Security Protection
Mechanisms for the Grid

Ken Modeste
Principal Engineer, Security and Global Communications
Underwriters Laboratories Inc.
Ken.modeste@ul.com

Yesterday
• 1894: UL founded by William Henry Merrill following 1893 Chicago World’s Fair
  Funded and sponsored by the National Board of Fire Underwriters
• 1897: First published list of approved electrical devices
• 1901: Takes name of Underwriters’ Laboratories, Inc.
• 1903: First UL standard published
• 1916: First international office opened in London
• 1958: Fire protection lab built
• 1980: UL/CCIC agreement for inspections
• 1988: Hong Kong and Taiwan offices open, followed by many international offices

Today
Underwriters Laboratories’ history: 1894 William Henry Merrill, an electrical engineer hired to examine the electrical safety of the Columbian Exposition’s Palace of Electricity at the 1893 World’s Fair in Chicago, founds Underwriters Laboratories as an independent testing agency. Its mission: to render expert opinions concerning fire hazards and certify electrical devices.

• Leading safety brand
  • 20 billion UL Marks on products annually
  • 100,000 products tested annually
• Worldwide presence
  • 57,000 customers in 100 countries
  • 64 labs and certification facilities across the world
Safe Living and Working Environments

Lead the world in creating safe living and working environments that meet the evolving needs of people.

- Safe buildings
- Safe workplaces
- Safe products
- Safe food, water & health
- Safe, clean energy

Be the best and achieve meaningful size in all that we do

North American UL/ULC Standardization

- UL Standards (USA) & ULC Standards (Canada) working in collaboration for standardization in new & emerging technologies (e.g. smart grids & cyber security) for Canada and USA.
- Standardization efforts may be for Canada only, USA only, or Canada/USA, as needs justify.
- Developing a strategy to pursue standardization meeting stakeholder needs in both USA and Canada.
- Service offerings is evolving: UL/ULC to be driver in SG & CS markets.
Utilities & Energy industry have second highest cost of cyber crime

Average annualized cost by industry sector

<table>
<thead>
<tr>
<th>Industry</th>
<th>FY 2010</th>
<th>FY 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defense</td>
<td>$16.31</td>
<td>$19.90</td>
</tr>
<tr>
<td>Utilities &amp; Energy</td>
<td>$15.63</td>
<td>$19.78</td>
</tr>
<tr>
<td>Financial services</td>
<td>$12.37</td>
<td>$14.70</td>
</tr>
<tr>
<td>Technology</td>
<td>$6.24</td>
<td>$6.29</td>
</tr>
<tr>
<td>Communications</td>
<td>$2.06</td>
<td>$0.09</td>
</tr>
<tr>
<td>Services</td>
<td>$2.58</td>
<td>$1.86</td>
</tr>
<tr>
<td>Healthcare</td>
<td>$1.86</td>
<td>$0.96</td>
</tr>
<tr>
<td>Public sector</td>
<td>$1.24</td>
<td>$0.60</td>
</tr>
<tr>
<td>Transportation</td>
<td>$2.58</td>
<td>$0.75</td>
</tr>
<tr>
<td>Industrial</td>
<td>$4.62</td>
<td>$1.82</td>
</tr>
<tr>
<td>Consumer products</td>
<td>$2.06</td>
<td>$1.80</td>
</tr>
<tr>
<td>Hospitality</td>
<td>$3.31</td>
<td>$3.77</td>
</tr>
<tr>
<td>Retail</td>
<td>$3.77</td>
<td>$4.36</td>
</tr>
</tbody>
</table>

*Industry was not represented in the FY2010 benchmark sample.

Source: Ponemon Institute; Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies; August 2011.

Smart Grid Architectural View

Central System

- IEC 62351
- EtherCAT
- LTE
- W-CDMA
- CIM

Data Concentrator

- IEC 62351
- EtherCAT
- LTE
- W-CDMA
- CIM

Substations (Wind Farm or Solar Power Plant)

- IEC 62351
- EtherCAT
- LTE
- W-CDMA
- CIM

Smart Home

- Zigbee Alliance
- Zigbee Smart Energy 2.0
- Home Plug Powerline alliance
- Wi-Fi
- Climate Talk
- L2LAP
- IEEE 1905

End customer devices

- CHAdeMO
- SAE J1772
- SAJ2954
- M/468

Multi-Utility Meter

- DLMS/COSEM (IEC62056)
- UCA-559 (Open AMI)

Meter & Gateway

- DLMS/COSEM (IEC62056)
- UCA-559 (Open AMI)

Handheld terminal

- IEC 62351
- EtherCAT
- LTE
- W-CDMA
- CIM

Grid Control Centre (Billing, DMS, GIS)
Vulnerabilities in COTS products

- Known vulnerabilities that exist with the current technologies.
  - Known vulnerabilities should be patched as best as possible.
  - Different lifecycle for IT compared to control systems on patching should be identified and defined.
  - Fixes for known vulnerabilities should be tested extensively.
  - Awareness of new vulnerabilities.
Vulnerabilities in COTS products

- Test for unknown vulnerabilities
  - Fuzz testing
  - Vulnerability tree of knowledge
  - Denial of Service attacks

- Product Development Cycle Reviews
  - IEC 62443, ISA 99 are good tools that can be used to identify security flaws in a vendor’s development process

Implementation vulnerabilities in use of products

- Secure workstations, servers with known IT practices and policies
  - Whitelisting and blacklisting
  - Password and access control
  - Auditing trails with alerts
  - Antivirus, malware detection and prevention (digital ants)
  - Disable or uninstall unused applications
  - File Sharing
  - Remote Access
Implementation vulnerabilities in use of products

- Security assessments of facilities and infrastructure
  - Network penetration testing
  - Review of audit logs, security policies
  - Independent vulnerability and cyber-security assessments
    - Physically and/or logically disable access ports
    - Access control management
    - Intrusion detection and prevention reviews

Secure Communications

- Communications need to be reliable and secure.
  - Cryptography and key management
  - Low bandwidth is a challenge
  - Test and implement against known standards – FIPS 140
  - Firmware upgrades must be secure
  - IPads and tablets are commonplace (VPN connectivity)

- Implementation of IEC 62351. Used in:
  - IEC 60870-5,6; IEC 61850; IEC 61970 and IEC 61968
  - Digital signatures, intrusion detection
Infrastructure Attacks

- Physical Access to Outdoor Field Equipment/Meters
  - RFID tags for access.
  - Digital Video Monitoring, event reporting and recording.
  - Perimeter/fence sensor detection and reporting.
  - Tamper detection of equipment
  - Strong authentication for non-secure facilities (poletop)

Infrastructure Attacks

- Network Access Control
  - Firewalls
  - Intrusion Prevention and Detection Systems
  - Network Demilitarized zones (multiple functional security zones)

- Remote Access Permission
  - IPSEC VPN, SSL VPN, PPTP VPN
  - Security equipment should be using multi-factor authentication
    - Biometrics
    - Time-dependent passwords
Infrastructure Attacks

1. Access Control
2. Secure Perimeter
3. Security Classification
4. Security Zones
5. Intrusion Detection
6. Malware Prevention
7. Training

Availability and Integrity

- Security in products and services must be available and resilient before purchase and installation
- Standardize on policies and procedures
- Continuous Assess and Reassess
- System must be secure and resilient
- Uptime is #1
THANK YOU.