The Cyber Security Modeling Language and Cyber Security research at department for Industrial Information and Control Systems

Mathias Ekstedt, Associate Prof.

KTH Royal Institute of Technology, Stockholm
Agenda

Dept. for Industrial Information and Control Systems, KTH

Cyber Security Modeling Language (CySeMoL)

Areas for collaboration / exchange
Industrial Information and Control Systems

Research

- Focus is on developing theories, methods and prototypes in order to contribute to the development of cost-effective and resilient industrial IT-systems
- In particular for electric power utilities - the department has ever since its start in 1989 had a close cooperation with the power industry.
- Research groups
  - Power System Management with related Information Exchange
  - Information and Control Systems Architecture
  - Cyber Security
  - Technology Management

Size

- approximately 30 people out of which 5 faculty
Cyber Security @ Industrial Information and Control Systems

Research areas
- Security analysis of enterprise-level information systems architectures (user/customer-side system architectures)
- In particular for power utilities (i.e. SCADA and substation automation systems, and smart grid architectures)
- Information Security Management (security governance and organization)

Methodological approach
- Information systems architecture modelling
- Attack/defense graphs
- Probabilistic analyses

People
- 3 faculty, 3 PhD students (1 industry), 1 post doc (upstarting) +1, 1 programmer

Projects/financing
- EU FP7: VIKING – finished (security of "traditional" SCADA)
- EU FP7: SEGRID (smart power grid cyber security)
- EU ERA-NET: SALVAGE (smart low-voltage power grid cyber security)
- Swedish Centre for Smart Grids and Energy Storage
- Swedish National Grid/ Swedish Defence Research Agency
- European Institute of Innovation and Technology / InnoEnergy (commercialization)
Agenda

Dept. for Industrial Information and Control Systems, KTH

Cyber Security Modeling Language (CySeMoL)

Areas for collaboration / exchange
Cyber security management is difficult!

Is my control system secure enough?

Interconnected
Complex architecture and data flow
Many vendors (incl. off-the-shelf components)

Which parameters decides cyber security?
Any vulnerabilities? And where are they?

And how do vulnerabilities relate?
In practice, cyber security management and design has limited resources

Should I spend my budget on: a training program for my staff, logging functionality, or network scanning?
Cyber Security Modeling Language (CySeMoL) in summary

An “IT Auto-CAD Tool”
- User draws maps of IT architecture components/assets and their connections (current or future).
- Tool provides a “heat map” of how secure or vulnerable different parts of an IT architecture are towards cyber attacks
- The tool simulates hacker attacks and assesses risks in architecture components/assets through combining user input on system properties with built-in security expertise.
CySeMoL screen shot – attack success

Green – low probability
Yellow – medium probability
Red – high probability
CySeMoL screen shot – attack success in detail
(same system model but each attack step visualized individually)
The underlying magic: Attack / defense graphs

Access as root to operating system

Anti-malware

Network intrusion detection system

Execute arbitrary code

Exploit

Establish connection

Vulnerability exist
Bayesian networks

<table>
<thead>
<tr>
<th></th>
<th>T</th>
<th>T</th>
<th>T</th>
<th>T</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exploit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti-malware</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>Network intrusion detection</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>Execute code (TRUE)</td>
<td>0.21</td>
<td>0.32</td>
<td>0.41</td>
<td>0.7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

- **Exploit**
- **Anti-malware**
- **Network intrusion detection system**
- **Execute arbitrary code**
- **Establish connection**
- **Vulnerability exist**
Bayesian networks

<table>
<thead>
<tr>
<th></th>
<th>Exploit</th>
<th>Anti-malware</th>
<th>Network intrusion detection</th>
<th>Execute code (TRUE)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>0.21</td>
</tr>
<tr>
<td></td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>0.32</td>
</tr>
<tr>
<td></td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>0.41</td>
</tr>
<tr>
<td></td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>0.7</td>
</tr>
<tr>
<td></td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>0</td>
</tr>
</tbody>
</table>

Anti-malware

Network intrusion detection system

Execute arbitrary code

Exploit

Establish connection

Vulnerability exist
Attacks and defenses – relation to assets

Network Interface

Network zone

Network intrusion detection system

Operating System

Access as root

Execute arbitrary code

Exploit

Vulnerability exist

Establish connection

Anti-malware

Application Service
Studies/topics covered by CySeMoL

Attacks/malicious activities:
• Zero-day discovery
• Memory corruption exploitation
• Web application exploitation (XSS, RFI, SQLi, Command injection)
• Social engineering
• Code injection using removable media
• Password guessing (online/offline)
• Denial of service
• Man-in-the-middle
• Discovery of unknown entry-points
• …
Includes 59 attack steps
Studies/topics covered by CySeMoL

Defenses
- Network intrusion detection systems
  - Both detection and prevention-based
- Host intrusion detection systems
- Web application firewalls
- Anti-malware
- Firewalls
- Security training
- Encryption
- Software development best practice methods
- Network management (e.g., scanning, USB policy, etc)
- ...

Includes 58 defense types
Studies/topics covered by CySeMoL

Assets

- IT services
- Software components
- Operating systems
- Communication networks
- Users
- User accounts
- Data flow
- Protocols
- ...

23 asset types, 51 system relations types
Agenda

Dept. for Industrial Information and Control Systems, KTH

Cyber Security Modeling Language (CySeMoL)

Areas for collaboration / exchange
Areas for collaboration / exchange

Attack graphs, attack graphs, attack graphs…

- Refine attacks
- Expand attacks in “novel” areas
- Specialize for smart grids

- Automatic modeling / data collection
- Automatic design

In an academic setting or in a start-up company
Thank you for listening

Contact me!
mathias.ekstedt@ics.kth.se

More info
www.ics.kth.se/cysemol