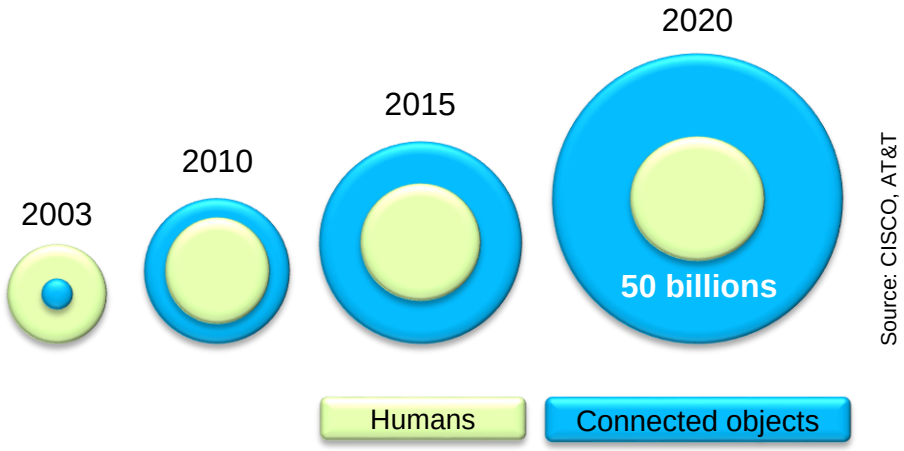
SÉCURITÉ : UNE APPROCHE GLOBALE

SEMINAIRE CAP'TRONIC : Cybersécurité des objets connectés - Le 22 juin à Valence

Alain MERLE, PhD
Strategic Marketing Manager
Alain.merle@cea.fr

IOT: SOME FIGURES

- Cisco predicts 50B of connected object by 2020
- Estimated market value $2 trillion by 2020
- Up-to 1 trillion sensors deployed
- Traffic grows by 25% per year



SECURITY: A SOCIETAL CHALLENGE

IEEE SPECTRUM

ZDNet.fr > News > Conficker est de retour...dans les caméras des policiers >

Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication

SHARE | TWEET | LINKEDIN | PIN IT | EMAIL | PRINT

Date Issued: July 31, 2015

Audience: Health care facilities using the Hospira Symbiq Infusion System

Device: Symbiq Infusion System, Version 3.13 and prior versions

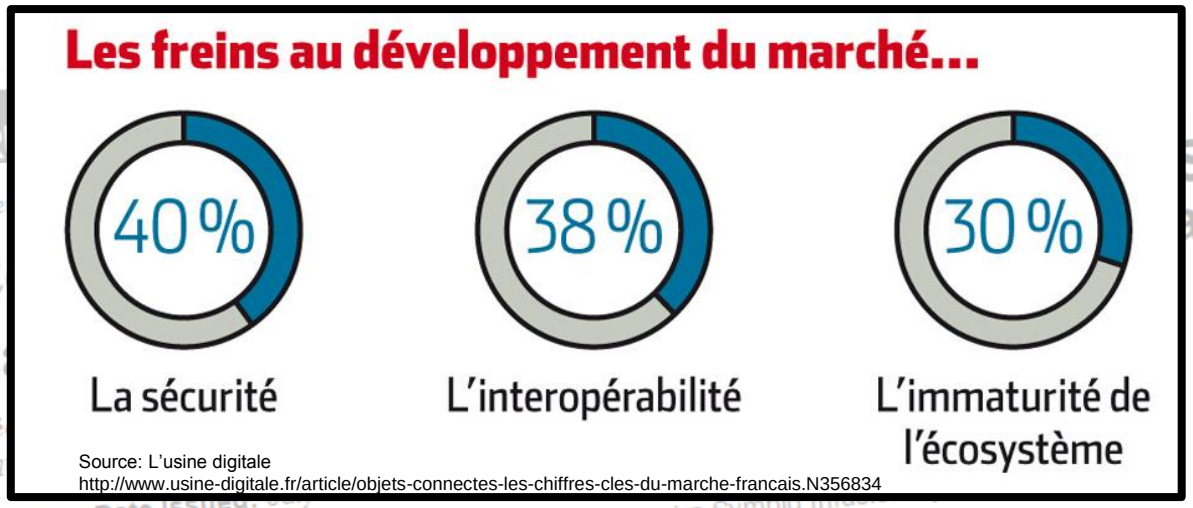
The Hospira Symbiq Infusion System is a computerized pump designed for the continuous delivery of general infusion therapy for a broad patient population.

It is primarily used in hospitals, or other acute and non-acute health care facilities, such as nursing homes and outpatient care centers. This infusion system can communicate with a Hospital Information System (HIS) via a wired or wireless connection over facility network infrastructures.

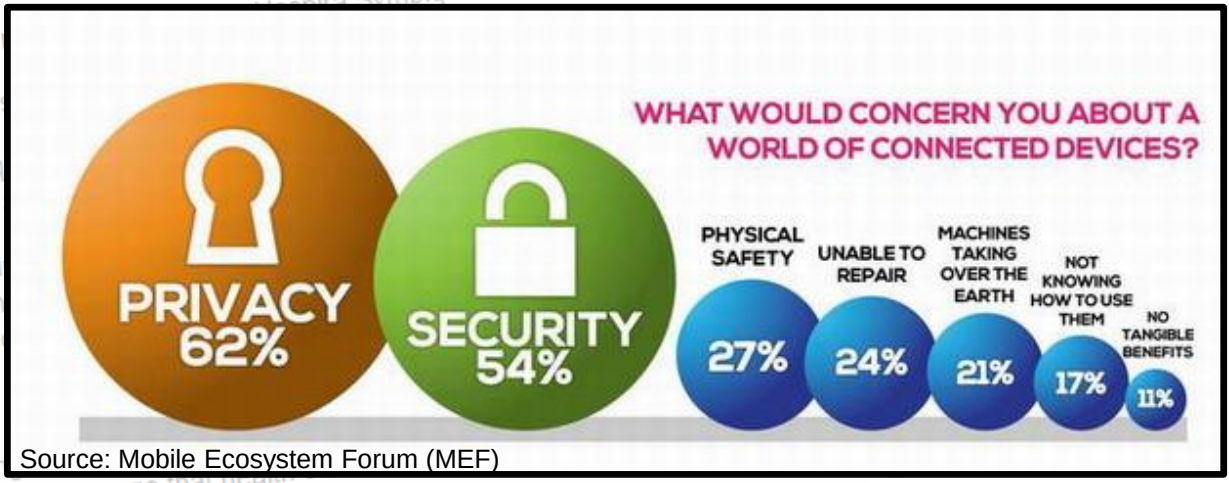
Purpose:

The FDA is alerting users of the Hospira Symbiq Infusion System to cybersecurity vulnerabilities with this infusion pump. We strongly encourage that health care facilities transition to alternative infusion systems, and discontinue use of these pumps.

SECURITY: A SOCIETAL CHALLENGE



Source: L'usine digitale
http://www.usine-digitale.fr/article/objets-connectes-les-chiffres-cles-du-marche-francais.N356834



Source: Mobile Ecosystem Forum (MEF)

Massive **adoption by citizens** relies on confidence on **security and privacy**

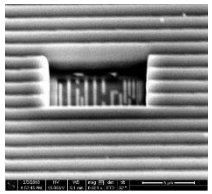
SECURITY IS COMPLEX

Internet

Debug

Update

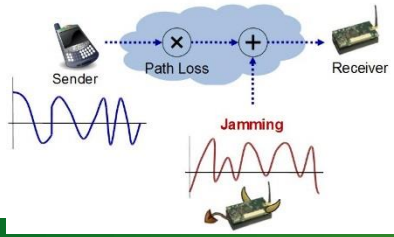
Physical attacks
Looking inside



Software
A single error is an entry door

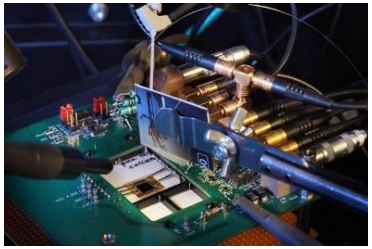
IOT Node

Communication
Attacks through communication interfaces:

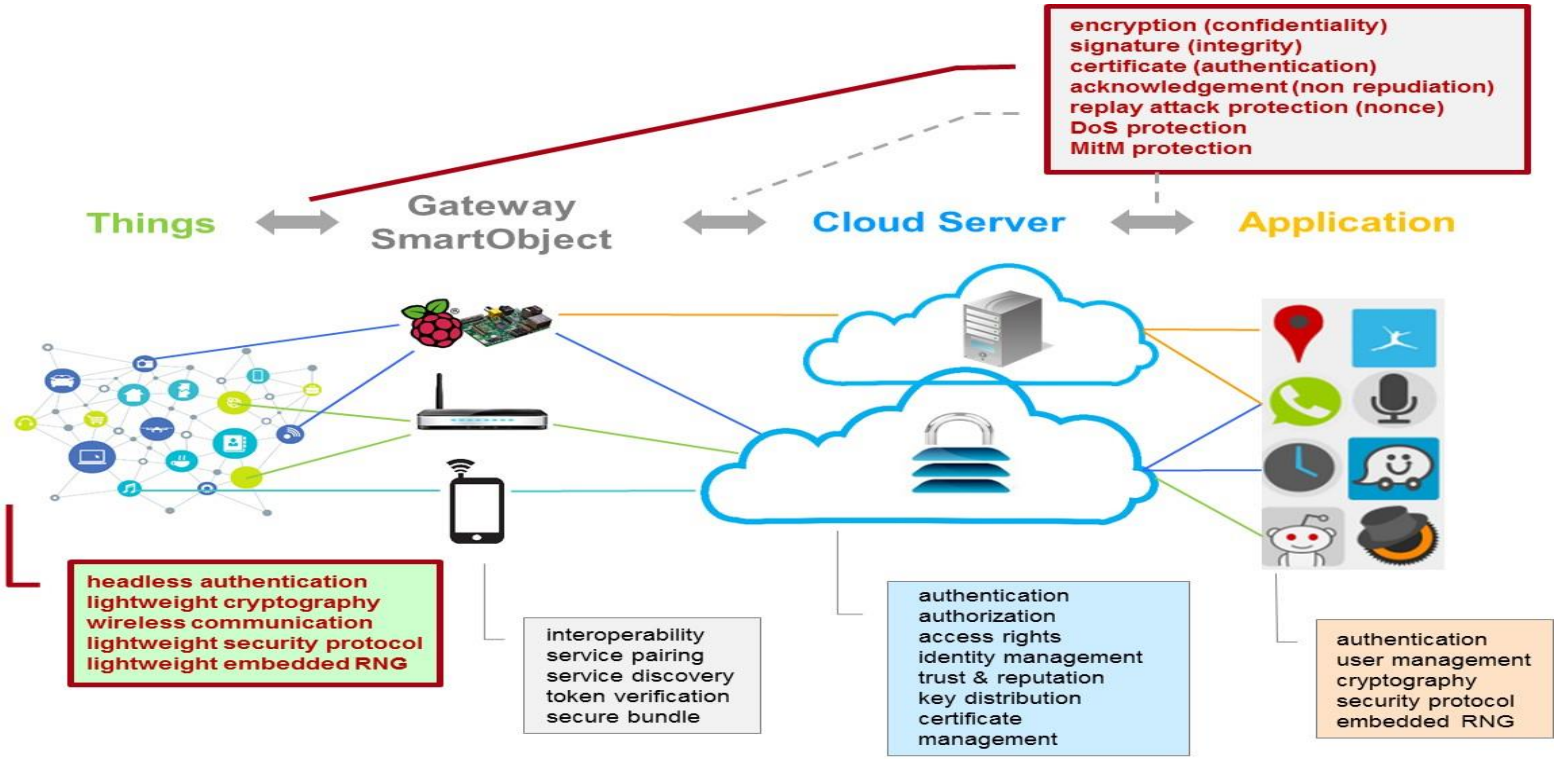


Fault injection
Glitches, light, laser, EM

Side channel
Monitoring time, power, EM



CRYPTOGRAPHY IS COMPLEX

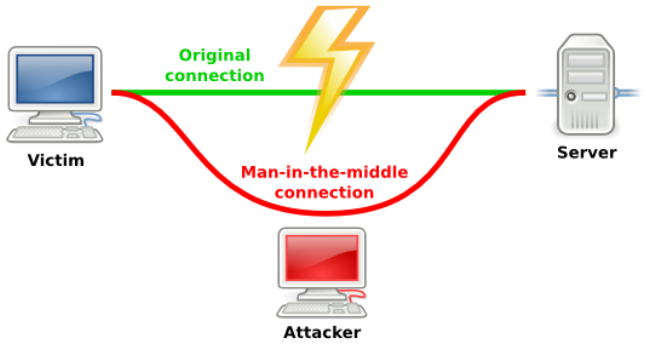


- **Key management: Bootstrap, Update, Recovery**

- **Intrinsic resistance**
  - Moore's law: increasing key size (DES, TDES, AES 128, AES 256)
  - Quantum computer : killing asymetric cryptography

ATTACKS TOWARDS THE WIRELESS LINK

- **Relay**
  - Independent of the crypto
- **Man on the middle**
- **Denial of service**
- **Eavesdropping/Skimming**



- **NFC characterization**
  - **Eavesdropping: > 20m**
  - **Skimming: > 1m**

COUNTERFEITING

Buying a fake branded handbag for your loved one?

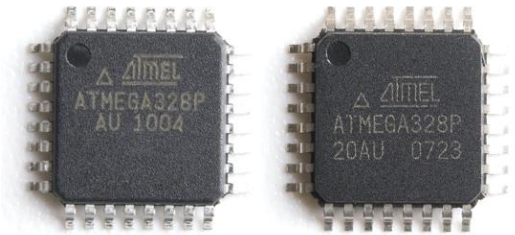
Finding horse meet in your beef lasagna?

Fake portable hard drive?

Having easy access to counterfeit medicines?

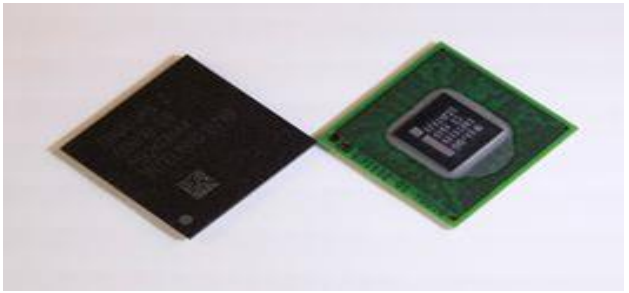
Counterfeiting accounts for 2% of the world trade!
Expected to exceed $1.7 trillion by 2015!

ALSO IN HARDWARE



Fake & genuine Atmel chips

Genuine & Fake Toshiba transistors



Fake chips sold to US military in 2010 (VisionTech scandal)

EXEMPLE: UN OUBLI FÂCHEUX !

autoblog

http://www.autoblog.com/2015/02/06/bmw-hack-cyber-security-warning-feature-video/

FOLLOWUP Feb 6th 2015 at 7:00PM 23

BMW Hack: the auto industry's big cyber-security warning sign [w/video]

Remote Nature Of Attack Is A Worrisome Landmark

No authentication

"They were able to reverse engineer some of the software that we use for our telematics," said Dave Buchko , a BMW spokesman. "With that they were able to mimic the BMW server."

"If all it does is open the locks, it's concerning, but if that vulnerability could have also sent messages to shut off the brakes, it would have been catastrophic," said Joshua Corman of The Cavalry, a non-profit that works with auto makers on cyber-security issues.

Correction:

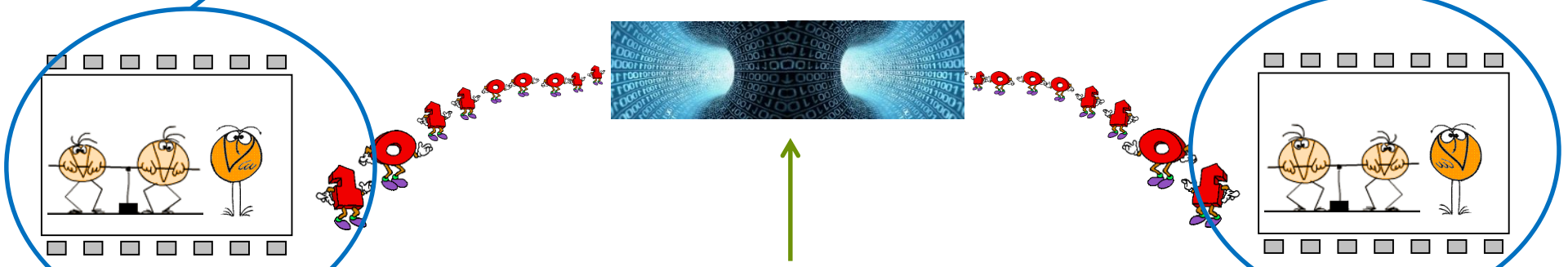
- Add authentication
- Integrity checking

The fix adds HTTPS encryption to the connection from BMW to the car, which runs over the public cellular network. The added encryption will not only safeguard the content of the messages but also ensures that the car only accepts connections from a server with the correct security certificate.

OUPS … J'AI OUBLIÉ L'AUTHENTIFICATION !

Source: http://www.ledauphine.com/france-monde/2015/09/01/lille-un-hacker-pirate-les-panneaux-de-parking

Secured by Cryptography



Channel is secured….

But, if an attacker has a physical access, he can extract the keys

ATTACKS ON SECURE DEVICES

Mathias Wagner, in "**700+ Attacks Published on Smart Cards**: The Need for a Systematic Counter Strategy" proceedings of Cosade 2012

Cr

RC5

MIFARE,

Brute force attacks,

Etc.

Buffer overflows,

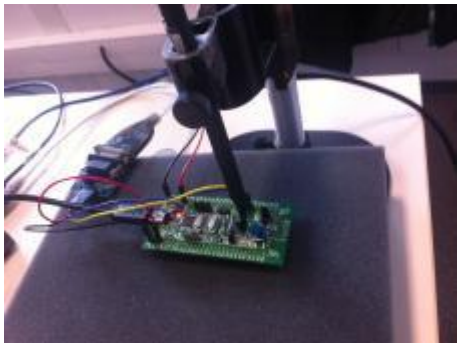
Brute force attacks,

Attacks on protocols

Etc.

Hardware attacks

Extremely powerfull thanks to the direct access to the component:



Example:
AES-128 key cracking in minutes on a 32-bit unsecure microcontroller

PRIVACY ?

- **TV magazine on June 5th, 2014**
  - Antenne2, « Envoyé spécial »

Selling Company

Risk

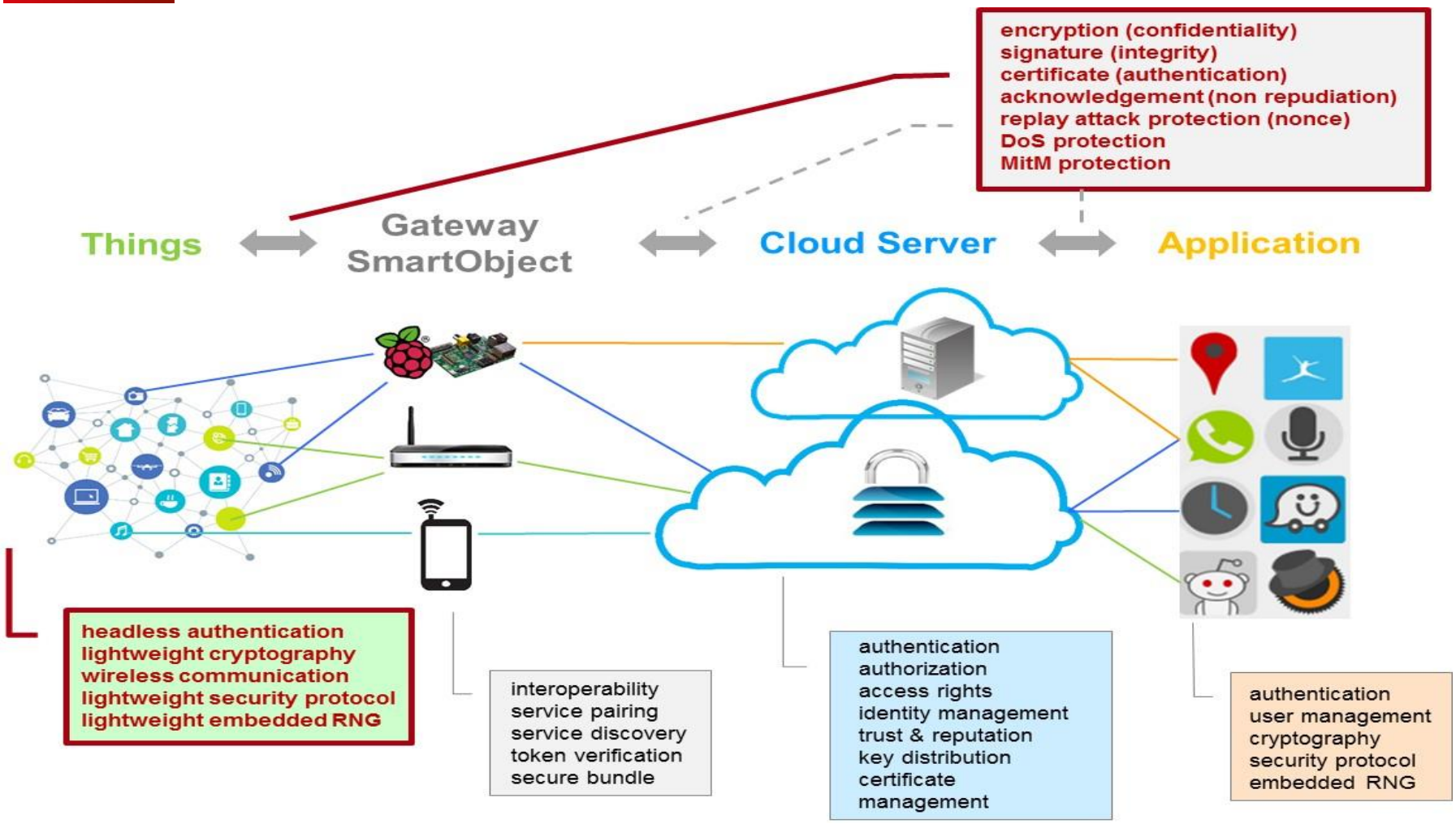
Reality

What do you expect.

NULL CTRL: DO NOT EXPECT TO STAY HIDDEN !

- Source:
  - http://www.dagbladet.no/2013/12/16/nyheter/nullctrl/shodan/english/english_versions/30861347/
  - Journalism in Dagbladet (Norway), European Press Prize 2013
- **Search engine: SHODAN**
- **2048 Cameras, 1781 Printers, 2500 Control systems**
  - Unprotected, « Open » access

CRYPTOGRAPHY IS COMPLEX …… BUT REQUIRED



BASIC SECURITY FEATURES

- **Risk analysis to define required security policy**
- **Authentication: I prove my identity, my interlocutor proves its own**
- **Integrity**
  - I check my integrity (embedded SW, HW components)
  - Each message must be integrity checked (CRC not enough)
- **Users role and privilege**
  - Administrator / User
- **Life cycle management**
  - Authentication & Integrity of new components
  - Update: Signature (authentication, integrity) of updates
  - Bootstrapping
  - End of life management
- **Security audit: Security actions must be recorded … and protected**
- **I know the attacks**
  - Replay (Stamp each message)
  - Man in the middle (shared secrets, certification authority)
  - Keys must be protected, adapted policy must be implemented

NEED FOR A OBJECTIVE MEASURE AND LABEL

Looking backwards

Efficiency of the Evaluation/Certification schemes for Smartcards

Common Criteria

No Security standard for emerging markets

Needs expressed:

- Emerging regulations: OIV, FDA for medical devices
- No standards: Automotive, IoT, Medical Devices, Biometrics, Home appliances…

Key elements for the future

Standard & trustworthy Certificates

Security Evaluations

Basic principles

- The developers express and justify
- The evaluator controls
- All steps of the life cycle are checked

AGD
Guides

ASE
Security Target

ADV
Development

ALC
Life Cycle

ATE
Testing
(Conformity)

AVA
Vulnerability
Analysis

UN MOT SUR LE LETI

LETI PIONNEERED SOI BUT IS ALSO…

Technological Research Institute

Alternative and Atomic Energy Commission

Defense Security

Military Applications Division

Staff: 4,500

Nuclear Energy

Nuclear Energy Division)

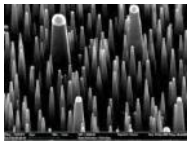
Staff: 4,500

Key Enabling Technologies

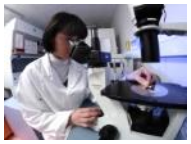
R…n

Staff: 4,500

Fundamental Research



Materials Sciences Division
Life Sciences Division

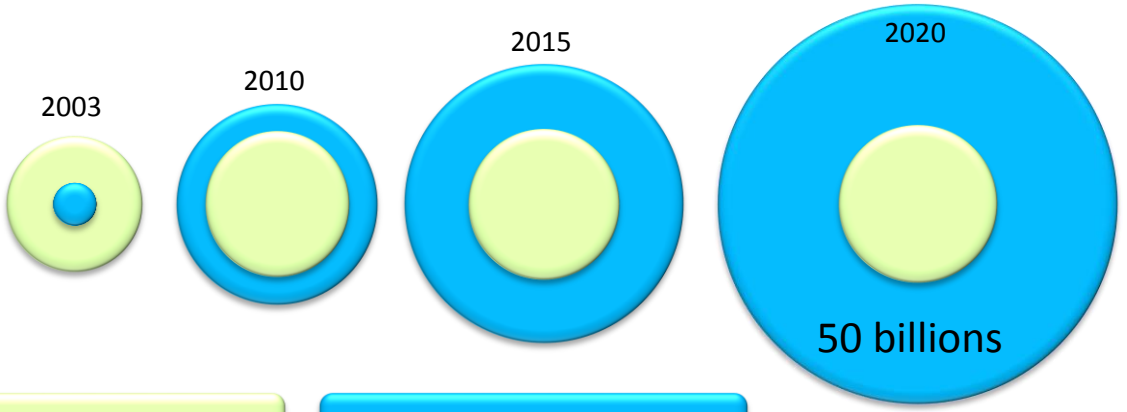


Low Power solution
Microelectronics
Connectivity
Security

Created in 1967

18000 folks

2015 - 2020: THE IOT HYPE



Worldwide population

Connected objects

Source: CISCO, AT&T

Smart Homes

Intelligent transport system

Business environment

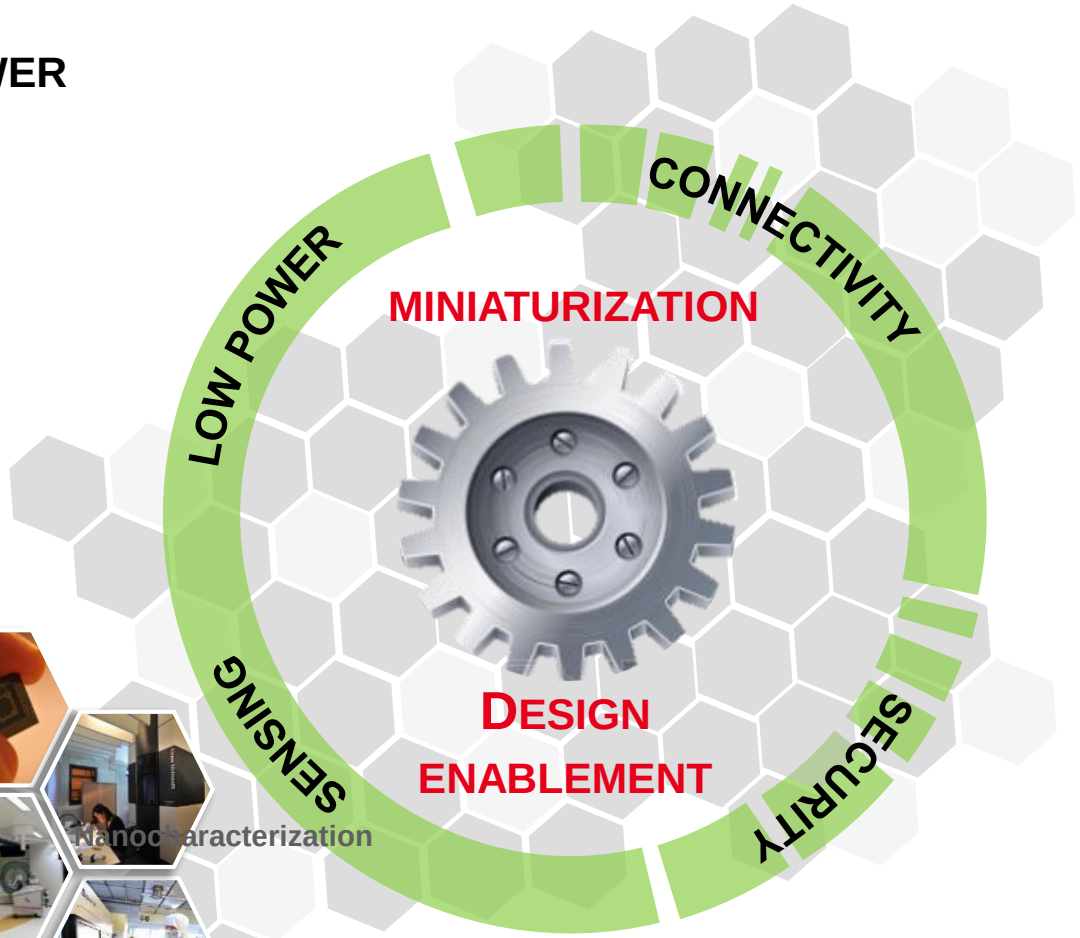
Logistics and retail environment

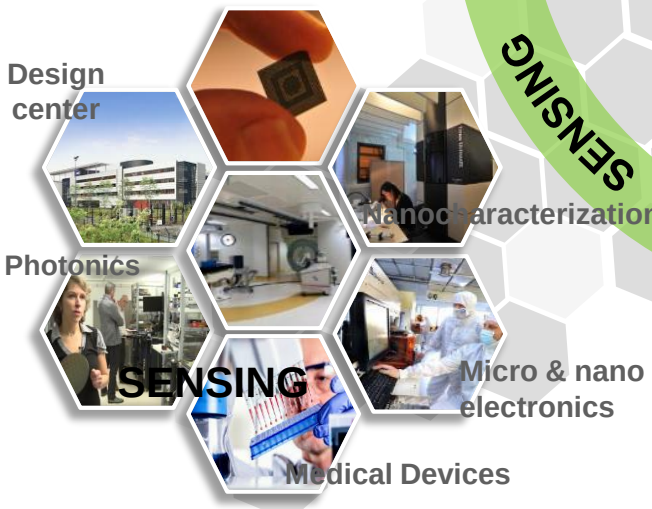
Health monitoring system

CORE BUSINESS

LOW POWER

CONNECTIVITY





SECURITY

Strong asset of Platforms

Reuters release – March 8th, 2016

www.reuters.com/article/us-innovation-rankings-idUSKCN0WA2A5

REUTERS EDITION: U.S. SIGN IN | REGISTER Search Reuters

HOME BUSINESS MARKETS WORLD POLITICS TECH OPINION BREAKINGVIEWS MONEY LIFE PICTURES VIDEO

Technology | Tue Mar 8, 2016 12:36pm EST

Related: SCIENCE, TECH

The World's Most Innovative Research Institutions

BY DAVID EWALT

"Silicon Valley's hoodie-wearing tech entrepreneurs are the poster kids of innovation. But the innovators who are really changing the world are more likely to wear labcoats and hold government-related jobs in ***Grenoble****, Munich or* ***Tokyo****."*

TOP 10 INSTITUTIONS|2015 RANKINGS

1 – CEA / FRANCE

2 - Fraunhofer Society / GERMANY

3 - Japan Science & Technology Agency / JAPAN

4 - U.S. Dept of Health & Human Services / USA

5 – CNRS / FRANCE

6 – KIST / SOUTH KOREA

7 – AIST / JAPAN

8 - U.S. Department of Energy / USA

9 – A*STAR / SINGAPORE

10 – INSERM (Health&Medical Research) / FRANCE

SMART OBJETS SECURITY

RISK ANALYSIS
IN CASE OF ATTACK

- Security risks classified by impact on the system with proven methodologies (EBIOS, STRIDE)

ARCHITECTURE ANALYSIS

- Identification of structural weaknesses on the global architecture
- System bricks faced to state-of-the-art threats and attacks

SECURITY TESTS

- Security tests on devices and system to detect and identify vulnerabilities
- Evaluation prior to ITSEF certification

SECURITY SOLUTION

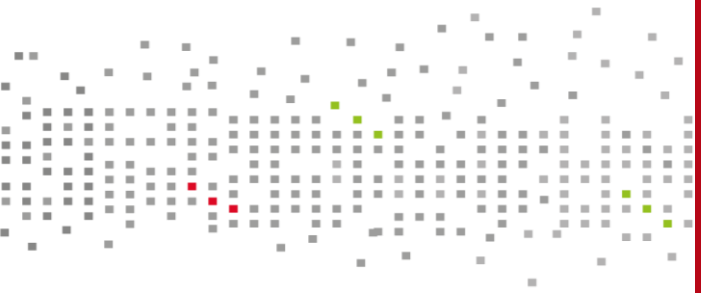
- Patch integration to fix identified vulnerabilities
- Specification of security blocs
- Security blocs design and integration into the system (HW/SW)

BENEFITS

- Robustness against external and physical attacks
- Compliance to regulatory requirements
- B2B and B2C product added-value
- Stronger brand image
- Trustworthy system

EXAMPLE

CONFIDENTIAL



Leti, technology research institute
Commissariat à l'énergie atomique et aux énergies alternatives
Minatec Campus | 17 rue des Martyrs | 38054 Grenoble Cedex | France
www.leti.fr