Security of IoT Devices

June 2016

Dirk Jan van den Heuvel
The world is growing more connected

In 2016, 12.5 million new “things” will get connected every day

10.4 billion connected things will be in use in 2016, and will reach 20-50 billion in 2020

Source: Gartner, other market reports
Connected Technologies Growth Trends

Global IoT/IIoE device forecasts

<table>
<thead>
<tr>
<th>Source</th>
<th>Date</th>
<th>CA GR%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco</td>
<td>2013</td>
<td>23%</td>
</tr>
<tr>
<td>Ericsson</td>
<td>2010</td>
<td>-</td>
</tr>
<tr>
<td>Gartner</td>
<td>2013</td>
<td>23%</td>
</tr>
<tr>
<td>IDC</td>
<td>2014</td>
<td>17%</td>
</tr>
<tr>
<td>Harbor Research</td>
<td>2014</td>
<td>29%</td>
</tr>
<tr>
<td>ABI Research</td>
<td>2014</td>
<td>21%</td>
</tr>
<tr>
<td>IoT-Analytics.com</td>
<td>2014</td>
<td>14%</td>
</tr>
</tbody>
</table>

Note: Some forecasts only for specific years, in that case all other years in between are extrapolated based on the corresponding growth rate. Ericsson does not specify today's number of connected devices – therefore: Average of all other studies assumed as starting point in 2014

1. CAGR = Compound annual growth rate
2. Connected devices includes all autonomous connected things (every forecaster has own definition) - does NOT include computers, mobile devices, tablets

Sources: Cisco, Ericsson, ABI Research, Gartner, IHS, IDC, Harbor Research, IoT-Analytics.com

Source: Gartner, IDC, IoT Analytics
“Things” that formerly were not connected...

Internet of Things

Internet of Everything
Web of Things
Machine to Machine (M2M)
Ubiquitous Computing

“A development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data.”
Life and Health Sciences IoT Example

Source: TI Medical
Connected industries

- Smart grid
- V2X technology
- Smart factories
- Smart logistics
- Supply chain optimization
- Smart appliances
- Home automation
- Fitness
- Smart electronics
- Smart meter
- Smart lighting
- Building automation
- Patient monitoring

Source: Goldman Sachs
UL’s experience in connected technologies

Connected Technologies Customers

Connected Technologies Experience

Cyber Security
20+ Years

>400 Skilled Security Engineers

Interoperability Testing
20+ Years

>100 Skilled Interoperability Engineers

Traditional Regulatory Experience

120+ Years

Global Market Access

Developed Thousands of Standards

Trusted Relationships: Consumers, Retailers, Government

>8,000 Skilled Engineers
How large is the IoT cyber threat?

70% of IoT devices vulnerable to attack

28% to 47% of organizations have experienced IoT-related breaches

By 2018, 66% of networks will have experienced an IoT security breach

Source: HP, Forrester/Cisco, IDC Research, MarketsandMarkets, CAGR 2015-20
A growing number of IoT-related breaches

Target hack started in HVAC system

FDA warns of cyber security flaws in Hospira infusion pump

Samsung faced queries on handling of Smart TV data

U.S. government thinks China could take down the power grid

Demonstrations of hacking auto software affects Jeep

300,000 American homes open to SimpliSafe hacks

Massive physical damage at a German steel mill
Case study: automotive attack surfaces

- Mobile Network
  - Communication Jamming
  - Packet Sniffing
  - False Data Injection
  - Spoofing
  - MITM Attack
  - (D)DOS

- WiFi
  - Input injection
  - Compromised Privacy
  - Web-Based Attacks
    - (Malware, Input Injections)
    - Pairing Attack

- Back-End
  - (D)DOS
  - Malware Infection

- Call Centers
  - Social Engineering

- CAN-Bus
  - Command Infection
  - Malware Infection
  - False Data Injection
  - Fuzzing
  - Supply Chain Attack
  - Reply Attack
  - DOS Attack
  - Spoofing
  - MITM Attack

- GPS
  - ADAS
  - DSRC/V2X
  - Reply Attack
  - Relay Attack
  - Malware
  - Spoofing
  - DOS

- OBD-II Port
  - Command Infection
  - Malware Infection
  - Supply Chain Attack
IoT security: a moving target

IoT security market is growing at CAGR 33+%*

* Source: MarketsandMarkets, CAGR 2015-20
Many IoT consortia & standards

- **Access Layer**
  - 3GPP
  - IEEE 802.15.4
  - Bluetooth SIG
  - Weightless SIG
  - HGI
  - BBF

- **Network Layer**
  - IETF
  - Zigbee Alliance
  - Thread Group

- **Regulatory Bodies**
  - FCC
  - HHS

- **Advocacy Groups**
  - IMC
  - IPSO

- **Global Platform**
  - ATIS
  - ETSI
  - GSMA

- **General**
  - IEEE P2413
  - ITU-T

- **Service Layer**
  - OneM2M
  - Allseen Alliance
  - OIC

- **Application Layer**
  - IETF
  - OASIS
  - W3C
  - OMA

- **Verticals**
  - IIC - Industrial
  - PCHA/Continua - Health
  - SGIP - Smart Grid
Communication in the IoT

Longer Range
- WAN
- LAN

Protocols

Shorter Range
- PAN

Cellular
* Wi-Fi
* Bluetooth
* NFC
* Zigbee
* Thread

Services

AllSeen
OIC
oneM2M

* OCF

* Allseen and OIC merge to form Open Connectivity Foundation (OCF)
UL is the first Thread lab to perform testing to ensure interoperability (and security) of Thread products.
UL is participating in the IIC testbed effort to validate security claims for industrial devices.
Security in the IoT

• In many IoT initiatives security not the first priority

• Or, security is partially addressed (authentication / key agreements)

• Current specs & guidelines are not enough

• To arrange security we need
  • More complete standards and guidelines
  • Security Evaluation processes
  • (Accredited) Certification Programs

• UL is pro-actively moving in this direction together with the IoT/– e.g. through IIC testbed efforts / Thread Lab
UL Cybersecurity Assurance Program

• CC and FIPS are insufficient for IoT / Industrial Internet

• UL developed a (generic) standard for the security of connectable devices (UL 2900). It will become an ANSI standard soon

• UL also offer the corresponding test & certification service

• Over time UL expects a variety of security standards & certification programs in the world of IoT (with a similar scope)
UL Launches CAP

“The Department of Homeland Security is collaborating with UL and other industry partners to develop a Cybersecurity Assurance Program to test and certify networked devices within the “Internet of Things,”...

WHITE HOUSE –
CYBERSECURITY NATIONAL ACTION PLAN (FEB 2016)
The technical criteria in UL 2900 are based on existing industry best practices and guidance documents as well as IEC, ISO, and other international standards work to create repeatable & reproducible test criteria for product/software security evaluations.
UL CAP Product Evaluation

- Robustness (Fuzz) Testing
- Common Vulnerability Enumeration
- Penetration Testing
- Malware Testing

Software Weaknesses
- Source Code Analysis
- Static Binary Analysis
- Common Weakness Enumeration

Vulnerabilities & Exploits

Security Controls
- Authentication
- Access Control
- Cryptography
- Data Security
- Communications
- Software Updates

Risk Evaluation
UL CAP Product Evaluation – Detail

**Vulnerabilities & Exploits**

- **Known Vulnerabilities Analysis** - All software binaries, including executables and libraries, in a product are assessed for known vulnerabilities at the time of evaluation. The vulnerabilities are identified from the NIST National Vulnerability Database (NVD).

- **Structured Penetration Testing** - A mechanism of evaluation of a product to exploit vulnerabilities and weaknesses discovered in the vulnerability assessment phase.

- **Malformed Input Testing (Fuzzing)** - A black box testing technique used to reveal software weaknesses and vulnerabilities in a product by triggering them with invalid or unexpected inputs on the external interfaces of the product. The product is evaluated for unexpected behavior based on the customer’s specifications.

**Software Weaknesses**

- **Static Code Analysis** - Static analysis of all compiled executables and libraries of the product, in order to look for known weaknesses.

- **Static Binary and Byte Code Analysis** – Analysis of all compiled or intermediate binary executables and libraries of the product.

- **Common Weakness Enumerations (CWE)** - The product shall not contain any software weakness identified from CWE/SANS Top 25 Most Dangerous Software Errors, CWE/SANS on the cusp list or OWASP Top 10 2013 web application software weaknesses.

**Security Controls**

- **Access Control** - Review of authorization testing, a process of determining if a requester is allowed to receive a service of perform an operation.

- **Cryptography** - Validates data is stored and transmitted in a form that can only be processed by its intended audience.

- **Communications** - Verifies the appropriate responses to random sets of logical information.

- **Software Update Support**
Benefits to Stakeholders

**Product Manufacturers** – Early adoption of the UL CAP provides a competitive advantage in the marketplace and can help with mitigating risk including:
- Unplanned downtime and loss of production
- Costly harm to assets
- Reputational damage
- Validation of Security Claims

**Government, NGOs, Asset Owners and Retailers** – Including UL 2900 as a procurement requirement can help:
- Provide transparency and validation
- Common set of technical criteria

**Insurance Companies** – UL CAP provides:
- Transparency to the security posture of products
- Easy to assess cyber risk
Stay informed and connected

We invest, research and collaborate to keep our and your knowledge up to date.

Download Whitepapers  Join Webinars/Seminars  Attend Training Courses  Read Case studies  View Presentations  Meet us locally

www.ul.com / ulcyber@ul.com
THANK YOU.