Cyber-physical Security
Protecting IT, OT and IoT

Itai Jaeger
Cyber Security Strategy Lead
IBM Research – Haifa
itaij@il.ibm.com
il.linkedin.com/pub/itai-jaeger/1/67a/926/
IBM Research: The World is Our Lab

Cognitive Analytics of Big Data
HW and SW Quality, Cyber Security
Cloud transformation; cloud storage
Mobile First

IBM Research labs
Labs added since 2010
IBM R&D labs in Israel

• Haifa Research Lab
  • Established in 1972
  • Largest IBM Research facility outside the US
  • Spanning all IBM Research strategy areas
  • Working with IBM business units and IBM clients worldwide
  • Collaborating with academia and industry
  • About 100 patents / year

• Israel Development Labs
Cyber security research @ IBM Research - Haifa

IBM Security Systems Portfolio

Security Intelligence and Analytics

<table>
<thead>
<tr>
<th>People</th>
<th>Data</th>
<th>Applications</th>
<th>Network</th>
<th>Infrastructure</th>
<th>Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>QRadar SIEM</td>
<td>QRadar Log Manager</td>
<td>QRadar Risk Manager</td>
<td>QRadar Vulnerability Manager</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trusteer Rapport</td>
<td>Trusteer Pinpoint Malware Detection</td>
<td>Trusteer Pinpoint ATO Detection</td>
<td>Trusteer Mobile Risk Engine</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **SIEM analytics**
- **Cyber-physical security**
- **Insider threat detection**
- **Secure design & test**
- **Mobile DLP**
- **Cloud storage security**
- **Data masking & anonymization**
- **Data fabrication**
- **Malware analysis automation**
- **Biometric authentication**

IBM X-Force Research
Cyber-physical systems (CPS): IT, OT .... and IoT
IoT goes to work…

- **IoT** is a network of devices where all the devices:
  - Have local intelligence
  - Have a shared API so they can speak with each other in a useful way
  - Push and pull status and command information from the networked world

- **HIoT** – Human IoT (or consumer IoT)
  - Revolving around and interacting with the human being

- **IIoT** - Industrial IoT (or enterprise IoT)
  - Must be Autonomous, reliable and… **secure**
  - Facilitate peer-to-peer device communication - without human intervention
  - Rely on and integrate many existing networks and communication protocols
CPS as an emerging security challenge

"We are seeing more cyber attacks focused on sabotage than espionage. These attacks are often aimed at causing physical damage, disruption, and safety issues — rather than accessing information. And they’re raising new concerns about shifts across the threat landscape."

IBM Security Services Cyber Security Intelligence Index, June 2013
A New Era of Smart

The CPS threat landscape

Attacks via the IT infrastructure
- Easy access – known vectors
- Increased risk compared to IT only attacks

- Device / identity takeover attacks
  - Extremely high risk
  - Hard to detect

- Offenses via the OT / IoT infrastructure and network
  - Emerging vectors – many times very simple to implement

- Risk is extremely high compared to regular IT attacks
  - Potential prolonged shutdown (weeks/months)
  - Human Life / health / safety
  - Disruption to society / region / nation
What makes OT cyber security unique?

- **Distributed systems**
  - Spread, connecting unmanned facilities
  - A hierarchy of control centers
    - With intricate Interdependencies

- **Protocol complexity**
  - Diversity in protocols and device types
    - Intermixed on the same domain
  - Multiple vendors
    - Using different proprietary protocols

- **Protocol obscurity**
  - Sensor reading and control commands are obscured
    - Same command may have different meanings based on context
  - IoT may present an opportunity here

- **Credentials and permissions**
  - OT systems assume users are trustworthy and meticulous

- **Old protocols and software**
  - Well known vulnerabilities
    - patches are rarely applied
  - Lateral movement of malware is greatly simplified

- **Intolerance of the physical domain**
  - Faults can have immediate consequences
    - With no easy remediation
  - Must not interfere with real-time actions
    - Prevention and healing is difficult
CPS security requires deep insight solutions

- Learning the unique characteristics of the CPS system
  - SCADA/DCS infrastructure
  - Control room network
  - Different components making up the system

- Adapting to the specifics of each system
  - Every SCADA/DCS has many unique features
  - Universal security mechanisms for the generic parts offer limited gain

- Understanding the problem domain
  - Model semantics of control commands and sensor signals
  - Adapt the security information extracted per industry / device type / vendor
  - Map signals and commands to the physical world

- IT vendors offer their existing cyber security products
  - A significant gap – no dedicated OT modeling

- OT vendors shifting towards addressing cyber security concerns
  - Some of the current solutions are basic / naive
Sample CPS security research directions @ IBM Research

- Smart monitoring of CPS and IoT
  - Design an OT/IoT network monitor
  - Build a reliable and secure reporting mechanism for things
  - Extend IBM’s SIEM platform to monitor OT and IoT events

- Applying analytics to monitored events
  - Look for anomalies in the OT historian
  - Analyze OPC metadata
  - Modbus data analysis

- CPS security intelligence and risk management
  - Discover vulnerabilities
  - Detect ongoing attacks
  - Protect & heal compromised systems
Open source intelligence, Current and future security threats, SCADA intrusion detection

- IBM Research invites you to a full-day seminar on the topics above and much, much more

- Please register
  - Monday, 1/12/2014 at the IBM Research – Haifa
  - Free of charge, registration required