Dynamic Application-Layer Protocol Analysis for Network Intrusion Detection

Technische Universität Berlin
Seminar Internetsicherheit

Elisa Jasinska
jasinska@informatik.hu-berlin.de

Berlin, 24.2.2007

Literatur

- “Dynamic Application-Layer Protocol Analysis for Network Intrusion Detection”, H. Dreger, A. Feldmann, M. Mai, V. Paxson & R. Sommer, In den Proceedings vom 15. Usenix Security Symposium
- Bro Intrusion Detection System, http://www.bro-ids.org/
- Snort, http://www.snort.org/

Agenda

- Intrusion-Detection-Systeme
- Problemanalyse
- Bro - Intrusion-Detection-System
- Dynamic Application-Layer Protocol Analysis
- Ergebnisse

Intrusion Detection Systems

- Intrusion Detection System (IDS)
  - Host-Basierte IDS
  - Netzwerk-Basierte IDS
  - Hybride IDS
- Intrusion Prevention System (IPS)

Problemanalyse

IDS arbeiten mit:

- Pattern Matching
  - Vorkommen bestimmter Zeichenfolgen
  - Signaturen (eg. RegExp)

➜ statisch

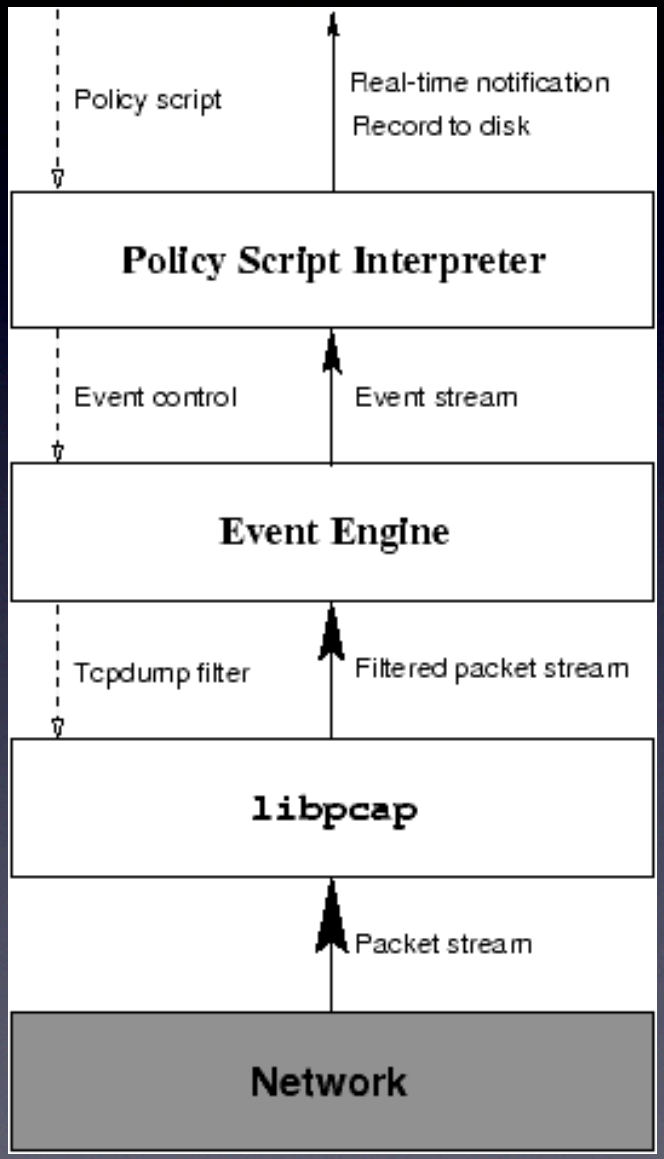
Problemanalyse

IDS arbeiten mit:

- Stateful Packet Inspection (SPI)
  - Zustandsanalysen auf verschiedenen Ebenen des Protokoll-Stacks
  - Protokoll-Analyzer

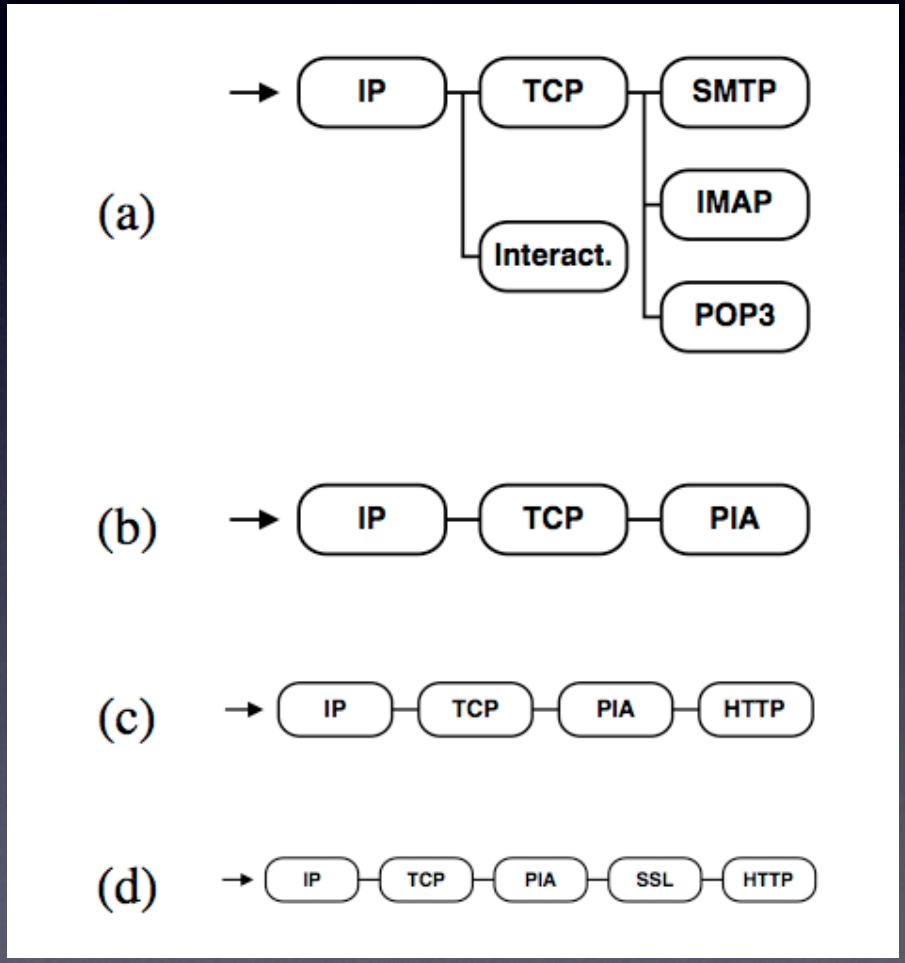
➜ genauer, jedoch immer noch statisch

Bro IDS



3. Policy Script Interpreter
   - Ereignisse ausloesen
2. Event Engine
   - Generiert Events
1. libpcap
   - Mischneiden und Vorfiltern

Dynamic Application-Layer Protocol Analysis



Dynamic Applikation-Layer Protocol Analysis

PIA (Protocol-Identification-Analyzer)

1. Signaturen um das Protokoll zu bestimmen
   - Statische Portnummern
   - Prediction Table
2. Protokoll-Analyzer um das Protokoll zu verifizieren und analysieren

Ergebnisse

- University of California, Berkeley (UCB)
  - 45 000 Hosts, 3 x 2Gbps Uplink, 5 TB/Tag
- Münchener Wissenschaftsnetz (MWN)
  - 50 000 Hosts, 1Gbps Uplink, 1-3 TB/Tag
- Lawrence Berkeley National Laboratory (LBNL)
  - 15 000 Hosts, 1Gbps Uplink, 1.5 TB/Tag

Ergebnisse

Nicht standardisierte Portnummern UBC

Protokoll	gefundene lokale Server	gefundene externe Server
FTP	6	17
HTTP	568	54 830
IRC	2	33
SMTP	8	8

Ergebnisse

Nicht standardisierte Portnummern MWN

Protokoll	gefundene lokale Server	gefundene externe Server
FTP	3	40
HTTP	108	18 844
IRC	3	58
SMTP	3	5

Ergebnisse

- Nutzlastbetrachtung von FTP
  - FTP auf unbekanntem Port erkannt
  - Nutzlast an speziellen Analyzer (z. B. libmagic) um Dateityp zu spezifizieren

Ergebnisse

- IRC-basierte Botneterkennung
  - Nickname des Clients
  - Topic im Channel
  - History von Botservern um Clients zu identifizieren

MWN	UCB
100	15

Questions?