A Network of IDS-Sensors for Attack-Statistics

Till Dörges
Olaf Gellert
Klaus-Peter Kossakowski
Outline / ToC

- Introduction
- Realisation
- Operation
- Statistics
- Conclusion / Perspectives
- Closing Remarks
Introduction: History

- Current project evolved from eCSIRT.net
  - Funded by European Commission
  - Improve Collaboration between European CSIRTs
  - Raise Public Awareness through Attack-Statistics
  - http://www.ecsirt.net/

- Realisation of Distributed IDS
  - Gather Information about Internet Attacks
  - Acquire “holistic” View
Introduction: Distributed IDS

■ Single IDS only have limited View
  ■ 1 Sensor
  ■ Single Host
  ■ Single Network

■ Distributed IDS get bigger Picture
  ■ n Sensors + m Managers
  ■ Technology / Software available
  ■ Problem: Deployment across administr. Domains
    ■ Different / Incompatible Policies
    ■ Trust
Outline / ToC

- Outline / ToC
- Introduction
- Realisation
- Operation
- Statistics
- Conclusion / Perspectives
- Closing Remarks
Realisation: Policy & Trust

- Each Sensors is assigned 1 IP-Address
- Other IP-Addresses must not be listened to
- Communication between Sensor and Manager
  - Encrypted
  - Authenticated
- Trust-Relation between all participating Parties
  - Common Code of Conduct
  - Strongly based on Trusted Introducer (TI)
    - http://ti.terena.nl/
Realisation: Architecture

Main Component:
Prelude (http://www.prelude-ids.org)
Realisation: Software

- Sensors
  - Primary Objective: Plug 'n Play
    - Simple Setup Menu
  - CDROM based on Knoppix (http://knoppix.org/)
    - Prelude-NIDS
    - Crypto-NTPD
    - Honeyd
  - Floppy containing Credentials

- Manager
  - Prelude-Manager
  - Crypto-NTPD
Realisation: Honeyd

- Sensors: No “Eavesdropping” due to Policy
  - Honeyd to help out (http://www.honeyd.org)

- Honeyd provides attackable Services
  - FTP TCP/21
  - SSH TCP/22
  - TELNET TCP/23
  - SMTP TCP/25
  - HTTP TCP/80
  - POP3 TCP/110

- Problem: No complete Simulation
Operation

- Smooth Operation of all Components

Current Sensor-Network

- Netherlands (2 Sensors)
- Germany (2 Sensors)
- Great Britain
- Spain (2 Sensors)
- Denmark
- Japan

More Sensors always welcome!

- No Geographic Restrictions
Outline / ToC

- Outline / ToC
- Introduction
- Realisation
- Operation
- Statistics
- Conclusion / Perspectives
- Closing Remarks
## Analyses: Prelude Webfrontend I

### Top Attacking Sites

<table>
<thead>
<tr>
<th>AttackNb</th>
<th>AttackTypeNb</th>
<th>TargetNb</th>
<th>Score</th>
<th>Address</th>
<th>Country</th>
<th>Host name</th>
</tr>
</thead>
<tbody>
<tr>
<td>15681</td>
<td>12</td>
<td>1</td>
<td>1306.75</td>
<td>213.131.73</td>
<td>EG</td>
<td>[redacted]</td>
</tr>
<tr>
<td>6671</td>
<td>17</td>
<td>2</td>
<td>222.068235294118</td>
<td>194.249.177</td>
<td>SI</td>
<td>n/a</td>
</tr>
<tr>
<td>6917</td>
<td>17</td>
<td>1</td>
<td>3989235294117847</td>
<td>213.136.117</td>
<td>CI</td>
<td>n/a</td>
</tr>
<tr>
<td>6513</td>
<td>10</td>
<td>11</td>
<td>60.1181818181818</td>
<td>127.0.0.1</td>
<td>Unk.</td>
<td>localhost</td>
</tr>
<tr>
<td>6401</td>
<td>17</td>
<td>1</td>
<td>376528411764706</td>
<td>192.204.188</td>
<td>US</td>
<td>n/a</td>
</tr>
<tr>
<td>6291</td>
<td>17</td>
<td>1</td>
<td>37995623529412</td>
<td>194.209.168</td>
<td>CH</td>
<td>n/a</td>
</tr>
<tr>
<td>6282</td>
<td>17</td>
<td>1</td>
<td>369528411764706</td>
<td>199.6.51</td>
<td>US</td>
<td>n/a</td>
</tr>
<tr>
<td>6160</td>
<td>20</td>
<td>2</td>
<td>154</td>
<td>219.106.1000</td>
<td>JP</td>
<td>[redacted]</td>
</tr>
<tr>
<td>5597</td>
<td>12</td>
<td>1</td>
<td>49641965696969</td>
<td>212.0.138</td>
<td>SD</td>
<td>n/a</td>
</tr>
<tr>
<td>5137</td>
<td>15</td>
<td>3</td>
<td>11415555555555555</td>
<td>80.108.86</td>
<td>SE</td>
<td>[redacted]</td>
</tr>
<tr>
<td>4684</td>
<td>5</td>
<td>3</td>
<td>32629606560667</td>
<td>210.212.89</td>
<td>IN</td>
<td>n/a</td>
</tr>
<tr>
<td>4392</td>
<td>14</td>
<td>1</td>
<td>311571428571428</td>
<td>30.142.231</td>
<td>DE</td>
<td>[redacted]</td>
</tr>
<tr>
<td>3574</td>
<td>5</td>
<td>2</td>
<td>3674</td>
<td>62.117.102</td>
<td>RU</td>
<td>n/a</td>
</tr>
<tr>
<td>3344</td>
<td>10</td>
<td>1</td>
<td>334.6</td>
<td>8237.219</td>
<td>GB</td>
<td>[redacted]</td>
</tr>
<tr>
<td>3143</td>
<td>17</td>
<td>1</td>
<td>185235294117647</td>
<td>211.38.233</td>
<td>KR</td>
<td>n/a</td>
</tr>
<tr>
<td>2884</td>
<td>8</td>
<td>4</td>
<td>33.25</td>
<td>81189.240</td>
<td>CN</td>
<td>n/a</td>
</tr>
<tr>
<td>2832</td>
<td>12</td>
<td>1</td>
<td>211</td>
<td>217.235.191</td>
<td>DE</td>
<td>[redacted]</td>
</tr>
<tr>
<td>2486</td>
<td>11</td>
<td>1</td>
<td>226</td>
<td>80.142.231</td>
<td>DE</td>
<td>[redacted]</td>
</tr>
<tr>
<td>2477</td>
<td>12</td>
<td>1</td>
<td>205.6185656565656565</td>
<td>80.142.233</td>
<td>DE</td>
<td>[redacted]</td>
</tr>
<tr>
<td>2460</td>
<td>12</td>
<td>1</td>
<td>205</td>
<td>217.235.181</td>
<td>DE</td>
<td>[redacted]</td>
</tr>
</tbody>
</table>
Analyses: Prelude Webfrontend II

- Top Attacks (May 21, 2004)
  - Most Attacks Target WWW-Services
Analyses: Overviews

- Overviews generated
  - Daily
  - Monthly
  - Complete

- Grouped into these Classes
  - IIS Access (cmd.exe & root.exe)
  - HTTP Request String Alerts
  - Other IIS Attacks
  - Other WEB Attacks
  - ICMP Scans
  - All Others
Analyses: Overviews: Example I

- Monthly Overview, Alerts per Day

![Graph showing monthly alerts per day from 2004-01 to 2004-03. The graph indicates different types of alerts such as All other Alerts, ICMP SCANS, Other WEB Attacks, HTTP request string Alerts, Other IIS Attacks, and IIS cmd.exe & root.exe Access.]
Analyses: Overviews: Example II

Daily Overview, Alerts per Hour

![Graph showing alerts per hour from 02:00 to 22:00 on April 19, 2004. The graph distinguishes between different types of alerts such as All other Alerts, ICMP SCAMS, Other WEB Attacks, and other IIS Attacks.](image-url)
Analyses: Overviews: Example III

■ Complete Overview, Alerts per Day

Alerts per Day 2003-09-01 to 2004-05-20
Analyses: Argus vs. Prelude I

- Problem: Prelude only sees, what it knows
  - Prelude-NIDS is a Signature-Based IDS
  - Most Attacks Require Answers from Victim
- Argus for Different Perspective
  - http://www.qosient.com/argus/
  - Records Connections / Statistics
- Comparison for PRESECURE-Sensor
  - Prelude: “Alert” (Match against Rule)
  - Argus: “Connection” (SYN-Packet)
## Access by Ports for PRESECURE-Sensor

<table>
<thead>
<tr>
<th>Port</th>
<th>Argus (PS)</th>
<th>Prelude (PS)</th>
<th>Prelude (Total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/tcp (h)</td>
<td>10091</td>
<td>1333</td>
<td>8073</td>
</tr>
<tr>
<td>22/tcp (h)</td>
<td>182</td>
<td>20</td>
<td>55</td>
</tr>
<tr>
<td>23/tcp (h)</td>
<td>137</td>
<td>1</td>
<td>17</td>
</tr>
<tr>
<td>25/tcp (h)</td>
<td>400</td>
<td>1</td>
<td>52</td>
</tr>
<tr>
<td>80/tcp (h)</td>
<td>23407</td>
<td>45131</td>
<td>887597</td>
</tr>
<tr>
<td>110/tcp(h)</td>
<td>47</td>
<td>0</td>
<td>14</td>
</tr>
<tr>
<td>135/tcp</td>
<td>47883</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>137/udp</td>
<td>4065</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>139/tcp</td>
<td>2302</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>445/tcp</td>
<td>5704</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>1080/tcp</td>
<td>600</td>
<td>1022</td>
<td>3416</td>
</tr>
<tr>
<td>1434/udp</td>
<td>2015</td>
<td>1983</td>
<td>8939</td>
</tr>
<tr>
<td>Not Incl.</td>
<td>16879</td>
<td>1488</td>
<td>22997</td>
</tr>
<tr>
<td>Total</td>
<td>113712</td>
<td>50979</td>
<td>931172</td>
</tr>
</tbody>
</table>
### Analyses: Different Attacks

- **Attackers try more than 1 Attack**

<table>
<thead>
<tr>
<th># Attacks</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>...</th>
<th>143</th>
<th>159</th>
<th>235</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003-09</td>
<td>13381</td>
<td>2393</td>
<td>1260</td>
<td>107</td>
<td>656</td>
<td>26</td>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2003-10</td>
<td>13547</td>
<td>3311</td>
<td>210</td>
<td>165</td>
<td>581</td>
<td>94</td>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2003-11</td>
<td>14027</td>
<td>3508</td>
<td>50</td>
<td>46</td>
<td>561</td>
<td>42</td>
<td>...</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2003-12</td>
<td>16472</td>
<td>6234</td>
<td>38</td>
<td>32</td>
<td>573</td>
<td>50</td>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2004-01</td>
<td>3595</td>
<td>1239</td>
<td>1363</td>
<td>60</td>
<td>502</td>
<td>51</td>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2004-02</td>
<td>3399</td>
<td>689</td>
<td>1381</td>
<td>56</td>
<td>465</td>
<td>41</td>
<td>...</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2004-03</td>
<td>5831</td>
<td>474</td>
<td>1080</td>
<td>59</td>
<td>464</td>
<td>42</td>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2004-04</td>
<td>8475</td>
<td>625</td>
<td>871</td>
<td>40</td>
<td>383</td>
<td>38</td>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>78727</strong></td>
<td><strong>18473</strong></td>
<td><strong>6253</strong></td>
<td><strong>565</strong></td>
<td><strong>4185</strong></td>
<td><strong>384</strong></td>
<td>...</td>
<td><strong>1</strong></td>
<td><strong>1</strong></td>
<td><strong>1</strong></td>
</tr>
</tbody>
</table>
### Analyses: Different Sensors Attacked

- Attackers attack different Sensors

<table>
<thead>
<tr>
<th># Sensors</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003-09</td>
<td>17543</td>
<td>267</td>
<td>32</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2003-10</td>
<td>17426</td>
<td>360</td>
<td>109</td>
<td>48</td>
<td>42</td>
<td>1</td>
</tr>
<tr>
<td>2003-11</td>
<td>17995</td>
<td>211</td>
<td>37</td>
<td>9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2003-12</td>
<td>23192</td>
<td>175</td>
<td>33</td>
<td>20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2004-01</td>
<td>6459</td>
<td>319</td>
<td>34</td>
<td>12</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>2004-02</td>
<td>5705</td>
<td>305</td>
<td>22</td>
<td>20</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>2004-03</td>
<td>7629</td>
<td>280</td>
<td>31</td>
<td>18</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>2004-04</td>
<td>10074</td>
<td>312</td>
<td>38</td>
<td>12</td>
<td>6</td>
<td>13</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>106023</strong></td>
<td><strong>2229</strong></td>
<td><strong>336</strong></td>
<td><strong>145</strong></td>
<td><strong>80</strong></td>
<td><strong>14</strong></td>
</tr>
</tbody>
</table>
Analyses: Mean Time Between Attack(er)s

- ~ 14000 Attackers per Month (Sep 03 – Mar 04)
- ~ 2000 Attackers per Month per Sensor
- ~ 3 Attackers per Hour per Sensor
- Average System Connected to Internet
  - ~ 20 Minutes between Attackers
- Only very Cautious Estimation
  - Attackers try ~ 1.5 Different Attacks
  - Prelude doesn't see all Attacks
Conclusion / Perspectives

- Successful Operation for over 10 Months
- Interesting Data Gathered
- Analyses (somewhat) limited
- Number of Sensors still increasing
- Active Development of Sensor-Technology
  - Automatic Updates of Signatures
  - Argus to be Included
- Participants Welcome
Contacting the Authors

■ Till Dörges
  ■ td@pre-secure.de      PGP-Key: 0x22A13E69
  ■ 2226 8447 3251 F6BE F8DC 6D4D 2F54 E55F

■ Olaf Gellert
  ■ og@pre-secure.de      PGP-Key: 0x799241C1
  ■ 6C6D E613 BEE4 1D6D B14B D266 2383 A735

■ Klaus-Peter Kossakowski
  ■ kpk@pre-secure.de      PGP-Key: 0x38B56E3D
  ■ 5B21 A75D 0820 1A93 835C 6EE3 4D1B F050
The End (of the Beginning...)

More Participants / Sensors are Welcome!

Thank You for Your Attention!

Questions?