Intrusion Detection and Malware Analysis
IDS Taxonomy and Architecture

Pavel Laskov
Wilhelm Schickard Institute for Computer Science
IDS functionality

- Restrict access to legitimate service
- Prevent malicious events from entering a system
- Detect malicious activity
- Repair infected data/events

Preventive

Misuse-centric

Automatic
IDS functionality

- Restrict access to legitimate service
- Prevent malicious events from entering a system
IDS functionality

- Restrict access to legitimate service
- Prevent malicious events from entering a system

- Detect malicious activity
- Repair infected data/events
IDS functionality

- Restrict access to legitimate service
- Prevent malicious events from entering a system

- Detect malicious activity
- Repair infected data/events

- Preventive
- Live events

- Misuse-centric
- Automatic
IDS design issues / taxonomy

- Location
  - network
  - host/operation system
  - host/application

- Detection methods
  - signature-based ("misuse detection")
  - anomaly-based
  - behavior based
Exemplary data: network dump

0x0000: 0030 85a2 a8ff 0016 cbb5 d720 0800 4500 .0............E.
0x0010: 01e4 8771 4000 4006 8c36 c0a8 11db d155 ...q@.@..6......U
0x0020: 8193 c721 0050 2e4d 453e 9262 6ab5 5018 ...!.P.ME>.bj.P.
0x0030: ffff 27fc 0000 4745 5420 2f69 672f 696d ..’...GET./ig/im
0x0040: 6167 6573 ages

Advantages
- easy to deploy
- wide coverage
- early detection

Disadvantages
- high false alarm rates
- high performance requirements
Exemplary data: system call traces

```c
execve("/bin/cat", ["cat", "/etc/passwd"], [/* 42 vars */]) = 0
open("/etc/passwd", 0_RDONLY|0_LARGEFILE) = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=1214, ...}) = 0
read(3, "root:x:0:0:root:/root:/bin/bash\n"..., 32768) = 1214
close(3) = 0
```

Advantages
- high accuracy
- precise context (-)

Disadvantages
- difficult to deploy
- extra load on a host
- late detection
Exemplary data: application logs

WAIT #1: nam='SQL*Net message from client' ela= 5 p1=1413697536
UPDATE users set password = encrypt('my_new_password')
PARSE #6:c=0,e=981,p=0,cr=0,cu=0,mis=1,r=0,dep=1,og=0
WAIT #6: nam='db file sequential read' ela= 9604 p1=19 p2=133999
EXEC #1:c=30000,e=116691,p=36,cr=35,cu=10,mis=0,r=1,dep=0

Advantages
- high accuracy
- precise context

Disadvantages
- difficult to deploy (-)
- extra load on a host
- late detection
Signature-based IDS

- Detection of attacks by matching a set of known misuse patterns ("signatures") against a stream of events

- Signature example:

  ```
  alert tcp any $EXTERNAL -> $HOME 143
  (content: "|90C8 C0FF FFFF|/bin/sh"; msg: "IMAP exploit");
  ```

- Advantages
  - low false alarm rates
  - precise diagnostics

- Disadvantages
  - insensitivity to attack variations
  - difficulty of signature maintenance
Anomaly-based IDS

- Detection of attacks by measuring deviation from statistical models of normality
  - traffic characteristics
  - protocol compliance
  - packet/connection content
  - system call sequences

- Advantages
  - detection of unknown attacks
  - adjustment to traffic/process drift

- Disadvantages
  - high false alarm rates
  - anomalies ≠ attacks
Behavior-based IDS

- Detection of attacks according to some general behavioral patterns

- Advantages
  - high accuracy
  - robustness to attack variation

- Disadvantages
  - difficulty to define general features
  - ad-hoc rules
- **Meta-level:**
  - intrusion description languages
  - alarm correlation tools
- **Event engines:**
  - signature-based detection
  - classification
  - anomaly detection
- **Audit streams:**
  - network traffic
  - security audit logs
  - application logs
Deployment issues

- Different devices:
  - router
  - firewall
  - NIDS
  - HIDS
- Scalability:
  - handling $X$ devices, $Y$ users and $Z$ applications
- Management challenges:
  - lots of alerts
  - alert correlation
  - incident diagnostics
Intrusion Detection vs. Prevention

How do you upgrade from intrusion detection to intrusion prevention?

Prevention issues:
- real-time operation (performance)
- timeliness (immediate action)
- getting access to events / OS interaction
- decision making (thresholds etc.)
- persuasion of human decision makers / operational issues
Intrusion Detection vs. Prevention

How do you upgrade from intrusion detection to intrusion prevention?
How do you upgrade from intrusion detection to intrusion prevention?

s/D/P/
Intrusion Detection vs. Prevention

How do you upgrade from intrusion detection to intrusion prevention?

s/D/P/

- Prevention issues:
  - real-time operation (performance)
  - timeliness (immediate action)
  - getting access to events / OS interaction
  - decision making (thresholds etc.)
  - persuasion of human decision makers / operational issues
Components of network IDS

Detection:
- signature-based detection
- classification
- anomaly detection

Feature extraction:
- analysis of protocol headers
- byte-level sequence analysis
- content parsing

Audit:
- packet capture and de-fragmentation
- TCP stream re-assembly
Components of network IDS

- **Audit:**
  - packet capture and de-fragmentation
  - TCP stream re-assembly
Components of network IDS

- **Feature extraction:**
  - analysis of protocol headers
  - byte-level sequence analysis
  - content parsing

- **Audit:**
  - packet capture and de-fragmentation
  - TCP stream re-assembly
Components of network IDS

- Detection:
  - signature-based detection
  - classification
  - anomaly detection

- Feature extraction:
  - analysis of protocol headers
  - byte-level sequence analysis
  - content parsing

- Audit:
  - packet capture and de-fragmentation
  - TCP stream re-assembly
### IDS in the overall security architecture

<table>
<thead>
<tr>
<th>Component</th>
<th>Cost</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>🏷️ ETF</td>
<td>🕑 ETF</td>
</tr>
<tr>
<td>Firewall</td>
<td>🏷️ ETF</td>
<td>🕑 ETF</td>
</tr>
<tr>
<td>IDS / IPS</td>
<td>🏷️ ETF</td>
<td>🕑 ETF</td>
</tr>
<tr>
<td>SSL VPN Gateway</td>
<td>🏷️ ETF</td>
<td>🕑 ETF</td>
</tr>
<tr>
<td>E-Mail/Spam Filter</td>
<td>🏷️ ETF</td>
<td>🕑 ETF</td>
</tr>
<tr>
<td>GW Antivirus-Filter</td>
<td>🏷️ ETF</td>
<td>🕑 ETF</td>
</tr>
<tr>
<td>Web-Filter</td>
<td>🏷️ ETF</td>
<td>🕑 ETF</td>
</tr>
<tr>
<td>WAN Link Balancer</td>
<td>🏷️ E</td>
<td>🕑 E</td>
</tr>
<tr>
<td>Load Balancer</td>
<td>🏷️ ETF</td>
<td>🕑 ETF</td>
</tr>
<tr>
<td><strong>Total:</strong></td>
<td>🏷️ ETF</td>
<td>🕑 ETF</td>
</tr>
</tbody>
</table>
Unified threat management

- Solutions are integrated as a single appliance (possibly virtualized)
- Example: Astaro Security Gateway

Essential Firewall
- Stateful Firewall
- Network Address Translation
- PPTP/L2TP Remote Access

Optional Subscriptions:
- Network Security:
  - Intrusion Prevention
  - IPSec/SSL VPN
  - IPSec/SSL Remote Access
- Mail Security:
  - Anti Spam & Phishing
  - Dual Virus Protection
  - Email Encryption
- Web Security:
  - URL Filter
  - Antivirus & Antispyware
  - IM & P2P Control
Take-home message

- There is no “one-size-fits-all” IDS!
- IDS are only useful if their alerts are properly managed.
- IPS bring a new level of complexity.
- As usual, integrated solutions are very welcome.