Vulnerability Assessment Using Attack Graphs (and securiCAD®) - A SEGRID Use Case Study

Alexandre Vernotte & Mathias Ekstedt
KTH Royal Institute of Technology
Sweden
Security management challenge

ICT infrastructure:
large, complex, heterogeneous, legacy, modern
...unknown!?

How secure/resilient is it..?
Vulnerability analysis of architectures

- How will attacks vary with vulnerabilities and defenses (and architectural design)?
  - Attack vector
  - Attack difficulty (Time To Compromise)
Attack/defense graphs – a simple example

Break in through window

Access to door

Bypass fence

Bypass door

Use key

Pick lock

Use axe

Break into house

Break in through door

Door material

Lock quality
Attack/defense graphs – securiCAD

Compromise host

Anti malware

IDS

DEP

ASLR

IPS

Deploy exploit

Compromise service

Bypass anti malware

Bypass IDS

Find exploit

Patched

Develop zero day

Develop exploit to known vulnerability

Acquire exploit

Access control

Login

Connect

Network compromise
Architecture-generated attack/defense graphs

**Host**
- Compromise
- Anti malware
  - DEP
  - ASLR

**Network**
- Compromise

**Service**
- Compromise service
- Bypass anti malware
- Bypass IDS
- Deploy exploit
- Find exploit
- Login
- Connect

**Router**

**Access control**
- Functioning

**IDS** functioning

**IPS** functioning
securiCAD meta model – examples

**Object**
- Host
- Service
- Software product
- Dataflow
- User
- Physical zone
- ...

**Attack step**
- MiTM
- DevelopZeroDay
- Exploit SQL injection
- Exploit XSS
- Guess password offline
- DenialOfService
- ...

**Defense**
- Patch level
- DNS Security
- Static ARP tables
- ASLR
- DeveloperSecurityAware
- Hardened
- ...

---

Dataflow

<table>
<thead>
<tr>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>DenialOfService</td>
</tr>
<tr>
<td>Eavesdrop</td>
</tr>
<tr>
<td>ManInTheMiddle</td>
</tr>
<tr>
<td>Replay</td>
</tr>
<tr>
<td>Request</td>
</tr>
<tr>
<td>Respond</td>
</tr>
</tbody>
</table>

Host

ASLR
AntiMalware
DEP
Hardened
HostFirewall
Patched
StaticARPTables
Attack and defense graphs – calculations

Compromise host → ... → Anti malware

Compromise service OR Bypass anti malware

IDS → Bypass IDS

DEP → Deploy exploit

ASLR → AND

IPS

Deploy exploit

Find exploit

Access control

Patched OR Develop zero day

Develop exploit to known vulnerability OR Acquire exploit

Login

Connect

Network compromise
Deploy exploit - Attack success statistic

\[ P(\text{Deploy exploit. Time To Compromise (TTC)}) = 1 - \exp(-\lambda \times \text{TTC}) \]

<table>
<thead>
<tr>
<th>AC</th>
<th>DEP</th>
<th>ASLR</th>
<th>IPS</th>
<th>Lambda</th>
<th>TTC Median (days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.248</td>
<td>2.8</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0.210</td>
<td>3.3</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0.156</td>
<td>4.4</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0.128</td>
<td>5.4</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0.140</td>
<td>5.0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0.118</td>
<td>5.9</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0.131</td>
<td>5.3</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0.106</td>
<td>6.5</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.112</td>
<td>6.2</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0.077</td>
<td>9.0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0.080</td>
<td>8.7</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0.055</td>
<td>12.6</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0.067</td>
<td>10.3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0.045</td>
<td>15.4</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0.055</td>
<td>12.6</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0.033</td>
<td>21.0</td>
</tr>
</tbody>
</table>
Sources - statistics

› **Logical necessities**, e.g. if the firewall allow you to connect to A from B and you have access to B, then you can connect to A.

› **Scientific studies**
  › Research from KTH.
  › Other’s research studies.
Demo time
High-level logical view of UC2:S2 architecture
Physical view of UC2:S2 architecture
## Data flows of UC2:S2 architecture (approx. 50)

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>From</th>
<th>To</th>
<th>Initiator</th>
<th>Protocols</th>
<th>Auth</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Remote substation login</td>
<td>Office Station</td>
<td>Substation workstation</td>
<td>DSO Office Station, Engineering zone</td>
<td>CITRIX format for remote desktop or RDP</td>
<td>yes</td>
</tr>
<tr>
<td>6</td>
<td>Process data (bidirectional)</td>
<td>Primary RTU</td>
<td>SCADA Front End</td>
<td>SCADA Front End</td>
<td>IEC 60870-5-101/104 DNP 3.0, Modbus, Proprietary protocols</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>SCADA Software updates</td>
<td>Vendor Server</td>
<td>File transfer server (DMZ)</td>
<td>File transfer server (DMZ)</td>
<td>Protocol unknown, over Internet</td>
<td>yes</td>
</tr>
<tr>
<td>34</td>
<td>Load Forecast Data</td>
<td>TSO</td>
<td>File Transfer server, DMZ</td>
<td>TSO</td>
<td>FTP format over Internet</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>Remote Login: Process Data (commands)</td>
<td>Office Station</td>
<td>SCADA HMI</td>
<td>Office Station</td>
<td>Internal format</td>
<td></td>
</tr>
</tbody>
</table>
## Additional parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>IT</th>
<th>OT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ASLR</td>
<td>On</td>
<td>On</td>
</tr>
<tr>
<td>Anti malware</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>DEP</td>
<td>On</td>
<td>On</td>
</tr>
<tr>
<td>Hardened</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>Host firewall</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>Patched</td>
<td>75%</td>
<td>25%</td>
</tr>
<tr>
<td>Static ARP tables</td>
<td>On</td>
<td>On</td>
</tr>
<tr>
<td><strong>Access control</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Back-off</td>
<td>50%</td>
<td>Off</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

› **Attacker location → Internet**
First assessment

› From the SEGRID risk assessment – sensitive components:
  › SCADA master
  › substation RTUs (primary, secondary, DER)

→ We choose these as evaluation points.
What happened?

- Inspect critical attack vector
What can be done?

- State-of-the-art propose the use of a SCADA DMZ
Are we securer?

▷ What happened this time?
## Results from some simulations

<table>
<thead>
<tr>
<th></th>
<th>RTU - prim</th>
<th>RTU - 2nd</th>
<th>RTU - DER</th>
<th>SCADA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No HMI browsing</strong> (Base case)</td>
<td>22 days</td>
<td>22 days</td>
<td>23 days</td>
<td>20 days</td>
</tr>
<tr>
<td>HMI browsing allowed</td>
<td>12 days</td>
<td>12 days</td>
<td>14 days</td>
<td>12 days</td>
</tr>
<tr>
<td>No HMI browsing, good (/reasonable) patching</td>
<td>54 days</td>
<td>54 days</td>
<td>55 days</td>
<td>49 days</td>
</tr>
<tr>
<td><strong>HMI replica placed in DMZ</strong> (shown improvement)</td>
<td>71 days</td>
<td>71 days</td>
<td>74 days</td>
<td>66 days</td>
</tr>
<tr>
<td>HMI replica placed in DMZ, good (/reasonable) patching</td>
<td>155 days</td>
<td>155 days</td>
<td>155 days</td>
<td>119 days</td>
</tr>
<tr>
<td>Add a diode from SCADA zone to DMZ</td>
<td>200 days (18%)</td>
<td>200 days (18%)</td>
<td>200 days (18%)</td>
<td>200 days (18%)</td>
</tr>
</tbody>
</table>
Other threat scenarios

› Can an attacker compromise the SCADA master from the smart meter?
  • Yes.

› ...

...
Conclusion & Wrap-up
No silver bullet security solution…

- Security depends on a large number of details…
  - Details that differ with SCADA system installation
- What assets are you interested in?
- What attacks are you interested in?
- Reference model helps to get started with a specific analysis

General observations
- The best protection is close to the internet and other attacker entry points.
- There are no isolated, completely secure segments
- Forcing the attacker to deploy zero days is a generally reasonable strategy.
How do I get to know my infrastructure?

- Manual modeling is extremely costly (sometimes necessary though)
- Automatic import of “ICT infrastructure raw data”
  - Nmap
  - Vulnerability scanners
  - Firewall rule config files
  - …

- Overlapping and seldomly 100% accurate
  - Poster on automatic modeling of inconsistent data
Thank you for listening!

- (More) questions?