ciab FEBRABAN 2016

Symantec FEBRABAN

IoT - Internet of Things

Sebastian Brenner, CISSP
Security Strategist for Latin America & Caribbean

IoT betters our lives countless ways…

Automatic Teller Machines & Point of Sale Terminals

Smart Cities

Consumer Electronics

5 Billion Connected Today, 20 Billion by 2020

Medical Devices

Connected Cars

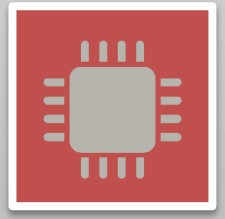
Industrial Control Systems

All Surface Areas Involved Need to be Evaluated

Many Surfaces Involved

Cloud / Data Center

Gateway



Devices & Sensors

Top 10 IoT Vulnerabilities

Insecure web interface
Insufficient authentication /authorization
Insecure network services
Lack of transport encryption
Privacy concerns
Insecure cloud interface
Insecure mobile
Insufficient security configurability
Insecure software/firmware
Poor physical security

Source: https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf

Quick History of Actual Events

- ATM Machines Hacked and Robbed with a Text Message
- Hospitals Breached via Medical Devices
- Cars: Digitally Stolen and Remotely Crashed
- Hundreds of Critical Infrastructure Sites
- Large Scale Power Grids Crashed

Each Market Segment has Different Complexities

FINANCIAL

MEDICAL

AUTOMOTIVE

INDUSTRIAL

Symantec Protects Over a Billon IoT Devices

Security Considerations for the Internet of Things (IoT)

Protect the Device

Strong Authentication

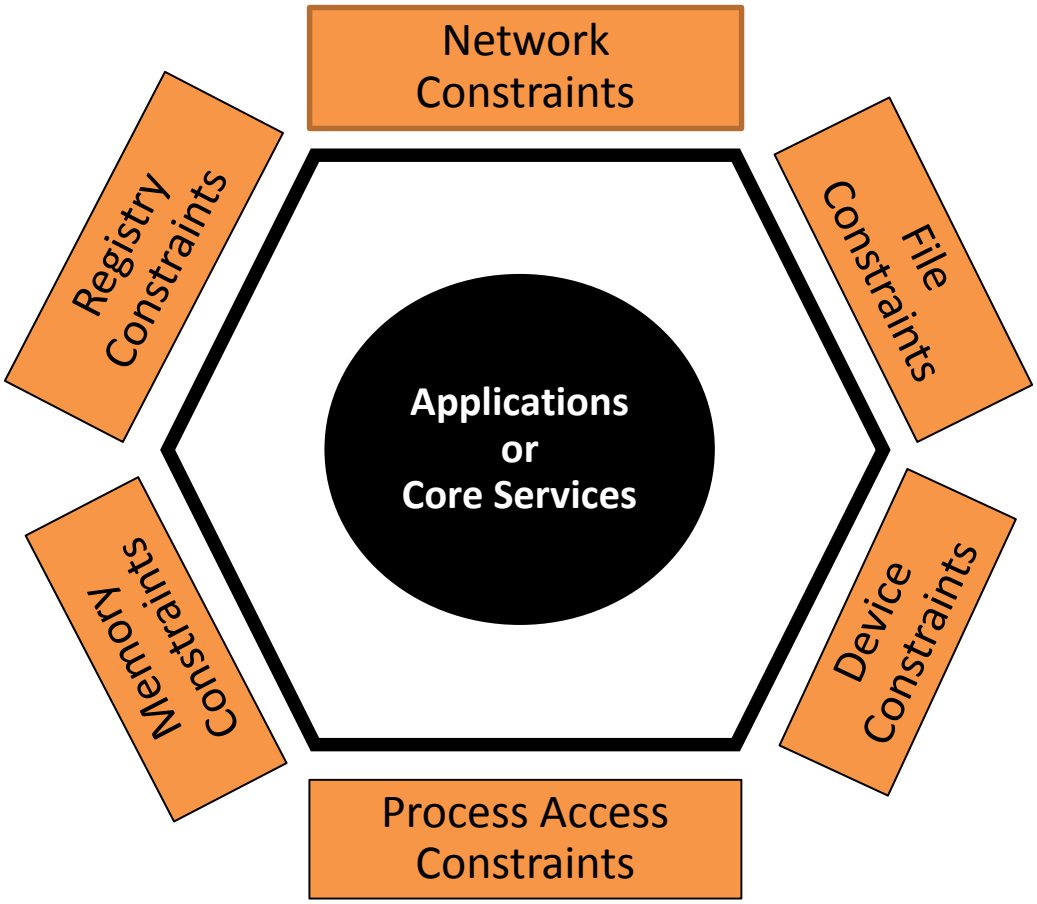
Strong Security Analytics

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 and its Infrastructure (Run Time)



- A sandbox is a containment jail for every program (processes)
- Confine an application to a sandbox
- Least privilege controls or “acceptable” resource access behaviors
- Restrict the application only to the required resources that are necessary to perform the defined use cases.

Use Case #1 – Sophisticated ATM Attack Methodology

Malware Attack

Infiltration	Propagation	Aggregation	Exfiltration
Attackers break into the bank / ATM network (e.g., via remote desktop connections, spear-phishing, vulnerable servers, unprotected USBs etc.)	Attacker searches for entry points to the ATMs / end points and install malware such as Green-dispenser, Conficker, Zeus and Citadel on target systems.	Malware steals critical information from the vulnerable devices or dispenses all the cash in the ATMs. The stolen data is either sent over to the hacker in real-time or is stored in a hidden location locally.	If the stolen data is stored locally, all the stolen data is aggregated in a hidden location from where the data is stolen.

Use Case #1 – Sophisticated ATM Attack Methodology

Malware Attack

Infiltration

Attackers break into the bank / (e.g.) via remote desktop connections.

Network Constraints

Device Constraints

unprotected USBs etc.)

Propagation

Attacker searches points

Green-dispenser,

target systems.

Network Constraints

File Constraints

Process Access Constraints

Aggregation

Malware steals critical information and dispenses all vulnerable devices

ATMs. The stolen data is either sent in real-time or is stored in a hidden location locally.

Network Constraints

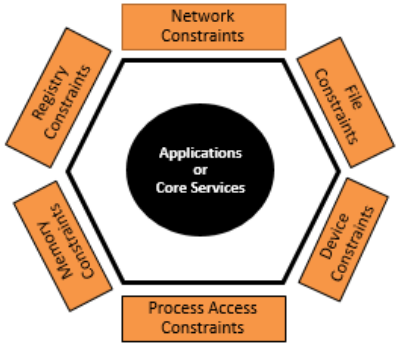
File Constraints

Process Access Constraints

Exfiltration

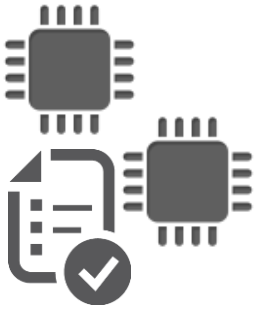
If the stolen data is stored locally, all hidden location from where the data is stolen.

Network Constraints



Strong Authentication

Allows IoT devices to know whether or not they can trust a remote system or user



DEVICE AUTHENTICATION

Use a device certificate
Never trust unauthenticated peripherals.

USER AUTHENTICATION

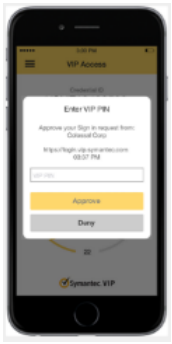
Validate user to access IoT device and data

Use Case #2 - IoT and User Authentication at Branch Office

Making Additional Factors Seamlessly Transparent

ATM, CARD, & PIN, as today.

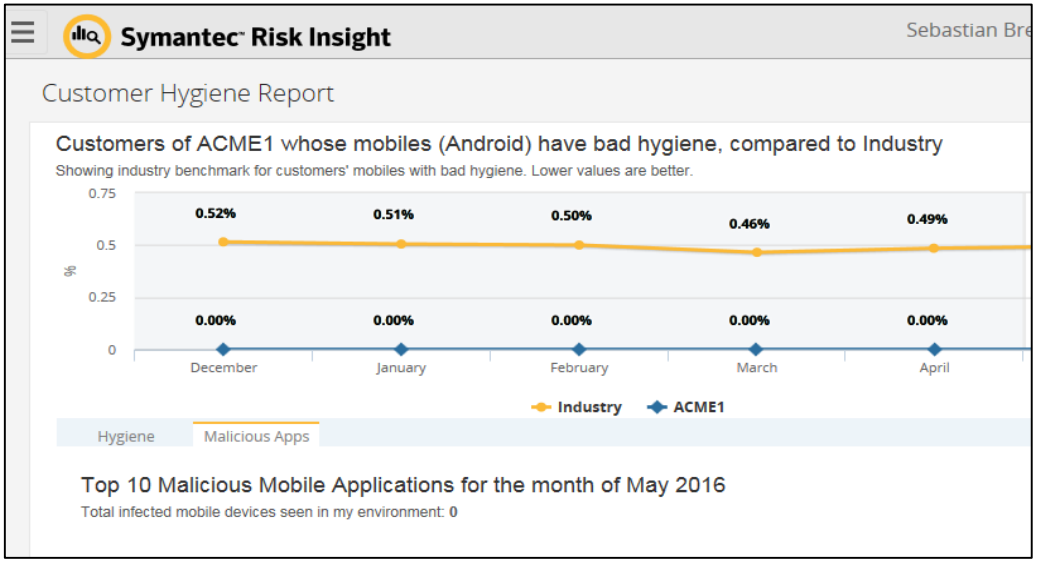
Is the cardholder's mobile device physically near the ATM?

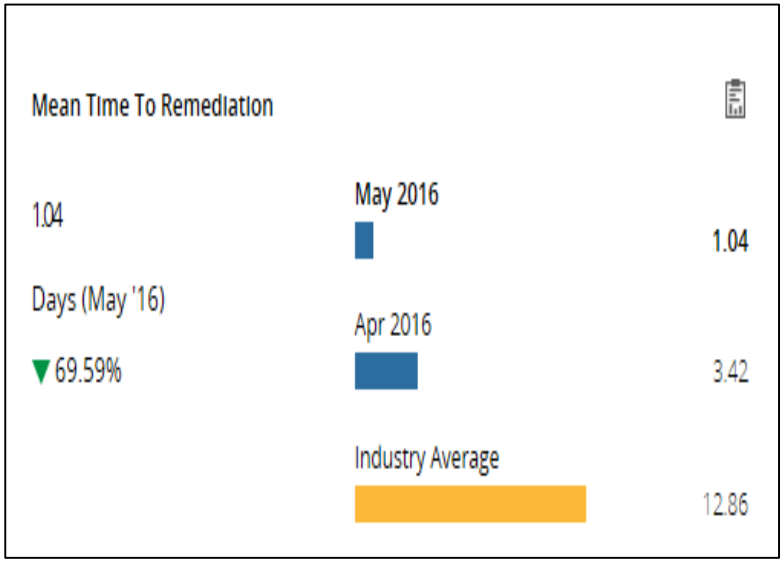


If suspicious, ask the cardholder on their mobile device, "Do you authorize this?"

For highest risk transactions, leverage biometrics built into the device.
Fingerprint, plus both facial and iris recognition with liveness detection.

Strong Security Analytics





- Some threats will still get past even the best defenses.
- Strong understanding of what your network and IoT “should” be doing.
- IoT Security Analytics are crucial in finding advanced threats.
- Complement with your Cloud Based security analytics

Conclusions

Threats

Threats to IoT systems, including financial services, are real and happening today

Defense In- Depth

Security is a necessity and an enabler, not a burden or a tax

Security By-Design

Consider a security by design approach, not just security as an add-on

ciab FEBRABAN 2016

FEBRABAN

Obrigado!

Sebastian Brenner, CISSP
sebastian_brenner@symantec.com