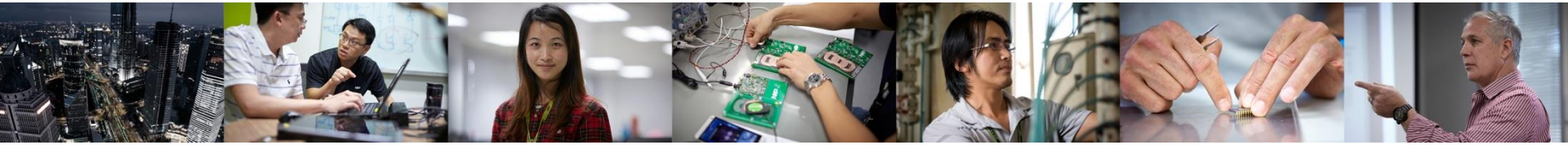
Sicherheitsanforderungen im Smart(en) Home

Jacques Kruse Brandao
Director Business Development



TeleTrust - IT-Sicherheit im Smart Home und in der Gebäudeautomation
Berlin – 12 November 2014

SECURE CONNECTIONS FOR A SMARTER WORLD

NXP Semiconductors – A global innovator

- Established in 2006
  (formerly a division of Royal Philips)
- Net sales: $4.82 billion in 2013
- In > 25 countries in Europe, Asia and US
- Manufacturing in Europe and Asia

Strong innovation pipeline:

- Over $600M / year in R&D
- 3,300 engineers
- 11,000 patents
- Analog mixed-signal portfolio focused on Secure Connectivity

Hack man

http://www.youtube.com/watch?v=nBdlLgudIQY

Source: http://www.youtube.com/watch?v=nBdlLgudIQY

Global Leader in Authenticating Identities and Securing Transactions

Smart Cards | Smart Devices

NXP is the Identification Industry's #1 Semiconductor Supplier

#1

eGovernment

#1
Reaching

Bank Cards

#1

Smart Mobility (MIFARE) Cards

#1

Tags & Authentication

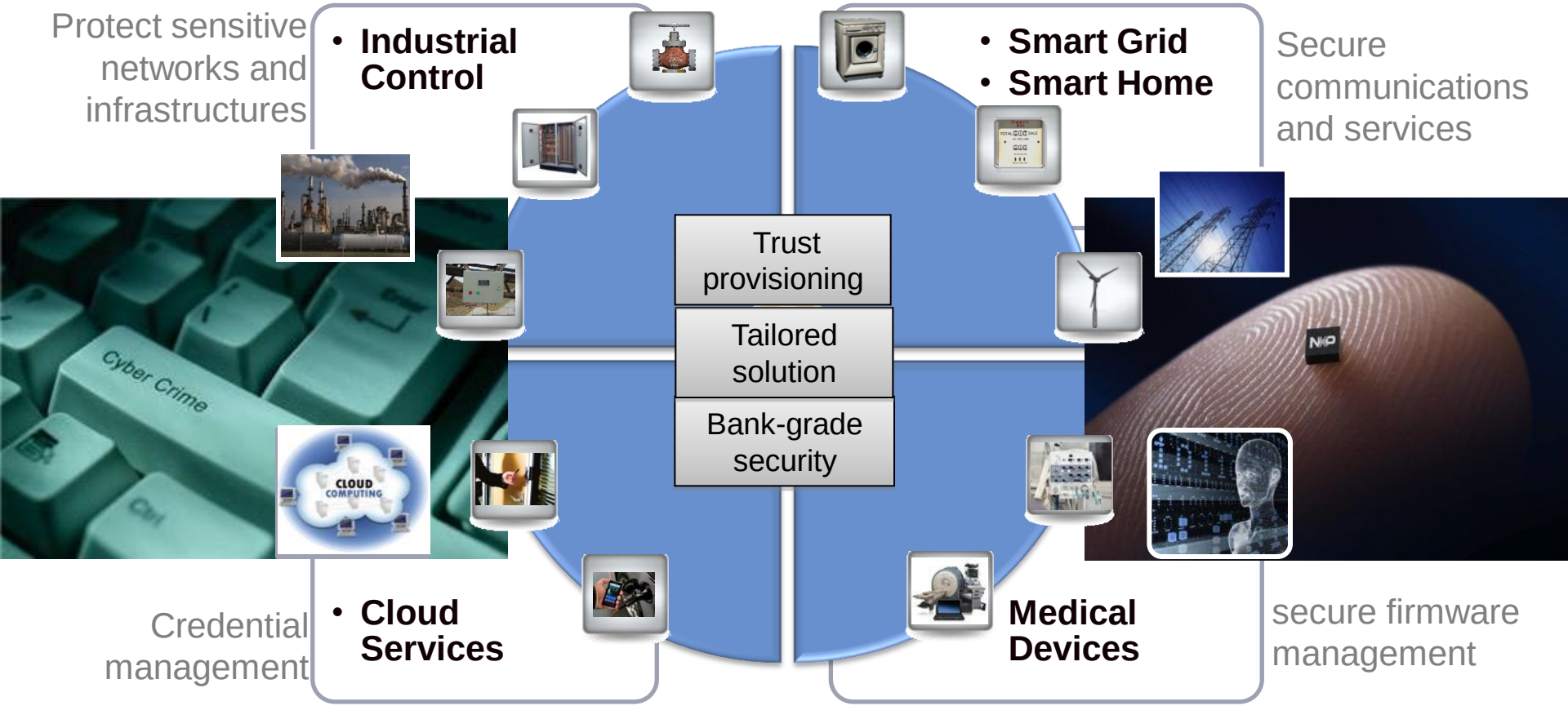
#1

Readers

#1

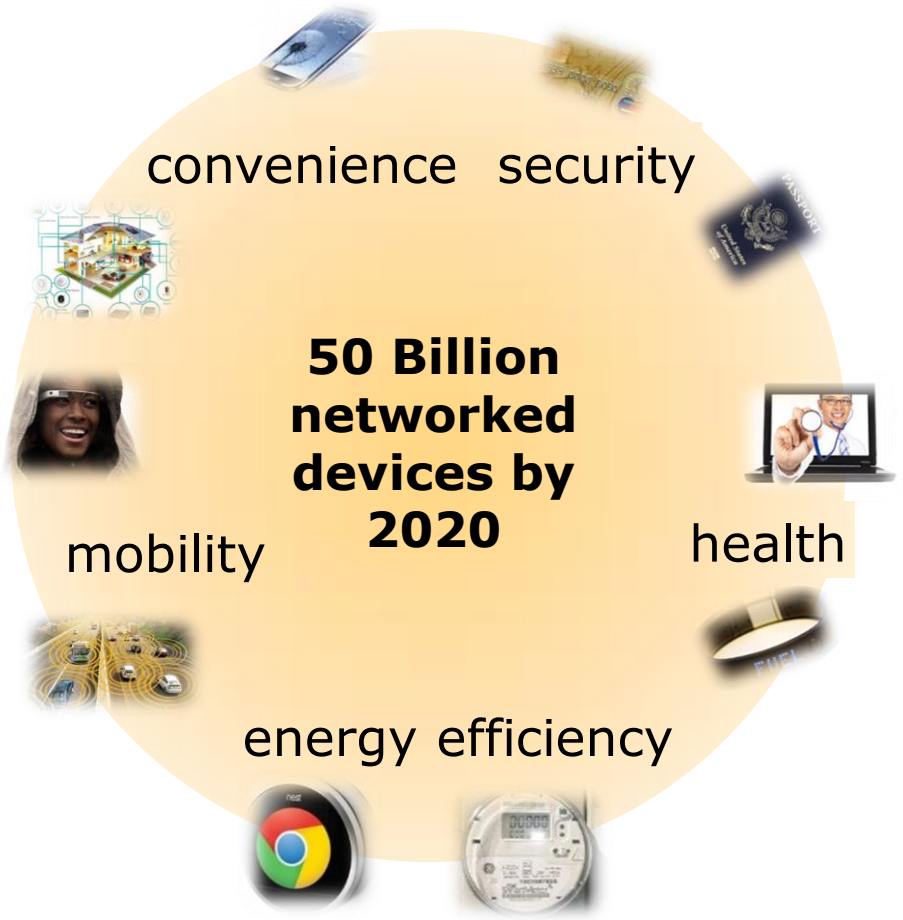
Mobile

NXP is approaching Device ID Solutions in 4 Cyber Security Markets

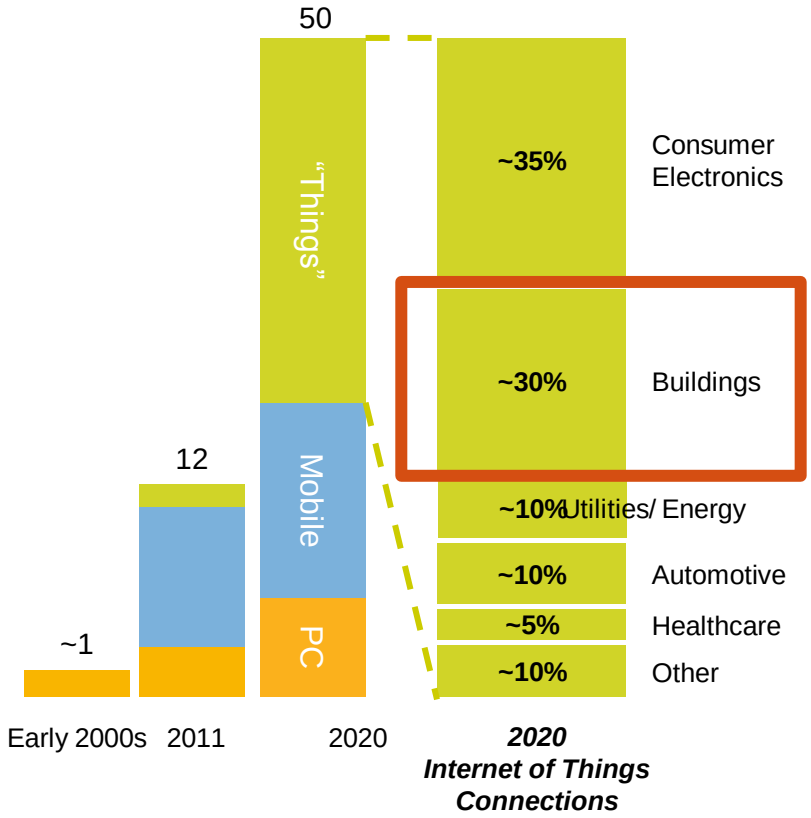


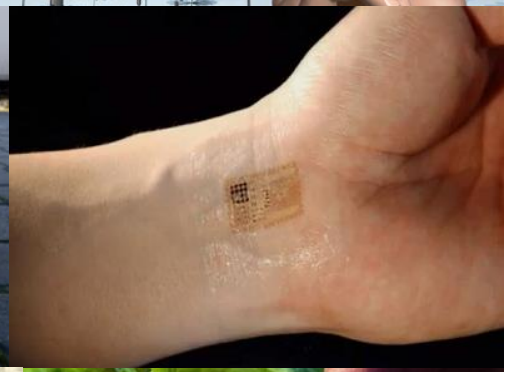
The Internet of Things

Smart Home and Building expected to reflect 30% of “Things”



CONNECTED DEVICES IN USE
(in bn units)





Enabling billions of efficient end nodes

- Ultra low power,
  >10 year autonomous field operation
- Multi-modal sensing capability
- Seamless interoperable wireless connectivity
- Secure data and privacy protection
- Ease of install, ease of use

Security challenges of the IoT

- The Internet of Things is facing major security challenges
- Connected Systems are increasingly prone to Security Threats
- This exposes device manufacturers and infrastructure owners to high financial risks and reputational damages

Internet of Things …Needs enhanced security

Beckstrom's Laws of Cyber Security*

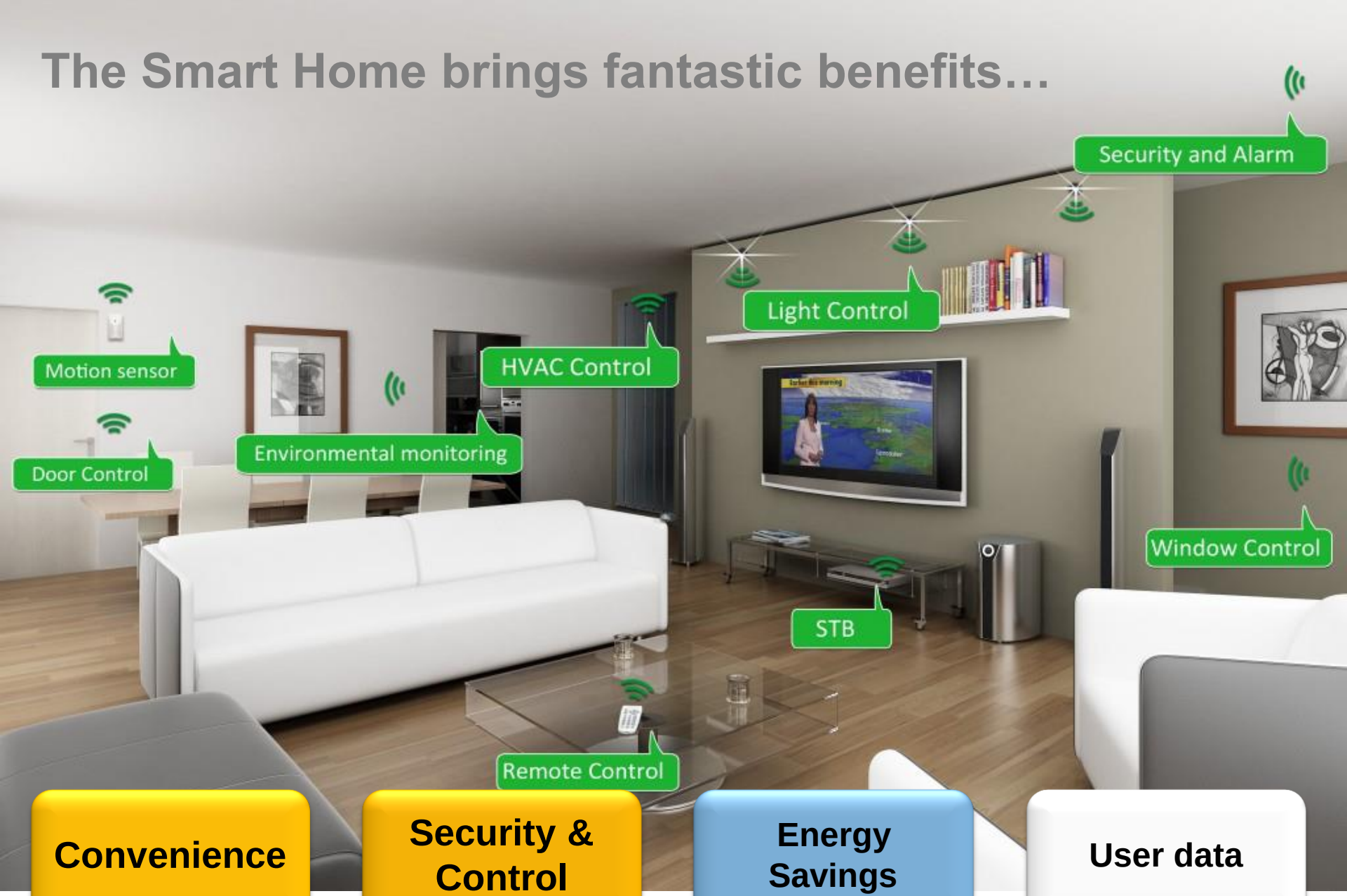
1. Everything that is connected to the Internet can be hacked
2. Everything is being connected to the Internet
3. Everything else follows from the first two laws

*Rod Beckstrom, CEO and President of ICANN, former Director of the National Cyber Security Center

- **NXP is your partner in security!**
- **Security by Design –**
  End-to-End security approach in Connected Systems
- **Security Module A70CM/A80SM**
  as next level of security

Security Requirements in Smart Home

The Smart Home brings fantastic benefits…



Convenience

Security & Control

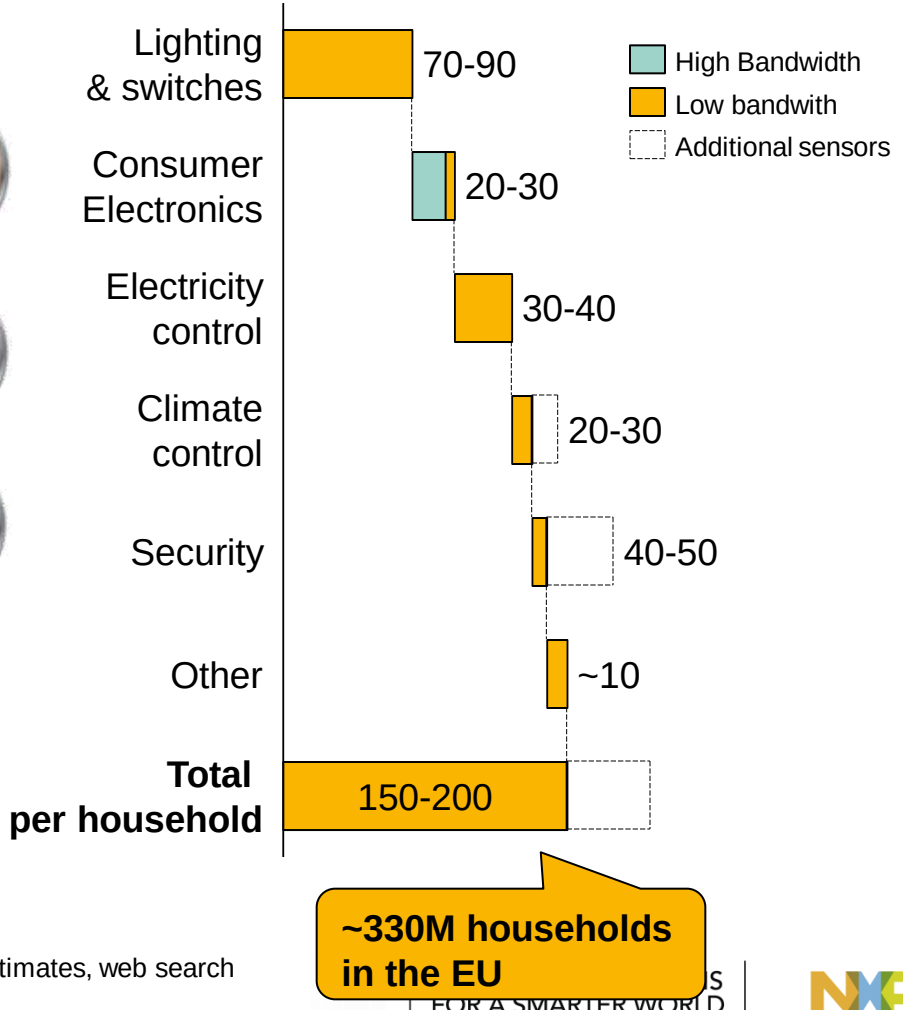
Energy Savings

User data

Smart Home may contain over 150 network nodes

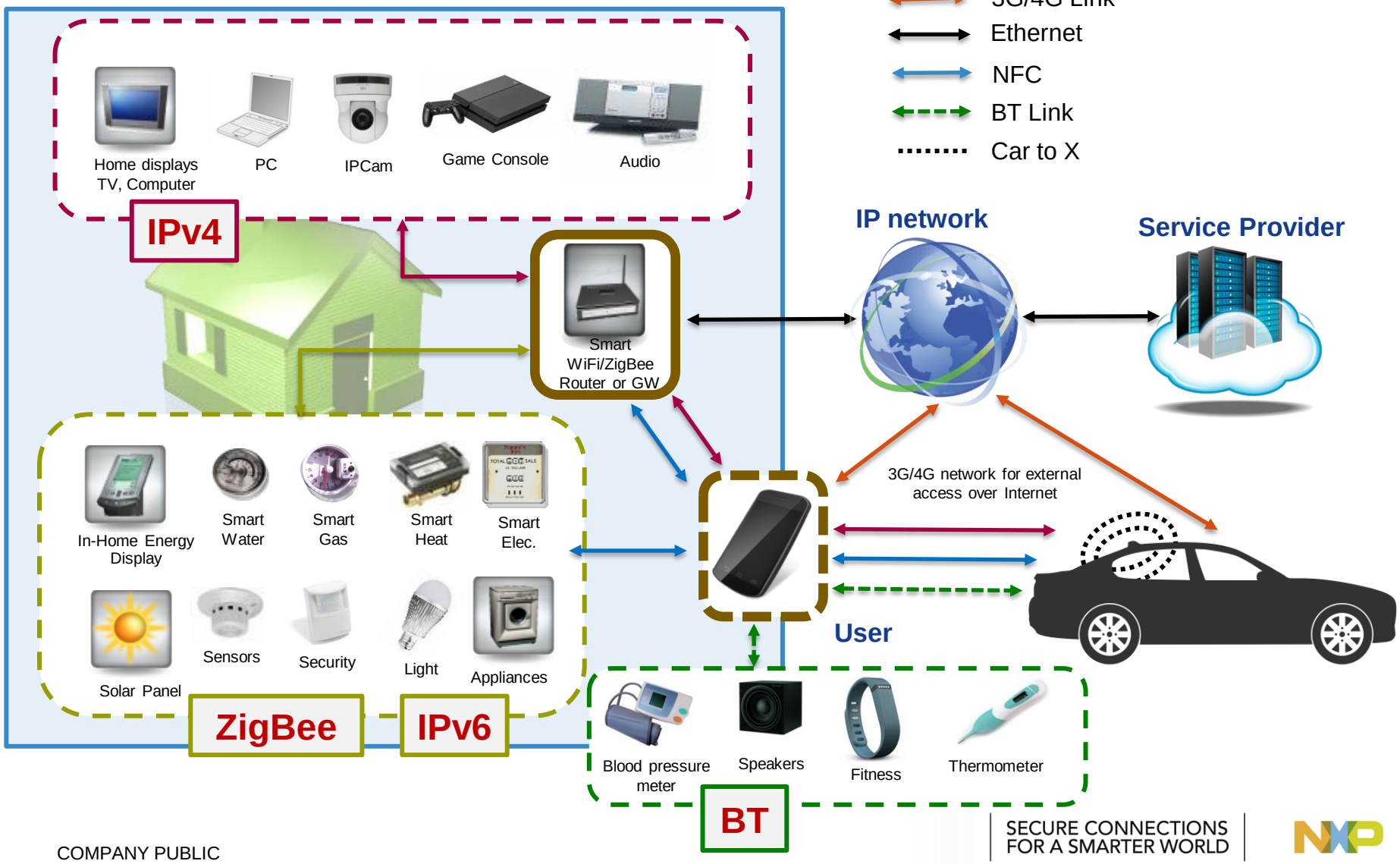
21Mio Residential flats in Germany

Smart Home nodes
Units (based on 'dumb' 2010 figures)

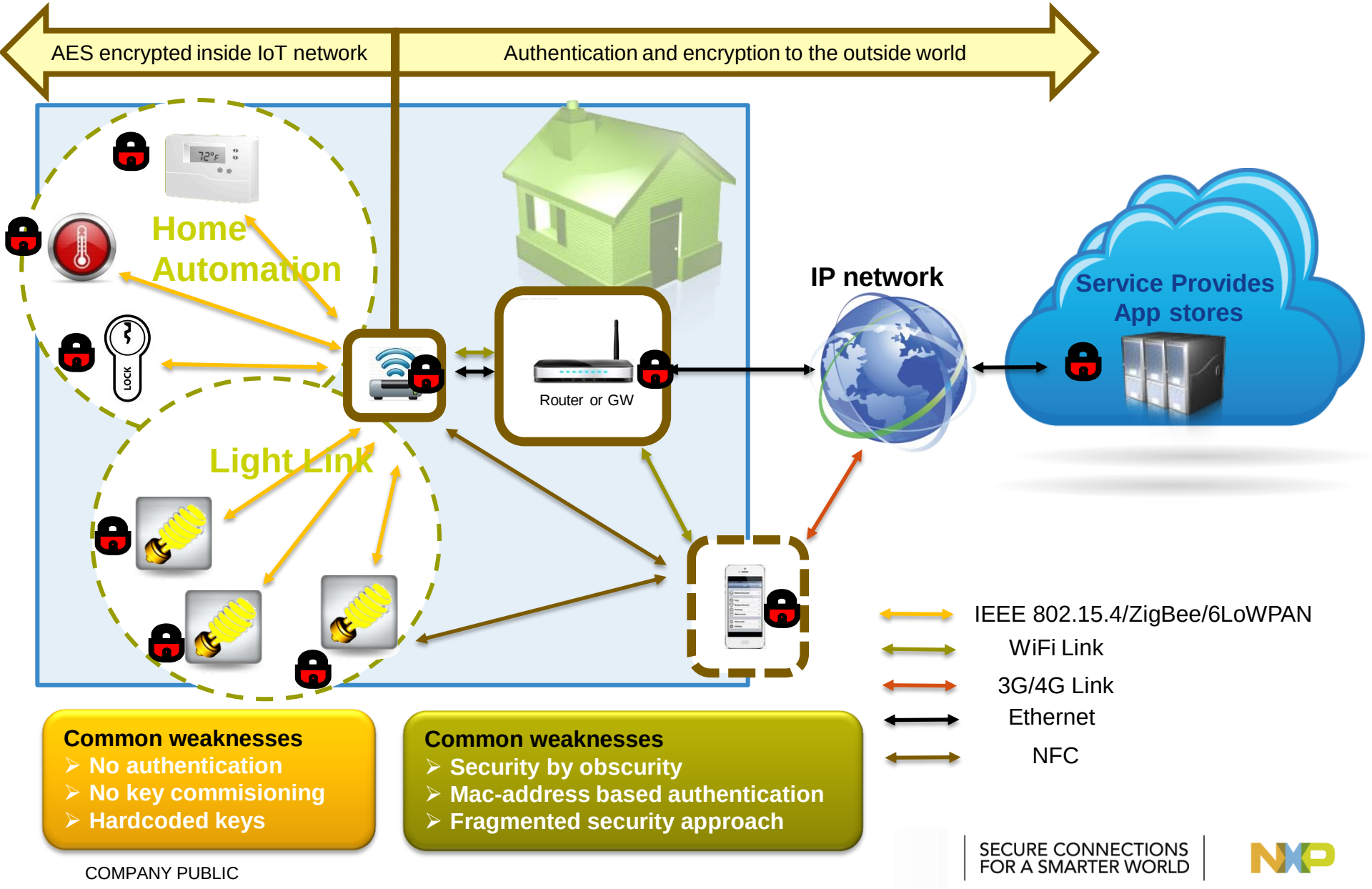


Source: team estimates, web search

Home IoT Connectivity: Various communications



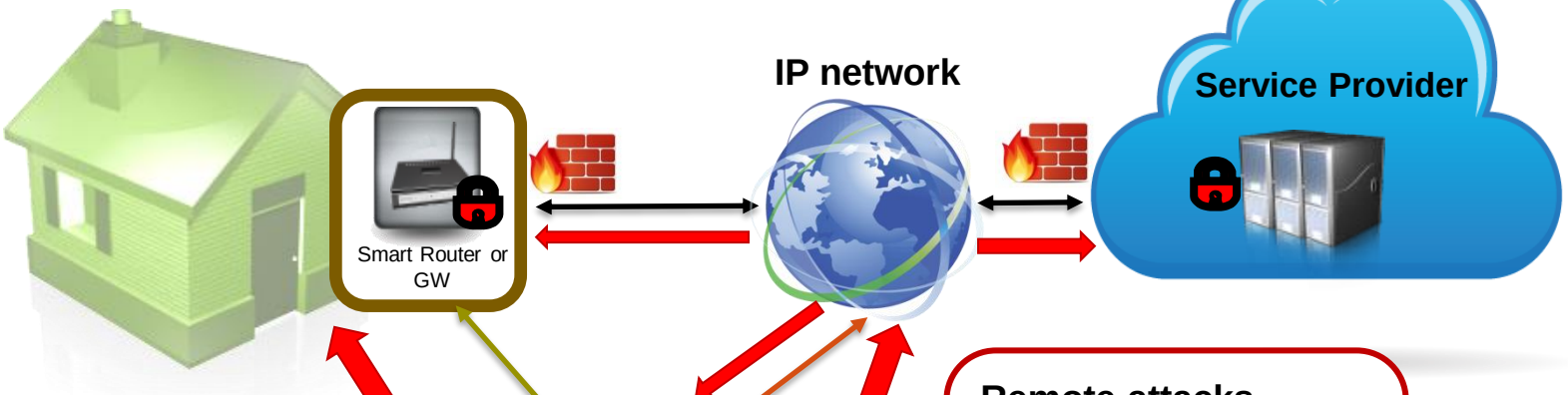
Best possible IoT setup today



Common weaknesses
- No authentication
- No key commisioning
- Hardcoded keys

Common weaknesses
- Security by obscurity
- Mac-address based authentication
- Fragmented security approach

Home IoT network attacks



Local attacks
- Eavesdropping (sniffing)
- Spoofing
- Replay/Injection
- ..

Remote attacks
- Scanning and Exploiting
- Mallware installation
- Gain access and control to IoT end-nodes
- ...

Physical attacks
- Key extraction
- Reverse engineering
- ...

Dangers and risks
- Stolen data – privacy violation
- Gain physical access
- Denial of service
- Danger by physical malfunction
- Access to PC etc. and create financial damage
- System hijacking and ransoming
- ...

Home IoT security concerns

Data security

Ownership? Storage location? Secure transport? Access by whom?

Network setup, device (de)commisioning and firmware updates

Key distribution and storage
Device authentication
Bridging across verticals
Lifecycle management

Mobile devices

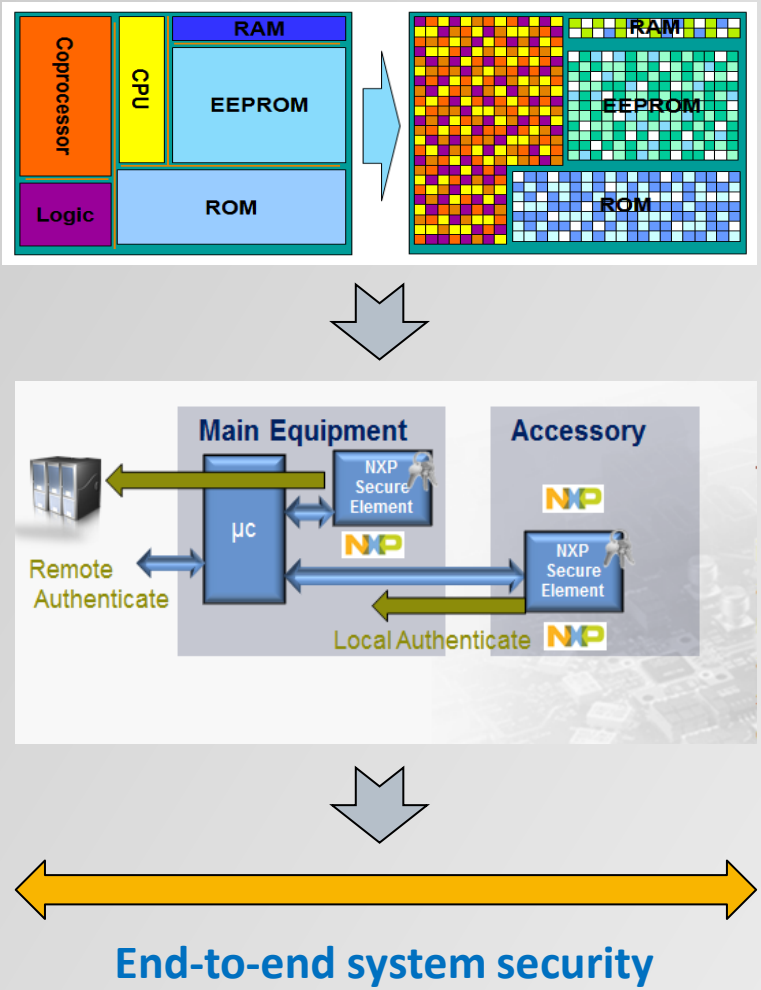
Moving in and out of local network
Network access through the cloud and peer-to-peer

Attacks will happen

How to raise the bar for attacks and still be cost effective?
Can we detect attacks?
Device revocation and cleaning

Security of Smart Homes is essential!

- **Secure access to home devices**
  - grant access to authorized servers only
  - authenticate application commands
  - prevent exposure of user related information (Privacy)
  - prevent exposure of Home Networks keys
  - protect device management commands (incl. SW upgrade)
- **Protect back-end servers**
  - any smart device (esp. gateways, routers) is a potential entry point into back-end
  - strongly authenticate all smart devices
- **Enhanced/managed user experience**
  - anti-counterfeit: only allow qualified hardware to interact with applications
  - authentication: enable traceability (accountability) to ecosystem vendors



Security @ remote heating maintenance

Fernwartung: Sicherheitslücke bedroht Hightech-Heizungen

Von Matthias Kremp

Vaillant

Mikro-Blockheizkraftwerk Vaillant ecoPower 1.0: Update per Speicherkarte

Hochmoderne Heizanlagen des deutschen Herstellers Vaillant haben ein Sicherheitsproblem - sie lassen sich übers Internet abschalten, womöglich beschädigen. Das notwendige Update kann nur von einem Techniker installiert werden. Bis der kommt, empfiehlt der Hersteller drastische Maßnahmen.

Dienstag, 16.04.2013 – 16:58 Uhr

Mehrere hundert Kunden des Heizanlagenherstellers Vaillant haben in den letzten Tagen beunruhigende Post bekommen. In einem

Vulnerabilities in connected heating systems identified !

Security @ Home Automation

Dienstag, 18:59

Gravierende Sicherheitslücke

Die auch in Deutschland vertriebene
laut IOActive nicht nur von Fremden
bösartiges Firmware-Update auch zu

Der Sicherheitsdienstleister IOActive
nachdem Belkin – Hersteller des Wem
von IOActive alarmierten US-CERT (Co
CERT veröffentlichte nach Aufdeckung

YOUR LIGHTSWITCH DOES WHAT?

Belkin WeMo Switch

Outfitting a home or office with home automation tools that let you control and remotely monitor electronics can quickly turn into a fun and addictive (if expensive) hobby. But things get somewhat more interesting when the whole setup is completely exposed to anyone on the Internet. That's basically what experts at **IOActive** found is the case with **Belkin**'s WeMo family of home automation devices.

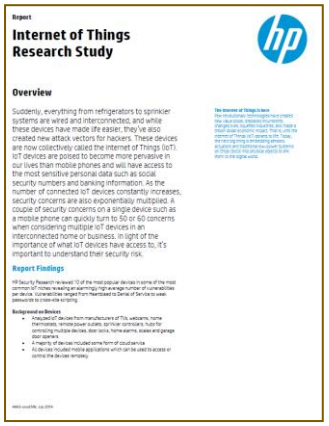
According to research released today, multiple vulnerabilities in these WeMo Home Automation tools give malicious hackers the ability to remotely control the devices over the Internet, perform malicious firmware updates, and access an internal home network. From IOActive's advisory (PDF):

> The Belkin WeMo firmware images that are used to update the devices are signed with public key encryption to protect against unauthorised modifications. However, the signing key and password are leaked on the firmware that is already installed on the devices. This allows attackers to use the same signing key and password to sign their own malicious firmware and bypass security checks during the firmware update process.

Vulnerabilities in Home Automation identified !

Example: Home Automation (HP Study)

HP Study

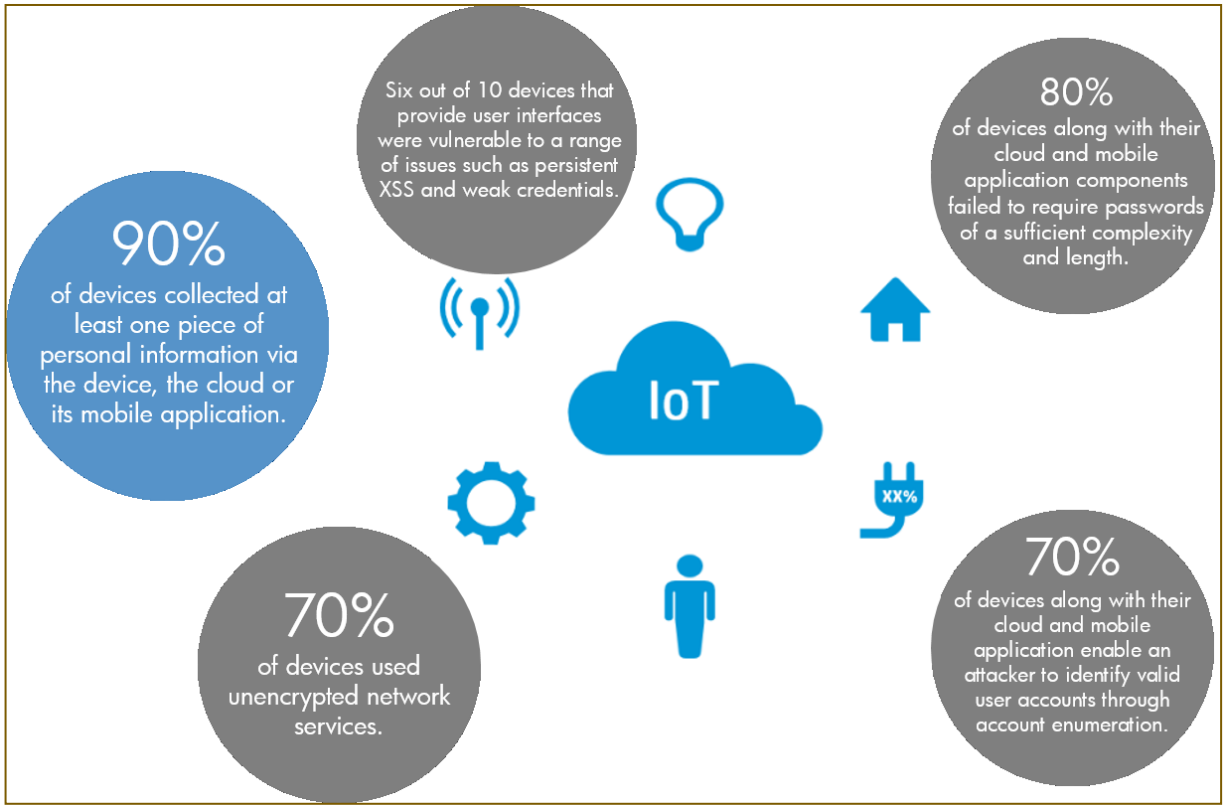

Report

Internet of Things Research Study

Overview

Suddenly, everything from refrigerators to sprinkler systems are wired and interconnected, and while these devices have made life easier, they've also created new attack vectors for hackers. These devices are now collectively called the Internet of Things (IoT). IoT devices are poised to become more pervasive in our lives than mobile phones and will have access to the most sensitive personal data such as social security numbers and banking information. As the number of connected IoT devices constantly increases, security concerns are also exponentially multiplied. A couple of security concerns on a single device such as a mobile phone can quickly turn to 50 or 60 concerns when considering multiple IoT devices in an interconnected home or business. In light of the importance of what IoT devices have access to, it's important to understand their security risk.

Report Findings



10 of the most popular IoT devices revealing a high average number of vulnerabilities per device.
Vulnerabilities ranged from Heartbleed to Denial of Service to weak passwords to cross-site scripting.
End Customer cannot trust webcams, TVs, thermostats, remote power outlets, sprinkler controllers, several control devices, door locks, home alarms, garage door openers.

Authentication is essential to Trust Infrastructures

- Trusted equipment (Proof of Origin)
- Trusted Role Based Access Control
- Trusted SW running on equipment
- Trusted commands (preventing exploitation of SW bugs and a multitude of other attacks)

The concept of Authentication

- A **Trusted** way to identify an individual or Device in a network
- Authentication means **strong** Identification
- Underlies the use of **cryptographic techniques**
- Underlies the **protection of keys**

Key learnings from recent security breaches

The ‘Heartbleed’ Case

- **Scale** of issue: **“** "Catastrophic" is the right word. On the scale of 1 to 10, this is an 11.**”** [Bruce Schneier, 09 April 2014]
- The **problem**: a bug in OpenSLL Cryptographic Software Library in Heartbeat implementation of TLS/SSL protocol
- **Impact:** gives access to confidential information on server and clients: private keys, keys, data (like login, passwords, emails, instant messages…)
- **Detectability**: leaves no trace, undetected by intrusion detectors; remote attack.
- **Fix:** applied by the international community: Install/integrate a new version of OpenSSL, change keys, passwords…No recovery for leaked confidential information! (2 years!)

KEY LEARNINGS

- **Security** is to a great extend **a matter of Implementation**
- **Clearly secure and isolate your keys and sensitive data**. Do you know where your keys are stored in your system? Anticipate impact of this kind of hack!
- **Use proven solutions**: Open source widely used SW packages does not mean secure implementation

Software only is not sufficient…

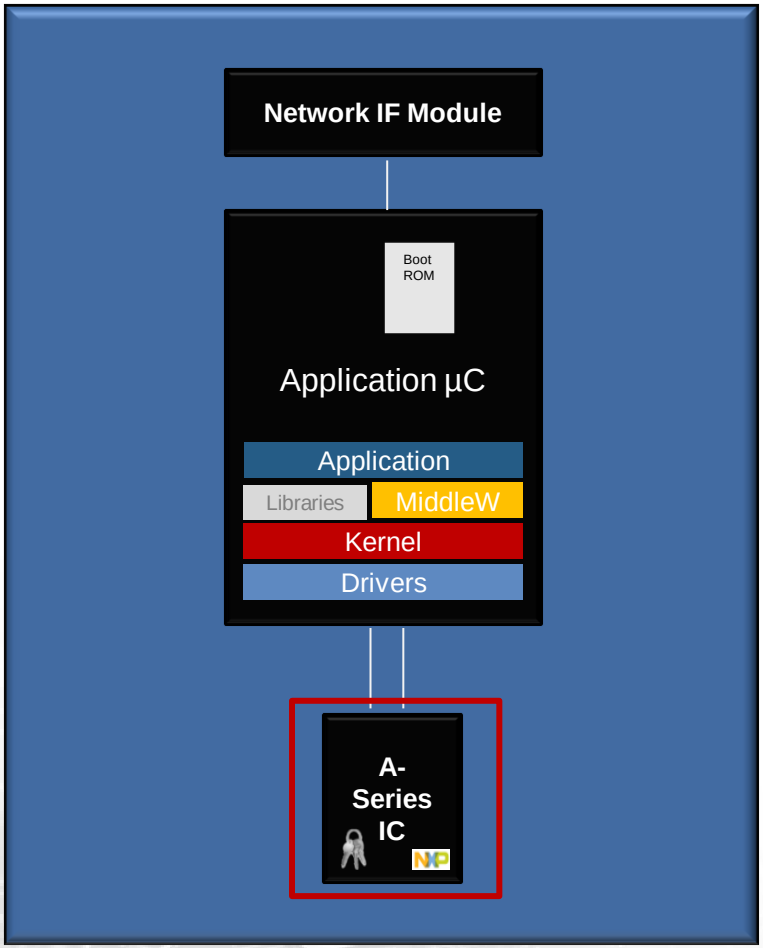
Currently no software-only solution has been proven secure!

- x It is extremely difficult to protect keys in software
- x Often very difficult to control where keys are stored (typical with open source software; case example: ‘’Heartbleed’’ attack)
- x Hacked software easy to distribute (leading to massive attacks)
- x Code size and runtime

This drives the need for a Security IC, decoupled from application software and its upgrades, and dedicated to the protection and management of credentials

A70CM: Key Functions

- **Secure key storage**: private keys, confidential data, credentials for connection to remote trusted entity, Proof of Device Origin, SW verification keys & version management
- **Secure Trust Provisioning, key generation and management**
- **Crypto processing:** set-up of secure connections (key agreement), key exchange, critical message encryption, etc

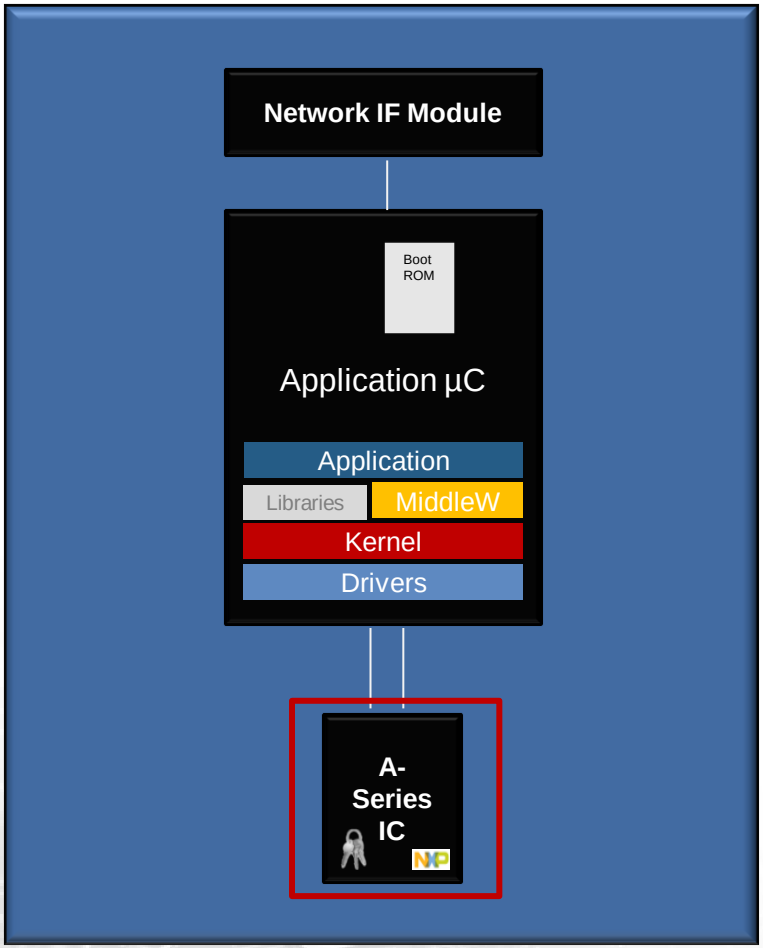


A-Series Security ICs

ADAPT TO ANY TYPE OF µC

A70CM: Key Benefits

- ✓ HW isolation of crypto operations and isolation of keys: Sensitive keys (long life keys) never leaves the A7!
- ✓ Best in class Tamper Resistance, including against non invasive attacks (box closed)
- ✓ True Random Number Generator, essential for crypto operations & protocols
- ✓ Secure transport of keys thru pre-inject at IC manufacturing, solving key management across untrusted supply chain and untrusted networks
- ✓ Proven/certified product, reduced attack perimeter on simple interface
- ✓ Crypto co-processing (energy budget)



A-Series Security ICs

ADAPT TO ANY TYPE OF µC

Device ID cryptography

PKI Cryptography

ECC

- FIPS PUB 186-3 curves:
  NIST P-192, NIST P-224, NIST P-256
- RFC 5639 curves:
  BP-192r1, BP-224r1, BP-256r1
- ECDSA, ECKA-DH
- Key pair generation

RSA

- 1024 & 2048 bits
- Signature verification and generation according to PKCS #1 v1.5
- Key pair generation

Storage

- 2 Device ID key pair with certificate
- 2 Root CA public key

Symmetric Cryptography

AES

- AES128/256 bits
- Modes: ECB, CBC, GCM, GMAC
- Key wrappings according to RFC3394:2002, DSMR4.0, ECB
- Key Generation

Storage

- 78 keys store
- 26 key sets:
  - Triplets master key/encryption key/authentication key
  - Couple master key/communication key

Security threats landscape – SmartMX

NXP comprehensive Security Concept

More than 100 unique security features harden the SmartMX

Proven by third party security assessments and type approvals:
EMVCo security evaluation
CAST
VISA
Common Criteria EAL5+
ZKA
Approval for German Signature Card


Deutsches IT-Sicherheitszertifikat

BSI-DSZ-CC-0227-2004

Philips P5CT072V0M and P5CC072V0M Secure Smart Card Controller

from

Philips Semiconductors GmbH Business Line Identification

Generic Key Use Cases in Authentication

- Proof of Device Origin/ counterfeit (cloning) protection
- Strong Device Authentication and protection of cloud servers/backend
- Secure Access to Devices/Infrastructures
- Secure Device Default Keys and Configuration
- Device SW Integrity Protection / Secure FW boot
- Secure Communications and Commands
- Secure access to services, licensing (enabling new business models)
- Traceability & accountability
- Cover security requirement of EU/ BSI /ANSII/ ENISA/ NIST/ IEEE/ etc.

to generate

1. **Functional Security**
2. **Platform Security**
3. **Hardware Security**

NXP Turnkey Solution: A70CM

Turnkey Solutions

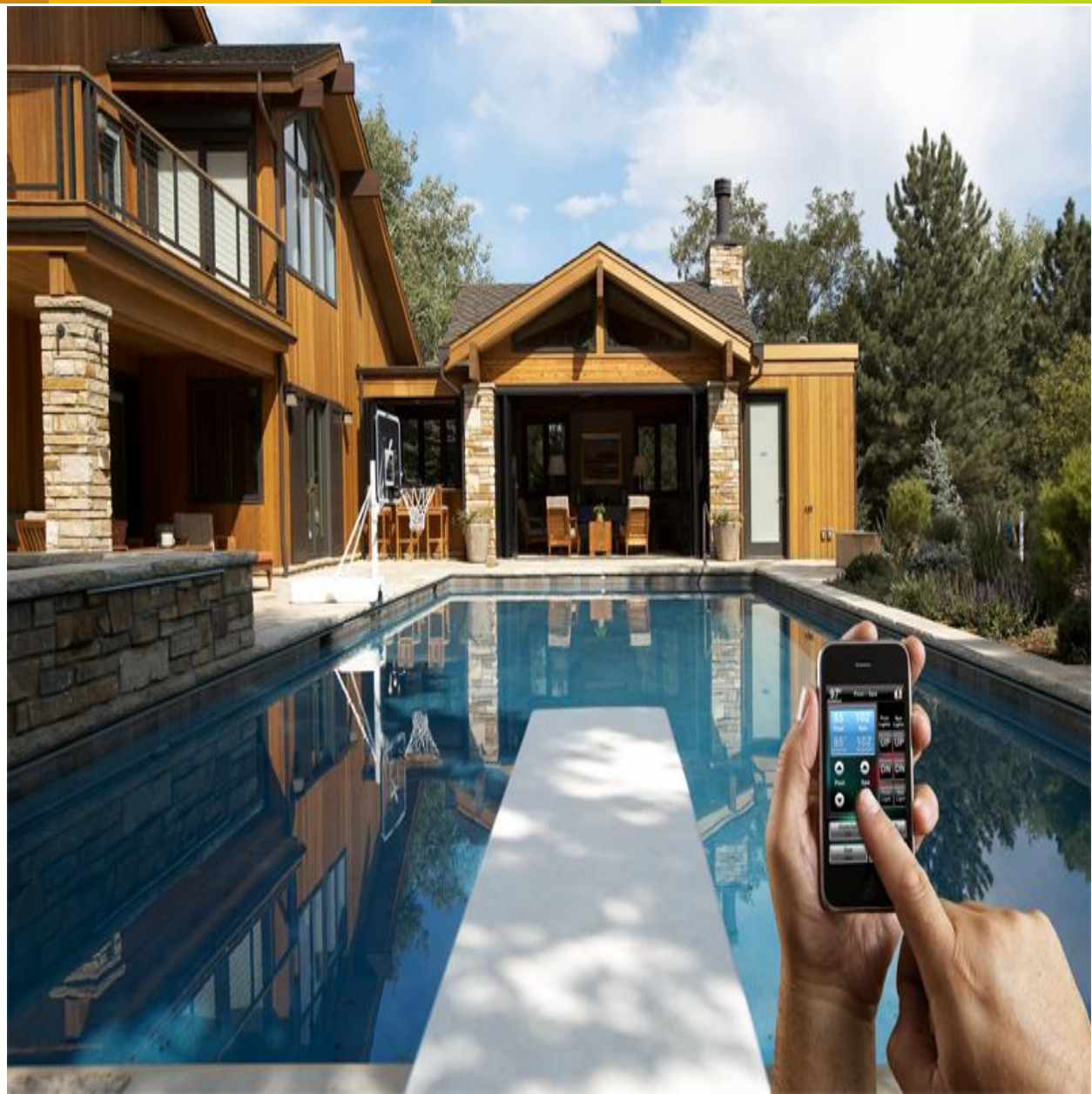
Off-the-Shelf Product featuring:

Security IC A700x	Key Injection Service
On-chip Application SW	Host Library, High-Level API

Key features

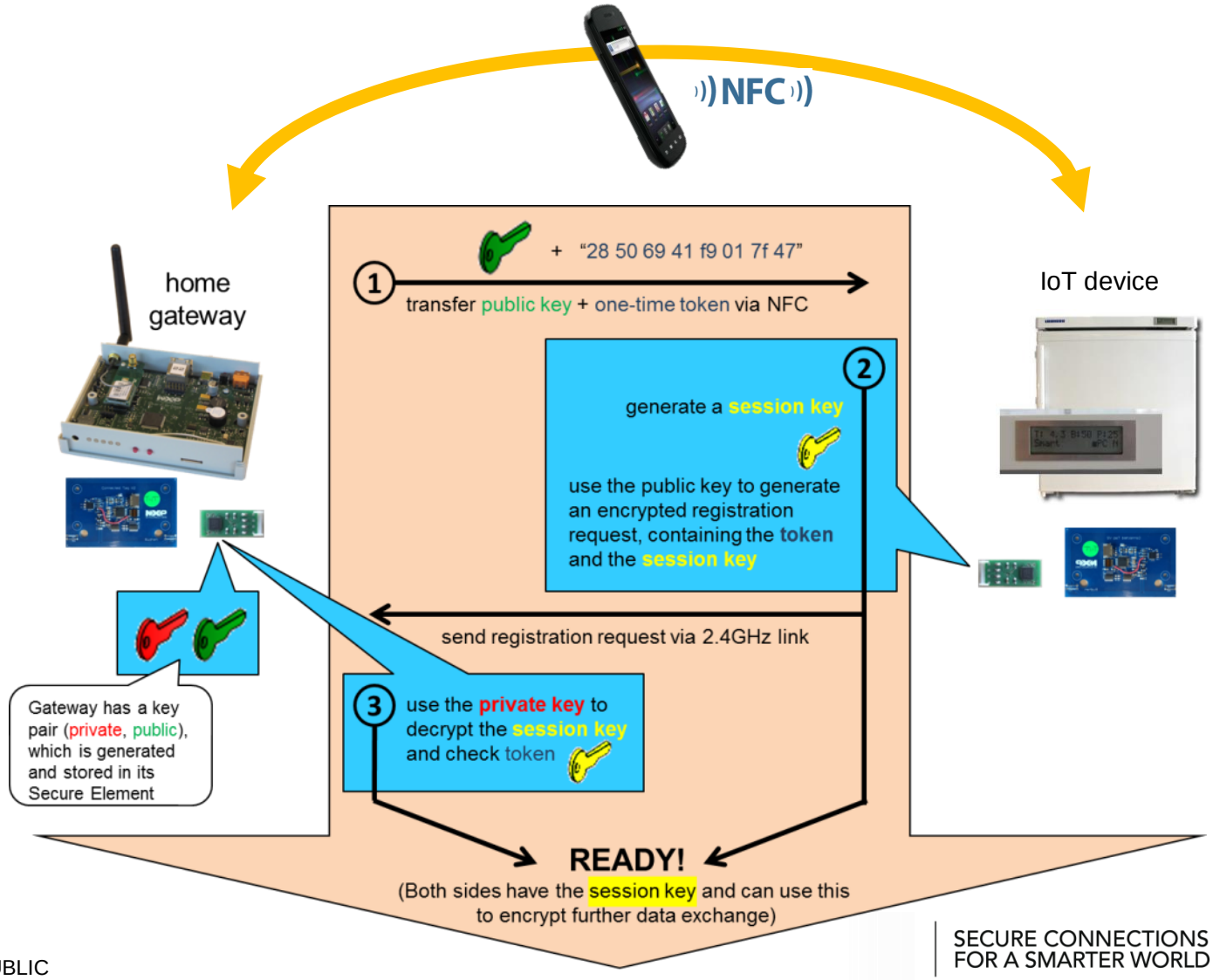
- Built on A700x NXP Security IC featuring state-of-the art Tamper Resistance technology
- Configurable Public Key cryptography with keys up to 2048 bits (RSA) and 256 bits (ECC)
- Signature generation and verification
- RSA encryption/decryption
- AES 128/256 bits encryption/decryption, large key store
- Key agreement
- Factory Key pre-injection in certified (Common Criteria) secure environment
- On chip key generation
- Secure key management, Device Life Cycle Management
- 100 Kbits/sec slave I^2C interface
- -25 °C to +85 °C (A7001CMHN1), -40 °C to +90 °C (A7002CMHN1) operational ambient temperature
- HVQFN32 package

Solution Examples



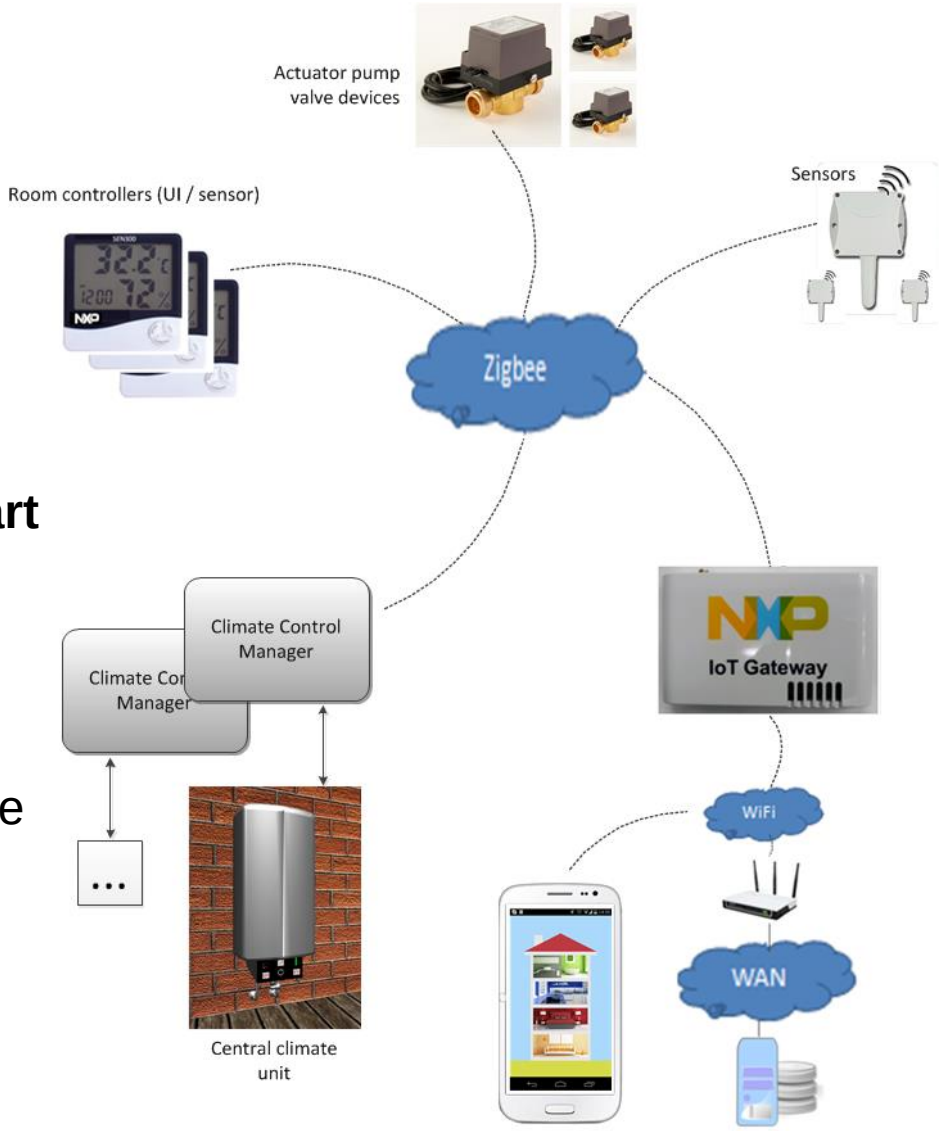
Smart Commissioning

Security needs to be easy to use
Example: simply touch to create a secure link



Smart Climate Control System

- **Multi-zone climate control**: control climate in every room individually
- Applicable to **heating or cooling**
- **IP Gateway enables control by smart phone** through WiFi or through the internet
- **Easy one-touch commissioning** of nodes using NFC enabled smartphone
- **Based on Zigbee** Home Automation low power networking



Secure commissioning

Step 1:
The mobile application identifies a gateway device.

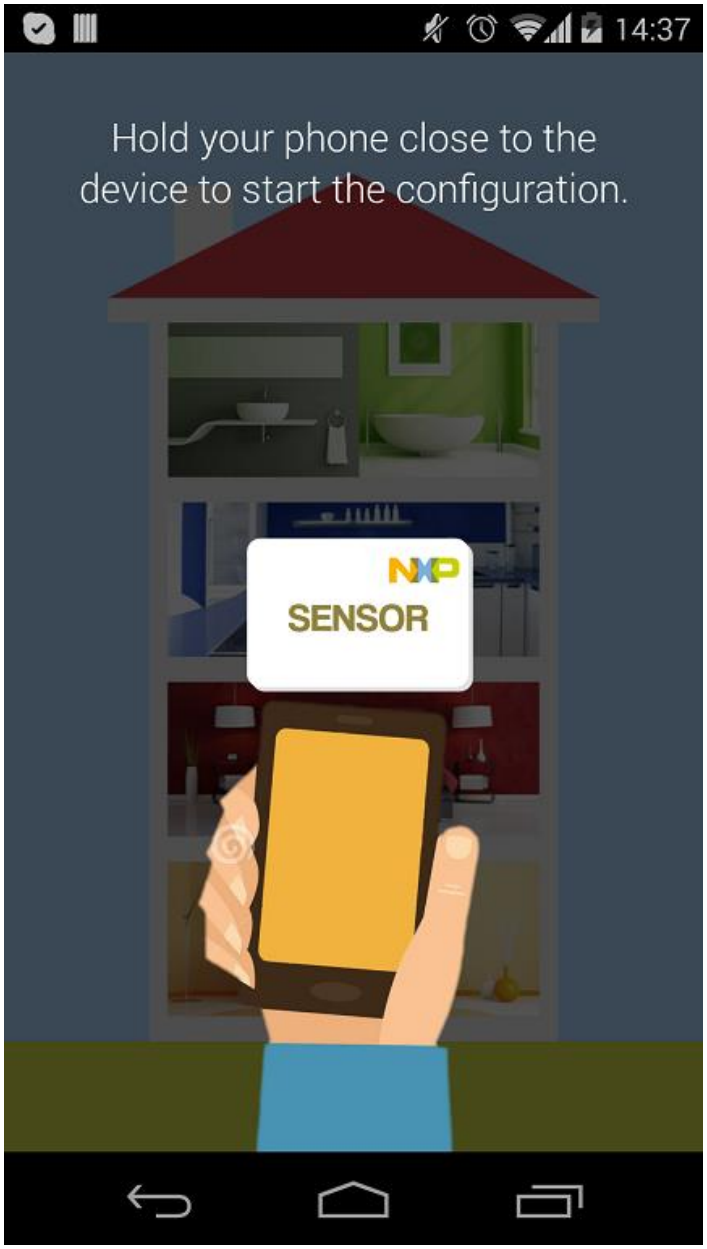
Phone registers in a secure way

Key physically located in a security module

Secure commissioning

Step 2:
Phone can now be taken to all nodes for single-touch commissioning.

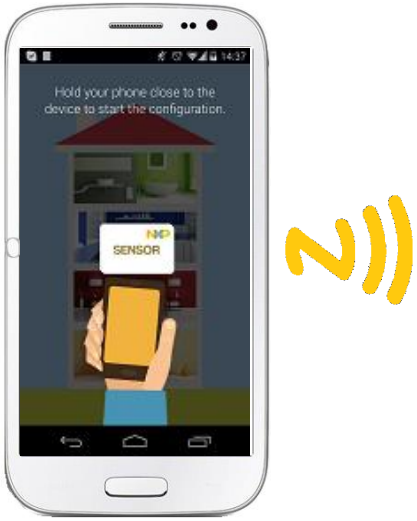
The mobile application identifies the type and capabilities of the touched device.

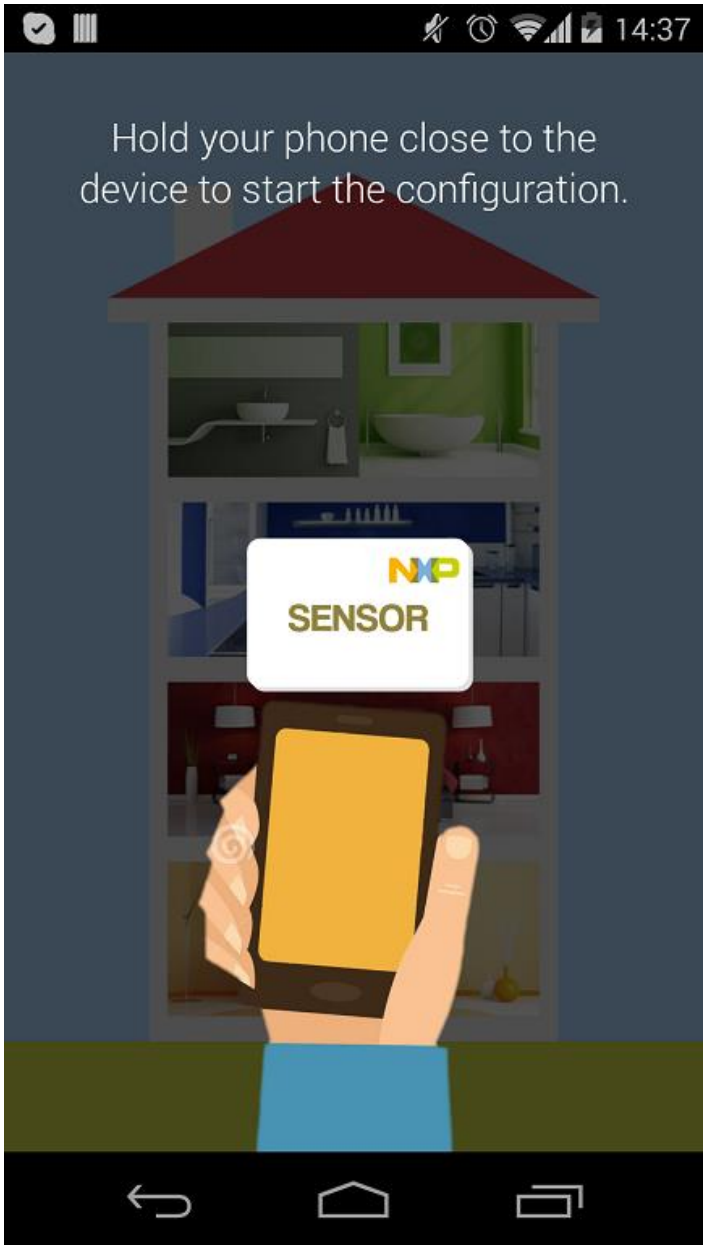


Secure commissioning

Step 2 continued:

Mobile application creates a database of devices.





Configure system
Create the relationship between devices

Now select a room of the previous touched device.

Configure system
Create the relationship between devices

Repeat the touched and assign procedure…..

Configure system
Create the relationship between devices

Ready!

What do you need to secure?

NXP receives Cyber Security Award

At Smart Metering Europe Summit 2014, London

Part of the judging panel:
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****"*

NXP Secure Connections for a Smarter World

http://m.youtube.com/watch?list=UUNtkvyhGV9oAmCHj8OGILuA&v=xpBznKL8kTA

THANK YOU!

SECURE CONNECTIONS
FOR A SMARTER WORLD

Jacques Kruse Brandão
jacques.kruse-brandao@nxp.com

Getting Started

Data sheets, Application Notes, Solution Packages are available on NXP DocStore: https://www.docstore.nxp.com (NDA required).

Product References:

A7001CMHN1/T1AGB39, Op. Temp: -25 °C…+85 °C, 12NC: 9353 015 22157

A7002CMHN1/T1AGB39, Op. Temp: -40 °C…+90 °C, 12NC: 9353 021 94157

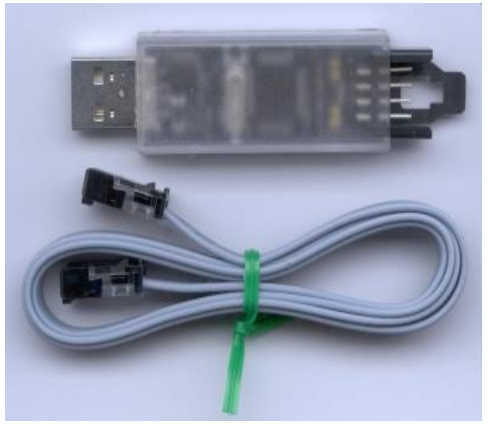
Export Control - ECCN:

5A002a1

Starter Kit

- **Hardware Components**
  - Mini PCB with soldered A70CM and 4 pin I2C connector
  - Complete I2C/USB set enabling connection to PC (I2CBird)
  - It includes a I2C female-to-female cable
- **OM3710/A7001CM0DEB mini PCB**
  - A70CM SW in debug version
  - Lifecycle status is reversible
- **PC Software**
  - Host Library Simulator for Windows
  - Running in Visual Studio
  - I2C Bird Driver (Win XP, Win 7)
  - CardManager as interface beetween Simulator and I2CBird
- **Documentation**

Mini PCB board



USB - I2C Bird adapter