RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SBX1-R05

Tactical Survival Tips Building & Leveraging Internet of Things (IoT) Systems

Brian Witten

Senior Director, IoT
Symantec Corporation
@WittenBrian

#RSAC

How to Protect Connected Things

IoT betters our lives countless ways…

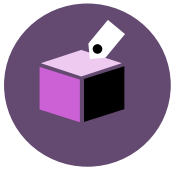
Medical Devices

Connected Cars

Digital Factories

Already 20 Billion Microcontrollers (MCU) annually
5 Billion Connected Today, 20 Billion by 2020

Smart Cities



Consumer Electronics

Quick History of Actual Events

Multi-Kiloton
Pipeline Explosion

Steel Mill Blast
Furnace Damaged

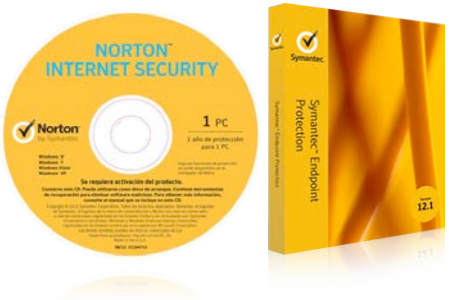
Hundreds of Critical
Infrastructure Sites

National Scale
Power Grid Crashed

Cars: Digitally Stolen,
Remotely Crashed

Hospitals Breached
via Medical Devices

What changed?



PC / Datacenter Era

*Security - most easily delivered by **disk** or by download*

IoT / Cloud Era

*Security - must be integrated by **design** to be effective*

Information Technology (IT)		Internet of Things (IoT)
All verticals have **same** Hardware/OS supply chain	***Fragmentation***	Each vertical has **different** Hardware/OS supply chain
"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)
"2" X86 and x64 by Intel and AMD	***Chipset Architectures***	**Many** 8/16/32/64 bit, AVR, ARM, MIPS, Over 12 vendors

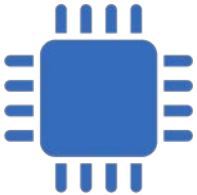
Internet of Things (IoT) Cornerstones of Security

Manage Devices

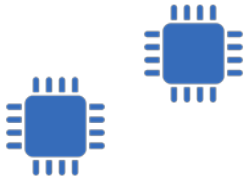
Understand Your System

Cloud/Data Center

Gateway



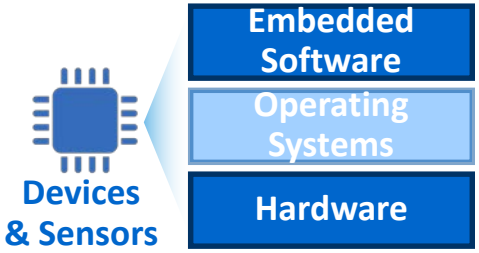
Devices & Sensors



Protect the Device

Protect the Communications

Protect The Communications



Protect the Communications

Required: Authentication

Helpful: Encryption

Note: Signing "objects" can avoid decrypt/re-encrypt burden

What's needed?	
Crypto Libraries:	Several good open-source and commercial options
Certificates:	Over a Billion IoT devices chain to a world class Certificate Authority (CA)
Roots of Trust:	IoT "Roots of Trust" can help identify foreign devices

Can extremely constrained devices do meaningful security?

Early 80's grade chip

Benchmark: ECC/ECDSA256

8 bit
8 Mhz
2 k SRAM

25 seconds

AA Battery: 20+ years

Leading 10 year old chips

$0.25

16 bit, 16 Mhz
30 k SRAM

3 seconds

AA Battery: 20+ years

Current 32 bit chips

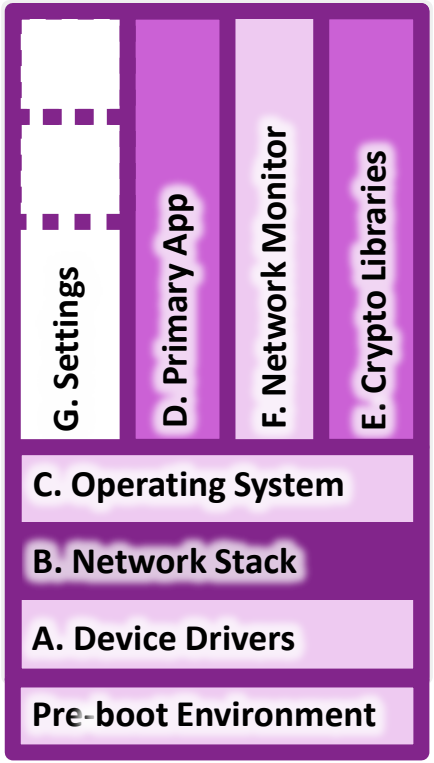
$0.50

32 bit, 84 Mhz
30+ k SRAM

150 ms

AA: 20 years

Protecting Devices (Boot Time)



- Never run unsigned code.
- Never trust unsigned configuration data.
- Never trust unsigned data. (Period.)
- Provide run-time protection for each device.

Protect the Code that Drives IoT

Protecting Devices (Run Time)

Traditional Approach: Malware Blocking	Whitelisting Behaviors: Sandboxing
Signature based	*Behavior / policy based*
Internet access required	*No internet access required*
Reactive	*Proactive*
Ineffective on zero-day	*Effective on zero day*
Ensures self-protection	*Protects OS critical resources*
Customization or separate product	*Protects applications from each other*
Large footprint	*Small footprint*

Internet of Things (IoT) Cornerstones of Security

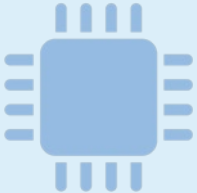
Manage Devices

Cloud/Data Center

Understand Your System

Gateway

Run Time



Devices & Sensors

Boot Time

Authentication

Protect the Device

Protect the Communications

Safely & Effectively Managing IoT Devices

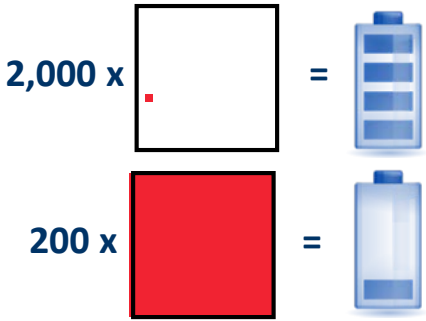
Why update devices?

Industrial Systems
19 years on average

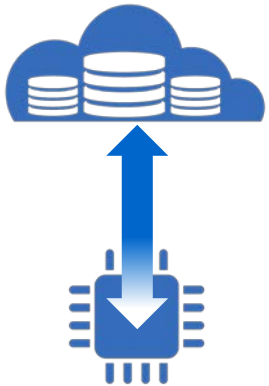
3 days
Vulnerability Discovery Rate (Linux)

Build in Over The Air (OTA) updates from the start

Granular Updates
Save Battery & Bandwidth



"Build it Right Once"
(Use it for Both General & Security Management)



General & Security Telemetry
Functionality & Security Updates
Configuration Changes
Diagnostics & Remediation
Network Access Control (NAC)
Credentials/Permissions, Policies

Understand Your System To Detect Strategic Threats

- No matter how well you do everything else, some threats will still get past even the best defenses.
- Detecting such threats requires strong understanding of what your network “should” be doing.
- Machine learning (ML) distills models of “normal” that can run in compact Single Board Computers (SBC).
- Some ML can “learn” in resource constrained gateways and small SBC to detect anomalies specific to specific networks.
- Such IoT Security Analytics are crucial in finding advanced threats.

Internet of Things (IoT) Cornerstones of Security

Manage Devices

Updates

Policies

Cloud/Data Center

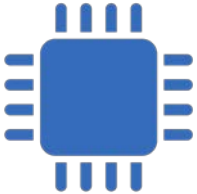
Understand Your System

Embedded Analytics

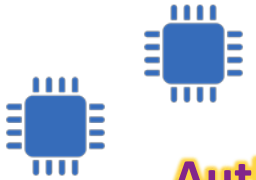
Gateway

Run Time

Boot Time



Devices & Sensors



Authentication

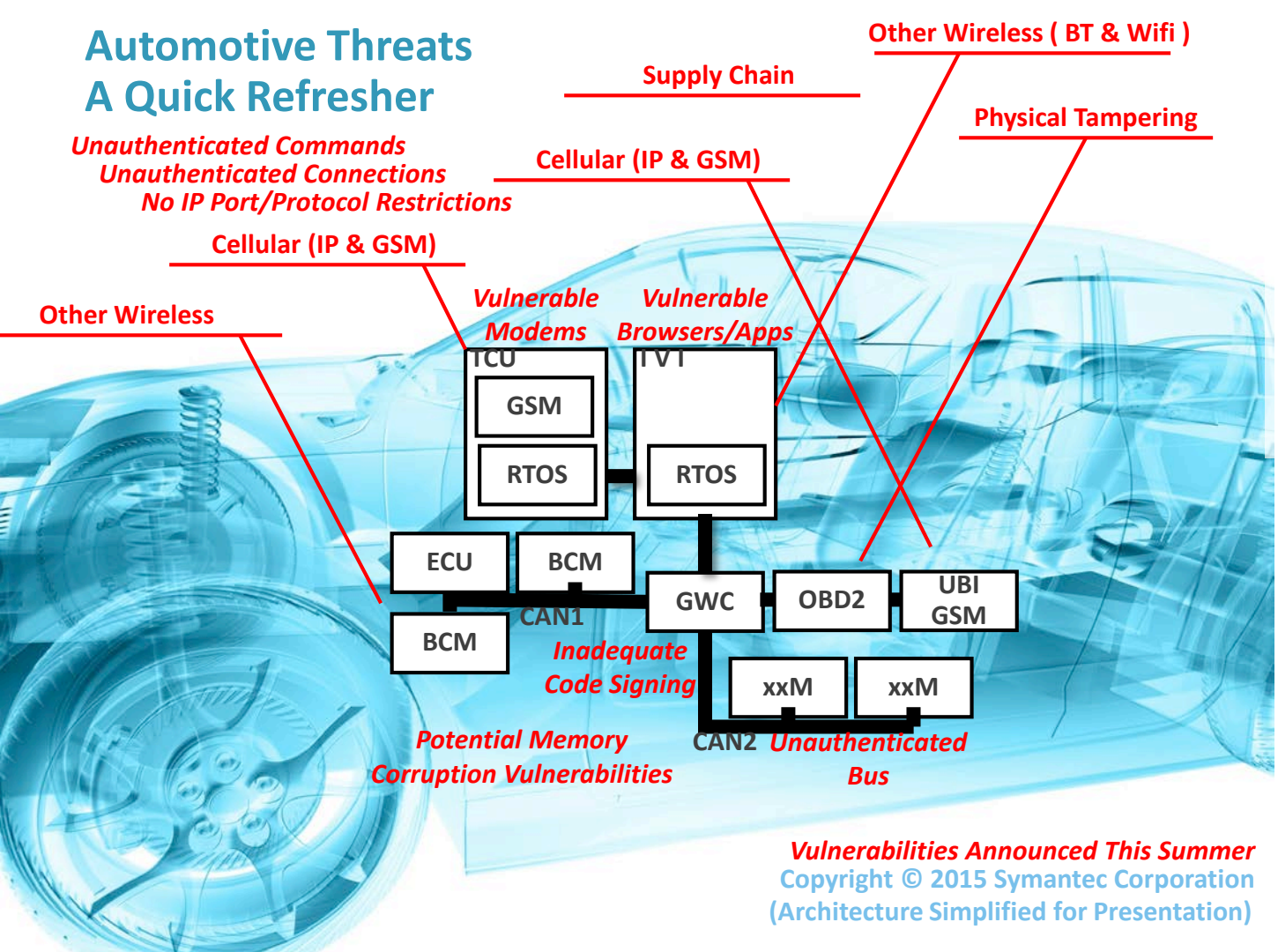
Protect the Device

Protect the Communications

Agenda

- Define a Simpler Framework for Building Security Into IoT Things
- Practical Example (2 slides)
- Tips & Tricks for Companies Leveraging (not Building) IoT Things

Automotive Threats
A Quick Refresher



TCU: Telecommunications Unit
IVI: In Vehicle Infotainment
RTOS: Real Time OS
ECU: Engine Control Unit
BCM: Body Control Module
xxM: Other Modules
CAN: Controller Area Network
CAN1/2: Hi, Med, Lo Speed CAN
GWC: “gateway chip”
OBD2: On Board Diagnostics port
UBI: Usage Based Insurance
GSM: Global System for Mobile Comm’s, aka "a modem”

Vulnerabilities Announced This Summer

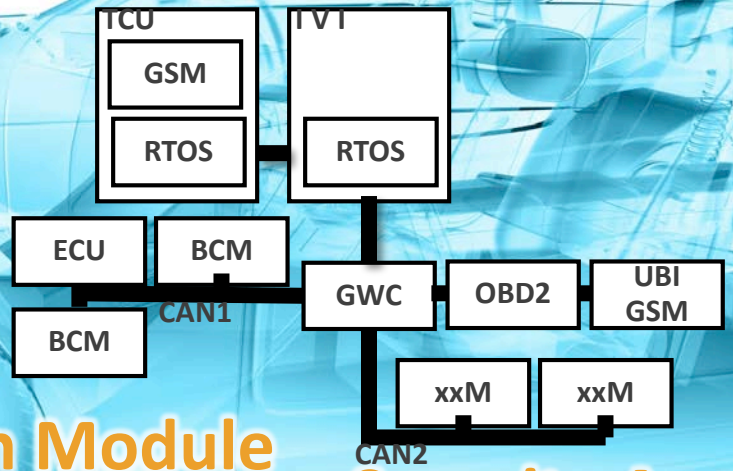
(Architecture Simplified for Presentation)

Business Constraints:
-- Consumers won't pay for security they "assume"
-- OEM & Tier 1 Suppliers: extremely thin margins
-- Security $ must be < "few %" of any car/module

Cornerstones of Security
Automotive Vehicles

CAMP VSC3, HIS SHE, EVITA HSM
Authenticate Comm's

OMA DM, SCOMO
Manage Devices



Protect Each Module
Code-Signing (Boot Time)
Host-Based (Run Time)
Compiler Based (No-OS)

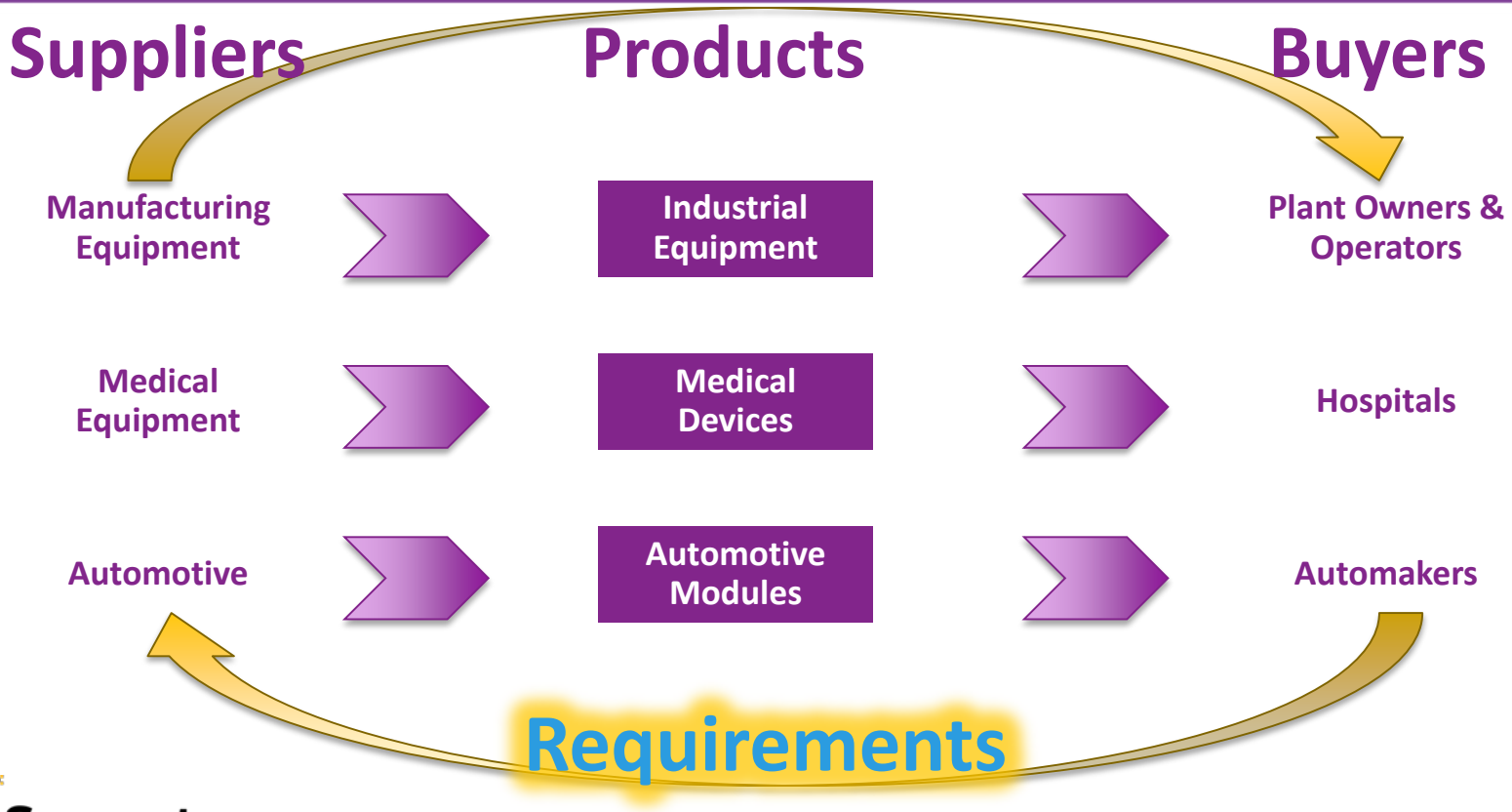
Security Analytics
Embedded (in-vehicle), Global

TCU: Telecommunications Unit
IVI: In Vehicle Infotainment
RTOS: Real Time OS
ECU: Engine Control Unit
BCM: Body Control Module
xxM: Other Modules
CAN: Controller Area Network
CAN1/2: Hi, Med, Lo Speed CAN
GWC: "gateway chip"
OBD2: On Board Diagnostics port
UBI: Usage Based Insurance
GSM: Global System for Mobile Comm's, aka "a modem"

CAMP: Crash Avoidance Metrics Program
VSC3: Vehicle Safety Comm's
HIS: Hersteller Initiative Software
SHE: Secure Hardware Extensions
EVITA: E-safety Vehicle Intrusion Protected Applications
HSM: Hardware Security Module

OMA DM: Open Mobile Alliance (OMA) Device Management (DM)
SCOMO: Software Component Management Object

Tips & Tricks LEVERAGING IoT Devices



Internet of Things (IoT) Cornerstones of Security

Manage Devices

Updates

Policies

Cloud/Data Center

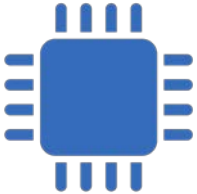
Understand Your System

Embedded Analytics

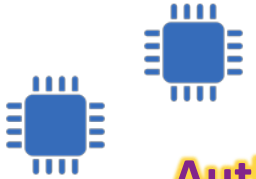
Gateway

Run Time

Boot Time



Devices & Sensors



Authentication

Protect the Device

Protect the Communications

IoT Security “Recipe”

- Protect your devices: *[(high assurance boot) + (runtime protection)]*
- Protect communications: *design in strong authentication mechanisms*
- Manage your devices: *build in update mechanisms for granular updates*
- Understand your system: *leverage analytics to catch strategic threats*

Strong Foundations Cover All Four IoT Security Cornerstones!

Apply What You Have Learned Today

- **Owners/Buyers of IoT Things:**
  - Next week: meet with your Procurement team to begin adding Security Requirements to all RFP for equipment and/or component suppliers
  - Next quarter: start educating other stakeholders on what it means to "build security into these things."
  - Next year: refuse to buy equipment without adequate security
- **Makers / Builders / Venders of IoT Things:**
  - Ensure you adequately cover all four "cornerstones" of security for your Things!

Thank You!

bwitten@symantec.com

Internet of Things (IoT) Security Reference Architecture: www.symantec.com/iot