What's The Right Security for IoT?

Infineon Technologies
September 2015

Agenda

1 Introduction to IoT

2 Risk Analysis

3 Countermeasures

4 Into the Future

Copyright © Infineon Technologies AG 2015. All rights reserved.

1 Introduction to IoT

2 Risk Analysis

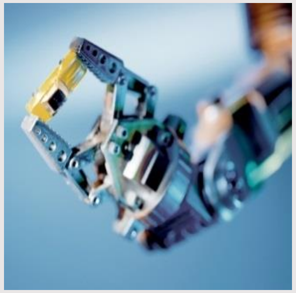
3 Countermeasures

4 Into the Future

Copyright © Infineon Technologies AG 2015. All rights reserved.

What is Internet of Things (IoT) all about?

IoT Definition



“A world where **physical objects** are seamlessly **integrated** into the **information network**.”

- Industrial
- Automotive
- Consumer
- Medical
- Networking
- Computing

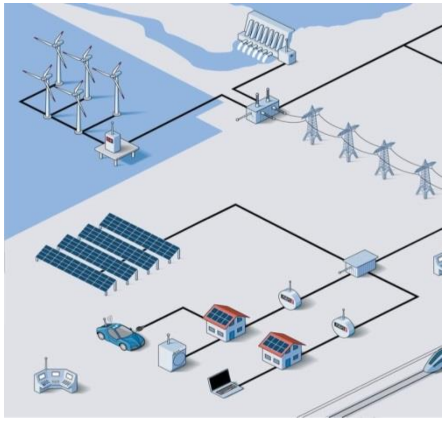
Internet of Things (IoT) Drives Increased Profits

Smart Home

Automotive

Industrial

ICT



1 New capabilities and services

2 Greater efficiency

3 Increased flexibility and customization

Copyright © Infineon Technologies AG 2015. All rights reserved.

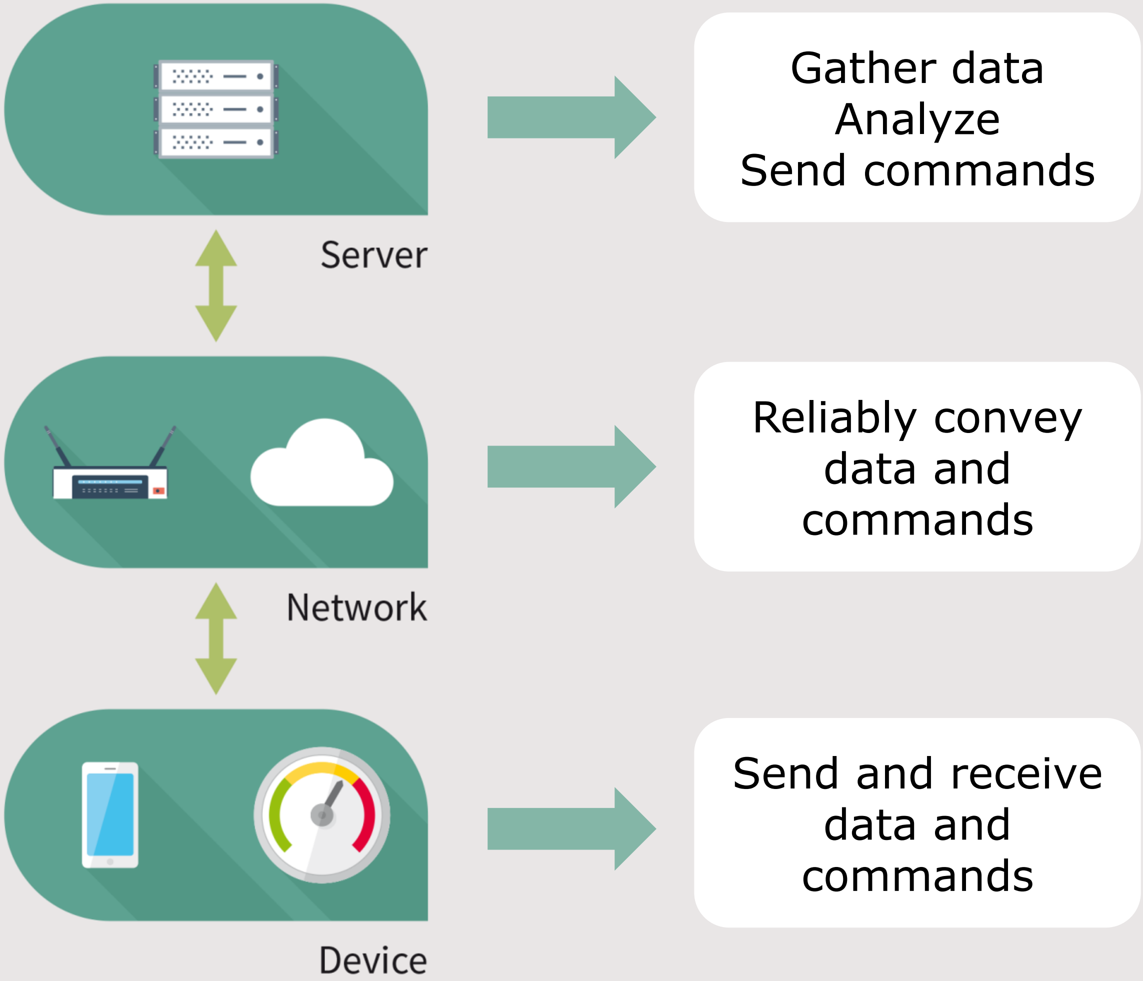
IoT Trend Affects All Markets

Consumer	Mobility	Energy	Industry & Logistics	ICT	Healthcare	Others
Smart Home	Cars	Solar PV	Industrial Motor Controls & Drives	Data Centers	Medical Equipment	Advertising
Major Home Appliances	Trucks & Buses	Wind Power	Automation Equipment	Cellular Networks	Assisted Living	Retail
Small Home Appliances	Construction Agricultural Vehicles	Other Power Generation	Building Automation	Other WAN	Lifestyle	Gambling
Consumer Electronics (incl. Wearables)	Traction	Energy Storage Systems	Logistics	Wireless LAN & PAN		Defense
Lighting	Light Electric Vehicles	Transmission & Distribution				Aerospace
Smartcards		Smart Meters				
Smartphones & Tablets		Charging Stations				
Desktops & Notebooks						

Copyright © Infineon Technologies AG 2015. All rights reserved.

IoT Has Many Layers

IoT Architecture



Gather data
Analyze
Send commands

Reliably convey data and commands

Send and receive data and commands

Copyright © Infineon Technologies AG 2015. All rights reserved.

Agenda

1 Introduction to IoT

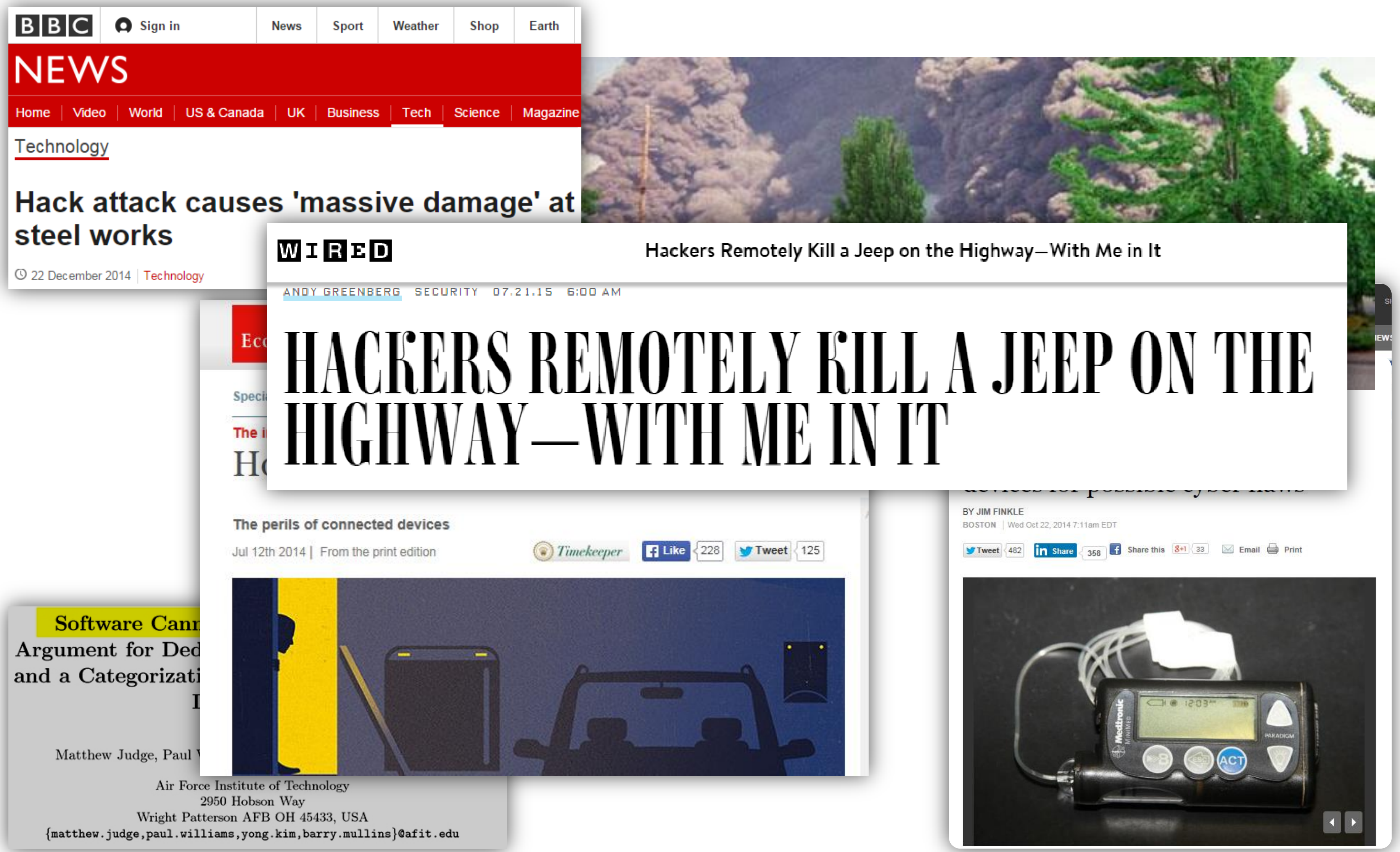
2 Risk Analysis

3 Countermeasures

4 Into the Future

Copyright © Infineon Technologies AG 2015. All rights reserved.

IoT Attacks Growing



BBC Sign in | News | Sport | Weather | Shop | Earth

NEWS

Home | Video | World | US & Canada | UK | Business | Tech | Science | Magazine

Technology

Hack attack causes 'massive damage' at steel works

22 December 2014 | Technology

WIRED Hackers Remotely Kill a Jeep on the Highway—With Me in It

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Ec

Speci

The i

H

The perils of connected devices

Jul 12th 2014 | From the print edition

Timekeeper Like 228 Tweet 125

devices for possible cyber flaws

BY JIM FINKLE

BOSTON | Wed Oct 22, 2014 7:11am EDT

Tweet 482 | Share 358 | Share this | 8+1 33 | Email | Print

Software Cann

Argument for Ded

and a Categorizati

I

Matthew Judge, Paul W

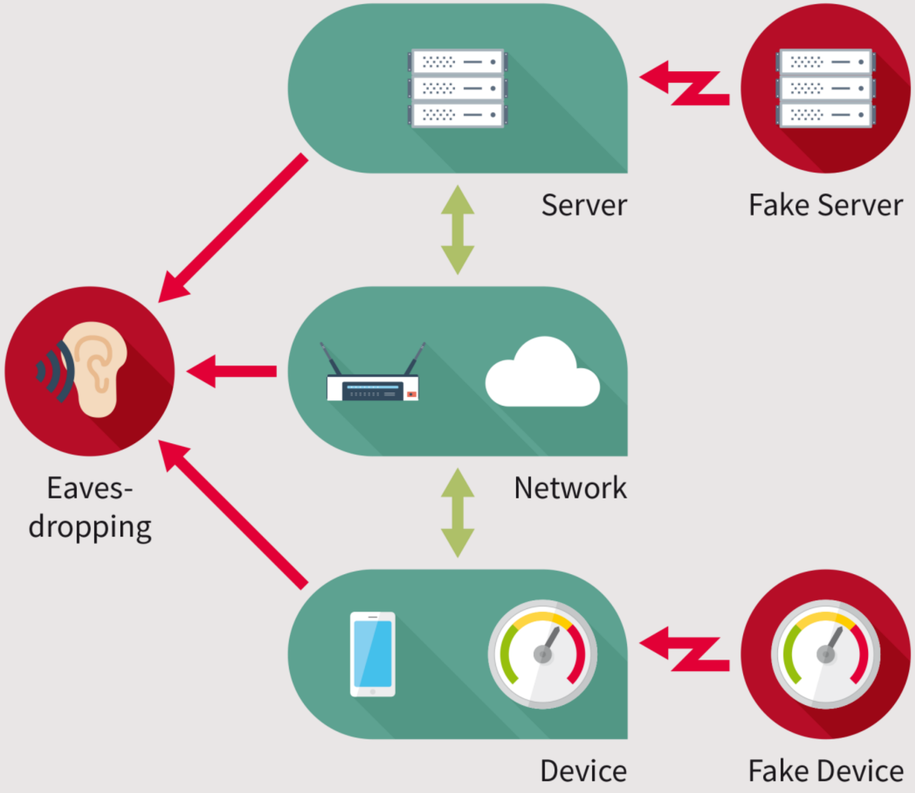
Air Force Institute of Technology
2950 Hobson Way
Wright Patterson AFB OH 45433, USA
{matthew.judge,paul.williams,yong.kim,barry.mullins}@afit.edu

Copyright © Infineon Technologies AG 2015. All rights reserved.

Each Layer can be Attacked

Security threats for IoT

An **Eavesdropper** listening in on data or commands can reveal confidential information about the operation of the infrastructure.



A **Fake Server** sending incorrect commands can be used to trigger unplanned events, to send some physical resource (water, oil, electricity, etc.) to an unplanned destination, and so forth.

A **Fake Device** injecting fake measurements can disrupt the control processes and cause them to react inappropriately or dangerously, or can be used to mask physical attacks.

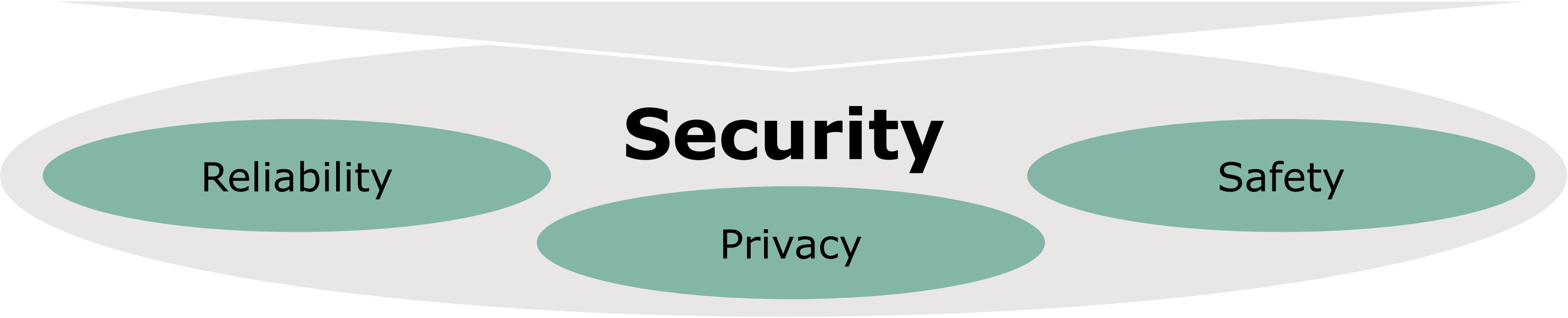
Copyright © Infineon Technologies AG 2015. All rights reserved.

Protecting Our Values with IoT Security

- Provide safety and privacy
- Maximize uptime
- Protect revenue stream

- Enable and create business models
- Differentiate from competition

- Reduce costs
- Increase quality and reliability



Copyright © Infineon Technologies AG 2015. All rights reserved.

1 Introduction to IoT

2 Risk Analysis

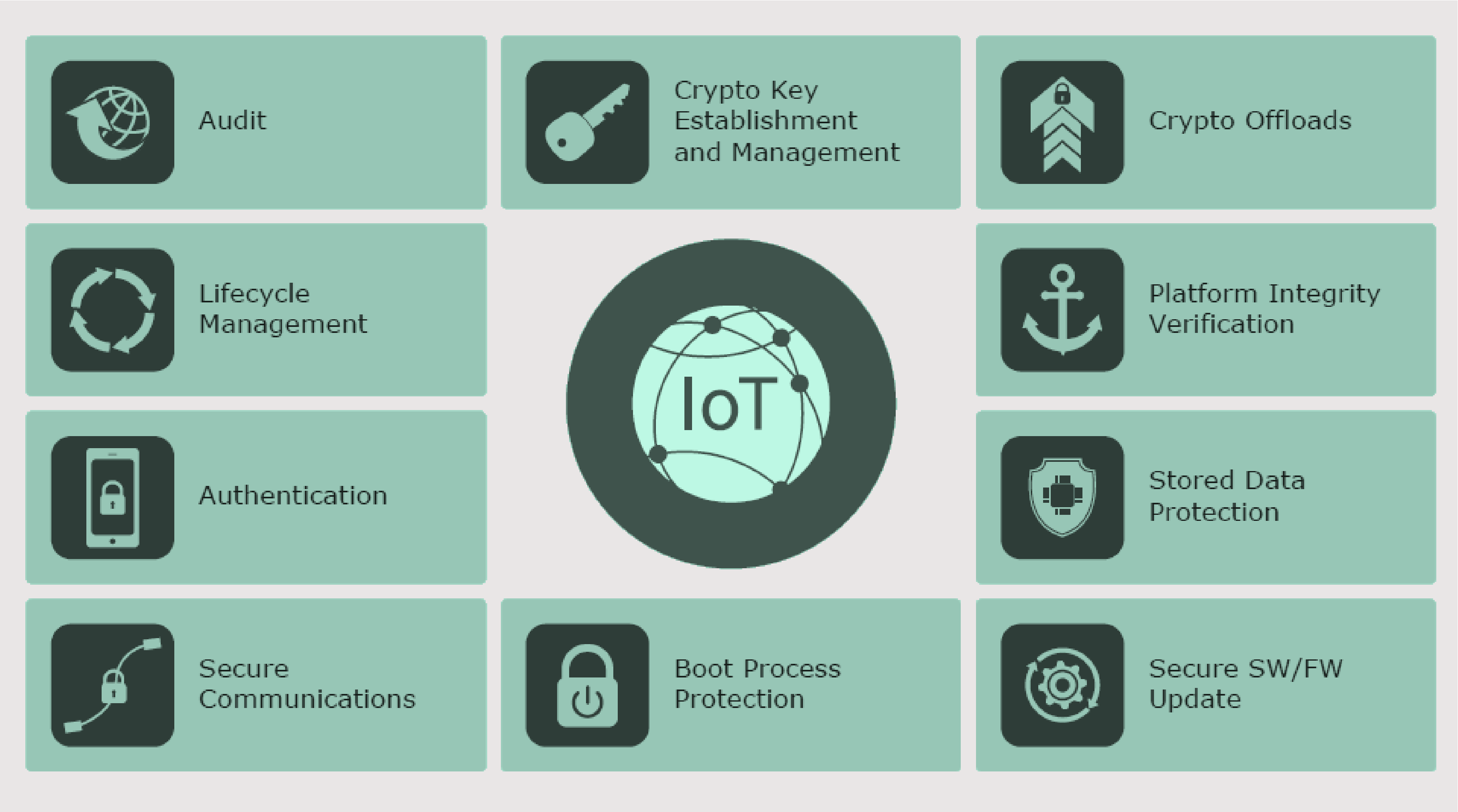
3 Countermeasures

4 Into the Future

Copyright © Infineon Technologies AG 2015. All rights reserved.

IoT Defenses

Common Defenses



Audit

Crypto Key Establishment and Management

Crypto Offloads

Lifecycle Management

Platform Integrity Verification

Authentication

Stored Data Protection

Secure Communications

Boot Process Protection

Secure SW/FW Update

Copyright © Infineon Technologies AG 2015. All rights reserved.

Bad-Better-Best: Options for IoT Security

No Security

Everything open for all to see

Software Only

Secures against casual intrusion and basic software attacks

Hardware Security

Secures against hardware attacks and hardens against software attacks

Reading	Software code easily readable by hackers	Hardware chip protects itself against code reading
Copying	Software code easily copied and shared by hackers	Secure hardware cannot be easily copied. Must be extensively reverse engineered and remanufactured.
Analyzing	Software code easily analyzed and understood using standard tools	Secure hardware use proprietary designs and non-standard code that is not easily understood
Root of Trust	Software has no "Root of Trust", recovery of broken system practically impossible	Secure hardware provides "Root of Trust" anchor for system, providing detection, recoverability, secured updates

Copyright © Infineon Technologies AG 2015. All rights reserved.

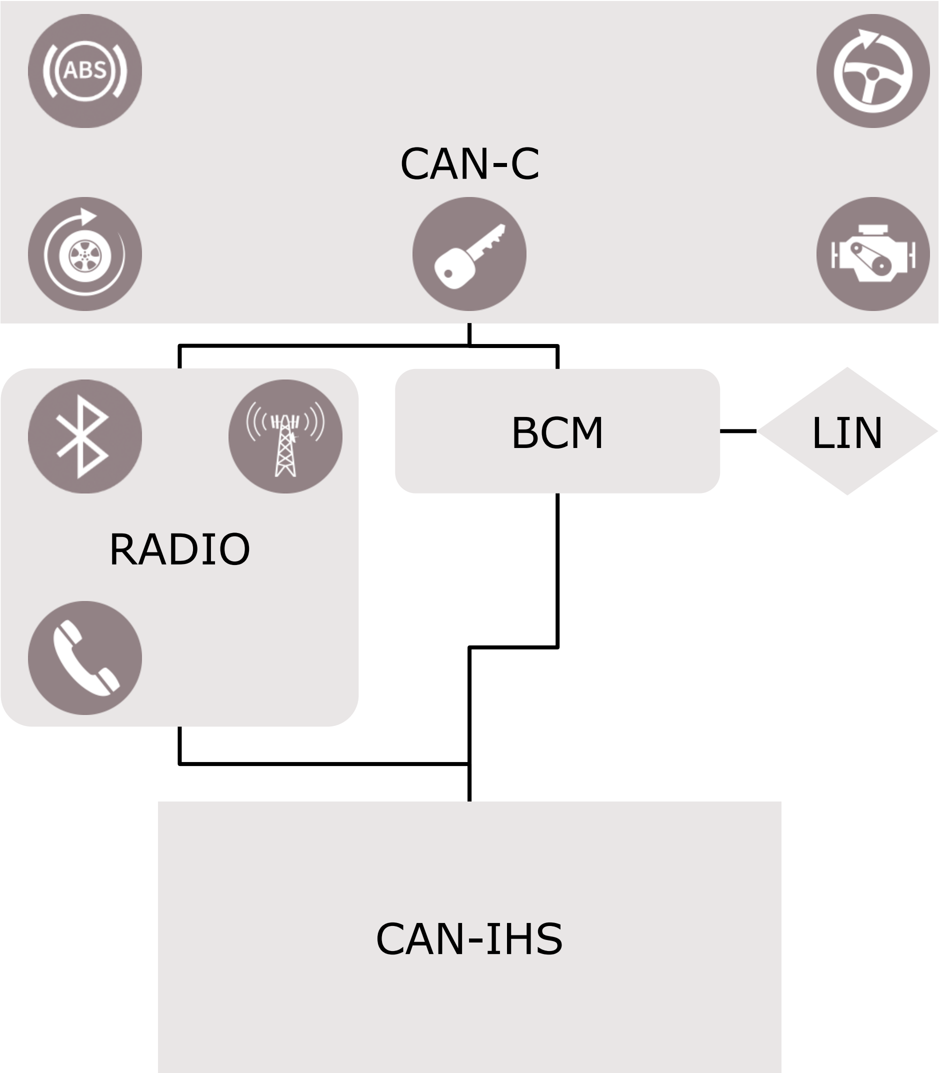
Miller & Valasek:
A Case Study in IoT Hacking

Miller & Valasek Attack Process

1. Evaluate Attack Surface
2. Investigate Potential Targets
3. Reverse Engineer Targets
4. Find Vulnerabilities
5. Develop Exploits
6. Use Exploits to Get New Targets

Countermeasures

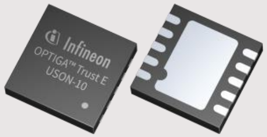
1. Adopt Secure Development Lifecycle
2. Develop Thorough Attack Tree
3. Prevent Reverse Engineering
4. Reduce Vulnerabilities
5. Detect and Respond to Attacks
6. Employ Layered Defenses



Source: Remote Exploitation of an Unaltered Passenger Vehicle, Miller & Valasek, 2015. http://illmatics.com/Remote%20Car%20Hacking.pdf

Copyright © Infineon Technologies AG 2015. All rights reserved.

Scalable Trust Anchors for IoT

	OPTIGA™ Trust	OPTIGA™ Trust E	OPTIGA™ Trust P	OPTIGA™ TPM
				
Security Level	+	+++	CC EAL 5+	CC EAL 4+
Design-in complexity	low	low	medium	medium
Feature set	Authentication	PKI-supported Authentication	Programmable	TPM standard
Personalization (loading of keys and certificates)	✓	✓	✓	✓

Security and Complexity

Copyright © Infineon Technologies AG 2015. All rights reserved.

1 Introduction to IoT

2 Risk Analysis

3 Countermeasures

4 Into the Future

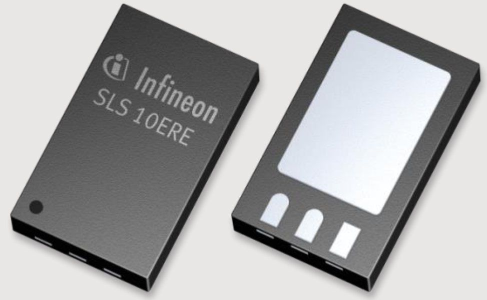
Copyright © Infineon Technologies AG 2015. All rights reserved.

Likely Future Developments in IoT Security

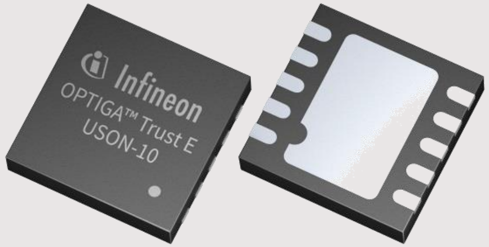
- **Additional functionality**
  - Expanded security features
  - Expanded cryptographic algorithms
- **Tighter integration with IoT systems**
  - Hardware Root of Trust standard in all IoT systems
    - As today for IT and payment
- **Growing external requirements for stronger security**
  - Regulations, insurance, etc.
- **Continuing exploitation and damage**

Copyright © Infineon Technologies AG 2015. All rights reserved.

Summary



IoT shows tremendous promise. ✓



To protect our values, strong IoT security is needed. ✓

Scalable Hardware Trust Anchors provide the Right Security for IoT. ✓

Copyright © Infineon Technologies AG 2015. All rights reserved.

Part of your life. Part of tomorrow.