian D. Alderman, David W. Parter, and Mary K. Vernon

Structural Comparison of Executable Objects	161
--	------------

Halvar Flake

Anti-Patterns in JDK Security and Refactorings	175
---	------------

Marc Schönefeld

Malware

LIV - The Linux Integrated Viruswall	187
---	------------

Teobaldo A. Dantas de Medeiros and Paulo S. Motta Pires

Risiken der Nichterkennung von Malware in komprimierter Form	201
---	------------

Heiko Fangmeier, Michel Messerschmidt, Fabian Müller and Jan Seedorf

Author Index	213
---------------------------	------------