Call for Papers

Detection of Intrusions and Malware & Vulnerability Assessment

DIMVA 2004

6. - 7. Juli 2004
Dortmund, Deutschland

Workshop der Fachgruppe SIDAR der Gesellschaft für Informatik e.V. (GI)
in Kooperation mit
IEEE Task Force on Information Assurance
German Chapter of the ACM
Universität Dortmund

http://www.gi-fg-sidar.de/dimva2004
mailto:dimva2004{at}gi-fg-sidar.de

Die Fachgruppe SIDAR (Security - Intrusion Detection and Response) der Gesellschaft für Informatik e.V. beschäftigt sich mit der Erkennung und Beherrschung von Vorfällen der Informationssicherheit und veranstaltet vom 6.-7. Juli 2004 einen Workshop zum Thema Erkennung von Schutzzielverletzungen (Intrusion Detection), Malwarebekämpfung (Malicious Agents) sowie Ermittlung von Verwundbarkeiten (Vulnerability Assessment).

Ziel des Workshops ist es, eine Übersicht zum Stand der Technik und Praxis in Industrie, Dienstleistung, Verwaltung und Wissenschaft im deutschsprachigen Raum zu geben. Insbesondere sollen Ergebnisse aus den Bereichen Forschung, Entwicklung und Integration vorgestellt, relevante Anwendungen aufgezeigt sowie neue Technologien und daraus resultierende Produktentwicklungen konzeptionell dargestellt werden. Rechtliche Rahmenbedingungen und wirtschaftliche Faktoren sollen ebenfalls betrachtet werden.

Das Programmkomitee lädt ein zur Einreichung von

- vollen Beiträgen über bisherige Ansätze und Erfahrungen sowie laufende Entwicklungen, insbesondere zu Theorie, Entwurf, Implementierung, Analyse und Evaluierung sowie über rechtliche Rahmenbedingungen.
- vollen Beiträgen und Kurzbeiträgen über Praxisstudien und wirtschaftliche Faktoren bei der Einführung oder Anwendung in Referenzprojekten (Fallstudien).

Die Beiträge können unter anderem (aber nicht ausschließlich) folgende Gesichtspunkte behandeln:

- Entdeckung von Schutzzielverletzungen (Intrusion Detection - ID):
  - Handhabung von großen Daten- und Alarmvolumina
  - Anwendung in Hochleistungsnetzen und Echtzeit-Umgebungen
  - Nachweisführung bei der Verfolgung von Schutzzielverletzungen
  - Entdeckung anwendungsspezifischer Schutzzielverletzungen
- Ermittlung von Verwundbarkeiten (Vulnerability Assessment - VA):
  - Dokumentation und Nachvollziehbarkeit
  - Analyse von dynamischem Server-Content
  - Verwundbarkeiten bei neuen Betriebssystemen (z.B. Windows 2003)
  - Sicherheitsanalyse von komplexen oder nicht-dokumentierten Protokollen (z.B. Windows-Protokolle, Enhanced Interior Gateway Routing Protocol)
- Agenten mit Schadensfunktion / Malware (Malicious Agents - MA):
  - Klassische und alternative Erkennungsmethoden
  - Bezeichnungs- und Beschreibungs-Methoden
  - Auswirkungen von Malware auf moderne Netze und deren Dienste (z.B. Email, Identitätsmanagement, WebServices, Single-Sign-On)

Sowie für alle Teilgebiete (ID, VA, MA):

- Trends und Herausforderungen
- Aspekte bei mobilen Endgeräten
- Nutzung wissenschaftlicher Ergebnisse bei der Produktentwicklung
- Technisch nutzbare Synergien, Querbezüge und Berührungspunkte der Teilgebiete ID, VA, MA sowie Netzwerk-Management:
  - gemeinsame Verwundbarkeits-Modelle und -Klassifikationen
  - Interoperabilität und Standardisierung
  - Kooperation und Integration verschiedener Produkte
  - auf Kooperation basierende Adaptivität
  - Korrelation, Aggregation und Fusion von Meldungen

Formalia

Die Einreichungsfrist für Beiträge wurde verlängert auf den **29.02.2004**. Beiträge werden bis zu diesem Termin entgegen genommen, wenn sie bis zum **11.02.2004** mit einem Abstract per Email angemeldet wurden. In der Email sind Beitragstitel, Autorennamen, Kontaktautor, Organisation und Email-Adresse anzugeben (ASCII) und der geplante Inhalt des Beitrags zusammenzufassen. Jeder Abstract-Eingang wird innerhalb von 7 Tagen per Email bestätigt.
Jeder Beitrag wird von mindestens drei Gutachtern bewertet. Angenommene Beiträge werden auf dem Workshop präsentiert. Es ist vorgesehen, angenommene volle Beiträge in einem Tagungsband der Reihe Lecture Notes in Informatics (LNI) zu veröffentlichen. Voraussetzung dafür ist eine unterzeichnete Copyright-Erklärung der Autoren. Beiträge können in deutscher oder in englischer Sprache verfasst werden. Volle Beiträge umfassen 10-14 Druckseiten im LNI-Format (Formatvorlage s. Webseite), Kurzbeiträge 4-9 Seiten. Beiträge sind per Email als MIME-Attachment im PDF-Format einzureichen. Andere Formate können nicht berücksichtigt werden. In der Email sind Beitragstitel, falls zutreffend, inhaltliche Kategorie des Beitrags (s.o.), Autorennamen, Kontaktautor, Organisation, Email-Adresse, postalische Adresse, Telefon- und Faxnummer anzugeben (ASCII). Jeder Beitrags-Eingang wird innerhalb von 7 Tagen per Email bestätigt.

Termine

11.02.2004	Einreichung der Abstracts an: dimva2004{at}gi-fg-sidar.de
29.02.2004	Einreichung der Beiträge an: dimva2004{at}gi-fg-sidar.de
31.03.2004	Annahme-Benachrichtigung an Autoren per E-Mail
31.04.2004	Elektronische Abgabe druckfertiger Beiträge

Tagungsleitung

Ulrich Flegel (Vorsitz), Universität Dortmund,
Fachbereich Informatik, LS6 - Informationssysteme und Sicherheit, D-44221 Dortmund
Tel.: +49-231-755-4775, ulrich.flegel{at}udo.edu

Michael Meier, Brandenburgische Technische Universität Cottbus,
Institut für Informatik, Lehrstuhl Rechnernetze, Postfach 10 13 44, D-03013 Cottbus
Tel.: +49-355-69-2028, mm{at}informatik.tu-cottbus.de

Programmkomitee

Thomas Biege (SuSE Linux AG)
Roland Büschkes (T-Mobile)
Toralv Dirro (Network Associates)
Anja Feldmann (TU München)
Ulrich Flegel (stv. Vorsitz) (Uni Dortmund)
Christian Freckmann (TÜV-IT)
Oliver Göbel (RUS-CERT)
Christian Götz (Cirosec)
Dirk Häger (BSI)
Marc Heuse (Unisys)
Klaus Julisch (IBM Research Zürich)
Oliver Karow (Symantec)
Klaus-Peter Kossakowski (Presecure)
Hartmut König (BTU Cottbus)
Heiko Krumm (Uni Dortmund)
Christopher Krügel (UCSB, Kalifornien)
Holger Mack (Secorvo)
Michael Meier (Vorsitz) (BTU Cottbus)
Jens Nedon (Consecur)
Christian Schmid (Linz, Österreich)
Morton Swimmer (IBM Research Zürich)
Stefan Strobel (Cirosec)
Marco Thorbrügge (DFN-CERT)
Andreas Wespi (IBM Research Zürich)
Stephen Wolthusen (Fraunhofer IGD Darmstadt)
Ralf Zessin (Maxpert AG)

Veranstalter

Fachgruppe SIDAR der
Gesellschaft für Informatik e.V. (GI)
Wissenschaftszentrum, Ahrstraße 45; D-53175 Bonn
Tel.: +49-228-302-145; Fax: +49-228-302-167
http://www.gi-ev.de

in Kooperation mit
IEEE Task Force on Information Assurance
German Chapter of the ACM
Universität Dortmund