

What's The Right Security for IoT?

Infineon Technologies AG
February 2017



Agenda

1

Introduction to IoT

2

Risk Analysis

3

Countermeasures

4

Into the Future

Agenda

1

Introduction to IoT

2

Risk Analysis

3

Countermeasures

4

Into the Future

What is IoT?

Definition



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

IoT is Growing Fast

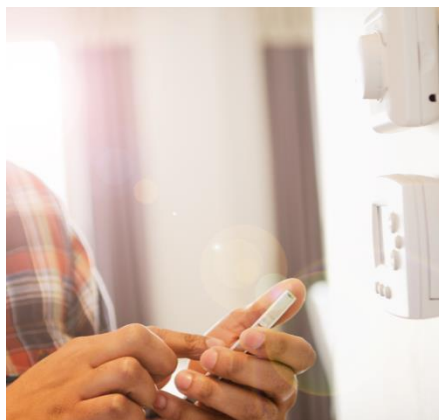


Why IoT?

Automotive



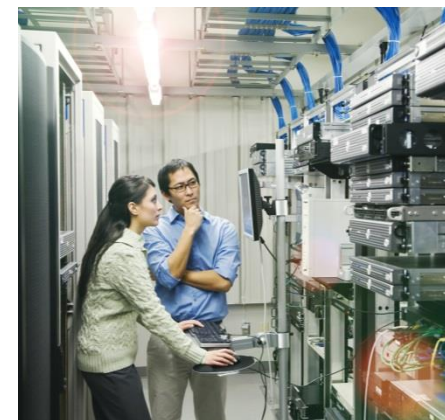
Smart Home



Industrial



ICT

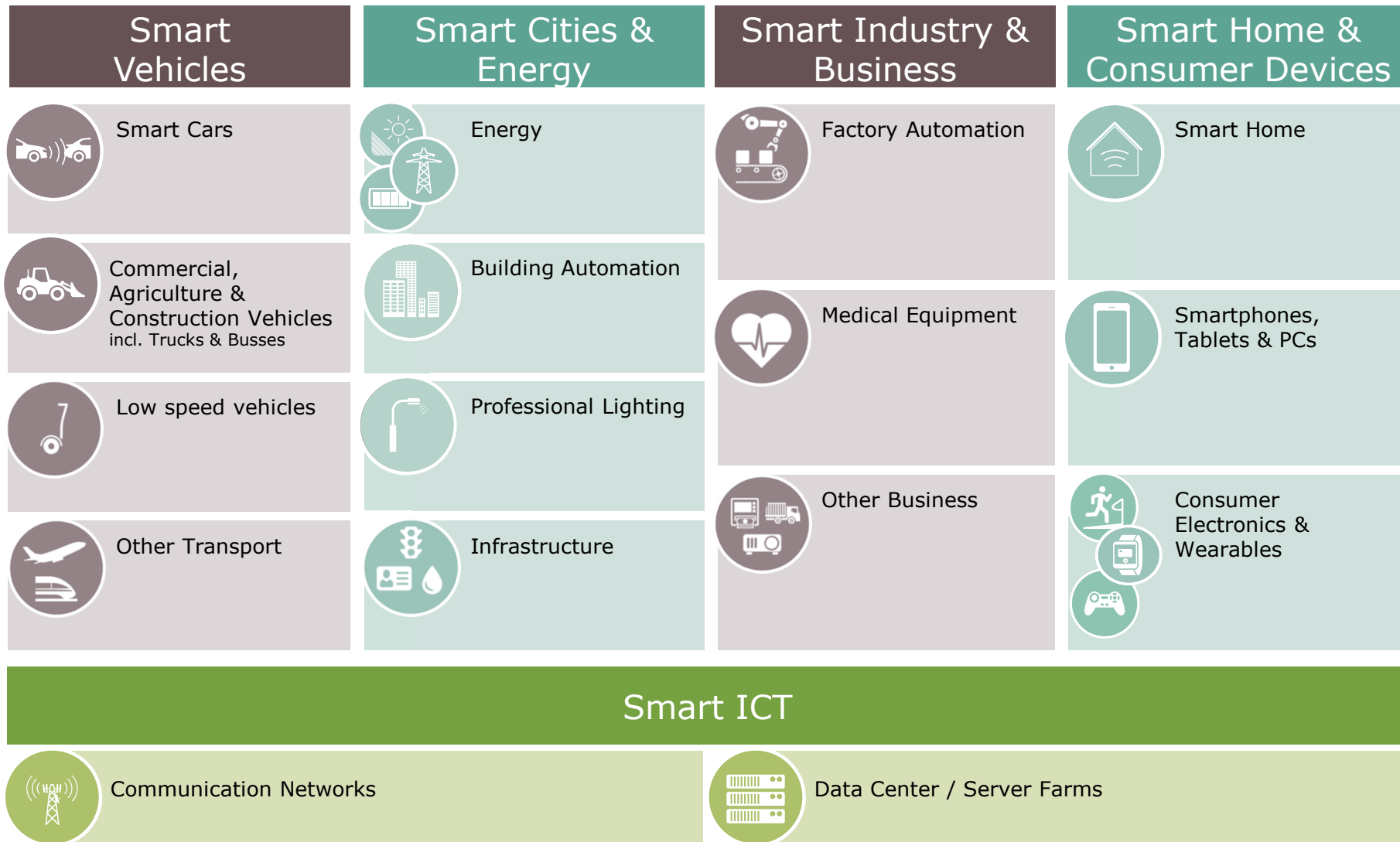


1 New capabilities and services

2 Greater efficiency

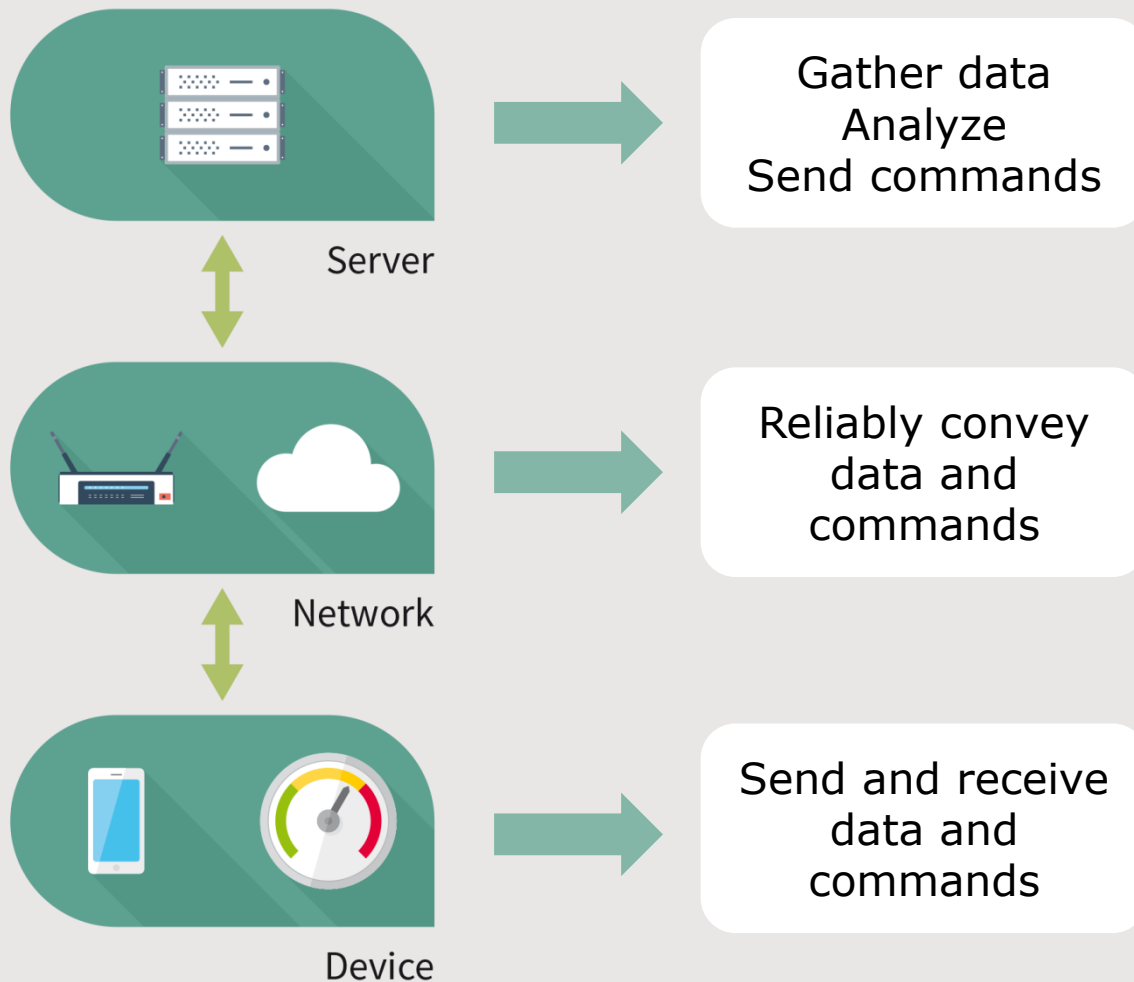
3 Increased flexibility and customization

IoT Trend Affects All Markets



How Does IoT Work?

IoT Architecture



Agenda

1

Introduction to IoT

2

Risk Analysis

3

Countermeasures

4

Into the Future

IoT Attacks Growing



NEWS

Home | Video | World | US & Canada | UK | E

Technology

Hack attack causes 'major disruption' at steel works

22 December 2014 | Technology



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

HOME ABOUT ICSJWG INFORMATION PRODUCTS TRAINING FAQ

Control Systems

Home

Alert (IR-ALERT-H-16-056-01)

Cyber-Attack Against Ukrainian Critical Infrastructure

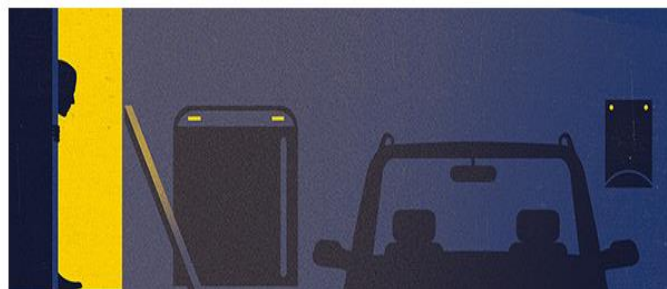
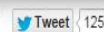
Original release date: February 25, 2016

Home,

HIGHWAY—WITH ME IN IT

The perils of co

Jul 12th 2014 | From the print edition



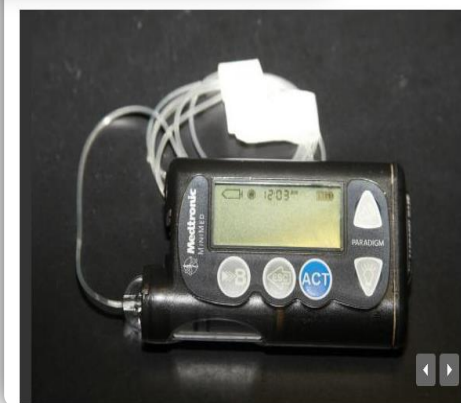
Fridge cyber attack

In the first documented attack of its kind, the Internet of Things has been used as part of an attack that sent out over 750,000 spam emails.

the Highway—With Me in It

A JEEP ON THE

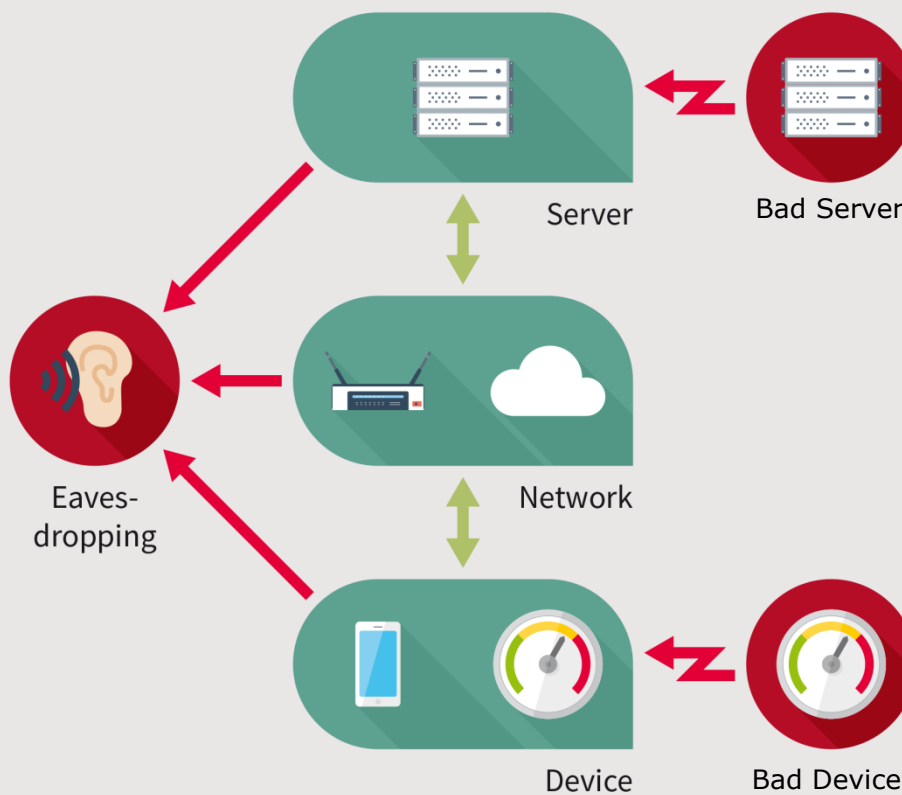
Print



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 **Bad 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 **Bad 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.*

Top Challenges for IoT Adopters



1

Cybersecurity

2

Integration

3

Managing business requirements

Source: Gartner survey results, March 3, 2016
<http://www.gartner.com/newsroom/id/3236718>

Value Proposition for IoT Security



- › Maximize uptime, reliability, and quality
- › Ensure customer satisfaction
- › Reduce support costs



- › Promote safety and reduce risk
- › Protect private and confidential data
- › Avoid damage to brand



- › Maintain steady ongoing revenue stream
- › Enable and create new business models
- › Differentiate from competition



Agenda

1

Introduction to IoT

2

Risk Analysis

3

Countermeasures

4

Into the Future

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

Bad-Better-Best: Options for IoT Security



	<div> <div>Main CPU</div> <div>Software</div> </div>	<div> <div>Main CPU</div> <div>Software</div> <div>Hardware</div> </div>
Crypto functionality	✓	✓
Strong isolation	—	✓
Security certified	—	✓
Tamper resistant	—	✓
Manufactured by security certified processes	—	✓
Resistant against IP Theft	—	✓

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

Note: ● basic | ● ● ● advanced

Agenda

1

Introduction to IoT

2

Risk Analysis

3

Countermeasures

4

Into the Future

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

Summary



IoT shows tremendous promise.



To protect our values, strong IoT security is needed.



Scalable Hardware Trust Anchors provide the Right Security for IoT.





Part of your life. Part of tomorrow.

