CYBERSECURITY OF MEDICAL DEVICES

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

SECURITY OF MD: A BRIEF HISTORY

THE LAST PUBLICATIONS

Security evaluation analysis

- Black box testing
- Covering the major potential vulnerabilities
- Huge Nb of potential flaws (>8000)

Highlighting the risks related to the implementation

RANSOMWARE

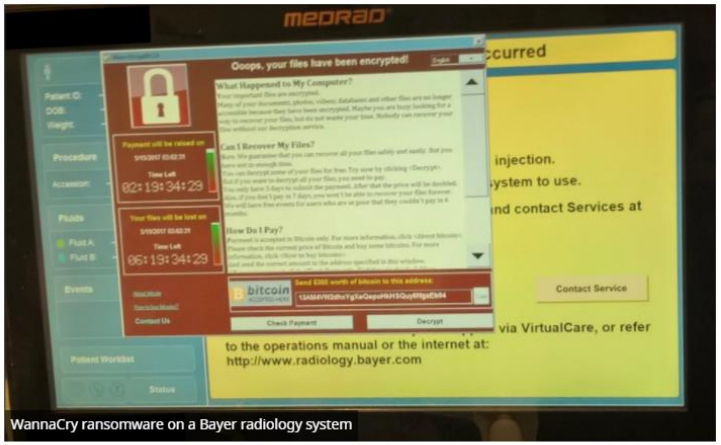
A Hospital Paralyzed by Hackers

A cyberattack in Los Angeles has left doctors locked out of patient records for more than a week. Unless the medical facility pays a ransom, it's unclear that they'll get that information back.

KAVEH WADDELL | FEB 17, 2016 | TECHNOLOGY

Share Tweet ... TEXT SIZE − +

https://www.theatlantic.com/technology/archive/2016/02/hackers-are-holding-a-hospitals-patient-data-ransom/463008/



WannaCry ransomware on a Bayer radiology system

A Bayer MedRad device used to assist in MRI scans infected with the WannaCry ransomware.

Security / #CyberSecurity

MAY 17, 2017 @ 09:00 AM 18,916

Medical Devices Hit By Ransomware For The First Time In US Hospitals

Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms. FULL BIO

https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#1ee7f73e425c

THE VERGE TECH SCIENCE MORE

TECH / CYBERSECURITY

52

UK hospitals hit with massive ransomware attack

Sixteen hospitals shut down as a result of the attack

by Russell Brandom | @russellbrandom | May 12, 2017, 11:36am EDT

MIRAI DDOS ATTACK

Un modèle de camera commercialisé par XiongMai.

ZDNet.fr > News > Mirai : Après l'attaque contre DynDNS, la riposte s'organise >

Mirai : Après l'attaque contre DynDNS, la riposte s'organise

Sécurité : *Passé l'attaque, la réaction s'organise afin de démanteler le botnet Mirai, à l'origine de plusieurs attaques Ddos retentissantes au cours du mois de septembre. L'effort risque d'impliquer aussi bien les constructeurs que les possesseurs d'objets connectés, les cibles préférées de Mirai.*

- **DDoS attack on Dyn's DNS nameservers**
  - 100s of websites (GitHub, Twitter, Netflix, AirBnb…) unaccessible for several hours.
  - Knocking off entire countries (Liberia)
  - Estimated over **a million of Mirai infected devices** involved!
  - > **1TBps attack**!

RISKS

- **Risk is on the device**
  - Ex pacemaker « killing » the patient
- **But also on the infrastructure**
  - DDOS
  - Worms
  - For ex: storing, distributing ransomware
- **And risk for the developer**

RECOMMENDATIONS / REGULATION

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document Issued on: October 2, 2014

The draft of this document was issued on June 14, 2013.

For questions regarding this document contact the Office of Device Evaluation at 301-796-5550 or Office of Communication, Outreach and Development (CBER) at 1-800-835-4709 or 240-402-7800.

2013/2014

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document issued on December 28, 2016.

The draft of this document was issued on January 22, 2016.

2016

2017

FDA RECOMMENDATIONS: PREMARKET (EXTRACT)

- **The approach should appropriately address the following elements:**
  - **Identification** of assets, threats, and vulnerabilities;
  - Assessment of the **impact of threats** and vulnerabilities on device functionality and end users/patients;
  - Assessment of the **likelihood of a threat** and of a vulnerability being exploited;
  - Determination of **risk levels and suitable mitigation strategies**;
  - Assessment of residual risk and **risk acceptance criteria**.

- **Cybersecurity fns**
  - **Identify & Protect**: Limit access, Ensure trusted content
  - **Detect, Respond, Recover:**
    - Implement features that allow for **security compromises** to be **detected, recognized, logged, timed, and acted** upon during normal use;
    - Develop and provide **information to the end user concerning appropriate actions** to take upon detection of a cybersecurity event;
    - Implement device features that **protect critical functionality**, even when the device's cybersecurity has been compromised;
    - Provide methods for retention and **recovery of device configuration** by an authenticated privileged user.

FDA RECOMMENDATIONS: POSTMARKET (EXTRACT)

- Effective cybersecurity risk management is intended to reduce the risk to patients by decreasing the likelihood that device functionality is intentionally or unintentionally compromised by **inadequate cybersecurity**. An **effective cybersecurity risk management program** should incorporate both premarket and postmarket **lifecycle** phases and address cybersecurity **from medical device conception to obsolescence**

- **Organizational**
  - **Risk management**: Continuous following, vulnerability scoring, evaluation of risk on patient harm

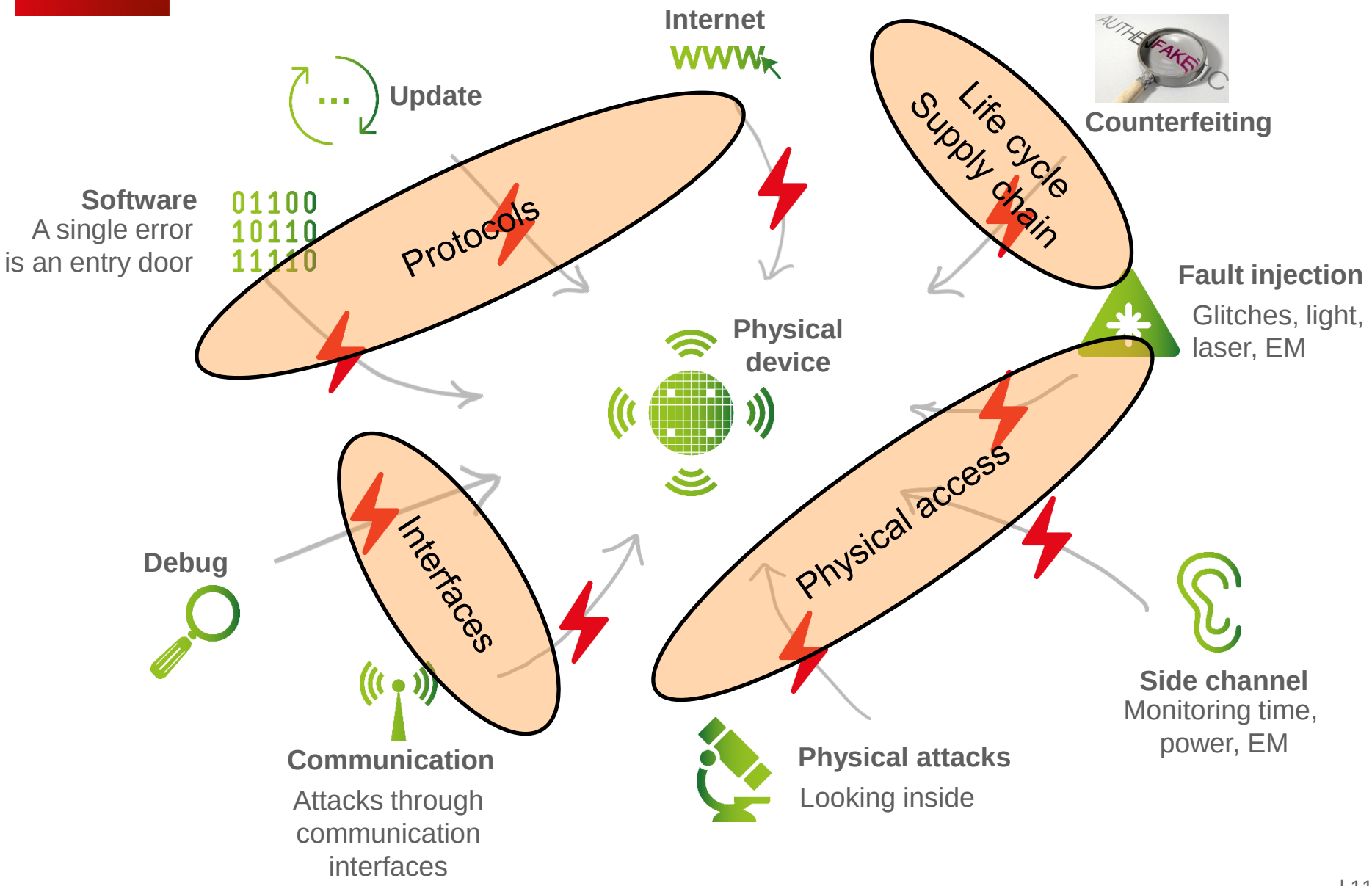
  - **Remediating & reporting vulnerabilities**
    - The customer communication should, at minimum: **Describe the vulnerability** including an **impact assessment** based on the manufacturer's current understanding,
    - State that manufacturer's efforts are underway to **address the risk of patient harm** as expeditiously as possible,
    - Describe **compensating controls**, if any, and
    - State that the manufacturer is working **to fix the vulnerability**, or provide a **defense-in-depth strategy** to reduce the probability of exploit and/or severity of harm, and will communicate regarding the availability of a fix in the future.

MAIS AUSSI

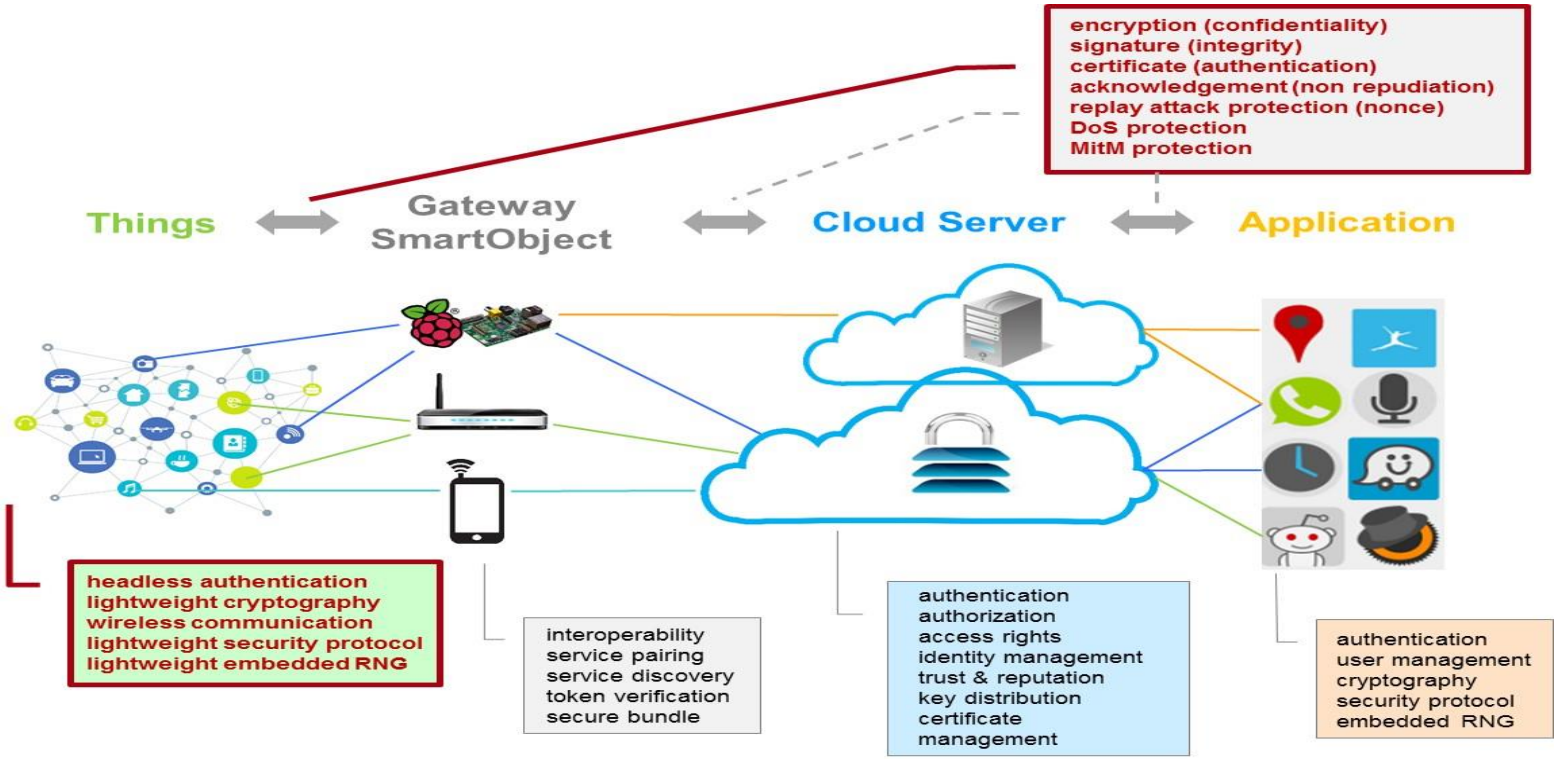
- Rappelons que la **procédure d'agrément des hébergeurs de données de santé** à caractère personnel a été instaurée par la loi n°2002-303 du 4 mars 2002, dite "loi Kouchner". Elle vise à assurer la **sécurité, la confidentialité et la disponibilité** des données de santé à caractère personnel, lorsque leur hébergement est externalisé

- Le **GDPR, «general data protection regulation»**, est le nouveau règlement européen décidé en décembre 2015 qui s'appliquera dès 2018 à toute entreprise qui collecte, traite et stocke des données personnelles dont **l'utilisation peut directement ou indirectement identifier une personne**.

SECURITY IS COMPLEX



CRYPTOGRAPHY IS COMPLEX

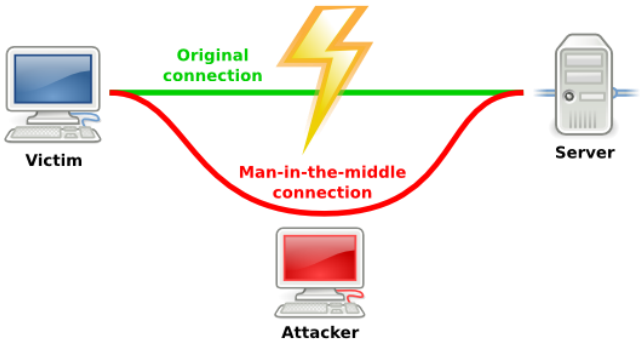


- **Key management: Bootstrap, Update, Recovery**

- **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**

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,

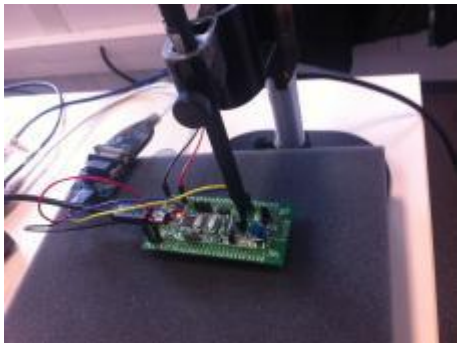
Brute force attacks,

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

SECURITY REQUIREMENTS

Security architecture
- Rôle
- Audits
- Logs

Software
- Bug free
- Proved SW

Tamper resistance
- Memory reading
- Probing
- Debug ports

Security of communications
- Authentication
- Confidentiality
- Integrity

Side channel resistance
- Time
- Power
- EM

Security protocols
- Bootstrap
- Update
- Recovery

Fault injection resistance
- Glitches,
- Light
- Laser
- EM

Lifecycle management
- Authenticity
- Integrity

By technology, architecture & embedded SW

CYBERSECURITY CERTIFICATION

European Certification
- All member states
- All products (incl « low » resistance)
- Driven by ENISA

« Historic » states (FR, DE, NL, S,)
- « High » security levels
- Common Criteria (extension CSPN)
- Driven by national Agencies
- Too complex (costly) for a generalization

Industrial offer

- Focused on conformity
- Numerous offers

Challenges:
- « All level » offer
- Efficiency: complexity/Time/Cost
- Attacks vs Conformity
- Standards ?

SECURITY CERTIFICATION: SUMMARY

- **Starting point is a risk analysis & security description**
- **Certificates does not guarantee that an attack is impossible, but guarantee that:**
  - The conformity of the product to its security specifications
  - A successful attack will be over a minimum level of complexity (cost, time, means, etc)
- **A certificate is a « picture » at a specific time**
  - Needs a « maintenance » to follow the state of the art

RECOMMENDATIONS

- **Always start with a risk analysis specific to the device**
- **Cybersecurity has to be the central element of the design**
  - Secure by design, in depth security, etc
  - Basic security functions have to be integrated
  - Role definition, authentication of users, of components
  - Integrity checking, attacks detection, security events recording, forensic, …
- **Pay a specific attention to the implementation**
- **Secured life cycle implementation**
  - Update, recovery, …
  - Surveillance, reaction capabilities
- **Use Certification when available, but for no more than expected**
- **For the future**
  - Define standards for cybersecurity
  - Merge safety and security assessment

NEEDS FOR THE FUTURE: SECURE BY DESIGN

MEDICAL DEVICE

Intrinsic resistance

- Security features (authentication, integrity, Attack detection, etc)
- Security Policy (audits, role, etc)

Life cycle Mgt

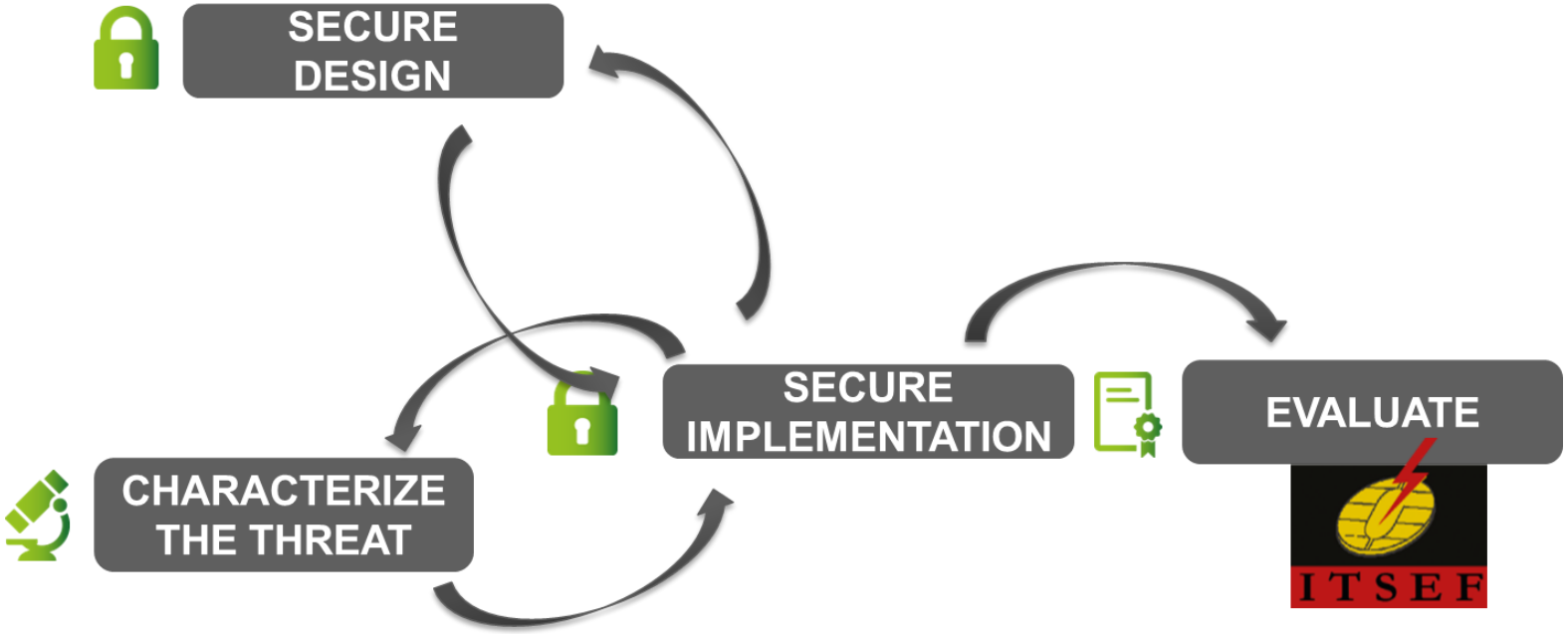
- Bootstrap, Recovery
- Update

- Ensure **safety** (for the patient) even in case of cyber attack
- Ensure **reliability** of the system even in case of cyber attack

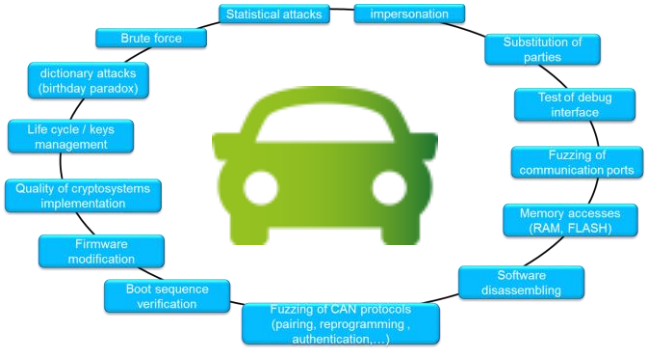
Certified Safety & Security

JUST A WORD ABOUT US

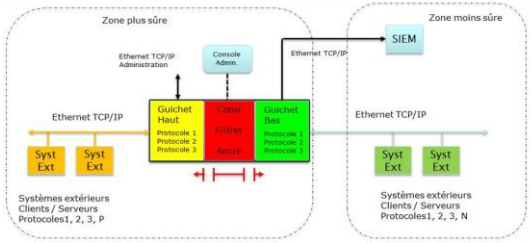
- **LETI is a RTO in micro and nanoelectronics**
  - One of the European leader
  - 2000p, clean rooms, 200mm, 300mm platforms, FDSOI 28nm
- **100p in cybersecurity**
  - From Integrated Circuits to applications
  - From vulnerability analysis to evaluation/certification

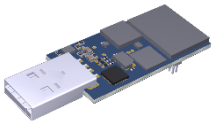


CYBERSECURITY @ LETI : SUCCESS STORIES IN SECURING PHYSICAL CYBER SYSTEMS

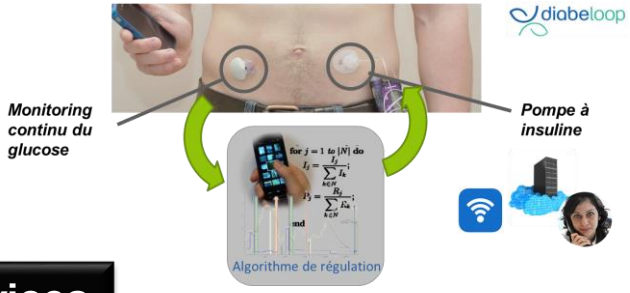


Automotive

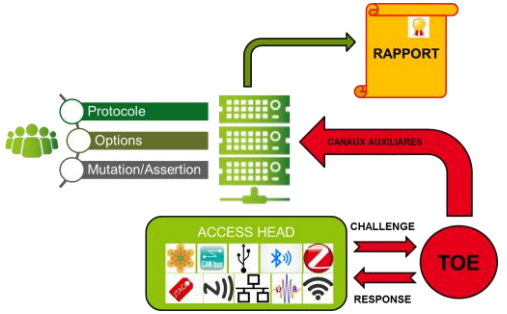




Industrial systems



Medical Devices



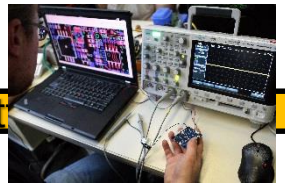
CEATECH / BUREAU VERITAS COLLABORATION

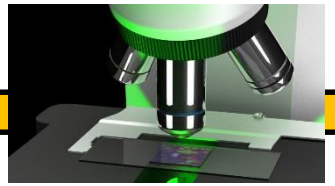
- **CEATech (LETI, LIST) are collaborating with BV to:**
  - Develop tools and methods to propose an efficient evaluation/certification framework
  - SW analysis
  - Devices testing (interfaces)

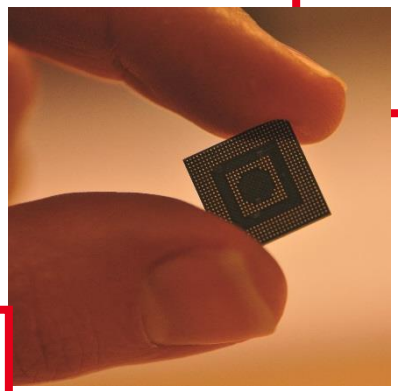
SW Testing
Good practices

Interfaces testing

CSPN
Common Criteria





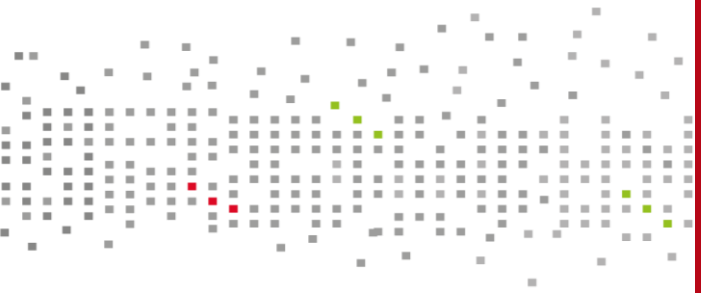



LETI proposes

Integrated & efficient security solutions

Security evaluation capabilities

to our partners for securing applications & systems



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