FROM RESEARCH TO INDUSTRY

cea tech

Sécurité des systèmes communicants
Focus sur l'Internet des objets

Assia TRIA , Alain Merle et Jacques Fournier

assia.tria@cea.fr

Séminaire Captronic, Gardanne, 8 décembre 2015

www.cea.fr

leti & list

L'internet des objets ?

- Repose sur le principe que chaque objet est en mesure de se connecter à l'internet pour échanger des informations
- L'objet connecté peut envoyer ou recevoir des informations par le biais d'une liaison sans fil, Bluetooth ou wifi
- Cette liaison permet de communiquer avec un ordinateur, un smartphone, une tablette etc.
- L'IoT représente la prochaine évolution de l'internet

Les enjeux

- Le nombre d'appareils connectés à Internet a atteint 12,5 milliards en 2010 ➔ 25 milliards d'objets connectés d'ici 2020.
- .. dont plus de la moitié concernera les applications dites 'grand public' ou «consummer» : contraintes fortes de coût, de consommation d'énergie et de sécurité.
- Proposer **des schémas efficaces** afin de pouvoir sécuriser demain :
  - la personnalisation,
  - la gestion à distance
  - .. et les transactions entre ces 13 milliards d'objets connectés.
- En matière de recherche, il s'agit d'un **champ émergent** pour lequel les bases théoriques et pratiques doivent encore être solidement établies.
- Ce qui pourrait **ouvrir d'autres champs** de recherches :
  - la gestion sécurisée de ces objets connectés,
  - la protection des couches de communication
  - la gestion de la vie privée ou l'anonymisation au sein de l'IoT...

Point critique !

- Les briques technologiques permettant de construire l'IoT existent déjà
  - Microprocesseurs
  - Microcontrôleurs
  - Capteurs en tout genre
  - Solutions de connectivité sans fil à courte et moyenne portée.
- Elles sont déjà largement utilisées aujourd'hui dans de multiples objets.
- Elles deviennent de plus en plus performantes, miniaturisées et économes en énergies.
- ..Mais le point crucial est qu'elles doivent intégrer une **infrastructure de services sécurisés** pour permettre à un grand nombre d'objets de travailler ensemble.

Problématique

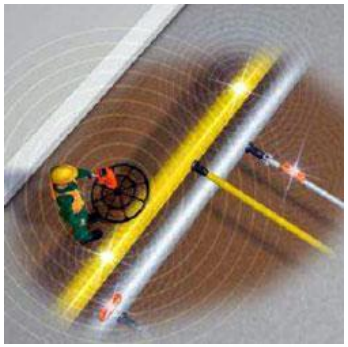
- Il existe aujourd'hui des solutions cryptographiques pour assurer des services de
  - Confidentialité
  - de contrôle d'intégrité,
  - d'authentification,
  - de non-répudiation.
- Mais il reste à faire pour rendre ces algorithmes efficaces et performants sur des dispositifs embarqués de plus en plus miniaturisés.
- De tels besoins en sécurité imposent la recherche d'algorithmes cryptographiques
  - efficaces
  - Ayant une petite empreinte matérielle.

De quoi parle-t-on?….

Circuit physique avec un accès physique pour l'attaquant

- Circuit intégré avec ou sans logiciel embarqué

- Internet des objets
- objets communicants



- Systèmes

Systèmes embarqués communicants sécurisés

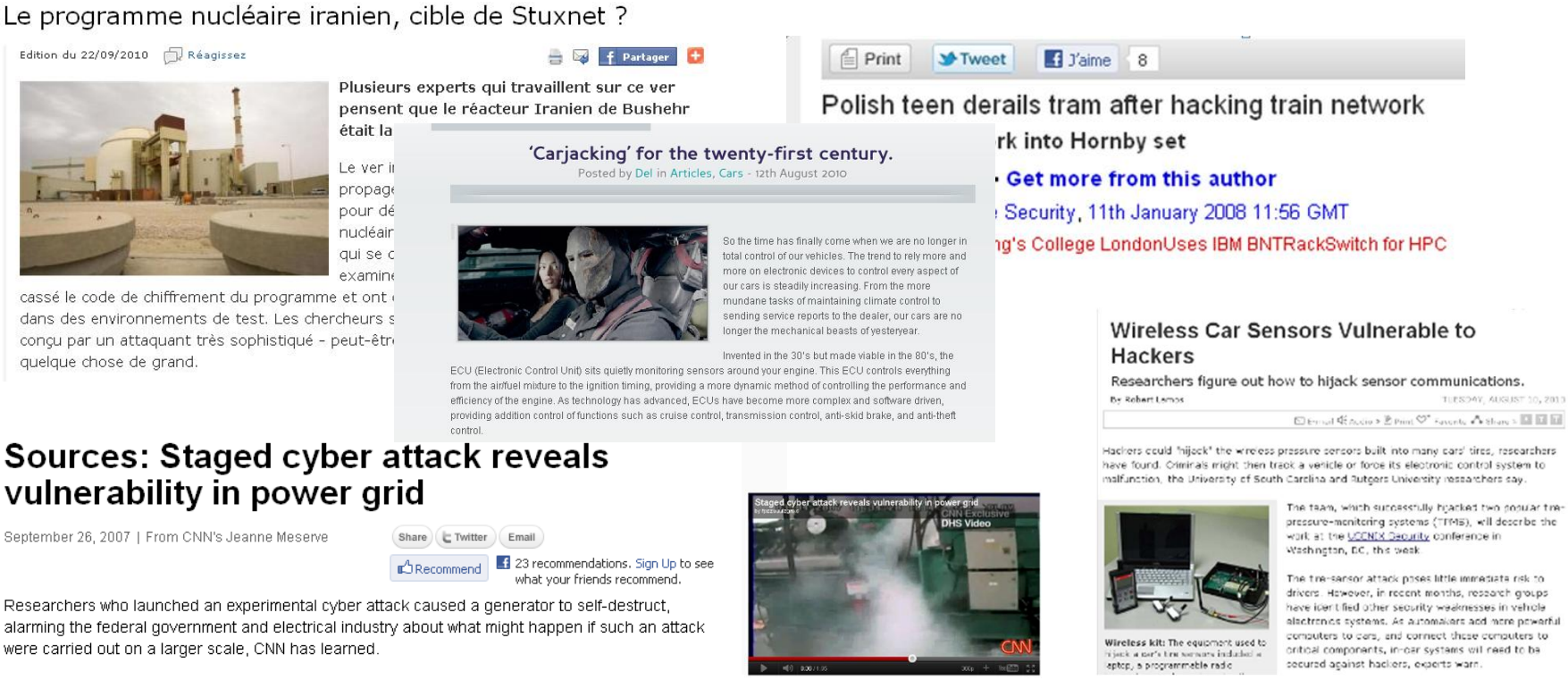
- ✓ Objets physiques réels
- ✓ Hardware et logiciel embarqué

- ✓ Il existe un accès physique à l'objet
- ✓ Lien « Telecom »
- ✓ Souvent connexion à l'internet

- ✓ Utilisation de cryptographie
- ✓ Cryptographie embarquée

Cyberattaques dans le monde réel

- 2007: Autodestruction d'un générateur dans une centrale par une cyberattaque expérimentale
- 2008: Un adolescent polonais fait dérailler un TRAM suite à une prise de contrôle via internet.
- 2010: STUXNET Ver ciblant le programme nucléaire iranien
- 2010: Des capteurs sans fil utilisés pour le "carjacking"



Et dans le domaine médical

AUSTRALIAN EDITION

SC MAGAZINE — SECURE BUSINESS INTELLIGENCE

POPULAR: encase , investigati

HOME | NEWS | IN DEPTH | REVIEWS | EVENTS | SC AWARDS

WHAT WE'RE FOLLOWING: AISA 2012 · Breakpoint · Ruxcon · Jobs · Print edition

Home / Security News / Hackers

Hacked terminals capable of causing pacemaker deaths

By Darren Pauli on Oct 17, 2012 12:33 PM
Filed under Hackers

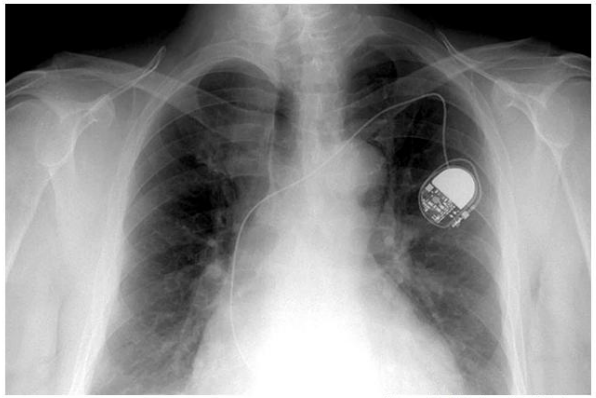
Security holes enable attackers to switch off pacemakers, rewrite firmware from 30 feet away.

Security

Medical Hacking Poses a Terrifying Threat, in Theory

By Joshua Brustein | August 15, 2013

SEND TO kindle

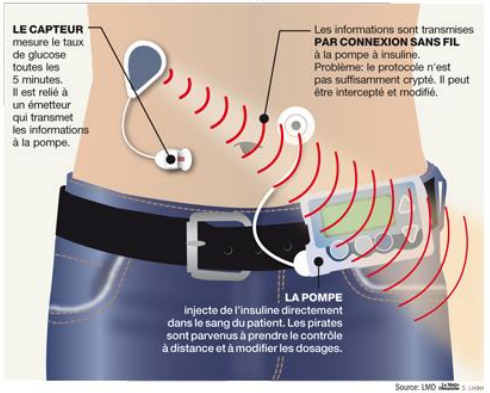


Photograph by Photo Researchers/Getty Images

Un hacker transforme une pompe à insuline Medtronic en arme

Posted on 13 NOVEMBRE 2011 *by* ALEXANDRE HAEDERLI

UNE CONNEXION SANS FIL VULNÉRABLE



Source: LMD

STORY: Your Medical Records Are for Sale

New vulnerabilities continue to arise. In June, ICS Cert, part of the Department of Homeland Security, reported that it had found security holes in 300 medical devices being made by 40 different companies, which it declined to name. This

Les communications (et le reste) aussi !

26 février 2009 (Source Le Monde)

Tout ce que vous avez toujours voulu pirater sans jamais savoir comment procéder

PREMIERE PARTIE : TOUT SE PIRATE…

Les réseaux domestiques… piratés… une fois de plus

Les téléphones sans fil… piratés (pour 23 euros !)

Le réseau GSM… piraté

Les terminaux de paiement par carte bancaire… piratés

Les sites Internet "sécurisés"… piratés

Les machines à voter… piratées

Les passeports et permis de conduire… piratés

Les pass de métro et les badges d'accès… piratés

Les badges RFID et autres tags électroniques… piratés

Les appareils médicaux et les pacemakers… piratés

La mémoire des ordinateurs… piratée

Les portes de garage, les portières de voiture et les sas d'accès… piratés

l'iPhone d'Apple… piraté

Internet… tout planté (troisième essai)

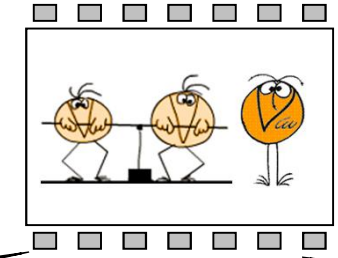
Les comptes en banque… piratés

Votre ADN… piraté

ZDNet.fr / Blogs / Infra | Net Suivre via:

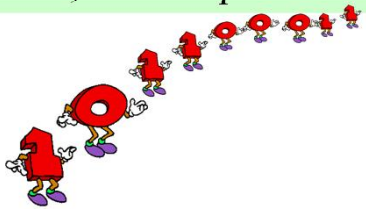
Comment un hacker aurait pu prendre le contrôle de 300.000 box d'un des plus grands FAI français…

Sécurité matérielle : le contexte



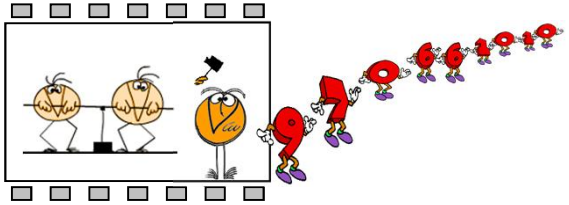
Vos secrets et données sensibles sont-elles protégées?

Clefs cryptographiques, certificats de sécurité, données personnelles…



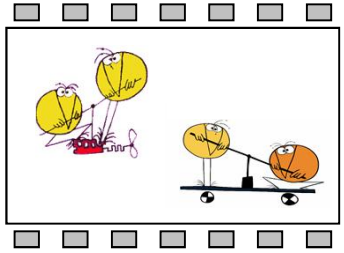
Votre programme s'exécute-t-il correctement?

Les fonctionnalités critiques peuvent-elle être contournées?



Votre HW est-il de confiance?

Clone?
Fonctionnalité malicieuses cachées?



Même si vous avez une carte à puce sécurisée ou un "Secure Element"' (qui pourrait convenir à TOUTES les applications), la réponse est

NON !

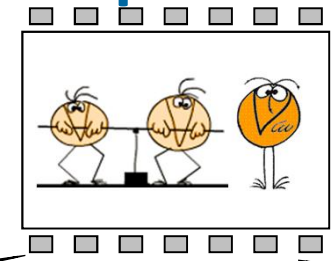
PAS GARANTI!

Votre chaîne d'approvisionnement d'IC est-elle sous contrôle ? Quelques facteurs 'accélérants' : délocalisation de sites de production, nombre croissant de « fabless », puces à plus de valeur ajoutée, plus de systèmes complexes

Conséquences : perte de données secrètes (et services associés),perte de revenus, fraude, risques pour les utilisateurs,…

Conséquences : perte de part de marché, dégradation d'image, sécurité dégradée, fiabilité dégradée, …

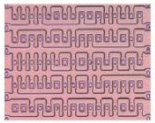
Sécurité matérielle : questions pratiques



Vos secrets et données sensibles sont-elles protégées?

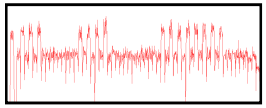
Retro conception

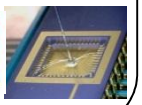
Dépendant de la méthode de conception ➔ Extraction du code



Canaux auxiliaires

Fuites d'informations dépendant des données manipulées : timing, consommation de courant, power(DPA, SPA…) or analyse électromagnétique





Injection de fautes

Analyse différentielles en fautes contre des algorithmes cryptographiques pour extraire des secrets : clefs (DES, AES, RSA, ECC, Pairings…)

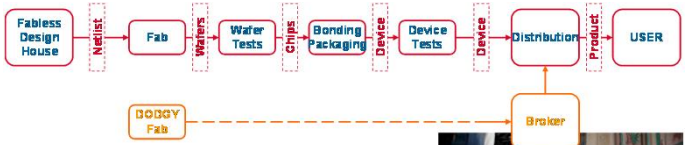
Votre programme s'exécute-t-il correctement?

Les attaques en fautes peuvent être utilisées pour corrompre l'exécution du logiciel, pour contourner des fonctions de sécurité (dump de code) …

Mise en œuvre des attaques en fautes

- **ElectroMagnetic Pulses**
- **Laser /Light**
- **Voltage Glitches**
- **Clock Glitches**
- **…**

Votre HW est-il de confiance?



Puce Corrompue : le matériel malveillant a été ajouté (déni de service, extraction des données sensibles …)

Contrefaçon : une copie exacte faisant les mêmes opérations … parfois du même fabricant

Clone fonctionnel : puce effectuant les mêmes opérations critiques et sensibles … peut être avec des caractéristiques(fonctions) dégradées.

Sécurité: définitions

Confidentialité

Objectif	Types d'attaques	Attaques récentes	Protections
S'assurer que les informations sont secrètes	Intrusion, vers, hacking, …	AREVA, MASTERCARD, SONY, …	Cryptographie, Carte à puce Module de confiance (TPM)

Intégrité

Objectif	Types d'attaques	Attaques récentes	Protections
S'assurer que le système n'est pas modifié	Vers, cheval de Troie	Terminal de paiement UK, Stuxnet	Cryptographie Processeur de confiance

Disponibilité

Objectif	Type d'attaques	Attaques récentes	Protections
S'assurer que le système reste disponible	Dénie de service, Anonymous	Estonie, Anonymous	Très difficiles!

Authenticité

Objectif	Types d'attaques	Attaques récentes	Protections
S'assurer que l'on a affaire au véritable système (authentique)	Clonage	Pay TV, contrefaçon	Carte à puce Module de confiance (TPM)

Sécuriser l'internet des objets

- Internet des objets existants (IoeT)
  - Implique l'utilisation des technologies existantes
  - Nécessite une adaptation des technologies en termes de puissance, performances, ….contraintes de l'IoT
  - Perspectives à court terme

- Internet des futurs objets (IofT)
  - Implique le développement de nouvelles technologies, méthodes de chiffrement et des outils adaptés
  - Les technologies qui conviennent mieux à la sécurité, à la scalabilité, à la privacy ..et surtout qui sont requises dans l'IoT
  - Perspectives à long terme

Cryptographie légère

- Le domaine de la cryptographie légère a été jusqu'à présent essentiellement étudié dans le contexte des cartes à puces sans contact (ou appelées aussi cartes RFID).
- Les solutions qui ont été proposées pour garantir la confidentialité des données sont de plusieurs types
  - Des schémas propriétaires
  - Des algorithmes de chiffrement par bloc ayant une structure proche de celle du DES ou de l'AES
  - Des algorithmes de chiffrement par flot
- des techniques dépendantes de structures matérielles telles que les PUFs ou « fonctions non clonables ».

Implémentations cryptographiques légères

- Nécessité de trouver un compromis entre
  - Consommation
  - Empreinte silicium
  - Résistance aux attaques physique
- Nécessité de disposer d'outils de simulation et d'aide à la conception pour étudier ces compromis
- Compatibilité de performance dans des problématiques de transchiffrement (notamment avec des traitements homomorphiques)

Challenges à court termes

- Implémentation d'algorithmes existants de manière efficace et très basse consommation.
- Conception bas cout (inhérente) résistante aux attaques physiques (canaux auxiliaires ou fautes)
- Génération et stockage de clés efficaces
- Procédures de gestion de clés efficaces pour des infrastructures exponentiellement croissantes.

Long terme

- la PKI dite ‘classique’, de par la lourdeur liée à la gestion des clefs et certificats associés, sera très peu adaptée à l’échelle du marché des objets IoT
- Une alternative envisagée est l’utilisation de schémas basés sur l’identité (‘Identity Based Encryption’ – IBE) qui permet de générer une clef publique portant l’identité de l’utilisateur
- chiffrement homomorphe qui permet
  - d’effectuer des opérations arithmétiques et booléennes sur des données chiffrées sans les déchiffrer.
  - à un serveur de faire du déchiffrement et de l’authentification sans avoir accès à la clef associée en clair.
- Une autre approche serait de s’intéresser aux jumelages entre les algorithmes LWC et le chiffrement homomorphe.
- De telles solutions de transchiffrements utilisant des algorithmes classiques tels que l’AES sont beaucoup trop coûteux, d’où l’intérêt d’avoir recours à des algorithmes plus légers.

Amélioration de la sécurité: Idées de base

- “Le logiciel digne de confiance ne peut pas exister avant que nous n'ayons le matériel digne de confiance pour le construire de matière sûre” (Dr. Dean Collins, Deputy Director, MTO, DARPA)
- “Même analysée, validée, certifiée, une organisation peut être corrompue, la vérification d'intégrité doit être la caractéristique intrinsèque des produits “ (DARPA, “Trust in IC” program)

- D’abord la sécurité puis le fonctionnel
- Noyau de sécurité Hardware
- Cryptographie **sécurisée** partout

Cryptographie: est-elle vraiment la solution ?

Tous les schémas crypto sont basés sur un secret

- L'accès à ce secret fait tomber le système
- **ATTENTION à la gestion des clefs**

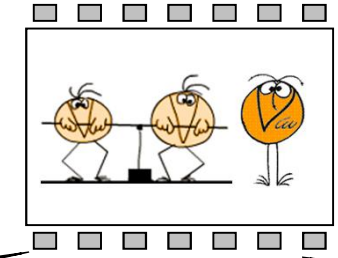
La résistance théorique évolue rapidement

- Loi de Moore de la microélectronique
- DES, TDES, AES, RSA key length, Hash fns

Techniques d'attaques physiques

- L'imagination comme seule limite ?

Sécurité matérielle au CEA Tech



Vos secrets et données sensibles sont-elles protégées?

Votre programme s'exécute-t-il correctement?

Votre HW est-il de confiance?

Caractérisation

- Bancs de caractérisation : EM, laser, Vcc, clock…
- Implémentation d'algorithmes cryptographiques (AES, Pairings…)
- Analyse des protocoles de communication (contactless, WLoPAN…)
- Outils d'analyse de code frama C Software Analyzers
- CESTI: labo accrédité ANSSI (Common Criteria, EMVCo…)

Solutions sécurisées

- Contre-mesures Hardware et software pour l'implémentation sécurisée d'algorithmes cryptographiques
- Bouclier, nouvelles technologies
- Contre-mesures run-time

Fonctions non clonables

- Aspects certification
- Implémentation de nouvelles structures PUFs
- Analyse de résistance

vérification d'intégrité

- Approche basée sur l'analyse par canaux auxiliaires
- Analysé basée sur de l'injection de fautes (glitchs)
- Capteurs embarqués

En complément

- Il n'y a pas de solution miracle: « Nobody's perfect »
  - Des vulnérabilités découvertes chaque jour
  - Le hardware sécurisé est la meilleure solution mais elle n'est pas parfaite
  - La cryptographie a aussi ses limites
  - Attention à la durée de vie des produits
- Toute erreur est un chemin d'attaque
- Le critère de disponibilité est un réel challenge pour les systèmes communicants
- L'évaluation/Certification sécuritaire est un bon outil
  - Tierce partie compétente
  - Garantie nationale (ANSSI)

Un bon système devrait proposer …

« Sécurité de bout en bout »
Applications sûres sur infrastructure non sûre
- « Device » de confiance aux 2 bouts de la chaîne

Gestion des clefs « adéquate »

Des composants de sécurité « up to date »
- Noyau de confiance par circuit sécurisé certifié
- Composantes logicielles certifiées

Un mécanisme de « recovery »
- Je dois savoir me remettre dans un état sûr après une compromission

Sureté et sécurité
- Noyau sûr en toute circonstance
- Disponibilité

Une sécurité « multi-barrière »
- « Trusted Computing »
- Contrôle d'intégrité / Audit

Des capacités d'évolution
- Réactions face à des publications et/ou à l'usure du temps

C'est la Sécurité qui doit définir l'architecture du système

Activités CEA-TECH

- Composants cryptographiques et systèmes physiques
  - Analyse des menaces, Attaques, Implémentations sûres
  - Evaluation/Certification
  - Compromis Sécurité/Complexité(coût)/Consommation

- Architectures de sécurité basées sur un noyau de confiance
  - Trusted Computing, Root of Trust, …
  - Sécurité intrinsèque

- Gestion des clefs cryptographiques
  - Smartcities, IOT, …


Merci !
Des questions?