RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: MBS-R04

FROM IT TO IOT: BRIDGING THE GROWING CYBERSECURITY DIVIDE

Senthil Ramakrishnan

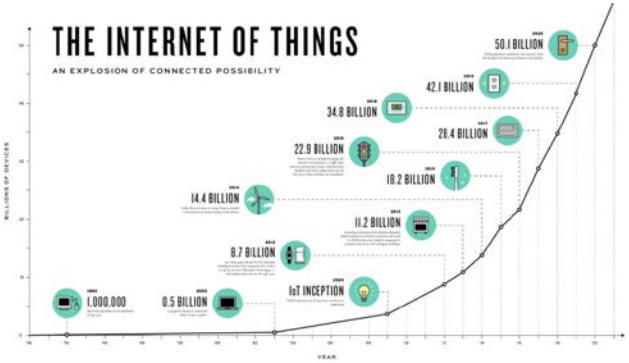
Lead Member of Technical Staff
AT&T IoT Solutions
@senthil_rn

Agenda

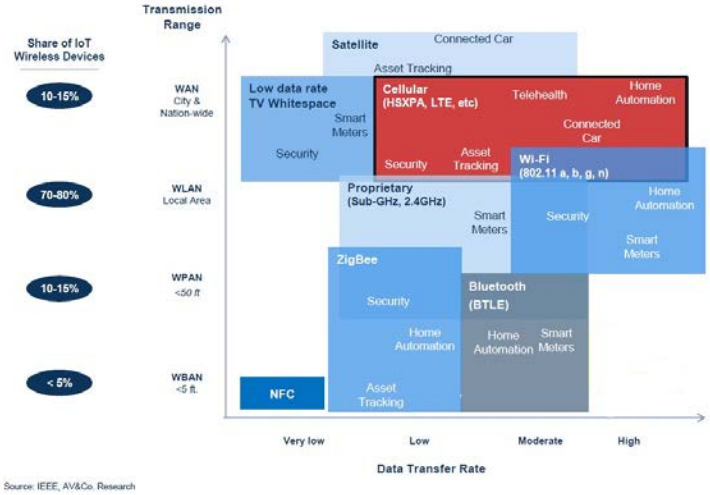
- Introduction
- Introduction to IoT
- IoT Security Challenges
- Moving from an IT to IoT Security Framework
- What about OT?
- Supply Chain and Security
- Security Incident Response and Management
- Designing with Security in Mind
- Summary

INTRODUCTION TO IOT

Introduction

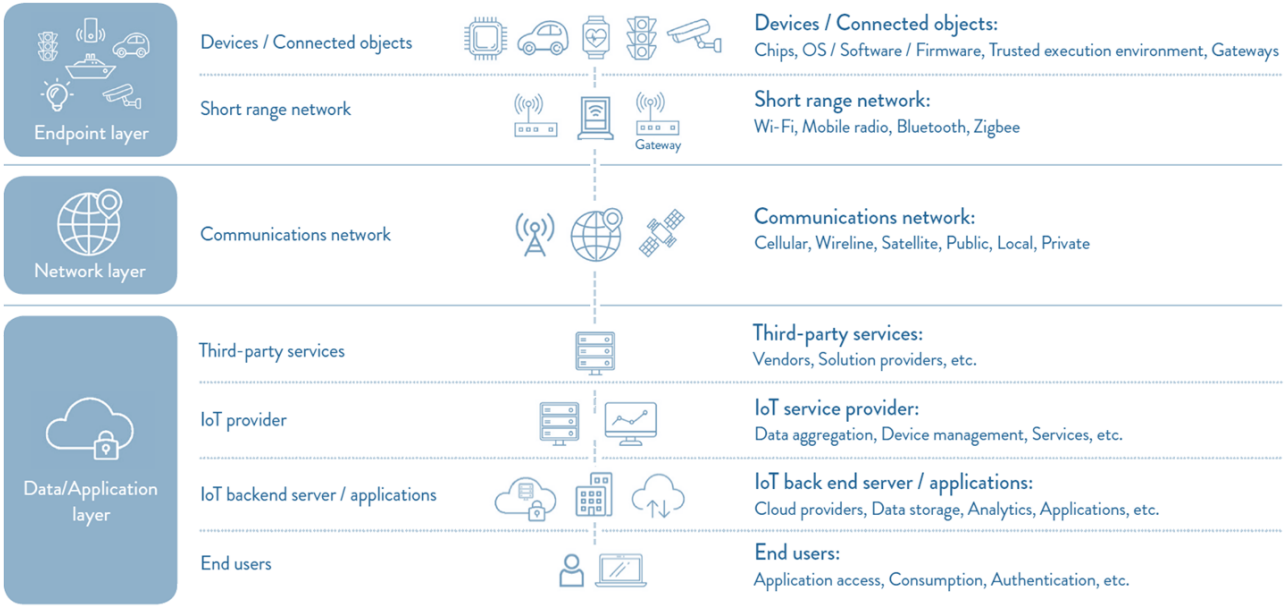


Source : http://www.t-ink.com



Source: IEEE, AV&Co. Research

IoT Architecture



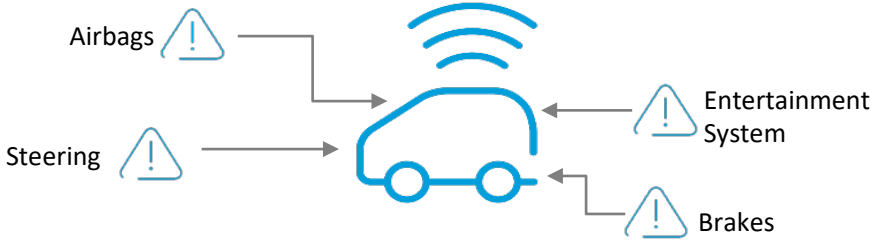
Source : https://www.iotca.org/

IoT in the Real World

Manufacturing	Logistics	UBI	Fleet OEM	Value Added Reseller	Retail	Security	Drones
Agri-Tech	Oil / Gas	Connected Car	Fleet Mgmt	Wearables	Automation	mHealth	Smart Cities

IOT SECURITY CHALLENGES

IoT Security in the news



Researchers infiltrated the networks of late model connected cars to gain control of their steering, radio and automated driving features.

Mobile Apps

Smartphone-based mobile apps were recently compromised to get access to in-vehicles services like telematics and other services.

Open ports

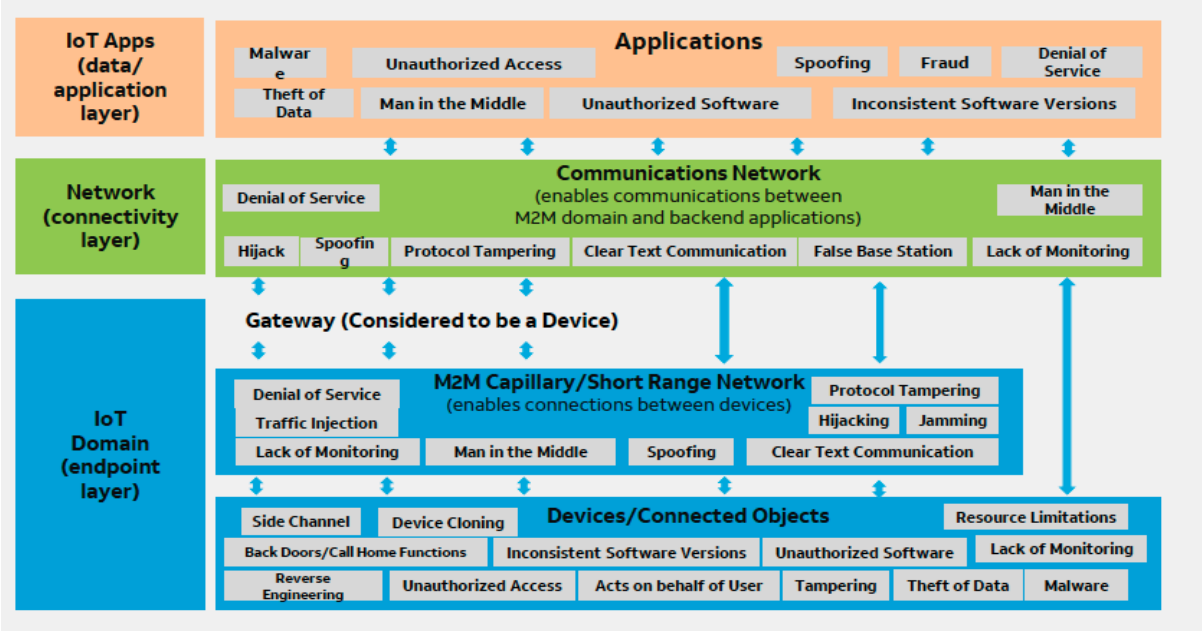
No authentication

Man-in-the-Middle type attacks on older cellular technologies like 2G

Potential security vulnerability

WIRED, "How the Internet of Things got Hacked" 12.28.15.
http://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/

IoT Security Considerations



Source : AT&T CSO Security Framework

IT vs IoT

	IT	IoT
Device Volume	Limited per Enterprise	Very large volumes
Device Types	Standardized	Wide variety of custom devices
Hardware/Software	Standardized	Custom and varied
Management and Control	Standardized Device Management capabilities	Primarily unmanaged devices
Applications/Backends	Standard and custom built	Fully custom
Device Access	Restricted	Restricted and Public
Risks	Data Loss, Lost Revenue	Life impacting
Connectivity	Quasi-private networks	Private and public

IoT Security Impacts

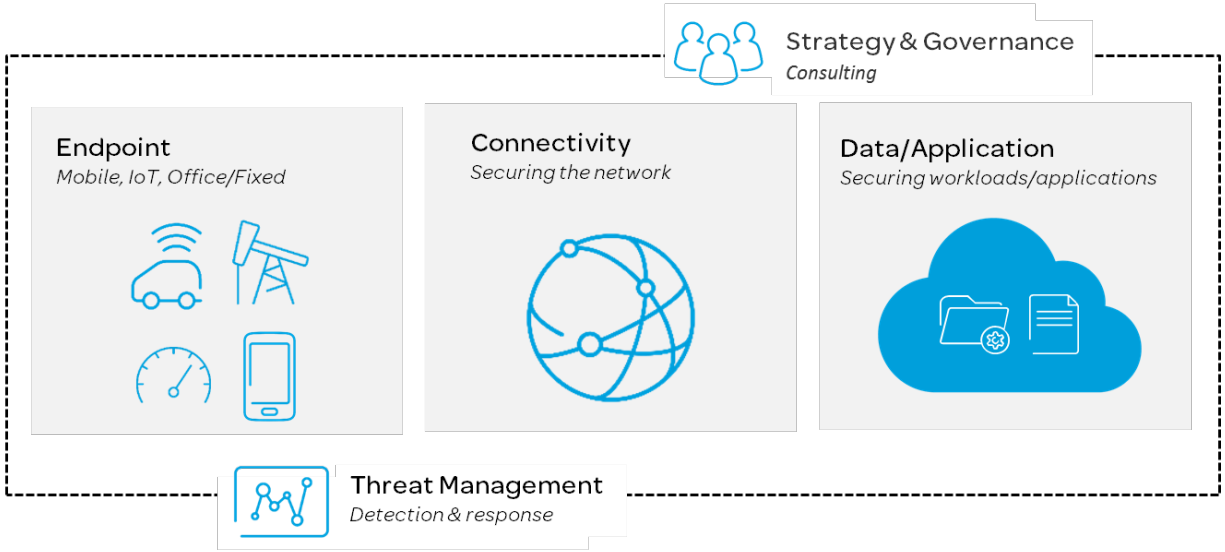
	IoT	Security Challenge
Device Volume	Very large volumes	• Need to monitor and manage a very large number of devices • Deployed in various environments and geo locations
Device Types	Wide variety of custom devices	• Wide variety of devices with varying security capabilities • Singular/standardized security solutions cannot be deployed across all device types
Hardware/Software	Custom and varied	• Custom hardware and software prevents • Complex lifecycle management
Management and Control	Primarily unmanaged devices	• Need for multiple device management solutions • Security patching and FOTA requirements are very complex
Applications/Backends	Fully custom	• Cannot integrate to existing security solutions
Device Access	Both remote and public depending on IoT vertical	• Vulnerable to tampering • Exposed to hostile environments • Not easily accessible
Risks	High risk for certain verticals	• Data Loss/compromise • Lost revenue • Impact to life

IoT Security Framework

Top IoT security concerns:

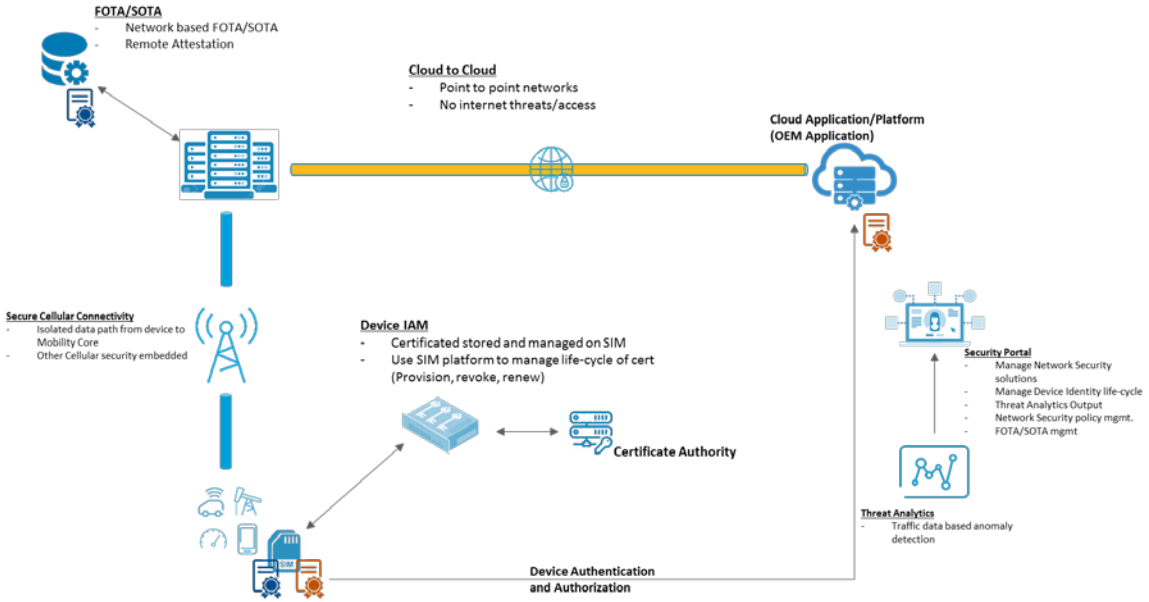
- Device security
- Secure data in transit
- Secure data at rest
- Integrity of the data
- Reliability of the data
- Convergence of OT and IT
- Operational efficiency
- Access & authentication (devices & users)
- Software/Firmware updates

AT&T recommends a multi-layered approach to security to help protect the IoT ecosystem end-to-end.



Moving from IT to IoT - Endpoints

- Key Learnings
  - Constrained devices offer challenges to traditional solutions like PKI and certificate-based solutions
  - Non-standard OS and SW/FW
    - Management of devices is near impossible using EMM type solutions
- IoT Solutions
  - Use light-weight solutions like PSK for constrained devices
    - Using the eUICC/eSIM as the PSK or PKI manager
  - Move the computation away from the device (Gateway based security)
  - Use LwM2M based Device Management solutions
  - Network-based endpoint anomaly detection
  - FOTA/SOTA capability is very crucial



Moving from IT to IoT - Connectivity

- Key Learnings
  - IT networks are traditionally quasi-private with very strict rules for internet access
  - Primary connectivity threat vectors originate from open internet
- IoT Connectivity
  - Isolate data from device to backend using secure connectivity
  - Use point-point networks
    - Cellular (Better than Wi-fi) + MPLS/NetBond
    - Secure but low cost options like LTE-M and NB-IOT
  - Need to provide that all connectivity models included
    - Cellular, Wireline, and Satellite
  - Use Edge computing for anomaly detection and management
  - 5G Networks on the horizon
    - Network Slicing
    - Edge Computing

Moving from IT to IoT – Data/Applications

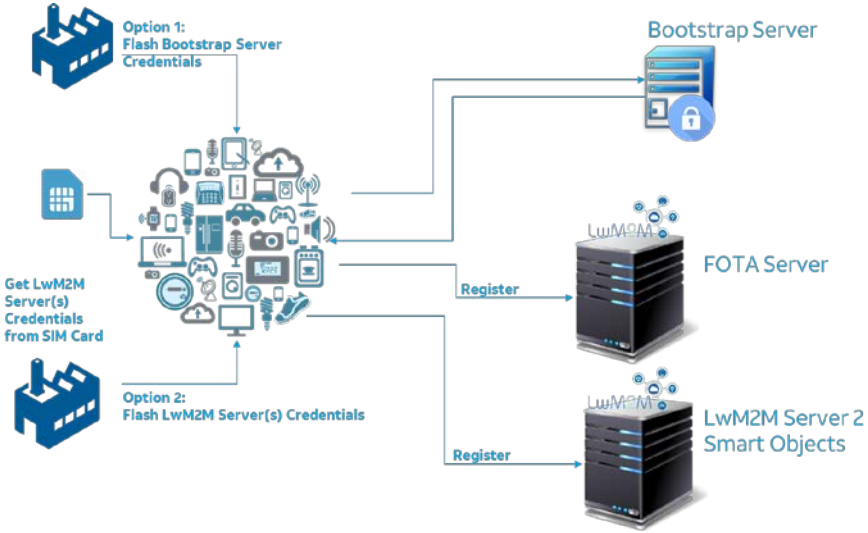
- Key Learnings
  - Highest risk since all data is centralized
  - IoT platforms are primarily on CSPs like AWS, Azure and others
  - Integration to existing IT systems is necessary
- IoT Solutions
  - Bi-directional authentication of device and cloud
  - Use data from devices to build Threat intelligence and use that to set up security policy
  - Defined secure data handling and storage requirements
    - Data classification and security policy
    - Encryption of data
  - Secure access controls
  - Use IDS/IPS solutions to detect intrusions
  - Physical security
  - Remote monitoring of services and devices

Moving from IT to IoT – Policy & Controls

- Key Learnings
  - Enterprise CSO Policies and Requirements are very IT focused
    - Data integrity and handling requirements do not take into account IoT devices, networks and their constraints
    - Applying these policies is a challenge when deploying IoT solutions and may increase cost and time to market
- IoT Solutions
  - Understanding the key differences and challenges of IoT is important
  - Update CSO policies and requirements, and include the type of IoT deployments that the enterprise will require
  - Use the new IoT Security Framework rather than the IT Framework
  - Better support Audits and Compliance specific to IoT

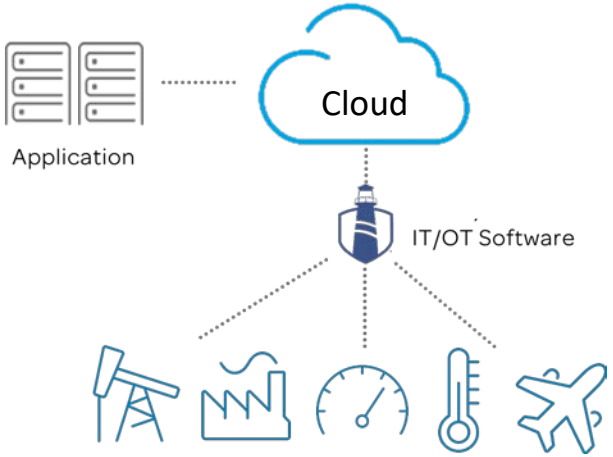
The Importance of FOTA

- Life-cycle management of the IoT eco-system is crucial
- MNOs will manage connectivity life-cycle
  - 3G -> 4G -> 5G
- CSPs self-manage security updates
- Life-cycle management of device is necessary
  - Deployment is just the start
  - Updating and managing the device through it entire lifetime will help ensure security
- Secure FOTA
  - FOTA source must be highly secure
  - Integrity of FOTA– FW Signature
  - Secure Connectivity for the FOTA update
  - Rollback capability



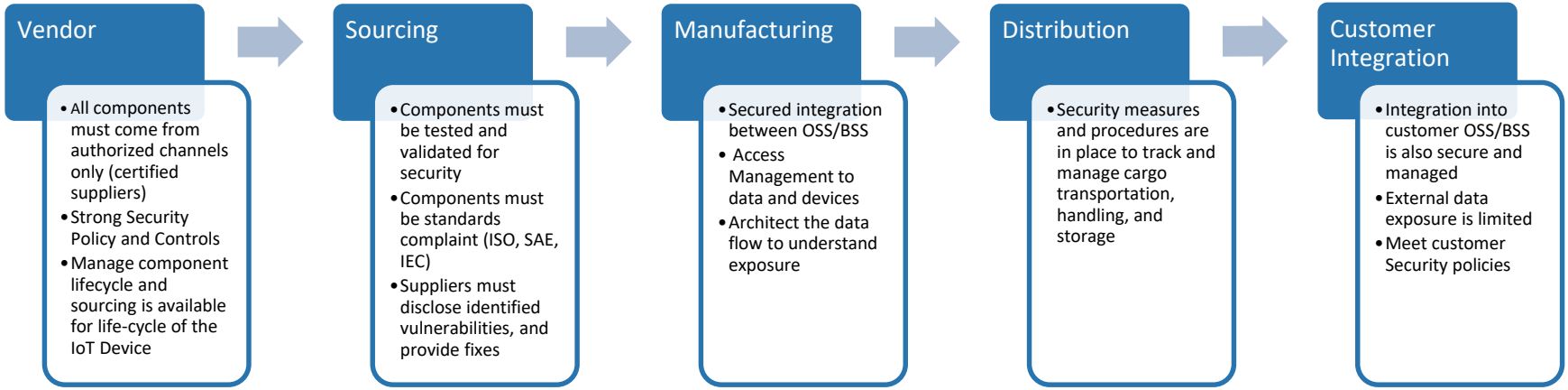
What about OT?

- OT systems include SCADA, ICS and other manufacturing systems used in critical infrastructure
  - Older command and control type systems being “connected”
  - Legacy OSes, protocols and proprietary systems
  - Security implemented essentially through obscurity
  - Convergence of IT and OT adds many new challenges
- Securing OT (in addition)
  - Network segmentation
  - Secure remote user access with identity-based policy enforcement
    (3rd parties, internal/external communications, maintenance, troubleshooting)
  - Granular content & context-based DPI (Deep Packet Inspection)



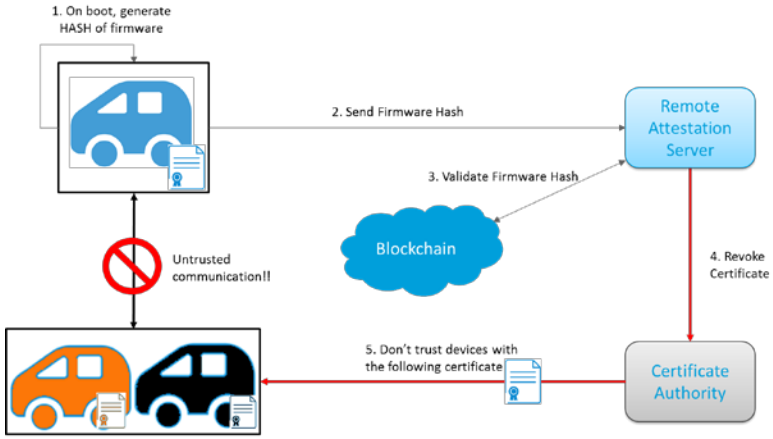
Supply Chain Security

- Security must be part of complete supply chain process
  - Includes both hardware and software, manufacturing and assembly setup, and other tools
- Connected Car customer deploying IoT across the supply chain
  - Solutions in addition to IoT



Security Incident Management and Response

- As technology advances, new security vulnerabilities will be uncovered
- Define a Security Incident Response process
  - Isolation/quarantine impacted devices
  - Notification of consumers
  - Manage the breach or attack
  - Identify the issue and define possible solutions
  - Resolution path and team
  - Follow up with all affected parties
- FOTA/SOTA is an invaluable security tool



Designing with Security in Mind

- Implement a Security Development Lifecycle (SDL)
  - Understand the threat vectors
  - Understand the risks and possible exposure
  - Set the acceptable risk profile (Risk Assessment)
  - Identify the security solutions
  - Define implementation architecture
  - Define a cyber-security incident response path
- Convergence of IT and IoT systems
  - Special care must be taken at these integration points
  - New and expanded attack surfaces at integration points
- Security must be incorporated into design
  - Device design
  - Manufacturing
  - Testing and validation
  - Shipping and Logistics
  - Post-purchase maintenance and aftermarket
- Continued testing and vulnerability discovery

Across the Bridge

Today

- Understand the differences between IoT and IT environments
- Include IoT specific security requirements for Day 1 of design lifecycle
- Define a Security Development Lifecycle for the deployment

Short-term

- Define IoT security policies and controls for the enterprise
- Identify threat vectors, and implement security solutions that fall within IoT specifications

Long-term

- Secure convergence of IT and IoT must be an enterprise-wide strategy
- Security must extend across the entire Supply Chain