Towards a Certification Framework for Cybersecurity

European Parliament
ITRE Public Hearing, November 27th, 2017

Ilias Chantzos
Senior Director Government Affairs EMEA-APJ
Global Leader In Cybersecurity

What We Do
• Software
• Cloud services
• Managed services
• Appliances
• Research
• PPP

Who We Protect
• Government
• Critical Infrastructure
• Large Enterprise
• SMB
• Consumer

Who We Work With
• CERT-EU
• ENISA
• Europol EC3
• NATO NCIA
• Member States
The Internet of Things is a prime hacking target
IoT Security: Fast Moving Target + Global Challenge

Internet of Things

2 minutes: time it takes for an IoT device to be attacked

Top 10 countries where attacks on the Symantec IoT honeypot were initiated

United States 17.7%

United Kingdom 2.1%

France 2.5%

Germany 4.9%

Ukraine 2.5%

Russian Federation 5.8%

China 26.5%

Japan 2.3%

Vietnam 3.8%

Others 28.8%

Hourly attacks on the IoT honeypot per month (2016)

The growth in hourly attacks on the Symantec honeypot from January to December can be clearly observed, almost doubling over the course of the year.
## IoT security is NOT like PC

<table>
<thead>
<tr>
<th>PC</th>
<th>IoT</th>
</tr>
</thead>
</table>
| **“Open”**  
Easy to install | **Openness**  
Not open to new software after device leaves factory |
| **“3”**  
(Mostly UDP, TCP, IP) | **Protocols**  
Thousands of Protocols  
(Hundreds in each vertical) |
| **“5”**  
(Mostly Windows, Linux, OSX, iOS, Android) | **Operating Systems (OS)**  
Dozens  
(Heavily fragmented by vertical) |
| **20k seat enterprise**  
(Typical Enterprise) | **Scale**  
100M “things”  
(Typical Car Maker) |
| All verticals have **same** Hardware/OS supply chain | **Fragmentation**  
Each verticals has **different** Hardware/OS supply chain |
| **“2”**  
X86 and x64 by Intel and AMD | **Chipset Architectures**  
Many  
8bit AVR,16bit MCU,32/64bit ARM,x86/64;12+vendors |
Therefore IoT security has to be different than PC

**Manage Devices**

- Cloud/Data Center
- Gateway
- Devices & Sensors

**Understand Your System**

- Know what to trust IoT Security Analytics
- A strong IoT trust model

**Protect the Communications**

- Protect the code that drives IoT
- Host Based Protection

**Protect the Device**

- Safely & Effectively managing IoT
Cloud / Data Center

Gateway

Devices and Sensors

Backend Services (Oracle, SAP, ERP)

IoT Platform (Big Data, Manage Devices)

Analytics

Hub (Edge Analytics, Control Systems)

Security Analytics

Certificate Authority

IoT Portal

Security Analytics: Anomaly Detection

Embedded Software

Operating Systems

Hardware (Chipset, Firmware, RF, Sensors)

Code Protection

Device Security

Identity, Authentication

Securing communications
Is there a need for cybersecurity certification?

• Does the market fail to address cybersecurity in IoT space?
  In some segments, definitely.
  ➢ Consumer goods
  ➢ Legacy systems
  ➢ Products designed without security-by-design

• Can voluntary certification work?
  Only if there’s a market for it.
  ➢ Positive business case for vendors, not bureaucracy
  ➢ Clear assurance for users, not confusion
  ➢ True Single Market, not national fragmentation

• Are we moving in that direction?
  No
  ➢ ePrivacy as voted by the EP reduces IoT security
  ➢ Unclear what needs to be certified, why or what is even possible/suitable
  ➢ Different roles for different players (device manufacturers, software, infrastructure)
Future Of Cybersecurity Starts Today

- **IoT security will not work in the traditional way. It needs to be:**
  - Extremely large scale
  - Network-managed and automated
  - Mobile and context adaptive
  - Close to real time

- **Certification can help, provided it is:**
  - Voluntary on the basis of an identified need
  - Market/Operations driven
  - Capability based
  - Outcome oriented
  - Internationally compatible

- **Advisable policy objectives:**
  - Technology neutral requirements adapted for different product categories and use cases
  - Private sector involvement in the governance of the framework
  - Member State commitment to the Single Market principle
  - Model existing regulations (e.g. eIDAS)
  - Strong role for ENISA
Thank You!

Ilias Chantzos
Ilias_Chantzos@symantec.com