

What's The Right Security for IoT?

Juergen Spaenkuch
Division VP
Chip Card & Security
Infineon Technologies AG



Agenda

Introduction to IoT

Risk Analysis

Countermeasures

Into the Future

Agenda

Introduction to IoT

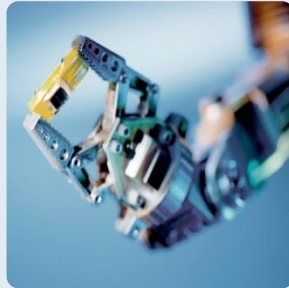
Risk Analysis

Countermeasures

Into the Future

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

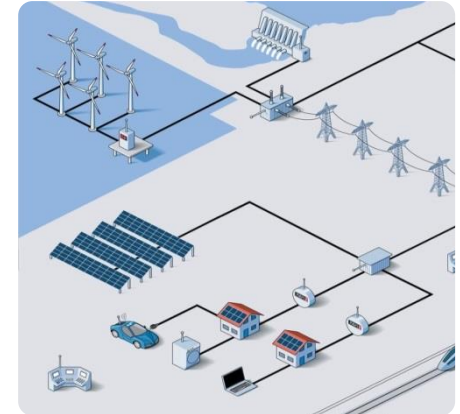
Internet of Things (IoT) Drives Increased Profits

Smart Home

Automotive

Industrial

Critical
Infrastructure



1

New capabilities and services





































2

Greater efficiency

3

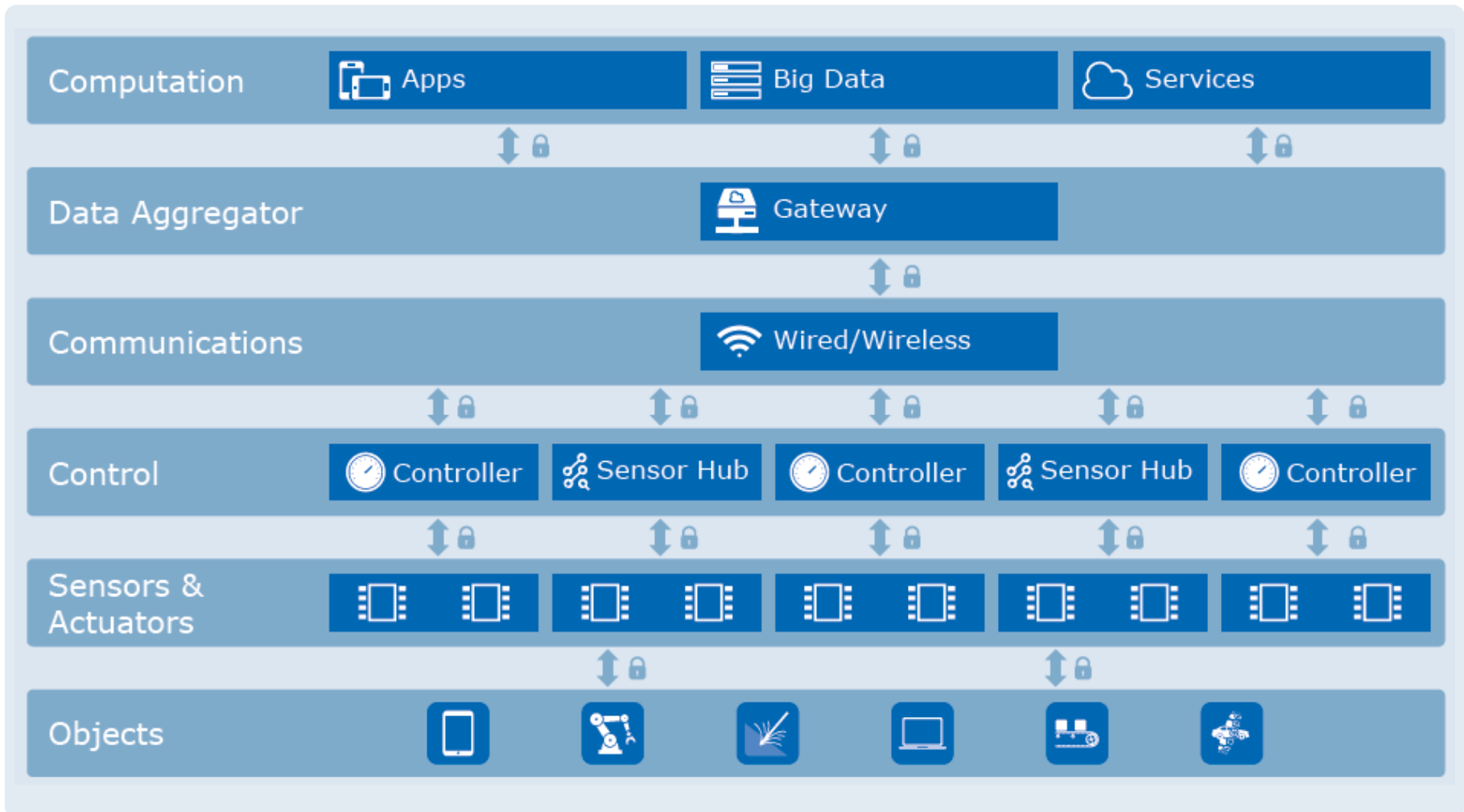
Increased flexibility and customization

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 						

IoT Has Many Layers

IoT Architecture



Agenda

Introduction to IoT

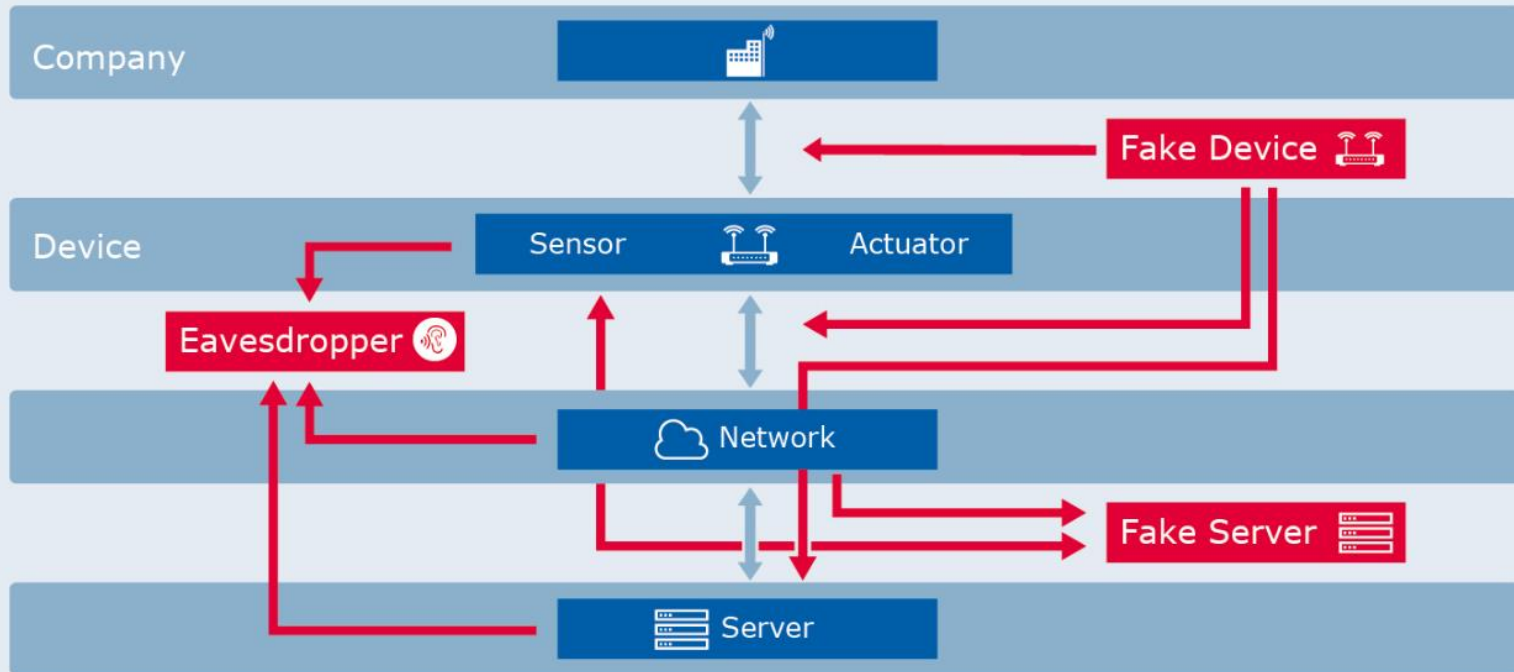
Risk Analysis

Countermeasures

Into the Future

Each Layer can be Attacked

Security threats for IoT



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

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.*

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.

*) Note: Fake Server sending incorrect commands can be used to unlock doors, handle chemicals incorrectly, disable car brakes, or trigger other unplanned events

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

NETWORKWORLD Most read:      

f5 Protecting Against Online Banking Fraud [More +](#)

Home > Security

Expert: Basic hacks can compromise industrial control systems

Threat of such attacks is up, but defenses lag

RELATED

The Economist World politics Business & finance Economics Science & technology Culture

Special report: Cyber-security

The internet of things

Home, hacked home

The perils of connected devices

Jul 12th 2014 | From the print edition

  228  125



REUTERS EDITION: U.S.        

U.S. government probes medical devices for possible cyber flaws

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

 452  358  Share this  Email  Print



Software Can
Argument for Dec
and a Categorizat

Matthew Judge, Paul

Air Force Institute of Technology
2950 Hobson Way

Wright Patterson AFB OH 45433, USA

{matthew.judge,paul.williams,yong.kim,barry.mullins}@afit.edu

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



Agenda

Introduction to IoT

Risk Analysis

Countermeasures

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



No SECURITY

Everything open
for all to see

Reading

Copying

Analyzing

Root of Trust



SOFTWARE ONLY

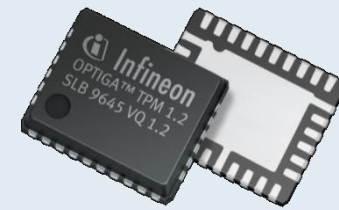
Secures against casual
intrusion and basic software
attacks

Software code easily readable by
hackers

Software code easily copied and
shared by hackers

Software code easily analyzed
and understood using standard
tools

Software has no "Root of Trust",
recovery of broken system
practically impossible



HARDWARE SECURITY

Secures against hardware
attacks and hardens against
software attacks

Hardware chip protects itself
against code reading

Secure hardware cannot be
easily copied. Must be
extensively reverse engineered
and remanufactured.

Secure hardware use proprietary
designs and non-standard code
that is not easily understood

Secure hardware provides "Root
of Trust" anchor for system,
providing detection,
recoverability, secured updates

Overall Security Architecture: Inside the Car & by Controlled Interfaces to the Outside World



Secure Application Microcontrollers and Secure Elements are the foundations to System Security



- **Security by design** (proven, open cryptography) vs. obfuscation
- **Hardware-based security** to ensure performance and tamper-proof

Secure Application Microcontrollers

- Application microcontroller with embedded security functions
- **Security tailored to application needs**
- Can be combined with secure elements

Example:

AURIX™ for secure communication in automotive and industry

Industrial equipment to be secured



Secure Elements

- Dedicated secure element alongside the application microcontroller
- **Serves as an anchor of trust**
- Eased implementation in legacy architectures

Example:

OPTIGA™ for authentication and secure boot

Agenda

The background of the slide features a light blue world map. Overlaid on the map are several semi-transparent icons: a car labeled "MOBILITY" in the upper center, a factory labeled "INDUSTRIAL" on the left, a smartphone labeled "BUILDINGS" on the right, and a server rack at the bottom center. A network of lines connects these icons, suggesting global connectivity.

Introduction to IoT

Risk Analysis

Countermeasures

Into the Future

Likely Future Developments in IoT Security

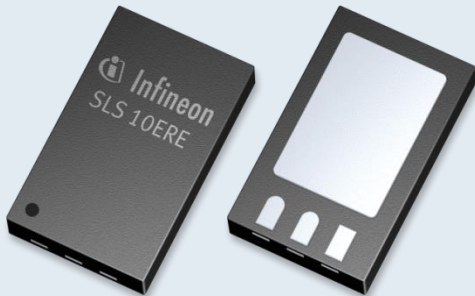
- Additional functionality
 - Expanded security features
 - Expanded cryptographic algorithms

- Tighter integration with industrial systems
 - Hardware Root of Trust standard in all IoT systems
 - As today for IT and payment

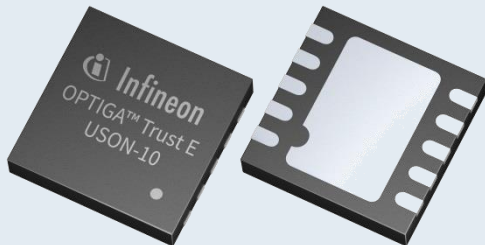
- Growing external requirements for stronger security
 - Regulations, insurance, etc.

- 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.



Infineon: Your partner of choice when it comes to the right security for IoT



We have shipped more than 20 billion security controllers worldwide

Four in every ten payment cards issued in 2014 have Infineon security chips inside

We power IDs in 61 countries representing 75% of the world's population

We pioneered and are the absolute leader in cellular machine-to-machine

Every second business laptop with Trusted Platforms Module (TPM) is from Infineon





ENERGY EFFICIENCY MOBILITY SECURITY

Innovative semiconductor solutions for energy efficiency, mobility and security.

