The world is growing more connected

In 2018 there were 5.2 BILLION connected CONSUMER DEVICES growing with 13.8% CAGR 2013-30

27 BILLION connected IoT devices were in use in 2018 and will reach 125 BILLION in 2030

Source: IHS Markit
THE PROBLEM

• Products are built to a functional / cost / time-to-market target
  • Security is not considered, or an after-thought
  • How to secure by design?
• Security is opaque to customers –
  • Why build security in, if it’s not part of the purchase decision?
  • How to measure and differentiate for security?
• Security is an every point-in-time concept –
  • How to provide ongoing security assurance?

IoT security primarily is a commercial problem
Increasingly, product functionality is distributed
The ‘end point’ device often requires functionality and control provided by remote systems – such as gateways, cloud systems, or mobile apps
Security issues at any one end can affect the entire solution
The ABC’s of UL IoT Security

**Advising (Education)**
- Qualify risk
- Gap assessment
- Filter the noise

**Benchmarking (Support)**
- Pentest and security assessment
- Prepare for verification/certification
- Secure Development Lifecycle

**Certifying (Partnership)**
- Differentiate early adopters
- Validate ROI
- Brand reputation

*Cybersecurity Maturity*
REGULATORY DEVELOPMENTS

Governments are moving, but will look upon industry initiatives to lead the way.
REGULATORY & INDUSTRY INITIATIVE EXAMPLES

- California IoT Bill
- EU Cybersecurity Act
- US Cybersecurity Improvement Act
- UK Code of Practice for Consumer IoT Security/ETSI TS 103 645
- NIST Core Baseline Cybersecurity Capabilities
- DoC/DHS Botnet Report
- CSDE/CTA Anti-Botnet Guide
- IEC 62443
- UL 2900 Series of Standards / UL Cybersecurity Assurance Program (CAP)
- UL IoT Security Rating Program
- Common Criteria (ISO 15408)
- FIPS
- ARM PSA
- CTIA Cybersecurity Certification Program
- Amazon Alexa Voice Service Security Program
- GSMA IoT Security Guidelines
- IoT Security Foundation Best Practices Guidelines
- Other
TIME VS SECURITY ASSURANCE

UL IoT Security Rating

Alexa Voice Service Security Program

CTIA Cybersecurity Certification Program

UL 2900 / Cybersecurity Assurance Program

Common Criteria*

FIPS 140-2

IEC 62443

Evaluation Time

Level of Assurance

* Depending on scheme and/or EAL
A COLLABORATIVE APPROACH

**INDUSTRIAL/BUILDING**

1. Standards and Technology Support
   - Idaho National Lab Technology Support

2. Information Technology Sector Coordinating Council

**US POLICY FOCUSED & OTHER INFLUENCERS**

- Support specification and testing of certificate profiles for electronic drivers licenses
- Working with authorities through the European Cyber Security Organization contractual Public-Private Partnership collaboration

**EU POLICY & OTHER INFLUENCERS**

- Joint Japan – US ICS Training Session
- Significant Botnet Report
- Thought Leadership & Policy Influence

**ACADEMIA**

- Standards Development
- Policy Collaboration

**RETAILERS**

- Development of Assessment and Certification capabilities

**DEVELOPMENT COLLABORATIONS**

- Standards Development
- Policy Collaboration

**US POLICY FOCUSED & OTHER INFLUENCERS**

- Establishing MOU on Cybersecurity Information Sharing
- Demonstrating the current automotive cybersecurity risks

**ASIA POLICY FOCUSED & OTHER INFLUENCERS**

- Contributing member on efforts related to Supply Chain Risk Management Task Force

**UL**

- Official U.S. Delegate

UL and the UL logo are trademarks of UL LLC © 2018. Proprietary & Confidential.
SUPPLY CHAIN SECURITY

Problem

• Tier 1 OEMs and asset owners struggle with understanding the security maturity of their suppliers
• Existing SLAs with suppliers are ineffective because most suppliers don’t understand security
• OEMs and asset owners don’t have the time and may not have the resources to validate each one of their suppliers’ security maturity

Solution

• An independent evaluation of suppliers with focus on suppliers’ security processes and/or product testing
• An independent evaluation that provides transparency to OEMS and asset owners for supplier security
• An independent 3rd party that can work with suppliers to improve their security maturity over time
Complexity is the problem

TRUST

IS THE SOLUTION

- Powers smarter decisions
- Makes brands easier to choose
- Makes supply chains simpler to manage
- Makes differentiation quicker to achieve
THANK YOU

Empowering Trust™