Security for the Internet of Things (IoT)

Challenges & Opportunities

Anand Rajan
Senior Director, Emerging Security Lab
Intel Labs

IEEE World Forum on IoT
February 2018

Legal Notices and Disclaimers

This presentation contains the general insights and opinions of Intel Corporation (“Intel”). The information in this presentation is provided for information only and is not to be relied upon for any other purpose than educational. Use at your own risk! Intel makes no representations or warranties regarding the accuracy or completeness of the information in this presentation. Intel accepts no duty to update this presentation based on more current information. Intel is not liable for any damages, direct or indirect, consequential or otherwise, that may arise, directly or indirectly, from the use or misuse of the information in this presentation.

Intel technologies’ features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at intel.com, or from the OEM or retailer.

No computer system can be absolutely secure.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel, the Intel Core, and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others.

Outline

- Motivation
- Challenges & Key Research Problems
- Summary / Call to Action

Internet of “Things” or “Threats”? *

“*Internet of Things has arrived – and so have massive security issues*”

Jan 2013 WIRED

“*Scariest search engine on Internet*”

Jan 2013 SHODAN Computer Search Engine

“*The Internet of Things is set to change security priorities*”

April 2013 ComputerWeekly

proofpoint

“IoT Cyber-attack by 100000 smart appliances” (Jan 2014)

ars technica

“Crypto weakness in smart light-bulbs exposes Wi-Fi passwords” (July 2014)

SMART CITY

USENIX-Security’2014 (Researchers find it’s terrifyingly easy to hack traffic lights)

SMART HOME

BlackHat’2014 (Nest thermostat turned into a smart spy in 15 seconds)

INTELLIGENT TRANSPORTATION

BlackHat’2015 (Attackers able to control cars remotely)

* Computer Technology Review, March 2015

intel

Security Across IoT Verticals



Energy



Transportation



Smart Building



Environment Monitoring



Smart Factory



Medical



Retail

Common Security Concerns

Example: IoT Transportation Usage

	Confidentiality & Privacy	Data Authenticity	Availability & Safety
Smart Highway	Telematics – Tracking User Location	Toll Payment – Incorrect Billing and Metering	Accidents – Compromise Life and Property
Inventory Tracking	Expose Company Strategy	Costly Misroute of Truck and Inventory	Affect Timely Delivery of Goods – Interruption of Commerce

Security Foundation for IoT



Energy



Transportation



Smart Building



Environment Monitoring



Smart Factory



Medical



Retail

Secure IoT Endpoints

Secure IoT Connections

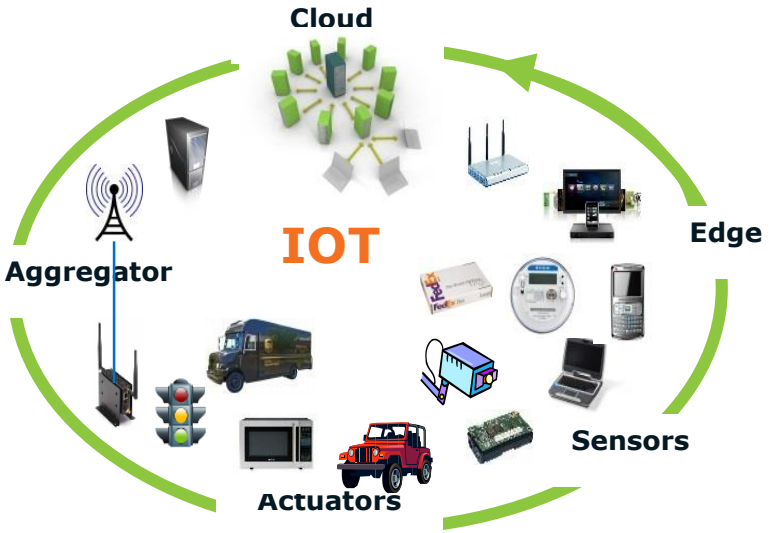
Secure IoT Lifecycle

Trustworthy, Safe and Reliable IoT Foundation

Outline

- Motivation
- Challenges & Key Research Problems
- Summary / Call to Action

Challenge #1: Secure IoT Endpoints



All Things need basic security capabilities

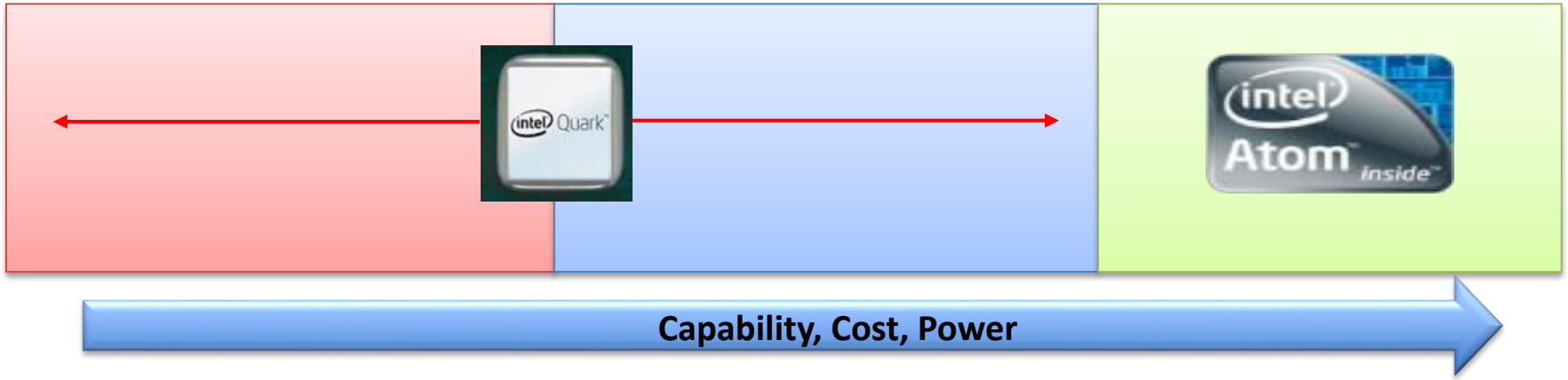
- HW Root of Trust & Secure Boot
- Remote Attestation
- Lightweight TEE
- Tiny Crypto

Huge challenge: Diversity of edge device

Even Motes may need to establish Trust

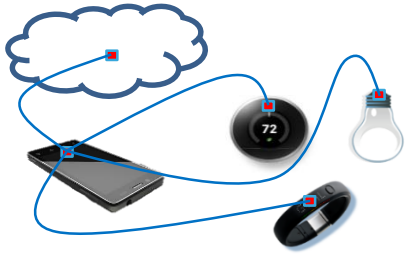
***Just-Enough Security* for each Thing**

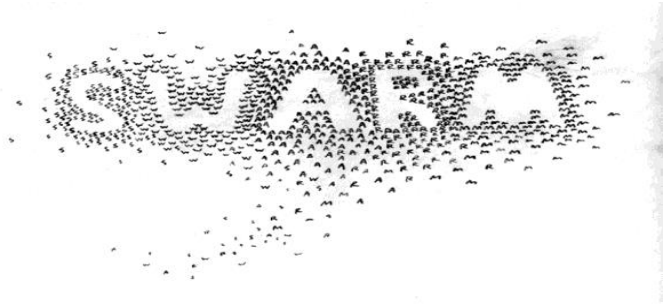
Key Research Questions



- Dedicated security co-processors (TPM), execution modes (TXT, SGX) intended for platforms with significantly higher capabilities
- Can we have credible security at constrained design points? Non trivial trade-offs

Challenge #2: Secure IoT Connections





IoT usages involve ensembles of devices

- Secure Device-to-Device Pairing
- Trustworthy & Flexible Grouping

Large Scale IoT: Authenticate IoT Swarms

- Self-learning to establish trust relationships
- Need to scale up to billions of endpoints & network devices

Usability is Key

- Eliminate need for Manual Configuration
- Seamless for Normal Users, Intuitive for Sysadmin

***Secure Channels* for Diverse Ensembles**

Source: http://keelyhoneywell.wordpress.com

Key Research Questions

Device-to-Device (D2D) Authentication

- Traditional approaches fail since devices have no I/O capabilities
- UX: Non-obtrusive bootstrapping with minimum human intervention

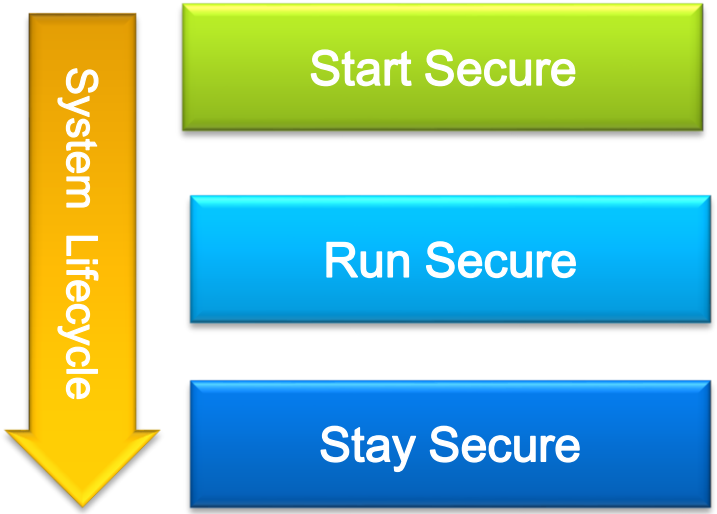
Groups

- Securely discover available and capable devices for grouping
- Secure Ad-hoc Grouping & Ungrouping
- Group Topologies & Communication Paradigms
- Smart City: Handle large swarms of mobile or dynamic devices

Secure Communication

- Authenticity, Integrity, Confidentiality, Anti-Replay & Audit
- Customized protocols for protecting specific IoT applications & workloads

Challenge #3: Secure IoT Lifecycle



System Deployment

- Endpoints: Measurable & Attestable

Sytem Execution

- Resistent to Malware during Runtime

System Management

- Detection & Diagnosis
- Patching & Remote Management
- Security for Long-Lived Devices

***Cradle-to-Grave* Secure Operation**

Key Research Questions

Build & Launch Secure IoT Systems

- How to build secure endpoints with right set of primitives? Programming Framework?

Runtime Security for IoT Systems

- Trusted Boot & Attestation? Fast, Lightweight, Real-Time? New Anti-Malware Solution?

Maintain Security for IoT Systems

- Real-Time Monitoring & Diagnosis? Fast reaction to attacks?

Secure Update of IoT Endpoints & Systems

- How to securely patch compromised endpoints? Lightweight, Real-Time, Large-Scale?
- High-Value problem across IoT Verticals; Unique requirements per Vertical

Outline

- Motivation
- Challenges & Key Research Problems
- Summary / Call to Action

Summary & Call to Action

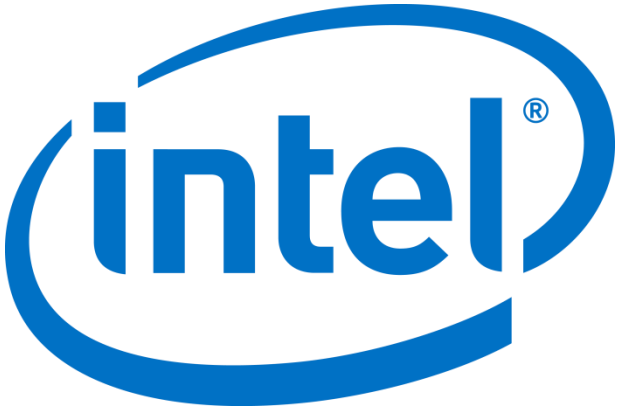
Trustworthy, Safe and Reliable IoT Foundation is Essential

- Secure Endpoints & Connections
- Security from Cradle to Grave

Scaling IoT *Securely* is Key Challenge

- Scaling ***down*** to extremely resource constrained environments
- Scaling ***across*** billions of IoT Endpoints

Significant Research Challenges to build out the Trustworthy IoT Foundation


intel