CRESITT INDUSTRIE

Centre de Ressources
Technologiques en Électronique

Sécurisation des systèmes électroniques

Panorama des enjeux et règles de bonnes pratiques

S. ROUXEL – 20 juin 2018 – v 1.0

Réf du document : Sem_Securisation_PPT_SR_Panorama_v1.0_20180620

Le CRT CRESITT est soutenu par :

L'action de diffusion technologique est cofinancée par l'Union européenne.
L'Europe s'engage en région Centre-Val de Loire avec le Fonds européen de développement régional.

SOMMAIRE

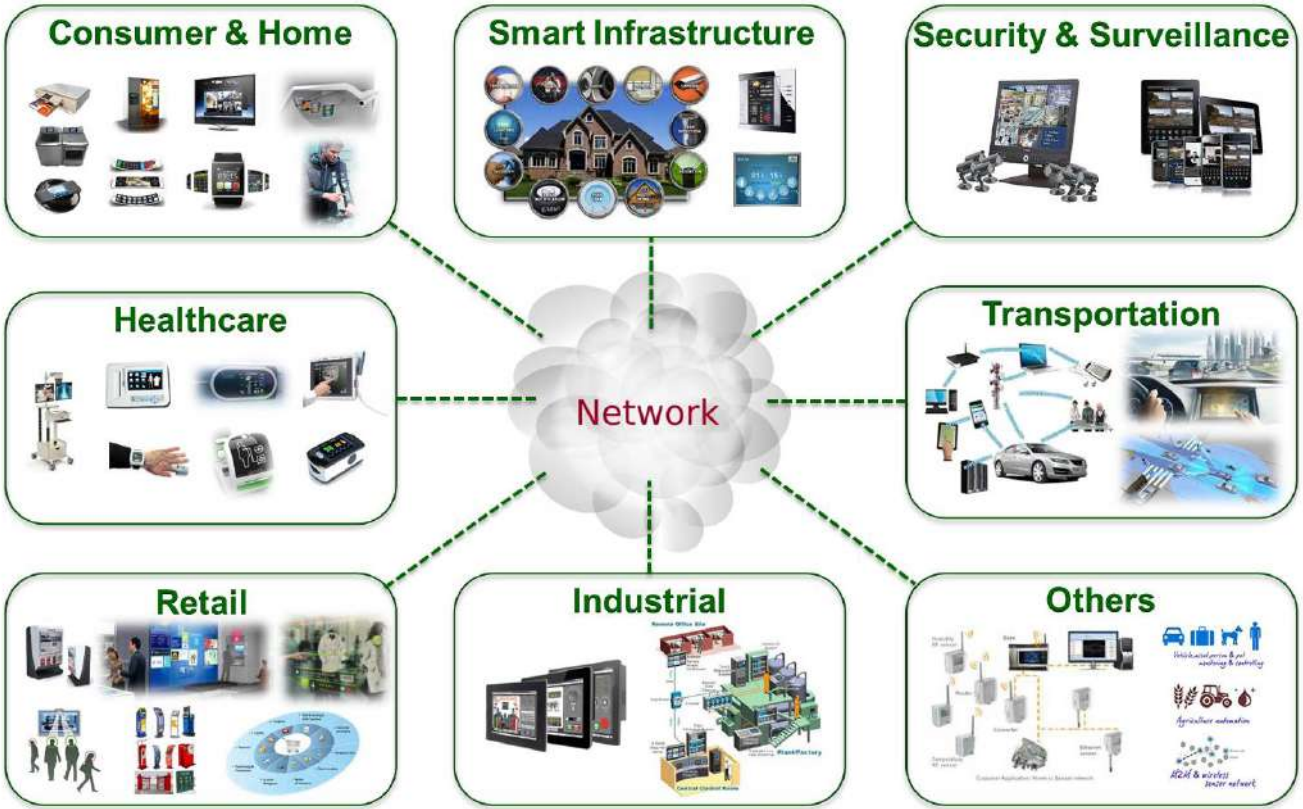
- Dynamique marché / cybercriminalité
- Enjeux
- Prévention
- Illustration

Dynamique marché / cybercriminalité

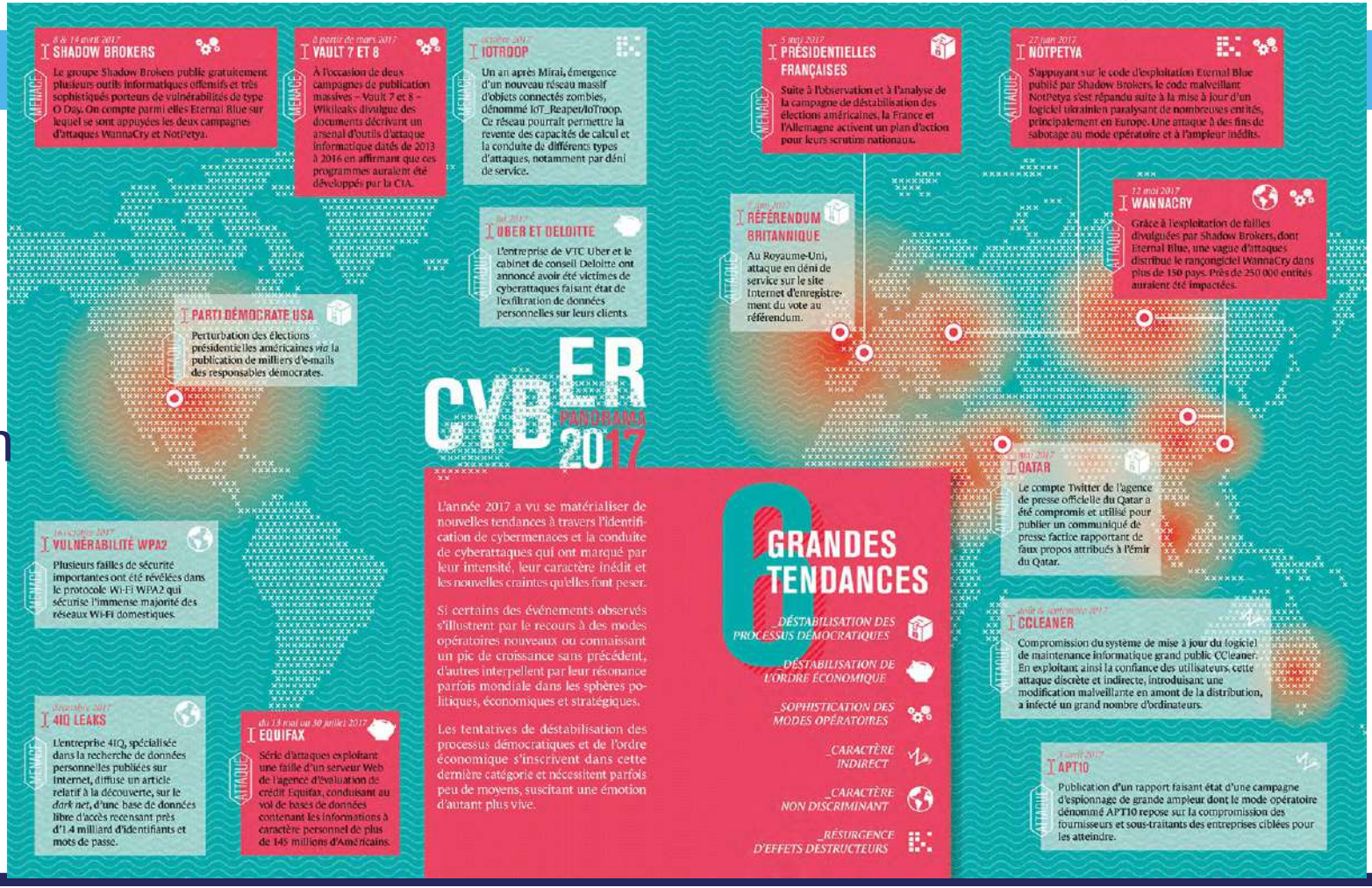
- Déploiement IoT
  - 2017 : 8.4 milliards (27 milliards d'unité)
  - 2020 : 20.4 milliards
  - 2030 : 125 milliards d'unité
- Autres
  - 2020 : 10 milliards d'unité

src : Gartner, (Arbor Networks), businessinsider.com

Dynamique marché / cybercriminalité



Cyber-Geddon



src : Anssi

Dynamique marché / cybercriminalité

- Type d’attaques
  - DDoS, DoS
  - Ransomware
  - Malware (trojan, worms, virus)
  - Spambots
  - Backdoors
  - Hameçonnage ...

Cybercriminalité

- Méthodes
  - Informatique (réseau)
  - Social engineering
    - téléphone
    - lettre
    - internet
    - contact direct
  - Clef usb
  - Failles de sécurité du matériel

Cybercriminalité

- Objectifs
  - Lucratif
  - Espionnage
  - Géopolitique
  - Propagande
  - Sabotage
  - Vol de données
  - Intelligence économique

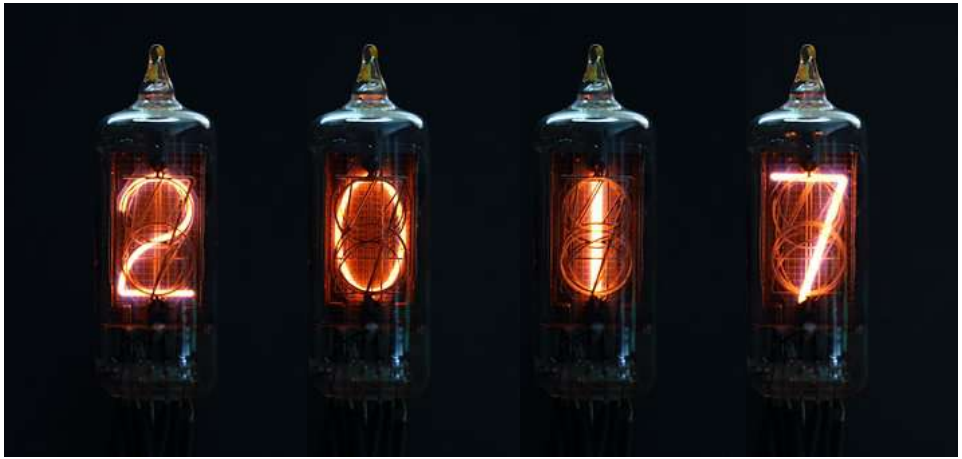
Cybercriminalité / Impacts

Top 10 risks in terms of **Likelihood**	Top 10 risks in terms of **Impact**
1 Extreme weather events	1 Weapons of mass destruction
2 Natural disasters	2 Extreme weather events
3 Cyberattacks	3 Natural disasters
4 Data fraud or theft	4 Failure of climate-change mitigation and adaptation
5 Failure of climate-change mitigation and adaptation	5 Water crises
6 Large-scale involuntary migration	6 Cyberattacks
7 Man-made environmental disasters	7 Food crises
8 Terrorist attacks	8 Biodiversity loss and ecosystem collapse
9 Illicit trade	9 Large-scale involuntary migration
10 Asset bubbles in a major economy	10 Spread of infectious diseases

src : World Economic Forum Global Risks Perception Survey 2017–2018

Cybercriminalité

- Chiffres France
  - 2435 signalements
  - 1621 traités
  - 794 incidents
  - 20 incidents majeurs
  - 12 opérations cyberdéfense
  - 3 crises



src : ANSSI

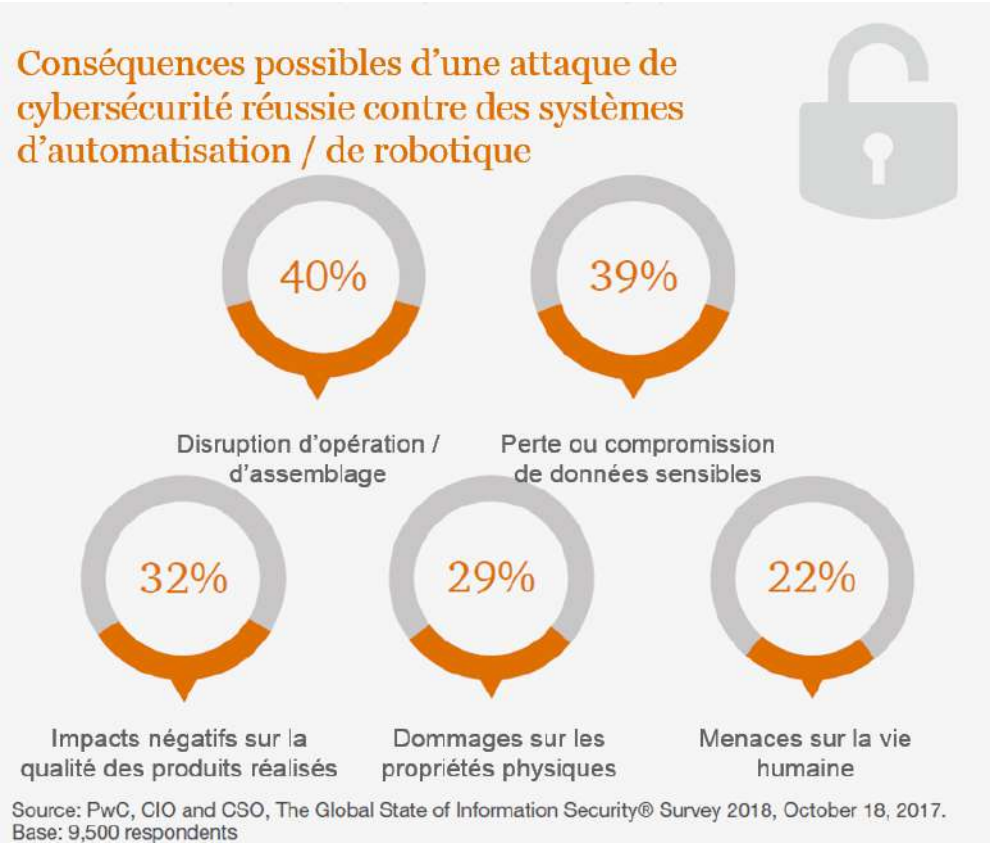
Cybercriminalité / Impacts

- 2017 - France
  - Pertes financières : +50 %
  - => 2.25 Millions €
  - investissement 4.3 Millions €
  - 4550 incidents identifiés /an par les entreprises.
- 2017 – Monde
  - $1 billion (860 milliards €)

src : figaro, cabinet PwC, telegraph.co.uk

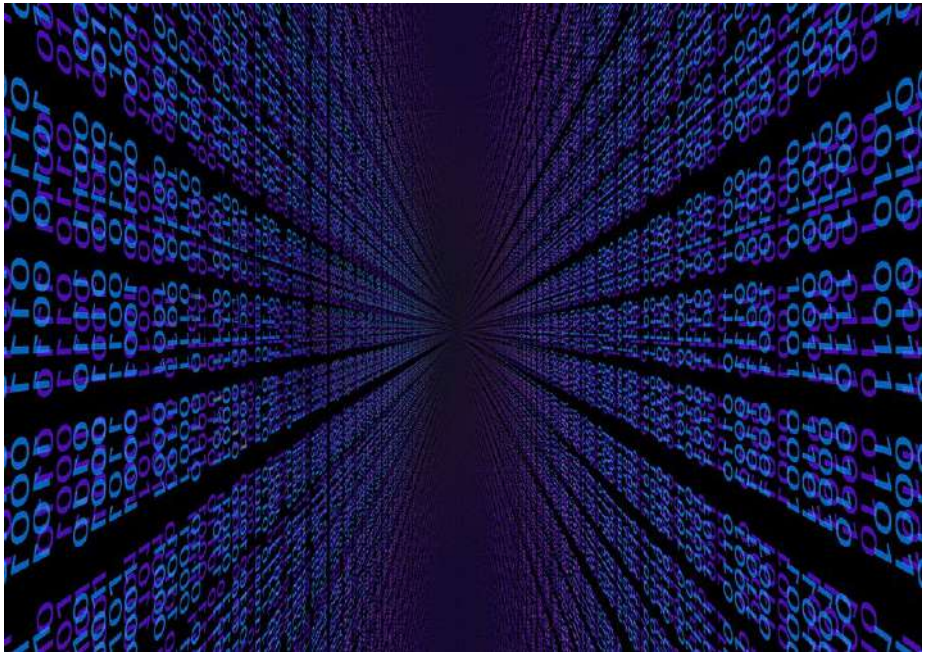
Enjeux

- Productivité



Enjeux

- RGPD – Protection des données



  - Sécurisation
  - Accès
  - Intégrité
  - Transparence

Enjeux

- Notoriété
  - Image
  - Renommée
  - Crédibilité
  - Confiance

Exemples - 2016/2017

- Thermomètre connecté
  - accès réseau informatique
    - Liste clients

- Cameras réseaux
  - zombie – attaque DDOS
    - Inaccessibilité DNS Dyn

Prévention

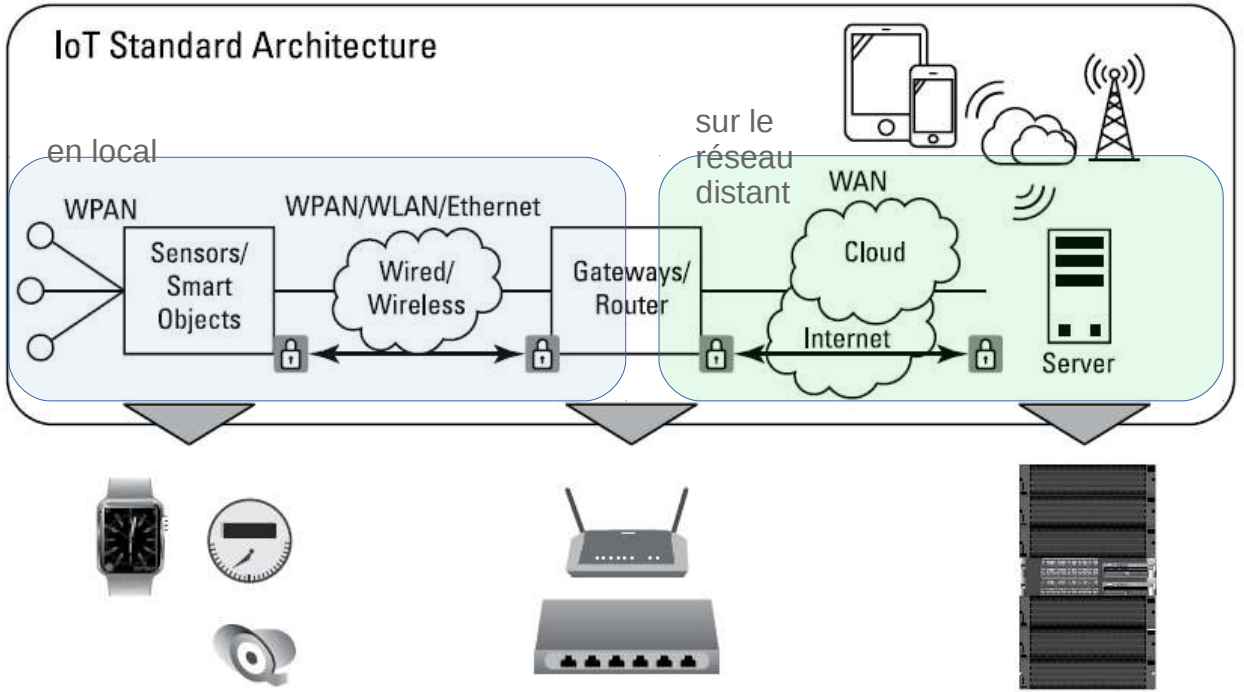


Figure 1-1: IoT system architecture and functional overview.

Prévention

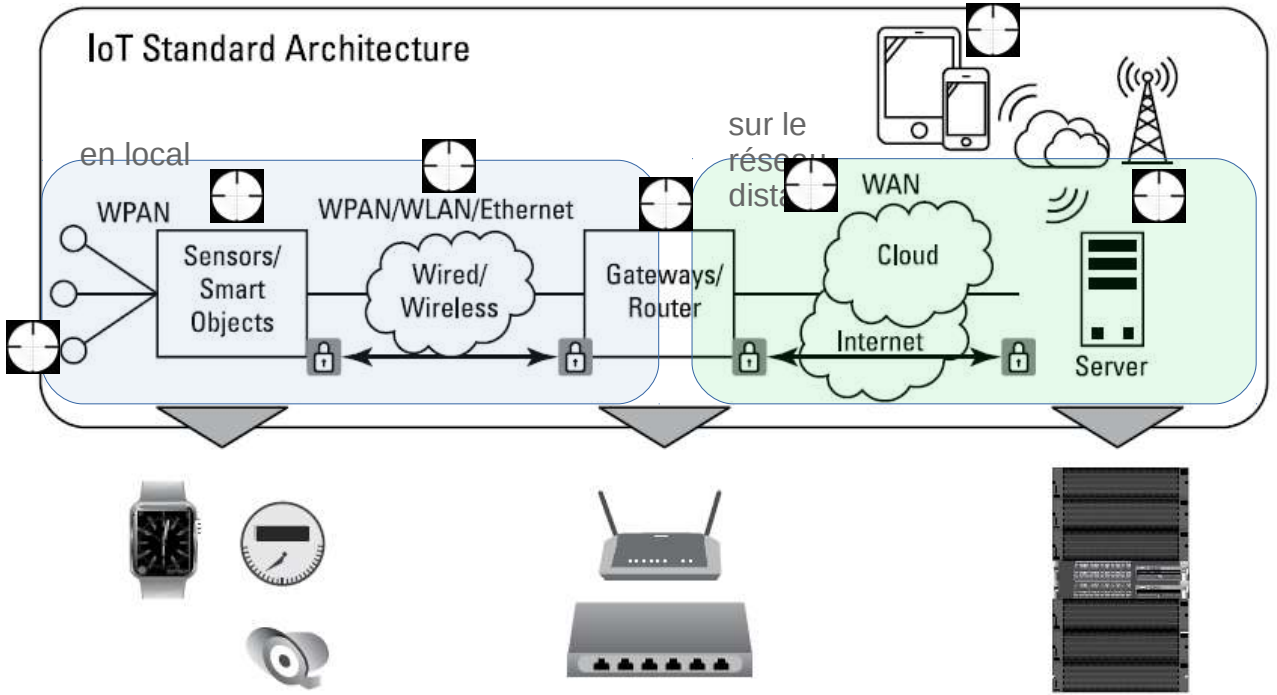


Figure 1-1: IoT system architecture and functional overview.

Chaîne de valeur pour la sécurité

Prévention

Sécurisation

Prévention

Matériel

Logiciel

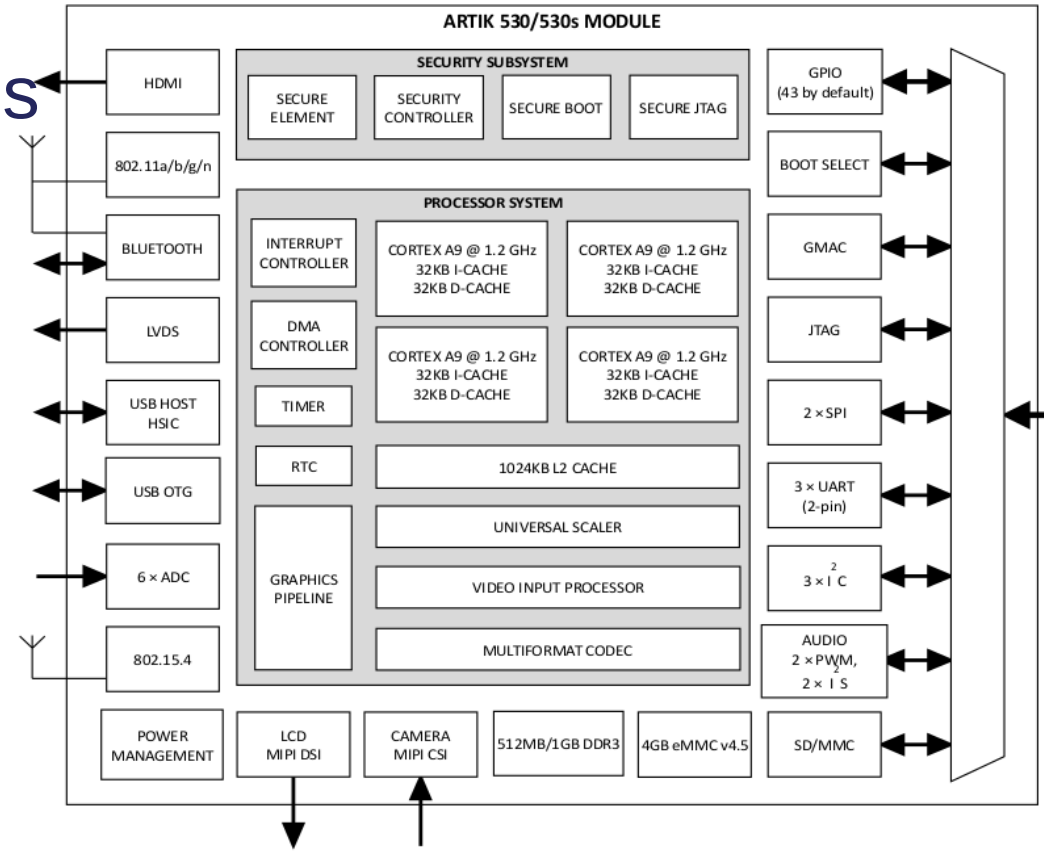
Préconisations logicielles

- Sécurisation des données
  - Stockage en mémoire
    - zone sécurisée, données chiffrées
  - Communication
    - confidentialité ...
      (algo (a)symétrique)
    - authentification ….
    - intégrité ...
    - non répudiation …

...des données transmises

Préconisations logicielles

- Sécurisation des données
  - bootloader
  - programme
  - firmware
  - certificats, clefs
  - flash en production



Préconisations locigielles

- Sécurisation des données
  - zones d'exécution séparées (TEE)
  - utilisation du chiffrement

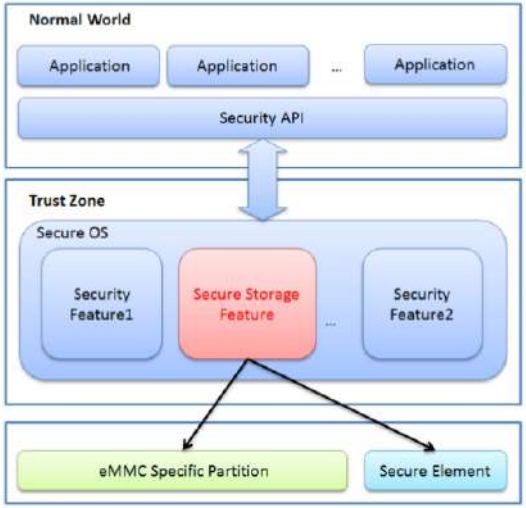
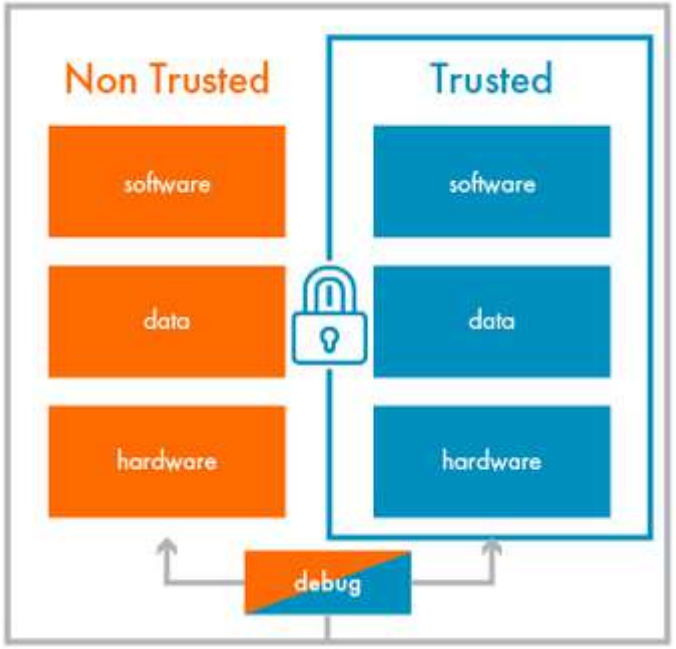
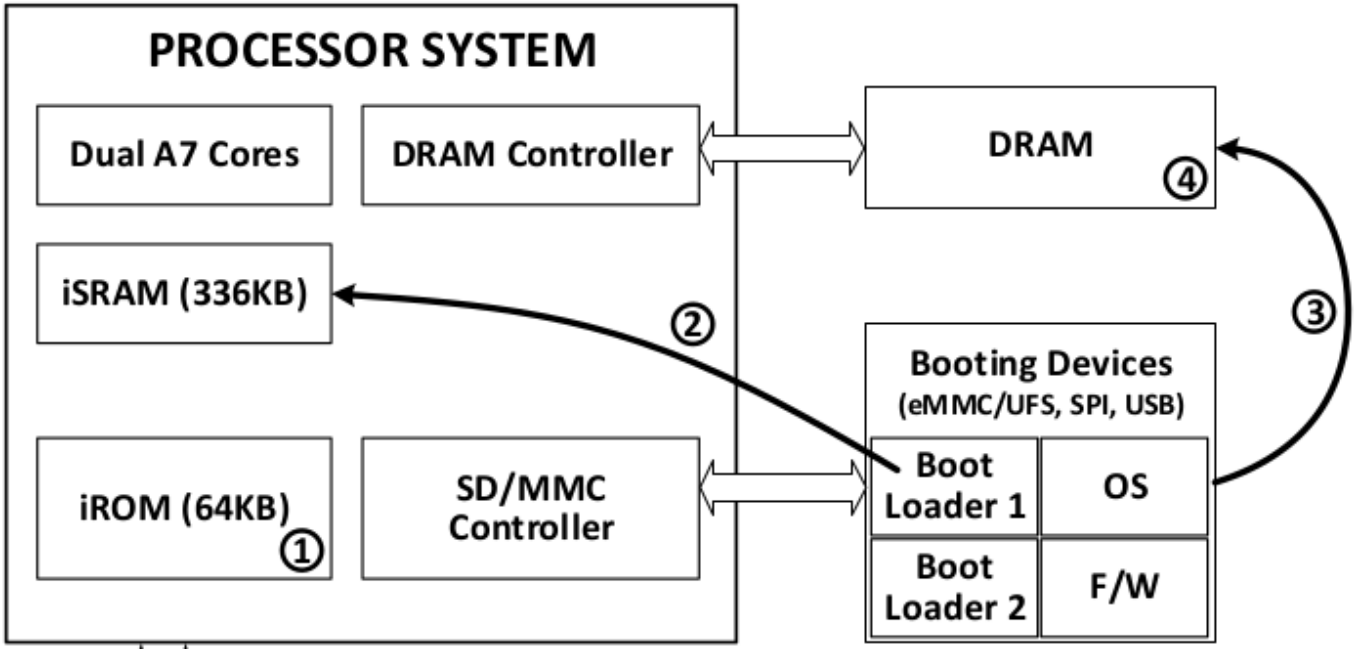


Figure 10. TEE Functionality Overview



Prévention - Préconisation

- Sécurisation des données
  - Processus de Boot
  - Programme intègre



Prévention - Préconisation

- Quelques règles
  - Stocker les clefs de manière sécurisée
  - Sécuriser les échanges (authentification, signature, intégrité)
  - Unicité des produits (clefs)
  - Sécuriser le réseau
  - Sécuriser l’application
  - Sécuriser la mise à jour
  - Sécuriser le matériel

Prévention - Préconisation

https://www.keylenght.com/fr/4/

Ce papier [5] correspond aux recommandations de l'agence nationale de la sécurité des systèmes d'information (ANSSI). Il représente l'expression du gouvernement français en termes de qualité cryptographique.

Date	Symétrique	Factorisation Module	Logarithme discret Clef	Logarithme discret Groupe	Courbe elliptique GF(p)	Courbe elliptique GF(2^n)	Hash
2014 - 2020	100	2048	200	2048	200	200	200
2021 - 2030	128	2048	200	2048	256	256	256
> 2030	128	3072	200	3072	256	256	256

Les tailles de clef sont exprimées en bit. Ces résultats garantissent une sécurité minimale.
Cliquer sur une valeur pour la comparer avec les autres méthodes.

Remarques et algorithmes recommandés pour les systèmes symétriques :

La taille recommandée pour les systèmes symétriques est de 128 bits.
La taille minimale des blocs de chiffrement par bloc est de 64 bits (128 bits recommandés et obligatoires après 2020).
Il est recommandé d'employer des algorithmes par bloc et non des algorithmes de chiffrement par flot.
Algorithme de chiffrement : AES-CBC (FIPS 197)
Algorithme d'authentification et d'intégrité : CBC-MAC "retail" avec AES et 2 clefs distinctes.

Remarques et algorithmes recommandés pour les systèmes asymétriques :

Pour le chiffrement RSA, les exposants publics doivent être strictement supérieurs à 2^{16}=65536.
Les exposants secrets doivent être de la même taille que le module (3072 bits recommandés).
Les nombres premiers constituant le module RSA sont choisis aléatoirement uniformément et d'une taille égale à la moitié de celle du module.
Algorithme de chiffrement : RSAES-OAEP (PKCS#1 v2.1)
Algorithme de signature : RSA-SSA-PSS (PKCS#1 v2.1)
Algorithme de signature : ECDSA/ECKCDSA avec FRP256v1 ou P-256, P-384, P-521, B-283, B-409, B-571 dans FIPS 186-2
Courbes elliptiques GF(p) : FRP256v1 et P-256, P-384, P-521 dans FIPS 186-2
Courbes elliptiques GF(2^n) : B-283, B-409 et B-571 (FIPS 186-2)

Algorithme recommandé pour les fonctions de hachage : SHA-256 (FIPS 180-2)

Prévention - Préconisation

- Organismes
  - ANSSI :
    - recense faille de sécurité
    - propose des guides
  - NIST :
    - publie manuel de référence, guide sur la sécurité
  - C.E.S.T.I. :
    - laboratoire de THALES pour la certification
    - audit de sécurité (EAL7)

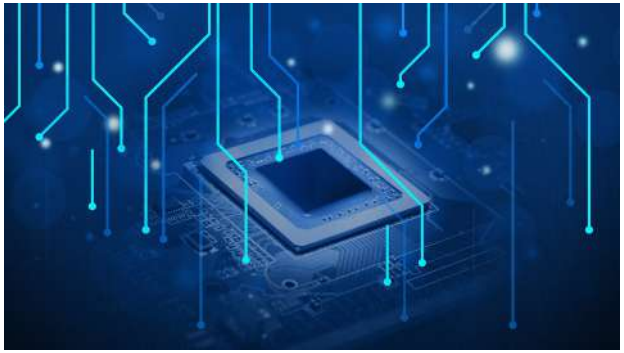
Préconisation matérielles

- Sécurisation du matériel
  - Fonctions intégrées
    - secure element
    - bootloader sécurisé
    - jtag securisé
    - mémoires compartimentées
  - BlockChain
  - Critère commun > EAL5

Prévention

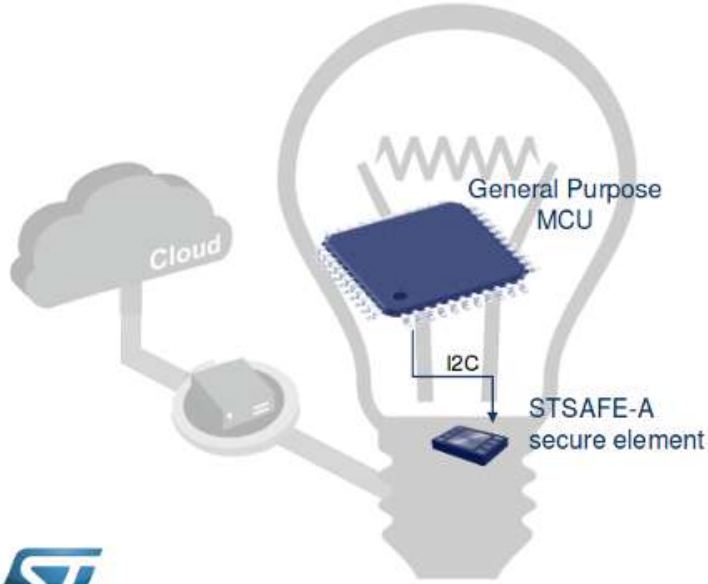
Secure element

- Dedicated secure CPU
- Crypto Accelerator
  - Hardware based AES/DES/3DES
  - TORNADO-E
  - 5KB crypto RAM
- Crypto co-processor
  - Modular exponential accelerator
  - RSA 4128bits/ECC 544 bits
- Data security
  - Abnormal-condition detectors for: reset, interrupt, voltage, temperature, laser exposure, shield removal
  - Random Wait Generator, Random Current Generator
  - Secure optimized layout
  - Dynamic bus encryption
- Embedded tamper-free memory
  - 1.5MB flash (program and data)
  - 32KB MASK ROM
  - 48KB Static RAM
  - 5KB Crypto RAM
  - Memory Protection Unit with 4GB addressable space
  - Secure flash write operation with fast page (0.5ms) and sector erase (4ms)
  - 500K erase/write cycles/s
- Serial interfaces:
  - I^2C/SPI/UART (ISO 7816)
- A guaranteed 25 years data retention at room temperature



Prévention

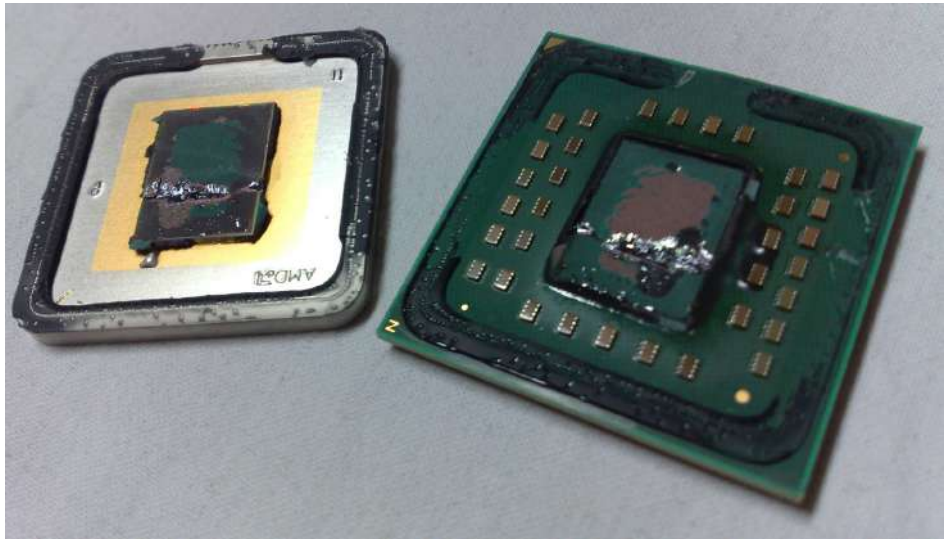
Secure element



- Authentication
- Secure communication
- Secure storage
- Secure Firmware upgrade
- USB Type-C

Préconisations matérielles

- Composants protégés des attaques matérielles
  - analyse différentielle
  - attaque laser
  - active shield
  - attaques side-channel
  - détection d'ouverture…
  - protections
    - Glu logique, scrambled memory...
  - Critère commun (EAL)



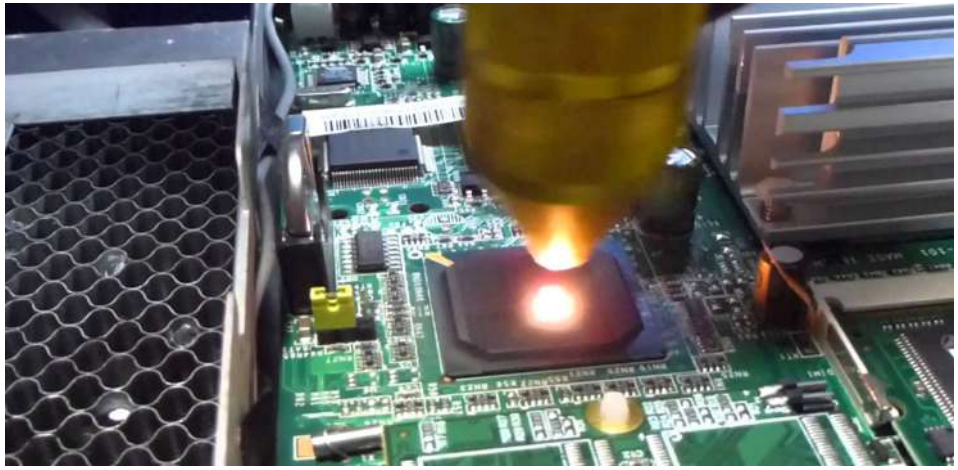
Prévention - Préconisation

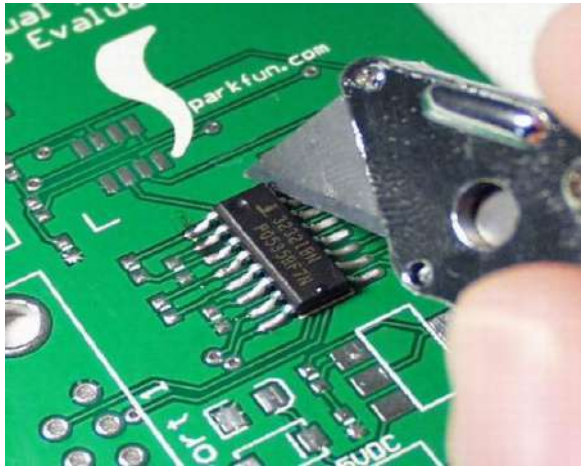
- Critères communs
  - référence de sécurité apportée
  - niveau de confiance
  - critères génériques
  - EAL1 - EAL7

EAL1	:	testé fonctionnellement
EAL2	:	testé structurellement
EAL3	:	testé et vérifié méthodiquement
EAL4	:	conçu, testé et vérifié méthodiquement
EAL5	:	conçu de façon semi-formelle et testé
EAL6	:	conception vérifiée de façon semi-formelle, et testé
EAL7	:	conception vérifiée de façon formelle, et testé

Préconisations matérielles

- Effacer les références des composants
- Noyer le système dans des résines/colles/silicones
- Sceller les boîtiers (collage, boulon anti-retour...)





Plan d’action

- Roadmap
  - ANSSI :
    - 2013: livre banc + loi de programmation militaire (cyber-sécurité)
    - 2015 : workshop VPN
    - 2016 : décret d’application
    - 2017 : Mise en application OIV
    - oct 2018 : Mois européen de la cybersécurité
    - loi de programmation militaire 2014-2019 et 2019-2025

Plan d’action

- Roadmap
  - Europe 2018 :
    - paquet cybersécurité
      - informations
      - règlement / certification de sécurité
      - recommandation : réponse aux crises cybersécurité
      - plate-forme de formation et d’enseignement
      - agence de cybersécurité de L’UE renforcée
      - répression pénale
  -

Conclusion

Approfondir

Formation « Sécurisation des systèmes embarqués »

3 juillet 2018 au CRESITT

‘cryptographie’, ‘sécurité HW / OTA’
’méthode et outils de validation’...

Démo sur stand

Merci