Technische Universität Ilmenau
Fakultät für Informatik und Automatisierung
Institut für Praktische Informatik und Medieninformatik
Fachgebiet Telematik
Prof. Dr. Dietrich Reschke

Klassifikation und Einsatzmöglichkeiten von Intrusion Detection Systems (IDS)

Projektarbeit

Vortrag am 2002-11-15
von Heiko Steigerwald
Wirtschaftsinformatik, M97

Motivation - Zielstellung

- CERT/CC:
  Anzahl der gemeldeten sicherheitsrelevanten Vorfälle hat sich von 1998 – 2001 jährlich mehr als verdoppelt

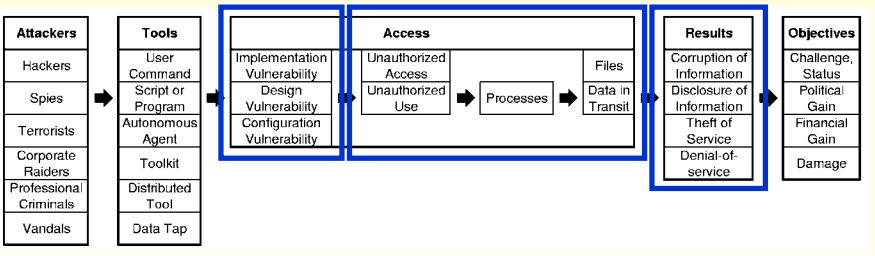
- Zielstellung der Arbeit:
  - Systematische Klassifikation von IDS
  - Gründe für den Einsatz von IDS im Rahmen eines Sicherheitskonzeptes
  - Herausforderungen für IDS

Begriffsbestimmung IT-Sicherheit

- Klassische Schutzziele der IT-Sicherheit:
  - Verfügbarkeit (availability)
  - Vertraulichkeit (confidentiality)
  - Unversehrtheit (integrity)
- Sicherheitskonzept (security policy)
- Absolute IT-Sicherheit ist nicht zu erreichen!

Begriffsbestimmung IDS / Attack Taxonomy

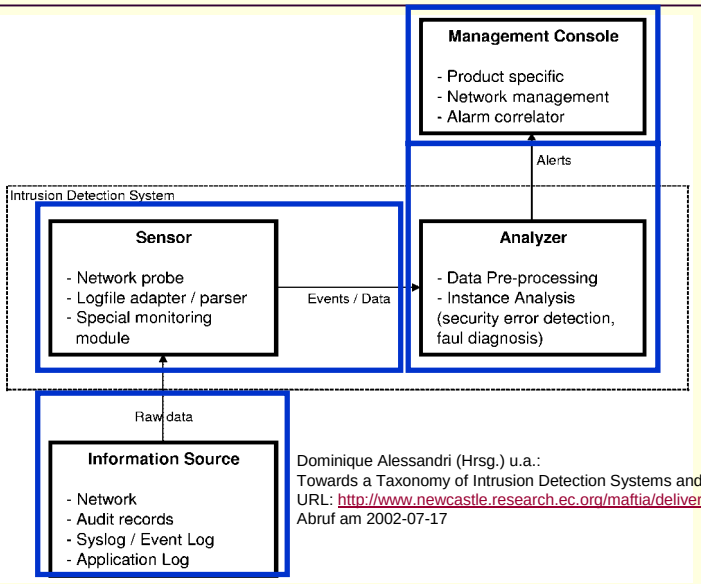
„An intrusion-detection system dynamically monitors the actions taken in a given environment, and decides whether these actions are symptomatic of an attack [...]."[1]



[1] Hervé Debar u.a.: Towards a Taxonomy of Intrusion Detection Systems. In: Computer Networks 31 (1999), S. 806

Bild nach John D. Howard, An Analysis Of Security Incidents On The Internet 1989 – 1995. URL: http://www.cert.org/research/JHThesis/Chapter6.html - Abruf am 2002-11-13.

Funktionales Modell eines IDS



Dominique Alessandri (Hrsg.) u.a.:
Towards a Taxonomy of Intrusion Detection Systems and Attacks.
URL: http://www.newcastle.research.ec.org/maftia/deliverables/D3final.pdf - Abruf am 2002-07-17

Verwendete IDS-Taxonomie

- Funktionale Charakteristiken
  - **Audit source location**
  - **Detection methode / detection paradigma**
  - **Behavior on detection**
- Systemcharakteristiken
  - Usage frequency
  - Granularity of data-processing
  - Time of detection
  - Location of data-collection / data-processing
  - Security
  - Interoperability

Ausprägungen von „audit source locations“

- **Host log files** (**H**IDS)
  - Audit trails wie Syslog, C2 security audits
  - Application log files, IDS sensor alerts
- **Network Packets** (**N**IDS)
  - Packet capturing
  - Network sniffing
  - Überwiegend Ethernet bzw. TCP/IP-Protokollfamilie

Wesentliche Vor-/Nachteile von HIDS

- Vorteile:
  - Erkennung von lokalen Angriffen
  - Keine Einschränkung durch netzwerkspezifische Problematiken
  - Sehr umfangreiche und detaillierte Datenquellen
- Nachteile:
  - Viele (verschiedene) Datenquellen
  - Ausführung auf dem Zielsystem
    - Beansprucht Ressourcen
    - Performanzprobleme
    - Entdeckung

Wesentliche Vor-/Nachteile von NIDS

- Vorteile:
  - Wenige Sensoren um große Netzwerke zu überwachen
  - Dedizierte Sensoren
  - Passiver Charakter der Sensoren
  - Remote-Angriffe werden zeitlich früher erkannt
- Nachteile:
  - Traffic wird u.U. nicht erfasst
    (zu hoher Datendurchsatz, Switching-Technologie, Verschlüsselung, unbekannte Protokolle)
  - Keine Aussage über Erfolg des Angriffs möglich
  - Lokale Angriffe können nicht erkannt werden

Ausprägungen der „detection methode“

- **Anomaly detection** (behavior-based)
  - Kein Wissen über bestimmte Merkmale eines Angriffs ...
  - ... Sondern Wissen über „normales“ Verhalten
- **Misuse detection** (knowledge- / signature-based)
  - Charakteristische Merkmale eines Angriffes sind bekannt
  - Grundlage: Datenbank mit Angriffssignaturen
- Dimension „detection paradigma“:
  - State-based
  - Transition-based

Wesentliche Vor-/Nachteile von „anomaly detection“

- Vorteile:
  - Erkennung von unbekannten Angriffen
  - Hilfe bei der Analyse unbekannter Angriffe
  - Erkennung von Privilegienmíßbrauch
- Nachteile:
  - Komplexe Konfiguration („normales“ Verhalten)
  - Fehlende / ungenau Diagnose
  - Große Datenmengen

Wesentliche Vor-/Nachteile von „misuse detection“

- Vorteile:
  - Einfache Modelle und effiziente Implementierung
  - Einfachere Konfiguration
  - Effektive Erkennung von bekannten Angriffen
  - Mehr Diagnoseinformationen
- Nachteile:
  - Anpassung und Pflege der Signaturdatenbank (Praktische Unvollständigkeit)
  - Keine Erkennung von Insider Misuse

Ausprägungen im „behavior on detection“

- **Passive alerting**
  - Benachrichtigung von Personal
- **Active responding**
  - Zusätzliche Daten erheben
  - Systemumgebung ändern
  - Aktive Gegenmaßnahmen

Wesentliche Vor-/Nachteile im „behavior on detection“

- Nachteile „**passive alerting**“:
  - Zeitverzug
  - Zu wenige Informationen für qualifizierte Entscheidungen
- Vorteile „a**ctive responding**“:
  - Zeitnähere Reaktion
  - Mehr Informationen zur Verfügung
- Nachteile „a**ctive responding**“:
  - Gefahr der unangemessenen Reaktion
  - Provokation von weiteren Reaktionen
  - Rechtliche Problematik

Ausprägungen von Systemcharakteristiken

- Usage frequency (continous monitoring)
- Granularity of data-processing (continously)
- Time of detection ((near) real-time)

- Location of data-collection / data-processing
  - Centralized <> distributed

- Security
- Interoperability

Spezifische Funktionen eines IDS

- Erhöht Risiko einer Entdeckung und Verfolgung
- Erkennung von Angriffen
- Erkennung von Angriffsvorbereitungen
- Schutz von Systemen, die nicht durch andere Maßnahmen geschützt werden können
- Forensische Analyse
- Dokumentation von Bedrohungen
- „Qualitätskontrolle“ des Sicherheitskonzeptes

Externe Faktoren

- Komplexere Angriffsstrategien / Mächtigere Werkzeuge
- Neue ...
  - Technologien
  - Infrastrukturkomponenten
  - Anwendungen
- Angriffe gegen IDS selbst
- Mobiler Code

Funktionale & technische Herausforderungen

- Angriffe im frühesten möglichen Stadium erkennen
- Performanz
- Komplexität von IT-Infrastrukturen
  - Skalierung ?
  - Interoperabilität ?
- Mobile Nutzer / Geräte

Tests & Datenanalyse

- Problematik der Evaluierung
- Verarbeitung großer Mengen Analysedaten
- Fehlende Unterstützung der Forensischen Analyse

Organisation & menschliche Interaktion

- Verbesserung der Kooperation zwischen Organisationen zum Informationsaustausch
- Datenschutz und Arbeitsrecht
- Bessere Entscheidungsunterstützung des Menschen
- Nutzung der kreativ-analytischen Fähigkeiten des Menschen
- Qualifiziertes Personal

Trends und aktuelle Forschung

- Trends:
  - Netzwerk-basierte bzw. hybriden IDS
  - Verteilte Architekturen
  - Höhere Interoperabilität
- Aktuelle Forschung
  - Verbesserung der Anomaly Detection
  - Testumgebungen zur Evaluation
  - Standards / Frameworks
  - Multi sensor data fusion

... noch Fragen ?

Danke für die Aufmerksamkeit !

IDS Historie

- 1980: James P. Anderson
  „Computer Security Threat Monitoring and Surveillance“
- 1986: Dorothy E. Denning
  „An Intrusion Detection Model“
- Ab 1990 zunehmender kommerzieller Einsatz von IDS
  - Hybride IDS
  - Sprunghafte Zunahme vernetzter Systeme
  - Zunehmender Einsatz von IT in allen Unternehmensbereichen