SECURITY & PRIVACY IN CONNECTED INDUSTRY 4.0 MANUFACTURING FACILITIES

ABOUT THE NECESSITY TO GENERATE TRUST IN IOT

MARC GEBERT
SENIOR DIRECTOR
BUSINESS DEVELOPMENT

APRIL 27TH, 2017

NXP

SECURE CONNECTIONS FOR A SMARTER WORLD

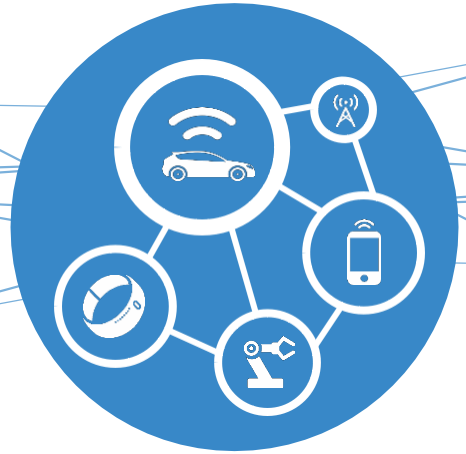
Secure Connections for the Smarter World

Everything **Smart**

40B+ devices with intelligence shipped in 2020

Processing

Everything **Connected**



1B+ additional consumers online, 30B+ connected devices

Connectivity

Everything **Secure**

Potential economy savings up to half trillion dollars

Security

Automotive | Industrial | Connected Devices | IoT

About NXP

- ✓ **#1** Automotive
- ✓ **#1** Broad-Based MCUs[1]
- ✓ **#1** Secure Identification
- ✓ **#1** Communications Processors
- ✓ **#1** RF Power Transistors
- ✓ **#1** Small Signal Discretes

- ✓ **5th Largest** semiconductor company[2]
- ✓ **45,000** employees
- ✓ **11,000** engineers
- ✓ **9,000** patent families
- ✓ **50+** year history
- ✓ **$9.8B** annual revenue[3]

Sources for market data: HIS, ABI Research, Strategy Analytics, The Linley Group

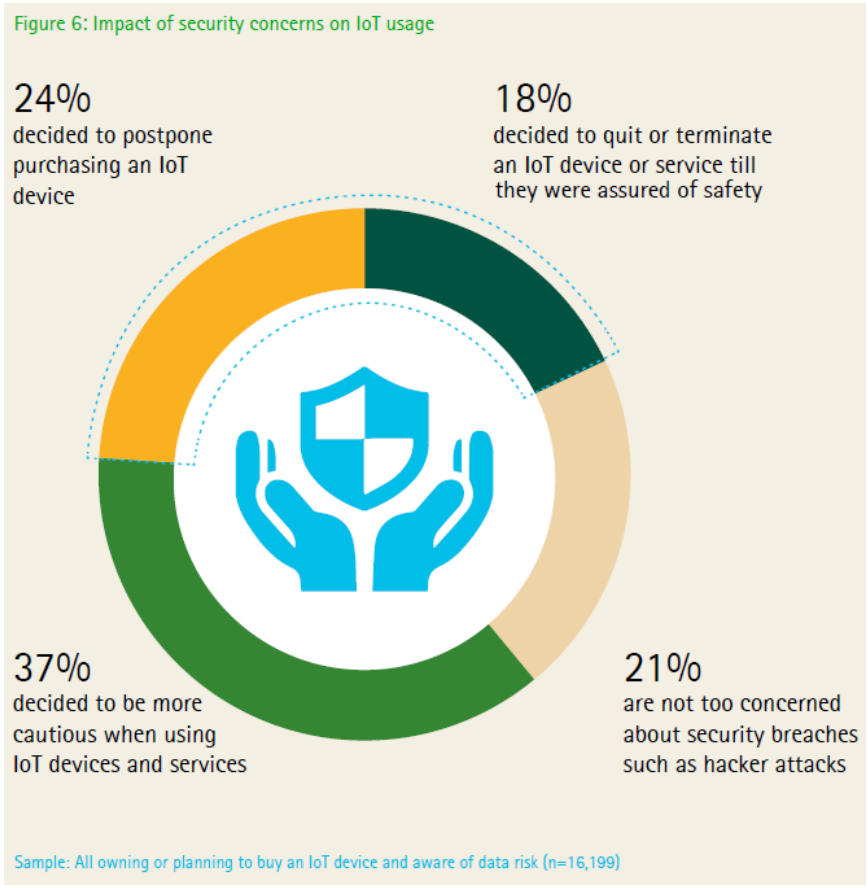
[1]MCU market excluding Automotive
[2]Excludes memory
[3]Pro forma revenue resulting from Dec 2015 acquisition of Freescale Semiconductor and Nov 2015 divestiture of Bipolar Power business

WHY TRUST IS KEY IN IOT

IoT Security generating Trust is key for market adoption

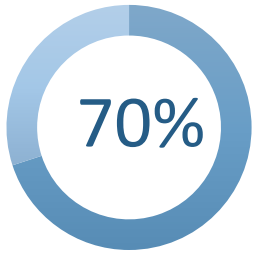
47%

Of consumers cites
“privacy risk/ security concerns”
as a barrier to adoption

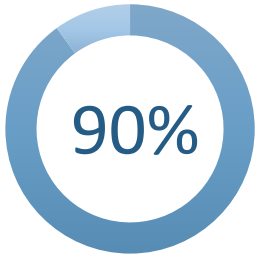


Source: Accenture, 2016

Can we really trust IoT devices…?



of the most commonly used IoT devices contain vulnerabilities (Ernst & Young, HP).



of devices along with their Cloud and mobile applications components failed to require passwords of a sufficient complexity and length

300%

increase of mobile malware in 2015 from 2014

Default passwords – Online attacks

Emergent Tech ▸ Internet of Things

152k cameras in 990Gbps record-breaking DDoS

Hacked low-powered cameras and internet-of-things things

The Register

Security

No wonder we're being hit by Internet of Things botnets. Ever tried patching a Thing?

Emergent Tech ▸ Internet of Things

Sweet, vulnerable IoT devices compromised 6 min after going online

BBC

Technology

'Smart' home devices used as weapons in website attack

Share

22 October 2016 | Technology

Key management - where physical hacking pays off

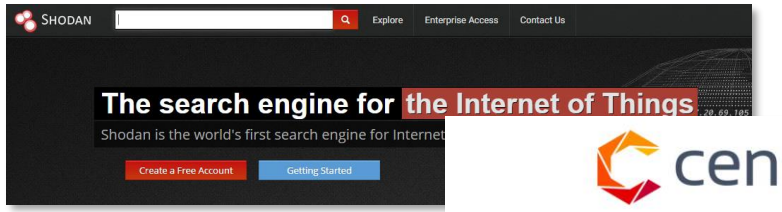
Petcube Remote Wireless Pet Camera Vulnerabilities

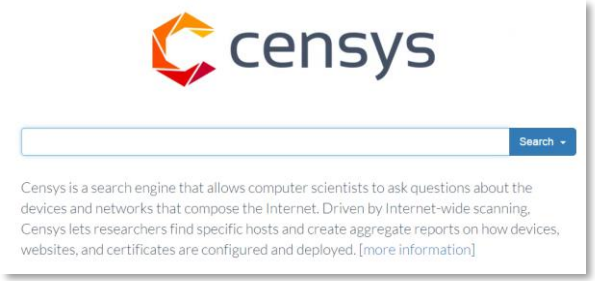
The security and privacy of Petcube users could be compromised through unauthorized access.

IOActive

Millions of IoT Devices Using Same Hard-Coded CRYPTO Keys

… and other online vulnerabilities



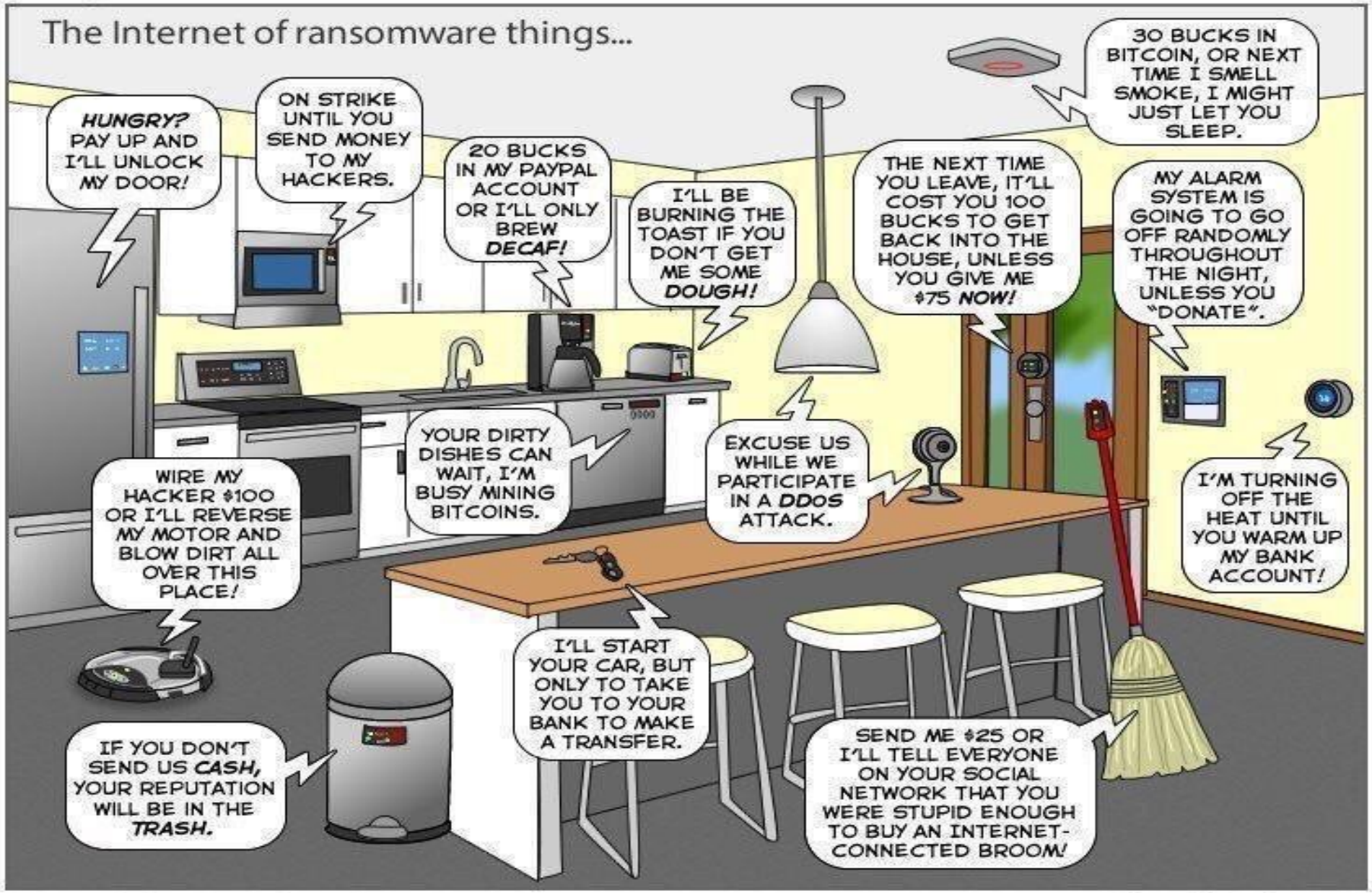


Local (network) attacks - Personal interests

Wi-Fi baby heart monitor may have the worst IoT security of 2016

NXP

The Joy of Tech™ by Nitrozac & Snaggy

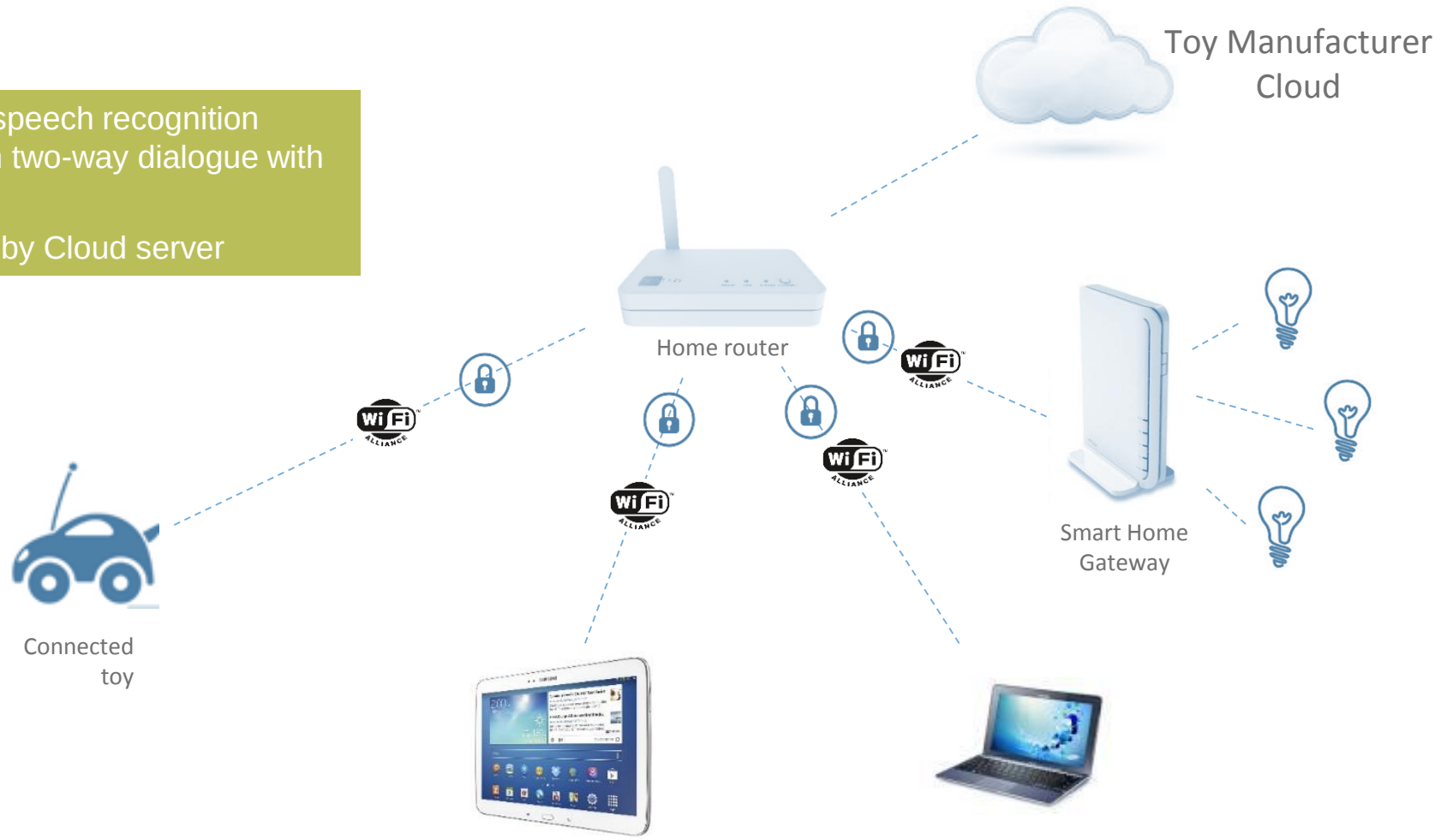


You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com

A Single Device can compromise your Privacy

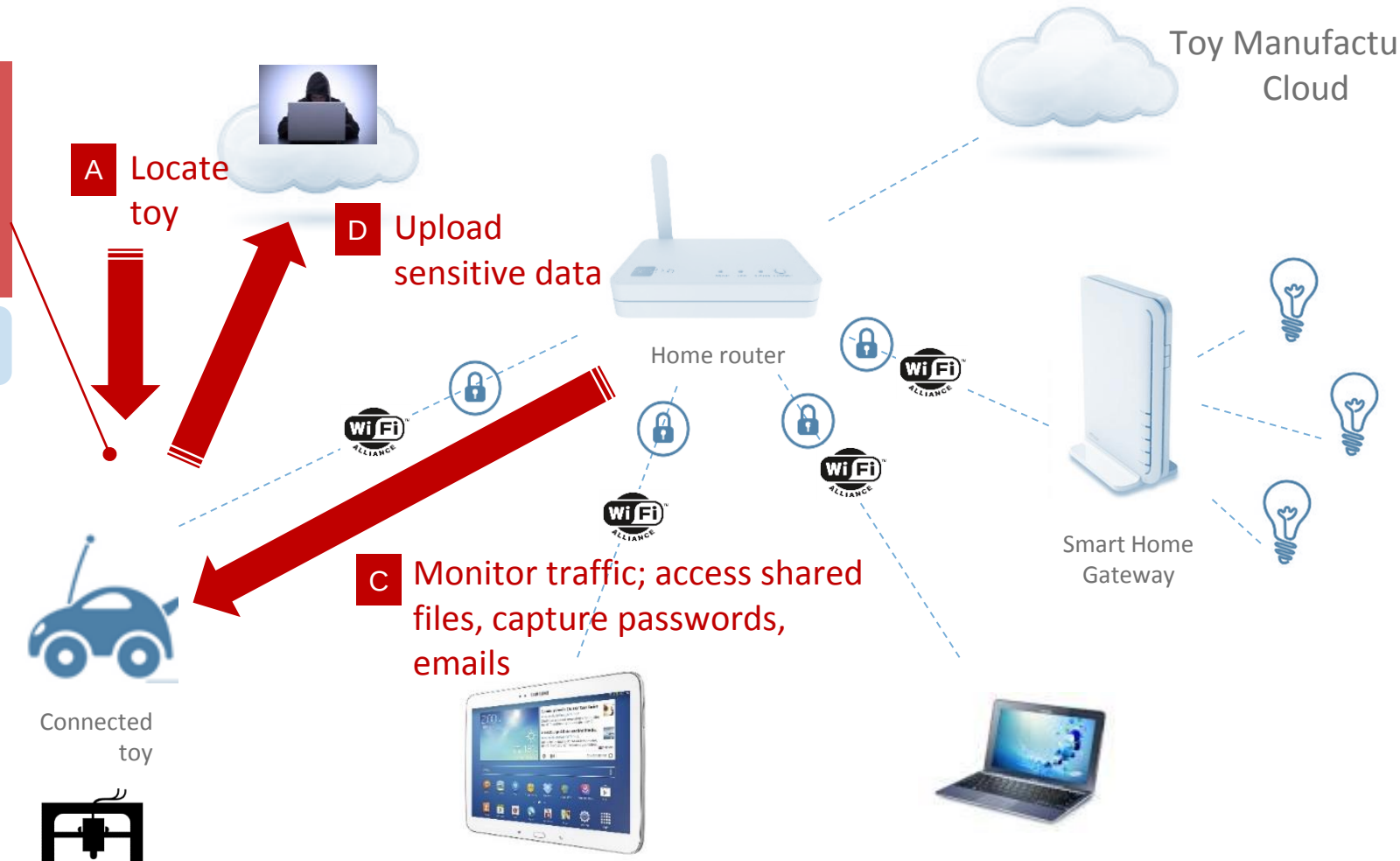
- The toy uses WiFi and speech recognition technology to engage in two-way dialogue with the child
- The response is issued by Cloud server



A Single Device can compromise your Privacy

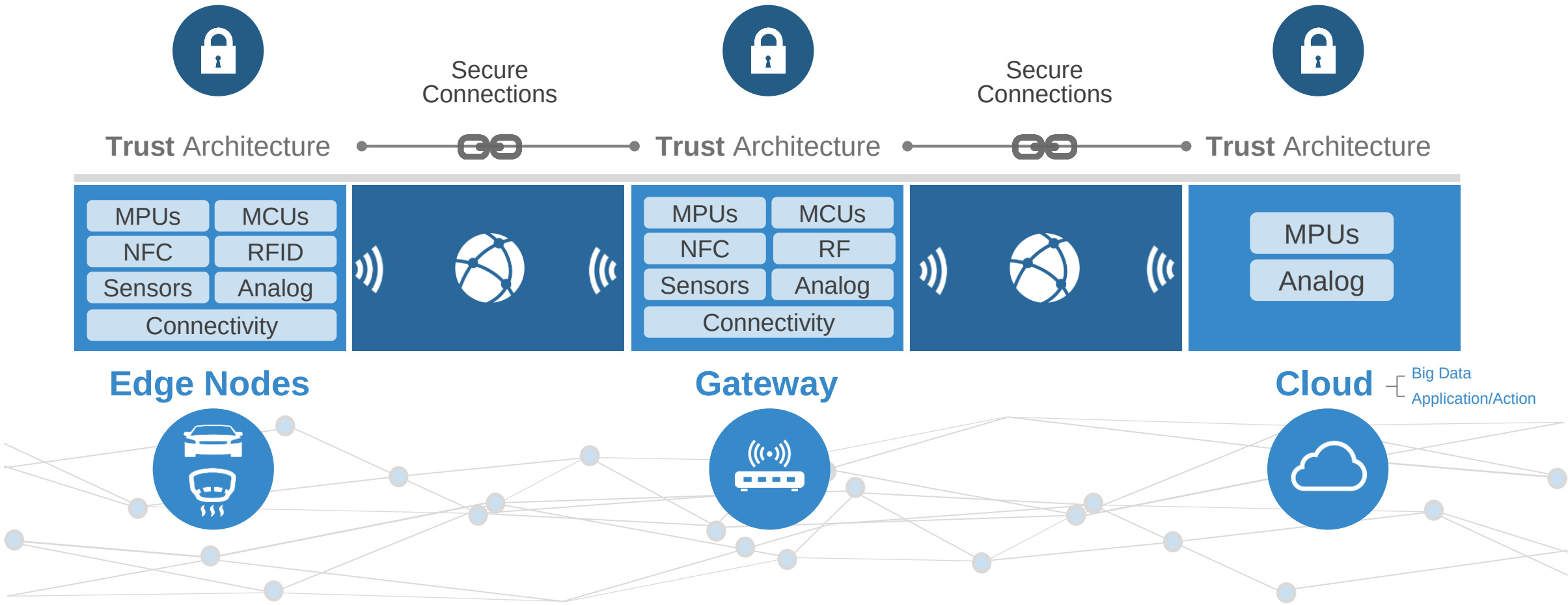
Attack:
Compromise connected toy by installing malware or reflashing firmware that monitors traffic and uploads data to attacker's server

Special equipment required to replicate attack ○○○



CYBERSECURITY = TRUST

IOT NEEDS A SECURE AND DYNAMIC NETWORK



Key Applications with Security as a MUST

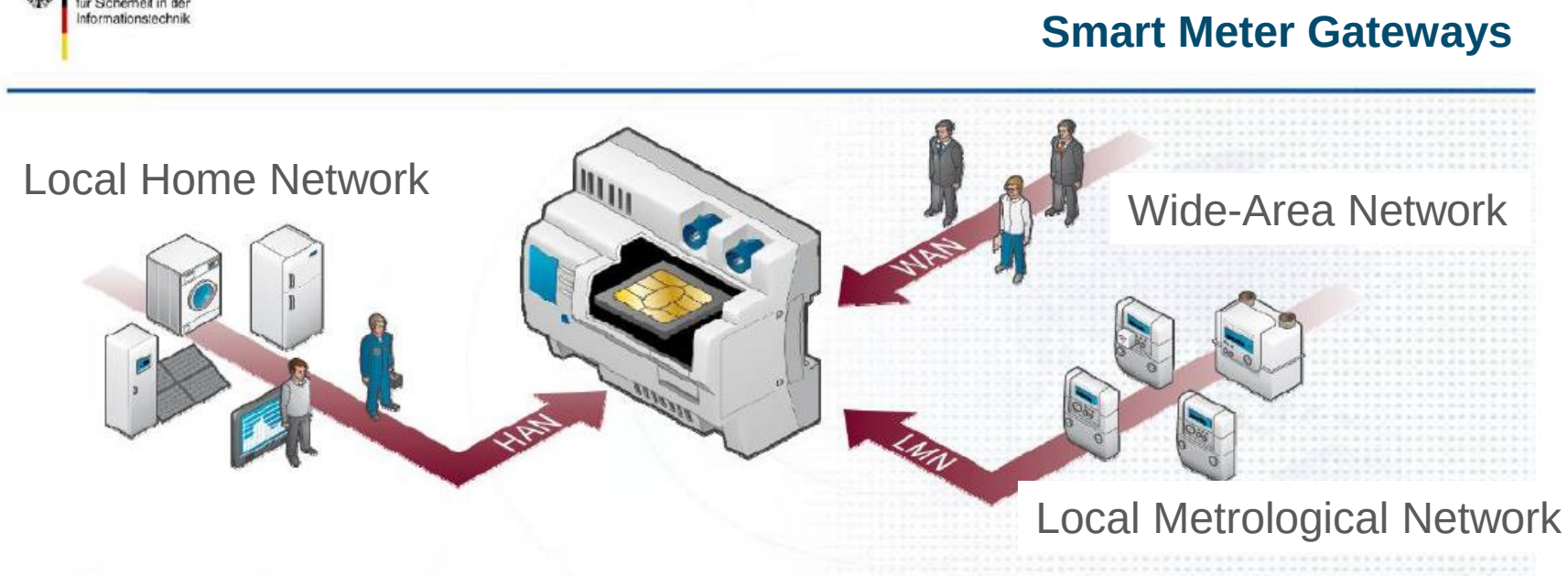
- **Energy Management / Smart Grid**
  - Smart Home Appliances, smart Plugs
  - Residential & Industrial Meters
  - Metering Gateways
  - Home & Building Automation systems
  - Grid Automation
  - Data concentrators, routers
  - Electrical & Hybrid Vehicles
  - (H)EV Charging Stations, batteries
  - Street Lighting, Solar panels
- **Industrial**
  - PLC, RTUs, IED, Industrial equipment & parts, remote monitoring systems
- **Medical & Healthcare**
  - Home care/monitoring Gateways
  - Medical Devices
  - Traceability solutions
- **Transport**
  - ITS (car2car), Telematics
  - Infrastructure networks, Tolling
- **Vending**
  - PoS terminals, ATMs
- **Smart Applications/Services**
  - IP cameras, sensors, Smart Cities, Smart Homes, Automation systems, etc
- **Security Systems**
  - Authentication tokens, access control systems, biometric controls, etc

SECURE CONNECTIONS
FOR A SMARTER WORLD

SECURITY SOLUTIONS IN SMART METERING

Role of the German Smart Meter Gateway

Bundesamt für Sicherheit in der Informationstechnik



Secure communication platform for Smart Grid

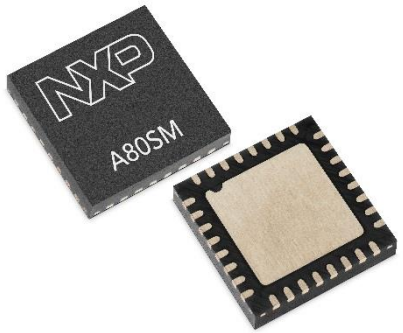
- Consumption transparency and secure transmission of measured data
- Control of consumer devices and production equipment

Source: BSI

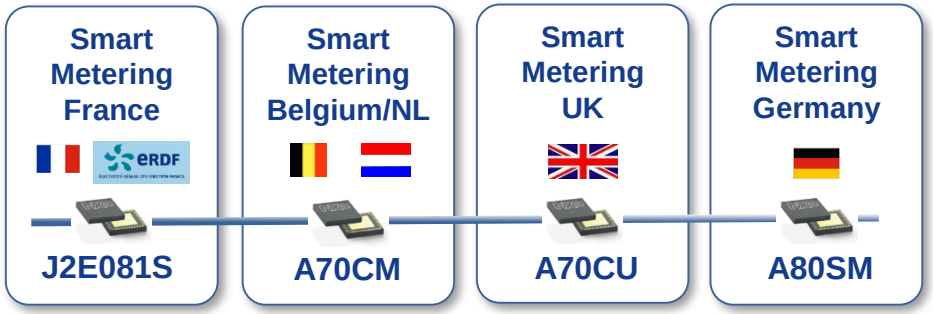
NXP A80SM Security Module

Certified by BSI and Available

Bundesamt
für Sicherheit in der
Informationstechnik



Common Criteria



- **The Key component** required to rollout Smart Metering Gateways and enable field trials **now available**!

SECURE CONNECTIONS
FOR A SMARTER WORLD

NXP receives Cyber Security Award

At Smart Metering Europe Summit 2014, London

Were part of the judging panel: the European Network for Cyber Security (ENCS), the European Smart Metering Industry Group (ESMIG), as well as several energy companies including RWE npower, Endesa, EDF Energy, Red Electrica.

"The winning company is supporting the delivery of next generation security architectures by exploiting recent innovations and developing adaptive platforms which evolve to meet the challenge of more sophisticated Cyber Security threats" said the jury.

And the jury to add: *"The winning choice is a provider which* ***takes the security responsibility of the shoulders of the smart meter manufacturers****, and* ***provides a building block that can be integrated into the smart meters to provide a large part of the security functionality****"*

GENERAL DATAPROTECTIONREGULATION (GDPR)

TAP THE POLITICAL MARKET: GDPR IS COMING NEXT YEAR

- The **new European General Data Protection Regulation (GDPR)** is something to keep CEOs up at night.
- With maximum **fines of up to 4% of the worldwide annual turnover** for non-compliance (e.g. data breach) it can have a severe impact on any companies balance.
- Becomes **effective in all EU member states in May 2018**.
- The GDPR applies to everyone who processes or controls **personal data of EU-citizens** in or outside the EU.

GDPR: KEY PROVISIONS

- The GDPR is strengthening the rights of individuals whose personal data is being processed, including through:

  - the need for the individual's **clear consent** to the processing of personal data
  - easier **access** by the subject to his or her personal data
  - the rights to rectification, to erasure and **'to be forgotten**‘
  - the **right to object**, including to the use of personal data for the purposes of 'profiling‘
  - the right to **data portability** from one service provider to another

GDPR: NO PRIVACY WITHOUT SECURITY BY DESIGN

The GDPR is requiring companies to take technical and organizational measures. This may include integration of **security & privacy by design features** within their products such as:

- Secure storage of keys e.g. in tamper resistant HW
- Individual Device ID
- Secure User Identities
- Decoupled User ID from Device ID
- Secure Communication channels

SECURE CONNECTIONS FOR A SMARTER WORLD

INDUSTRY 4.0 FINDINGS

WE NEED EU RULES IN INDUSTRY 4.0 | **SECURITY BY DESIGN**

- **Preset Certified Security Structures**
  Encryption requirement for identities and communication channels incl. secure storage of keys to ensure data integrity and confidentiality
- **Mutual Authentication of Identities / Connected Devices**
  Open to all technologies and applications
- **Need-to-Know Principle**
  As little as possible, as much as necessary (this also fits to Big Data if the customer is aware of who receives the data)
- **Testing and Certifying Security**
  Using existing, proven certifications like CCRA recognized as state-of-the-art
- **Manufacturer-Implemented Parametrization in the Connected Machines**
  Rights management for accessing data can be changed by the manufacturer / operator (Firmware vs. Data)

Only with **trust**, **transparency** and the **same legal framework** for all market participants there will be planning reliability for a prosperous future of Industry 4.0.

Q&A

Shape the future, Lead the Dialogue, Get involved.

SECURE CONNECTIONS
FOR A SMARTER WORLD

Marc Gebert
marc.gebert@nxp.com