CYBER SECURITE des objets connectés, un risque majeur

”BON RISK APPETIT”

Juin 2016

Les Objets connectés c'est un risque multiplié par 10

-Actuellement la menace cyber n'est pas « encore » maitrisée et la situation se dégrade

-La révolution du monde numérisé, mobile et dans les nuages: ce sont des fonctionnalités fantastiques mais des « nouveaux » risques majeurs

-Comment aller vers ce nouveau monde avec encore plus de confiance: un défi majeur que l'industrie DOIT résoudre: « bon risk appetit » ou comment apprendre à gérer le risque cyber

Les Objets connectés c'est un risque multiplié par 10

Actuellement la menace cyber n'est pas « encore » maitrisée et la situation se dégrade

De l’ombre à la lumière

De l'ombre vers la lumière

25 ans d'histoire.

Un risque marginal conduit par quelques « geek » est devenu en 25 ans un risque stratégique.

1989-2005: les virus, I love You en 2000

2005-2010: action des états, Stuxnet, espionnage,

2010-2015: cybercriminalité (dépasse le trafic de drogue)

2016: La Cyber Guerre: Ukraine-Russie

L'aspect ludique des années 1990 est devenu un risque mondial

C'est maintenant un élément stratégique de la défense des nations qui est comparé avec le nucléaire (dissuasion): Cyber…L'arme fatale ?

Pourquoi une telle évolution: augmentation de la menace, augmentation du risque….

La surface du risque augmente: 5 milliards d'objets connectés en 2015, 50 milliards en 2020 avec l'Internet des objets

Les menaces augmentent: 1 millions de hackers: des individus, des mercenaires ou des personnels étatiques.

Le niveau d'expertise des hackers augmente: partage d'expérience sur les réseaux sociaux

Profiles of attackers are working in such activity

-Individual hackers working in network: dark web, deep web

-Organized hackers in group

- mafia, cyber criminality

-activist:: anonymous….

-Cyber army: spying, breaking…

Individual hacker

56 Hackers Arrested in Cyber Crime 'Strike Week' Raids in UK

Friday, March 06, 2015 Mohit Kumar

The United Kingdom's ***National Crime Agency (NCA)*** has arrested 56 suspected hackers in a campaign against cybercrime called "strike week."

Law-enforcement officials conducted, in total, 25 separate operations across England, Scotland and Wales, and those arrested were suspected in a wide range of cyber crimes including:

China Arrested 900 Hackers With International Cooperation

Posted on November 12, 2015 by **Mohammad Rafati** in **Anonymous**, **Cyber security**, **Cybercrime**, **Cyberwar**, **Infosec** // 0 Comments

They use software available on dark web, example: ransonware, crypto locker

Cyber arms are on the net

Deep Web, Dark Web

Cyber Mafia

WANTED
BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

EVGENIY MIKHAILOVICH BOGACHEV

Multimedia: Images

Aliases:
Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

Cyber mafia employs cyber mercenaries from ukraine romania….

Cyber activist: anonymous against Daesh

WauchulaGhost a retweeté

Daily Mirror @DailyMirror · 10 juin

Voir la traduction

Anonymous hacker hijacks ISIS Twitter accounts and floods profiles with PORN mirror.co.uk/news/world-new…

65 85

Tweet épinglé

WauchulaGhost @WauchulaGhost · 17 h

Anonymous Hacker Hijacks ISIS Twitter Accounts and Floods Them with Adult Images
news.softpedia.com/news/anonymous…
via @campuscodi

Anonymous Hacker Hijacks ISIS Twitter Accounts ...

WauchulaGhost says he's promoting love and exposing IP addresses and real names behind ISIS supporters

news.softpedia.com

Cyber war of states: spying

ASML hack: Global Chip Machine producer in the Netherlands and France has been hacked

February 28, 2015 // 0 Comments

The high technology manufacturer ASML has been hacked by alleged Chinese state hackers. The ASML company has claimed that they have been breached by Chinese state hackers and [Continue reading]

Cyber war of states: spying

Twitter (204) Facebook (3,913) Share

May 19, 2014 12:00 PM

Five Chinese Military Hackers Charged with Cyber Espionage Against U.S.

From left, Chinese military officers Gu Chunhui, Huang Zhenyu, Sun Kailiang, Wang Dong, and Wen Xinyu have been indicted on cyber espionage charges.

In a case out of the Western District of Pennsylvania, five Chinese military hackers were indicted on charges of computer hacking, economic espionage, and other offenses directed at six American victims in the U.S. nuclear power, metals, and solar products industries. This marks the first time criminal charges have been filed against known state actors for hacking.

From 2006-2014, defendants Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, who were officers in Unit 61398 of the Third Department of the Chinese People's Liberation Army, were allegedly involved a hacking conspiracy that targeted Westinghouse Electric Co.; U.S. subsidiaries of SolarWorld AG; United States Steel Corp.; Allegheny Technologies Inc.; the United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union; and Alcoa, Inc.

Spying of States

…Today Soft Cyber war

Iran Cyber Army Hacked Obama Administration Email & Social Media Accounts

Posted on November 5, 2015 by **Mohammad Rafati** in **Cyber security**, **Cyberwar**, **Hacking**, **Infosec** // 0 Comments

Israel Informed Europe To Shut Down Iran Cyberspy Group C&C Servers

Posted on November 9, 2015 by **Mohammad Rafati** in **Anonymous**, **Cyber security**, **Cyberwar**, **Hacking**, **Infosec** // 1 Comment

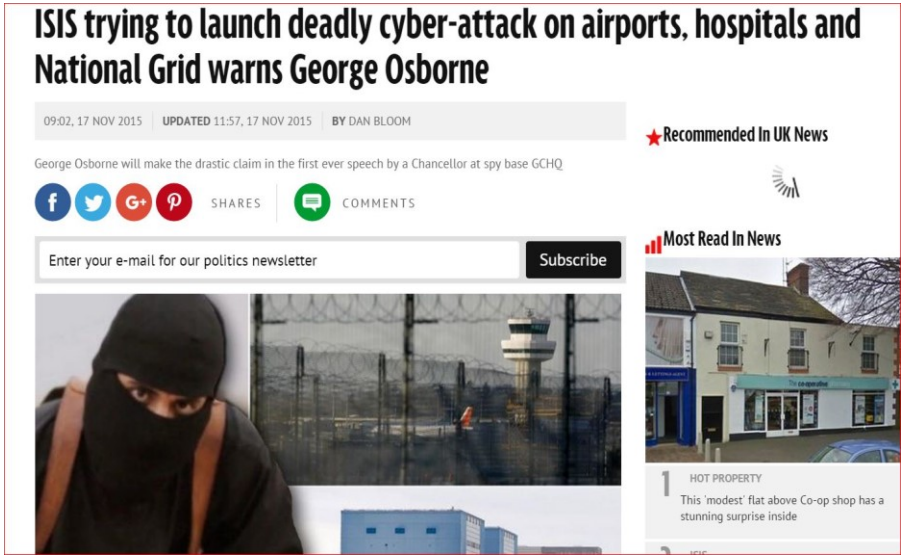
Tomorrow morning, cyber war with dead ?

News › UK › UK Politics

Isis plotting cyber warfare to kill people in UK, claims George Osborne

Chancellor George Osborne will announce the new National Cyber Centre, which will be based at GCHQ

Oliver Wright Political Editor | @oliver_wright | Thursday 19 November 2015 | 29 comments



ISIS trying to launch deadly cyber-attack on airports, hospitals and National Grid warns George Osborne

09:02, 17 NOV 2015 | **UPDATED** 11:57, 17 NOV 2015 | **BY** DAN BLOOM

George Osborne will make the drastic claim in the first ever speech by a Chancellor at spy base GCHQ

SHARES COMMENTS

Enter your e-mail for our politics newsletter Subscribe

Recommended In UK News

Most Read In News

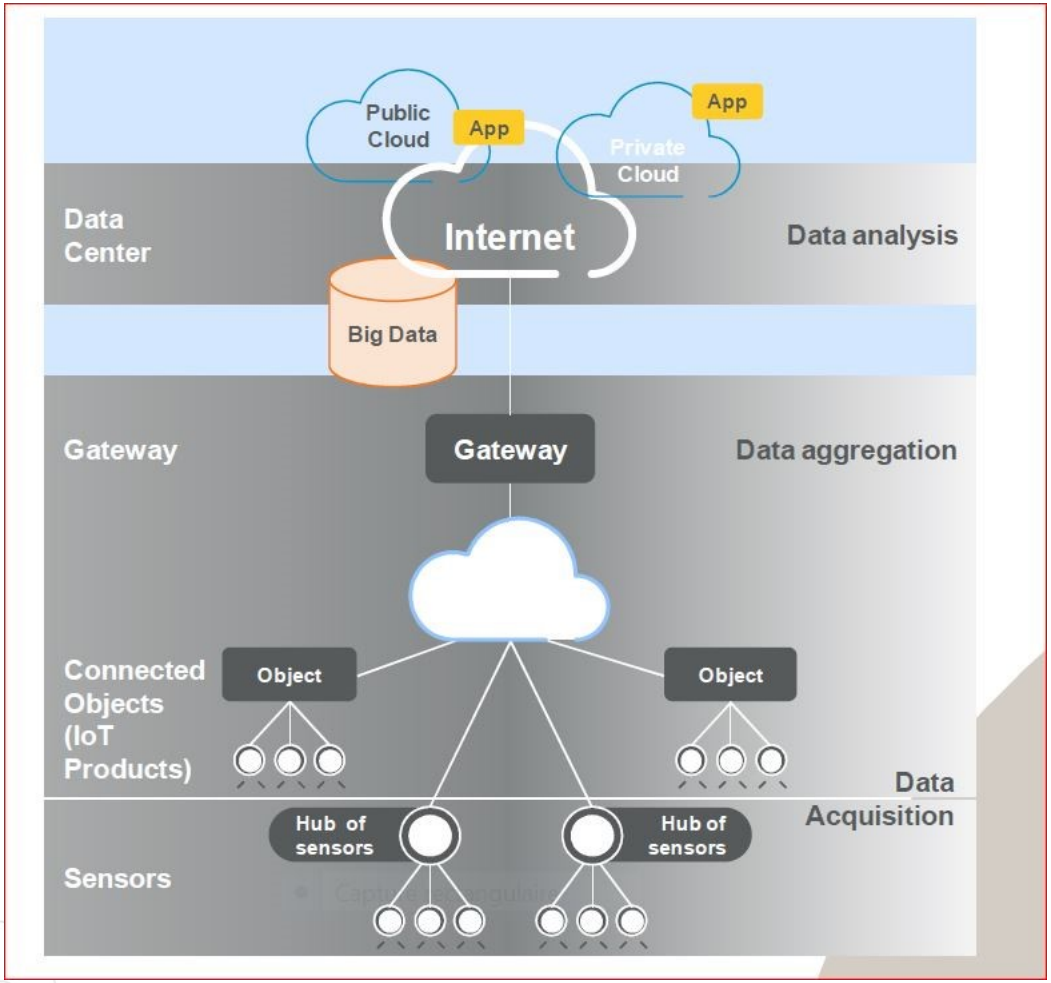
1 HOT PROPERTY

This 'modest' flat above Co-op shop has a stunning surprise inside

Les Objets connectés c'est un risque multiplié par 10

La révolution du monde numérisé,mobile et dans les nuages: ce sont des fonctionnalités fantastiques mais des « nouveaux » risques majeurs

Une surface d'attaque plus grande



Notre vie au quotidien en danger

La NON sécurité est partout

Desktop Viruses Coming to Your TV and Connected Home Appliances

Tuesday, April 22, 2014 Swati Khandelwal

G+1 47 Like 525 Share 196 Tweet 102 Share 15 share 499

Des services critiques sans sécurité

Cyber Attacks Leverages Internet of Things

Smart devices such as traffic and surveillance cameras, meters, street lights, traffic lights, smart pipes, and sensors are easy to implement, but are even easier to hack due to ***lack of stringent security measures and insecure encryption mechanisms***.

Last year, we saw a real cyber attack scenario involving IoTs in which hackers compromised more than 100,000 Smart TVs, Refrigerator, and other smart household appliances to send out millions of malicious spam emails.

La voiture du futur ? Quelle sécurité ??

Car Hacking ? Scary, But Now it's REALITY!

Saturday, July 25, 2015 Swati Khandelwal

Next time you find yourself hooked up behind the wheel, make sure that your car is actually in your control.

L’espion c’est Le chat du voisin

How to Weaponize your Cat to Hack Neighbours’ Wi-Fi Passwords

Saturday, August 09, 2014 Swati Khandelwal

G+1 655 Like 61K Share 40.1K Tweet 2282 Share 137 share 44.3K

What do you expect from your cat to come back with?? Perhaps with a mouse or a bird – none of your use. But what if she come back with your neighbours’ wifi details? Really Interesting!

La situation actuelle est critique

Les objets connectés actuels sont conçus pour leur fonctionnalité, pas ou peu de sécurité

Ces milliards d'objets connectés sont des « cibles » faciles

Comment les consommateurs peuvent accepter une telle situation et promouvoir la notion de « société » du risque zéro….

Le travail à accomplir est immense et il faut changer totalement de paradigme: « bon risk appetit », pas de risque zéro mais apprendre à gérer le risque

Les Objets connectés c'est un risque multiplié par 10

Comment aller vers ce nouveau monde avec encore plus de confiance: un défi majeur que l'industrie DOIT résoudre: « bon risk appetit », comment apprendre à gérer le risque cyber

A Quick and Strong reaction…. Bon risk appetit

https://www.capgemini.com/blog/cto-blog/2014/12/technovision-2015-bon-risk-appetit

The *Bon Risk Appétit* design principle is not about eliminating all risks – an impossible task. It is about doing business at an acceptable level of risk. It is also about taking a fresh perspective dealing with risks – a perspective which not only makes the risks acceptable, but also could well turn them into opportunities – a new competitive advantage or even a disruptive business model.

A Quick and Strong reaction.

CYBERSECURITY STRATEGY: MOVE OVER THE FORTRESS APPROACH, TIME FOR THE AIRPORT

IDENTIFY

MONITOR

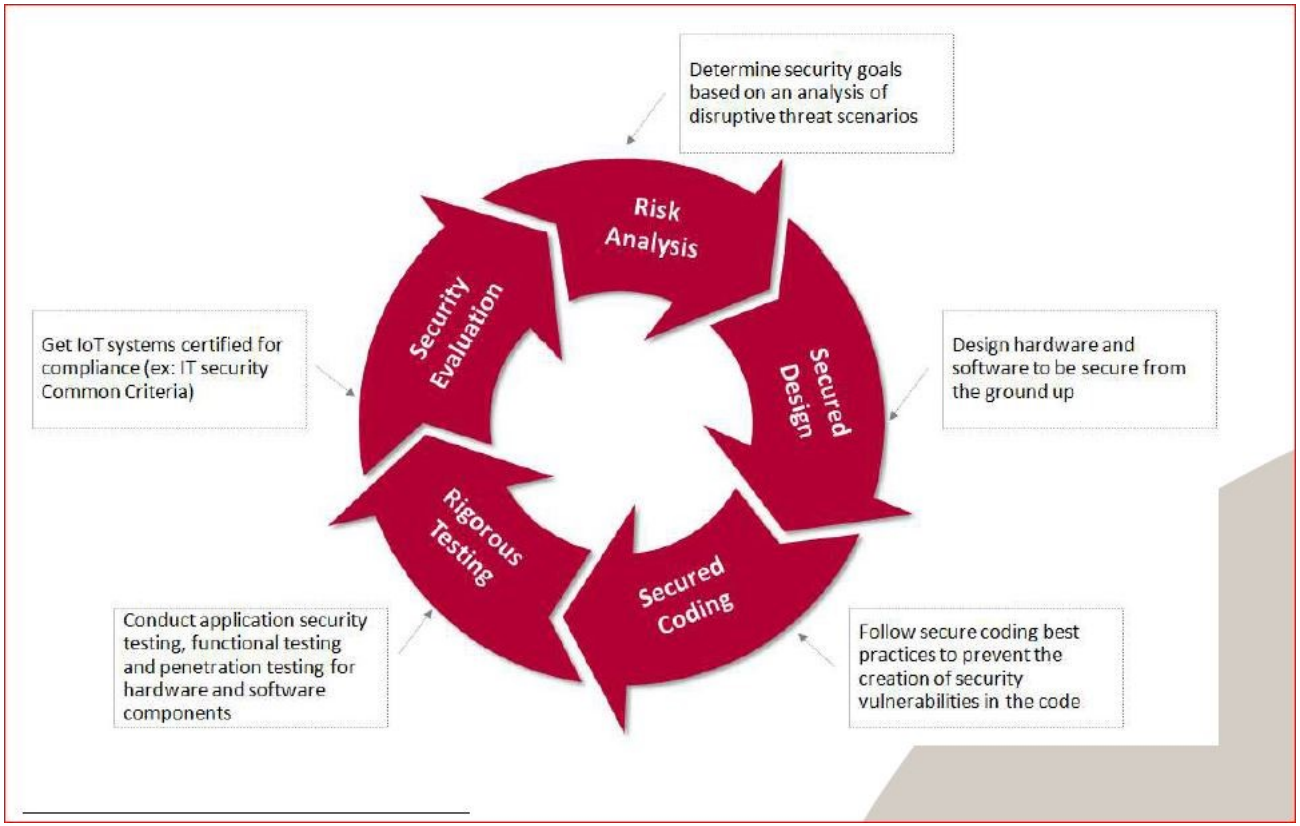
DETECT

REACT

PREVENT

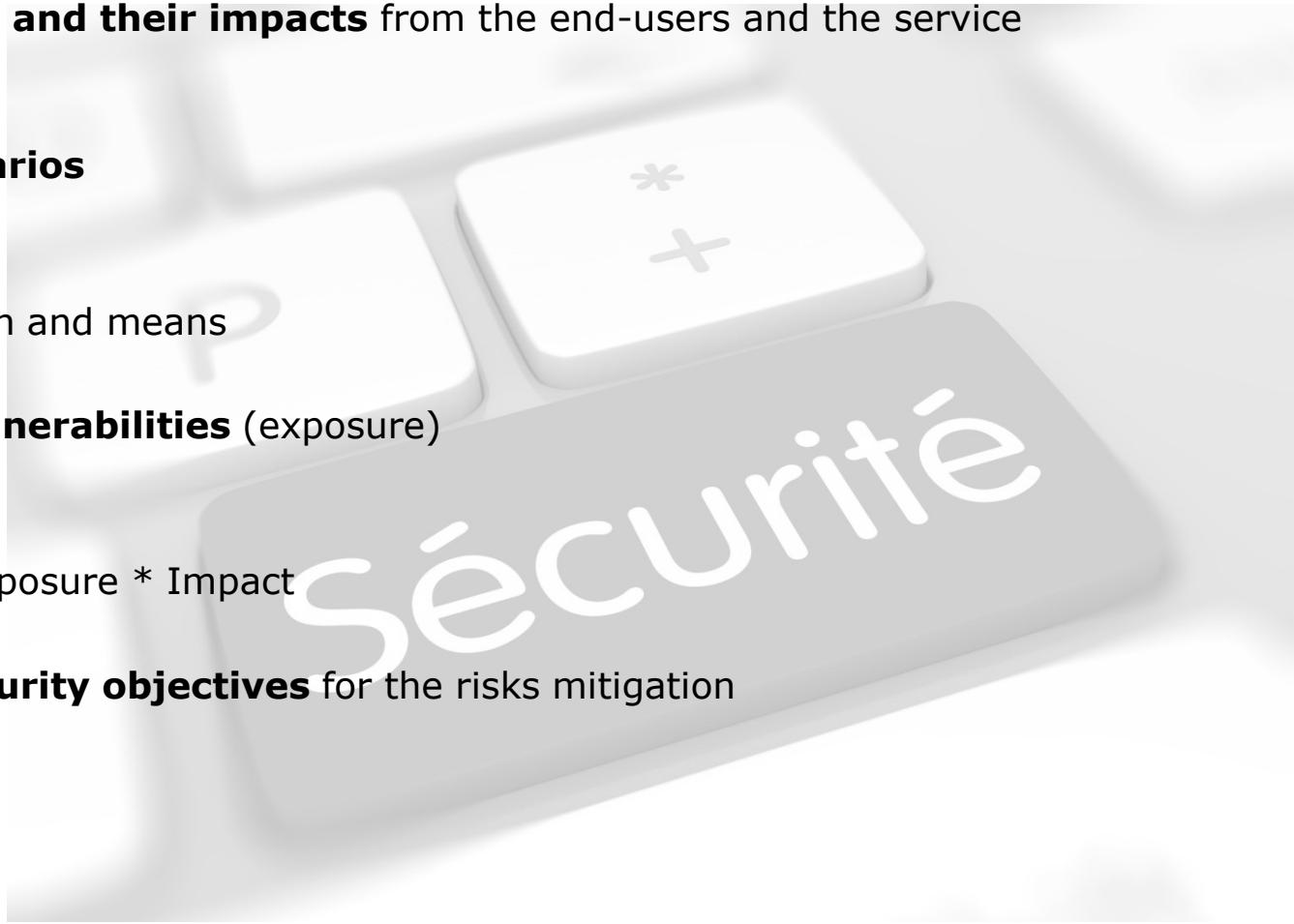
HARDENING INFRASTRUCTURE

Le mot clé: security by design



Risk…Risk…Risk… vive EBIOS

- Choosing from what we want to be protected
- Study of **feared events and their impacts** from the end-users and the service provider point of view
- Study **the threat scenarios**
  - Software attacks
  - Physical attacks
  - Attackers motivation and means
- Study of the **system vulnerabilities** (exposure)
- **Risks assessment**
  - Level of threat * Exposure * Impact
- Identification of the **security objectives** for the risks mitigation



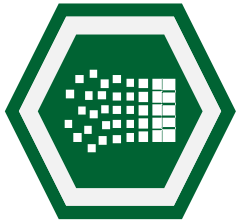
IT security solutions are not always applicable

Safety constraints

- Security recommendations must be complementary and not redundant
- Add the analysis of malicious actions to the engineering culture which focus on product failures

Operational constraints

- Regular security updates are made difficult (i.e.: Antiviral protection is not always feasible)
- Automatic screen-locking not advisable in the control room
- Excess of trust form end users



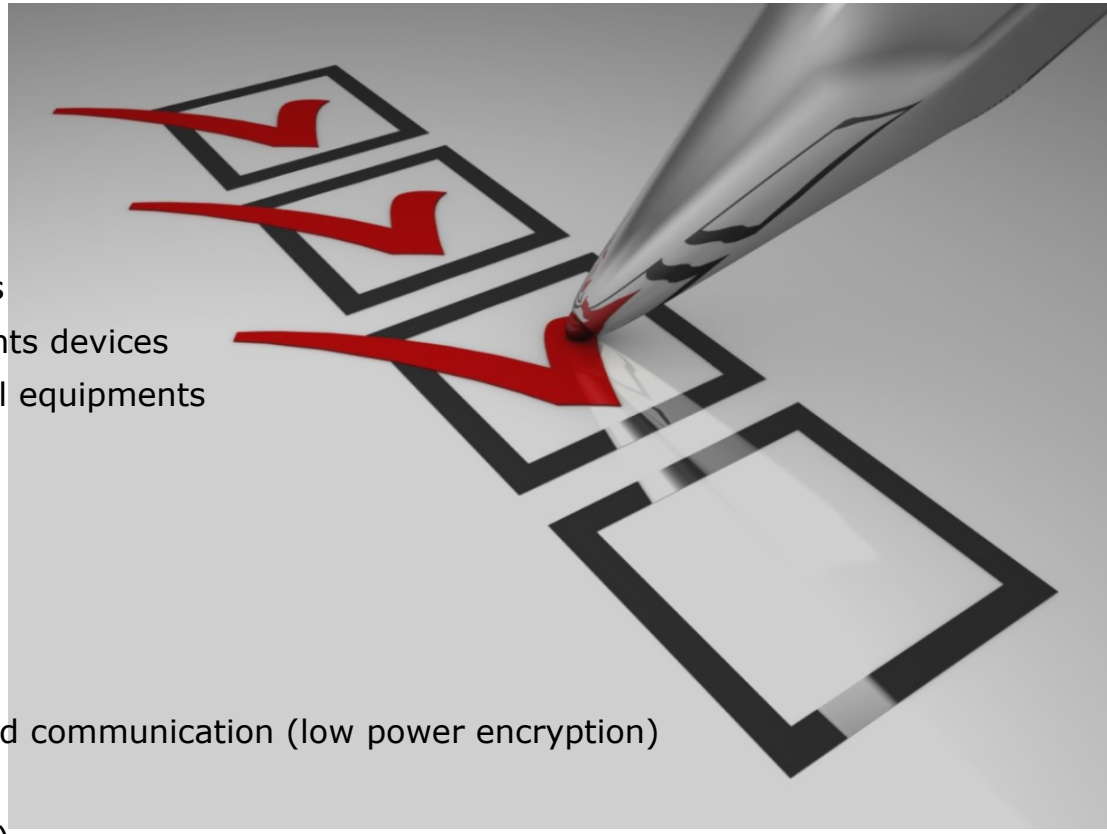
Technology constraints

- Firewalls and IDS have a poor knowledge of control system protocols
- Devices are fully open (USB port) and often easily accessible
- Embedded constraints (CPU, Memory …) are limiting the solutions choice (i.e., crypto, PKI …)

Standards and Regulations

- Lack of maturity
- ISA/IEC 62443, NIST SP 800-82
- ANSSI, Homeland Security
- Sectors regulations, products certifications

- **Securing** the system is at least securing :
  - the access
  - the communication channel
  - the data storage
  - the embedded software in devices
- **Defence in depth** to discourage attackers
- **Boundary defence**, focus on the end points devices
- **Reinforced physical protection** of critical equipments
- **Separate the privilege domains**
- **Segregate the networks**
- **Secure by default**
  - On OS, framework and devices configuration
  - On network for ICS, white list approach
  - Minimum privilege
- **Encryption** for data storage and end to end communication (low power encryption)
- **Remote wiping** of information
- **Resiliant coding** (design and coding rules)



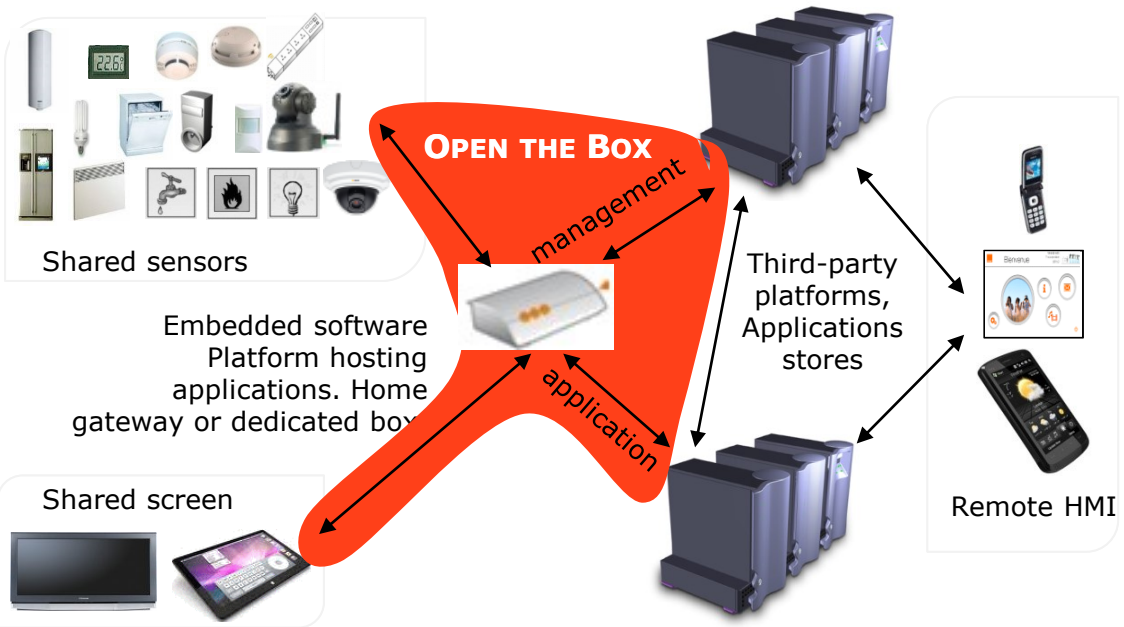
An example : Home Automation Box securization

Goals

- Among an entreprise consortium, Open the Box is a project aiming to design a home automation box by elaborating a prototype around a shared infrastructure built upon:
  - A restrited amount of normalized sensor networks
  - An embedded software platform of services
  - Standardized administration capabilities

SOGETI High Tech is focusing on security of the box and sensors

Approach

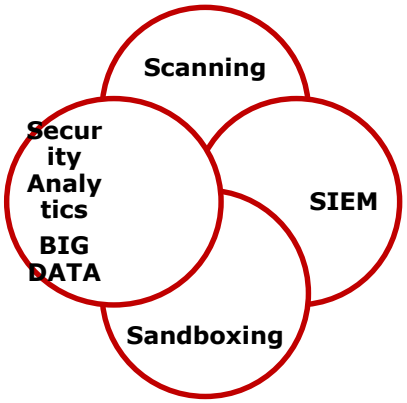


Activities

- Risk Analysis using EBIOS
  - Feared events analysis,
  - Threat scenarios analysis,
  - Risk analysis,
  - Security countermeasure definition
- Java Secure Coding guidelines
- Security testing (NIST SP800-115)
  - Intensive use of penetration tests tools
  - NeXpose, Metasploit, Ettercap, Wireshark, Kismet
- Implementation of a framework of 75 pentests on the JVM, OSGI layers and Zigbee
  - One java bundle per tests
  - Automated execution
- Linux kernel, Java OSGi

CYBERSECURITY MONITORING

SECURITY MONITORING
of IT systems, industrial systems & data



SECURITY OPERATION CENTERS