CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

CyberCrime : évolution des ~~technologies~~ ~~employées~~ cibles

Lille, 26 janvier 2012

Pascal LOINTIER
Président du CLUSIF
pascal.lointier@clusif.asso.fr

Le risque numérique et les Systèmes d'Information

… ou le Système d'information et ses infrastructures historiques

- ✓ Management
- ✓ Infogérance/Externalisation (dont CLOUD)
- ✓ Téléphonie (IPBX)
- ✓ Services Généraux
- ✓ Production/Régulation
- ✓ BYOD (*Bring Your Own Device*), équipement possédé par l'employé
- ✓ Biomédical, équipement embarqué sur l'employé ☺

Pas vraiment de nouvelles technologies d'attaques

Mise à jour ou développement sur les nouvelles ressources/versions logicielles

En raison de l'interopérabilité et de la standardisation (OS, ethernet, TCP-IP)… de nouvelles cibles mais à ce jour :

- ✓ Du PoC (*Proof of Concept* /faisabilité)
- ✓ Des accidents
- ✓ Des malveillances internes (individu)

2001 : virus CodeRed sur MFP (Multi Function Printer)

Un virus avec un moteur de scan IP très puissant pour détecter les cibles de contamination

- ✓ Saturation de la bande passante du réseau interne (et impossibilité de télécharger la mise à jour de l'antivirus ☺)
- ✓ Contamination des imprimantes sur le réseau (source Panorama 2001)
- ✓ Les imprimantes restent souvent du ressort des SG à cause des commandes de papier. Le rattachement à la DSI ou l'implication du RSSI (Responsable Sécurité) semble pourtant légitime

2002 : DISA et caméras WiFi, les prémices

Mai 2002, un service de sécurité américain (DISA) admet avoir utilisé une infrastructure WIFi non sécurisée (802.11b) pour la transmission de vidéos de sécurité

- ✓ Exploitation par un tiers des images, DoS (déni de service) combiné à une intrusion, connaissance des angles de vidéosurveillance, etc. (source Panorama 2002)

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

2007 : CNN et groupe électrogène

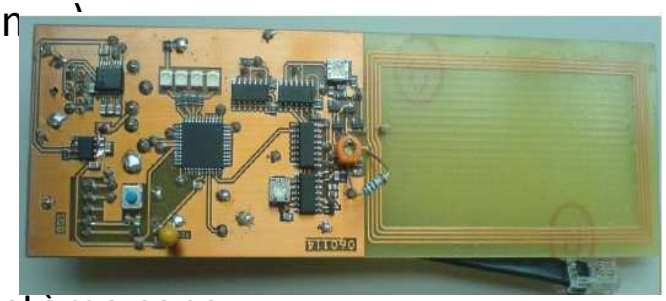
Septembre 2007 – Idaho (E-U): la chaîne CNN demande à des experts du DHS (*Department of Homeland Security*) de provoquer à distance la destruction d'u groupe électrogène. Cette action est rendu possible par l'injection de commandes numériques sur un équipement sans correctifs de sécurité (source Panorama 2007)

2008 : badges sur IP

Annonce faite par le CCC (Chaos Computer Club, Allemagne) le 1/1/2008 : Cassage de l'algorithme de chiffrement

Mifare : produit de la société NXP, destiné notamment à de l'authentification sans contact (technologie RFID)

- Système de transport public (Londres, Perth, Amsterdam, …)



Cas du système hollandais : 2 types de tickets

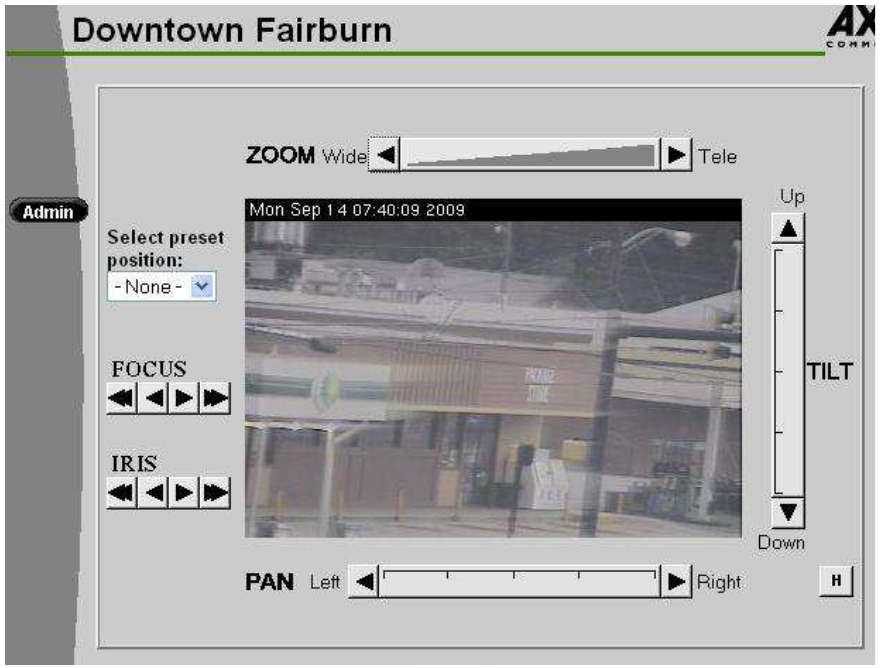
- ✓ « Ultralight card », usage unique : simple mémoire + système sans contact, aucune protection
- ✓ « Classic card », pour abonnements : idem, mais protection cryptographique des échanges par un algorithme « secret » (CRYPTO1)

Mifare est utilisé pour des contrôles d'accès par badge en entreprise (source Panorama 2008)

2009 : SWATTING for Money

- Hammond (Indiana, E-U), juillet 2009 : début du procès de jeunes hackers qui vendaient en ligne l'accès vidéo à une action SWAT en cours (partyvanpranks.com). Pour cela, ils ont commencé par prendre le contrôle à distance des caméras de surveillance

Google Search: camera linksys inurl:main.cgi
Another webcam, Linksys style.
****
* inurl:"ViewerFrame?Mode=
* intitle:Axis 2400 video server
* intitle:"Live View / - AXIS" | inurl:view/view.shtml^
* inurl:ViewerFrame?Mode=
* inurl:ViewerFrame?Mode=Refresh
* inurl:axis-cgi/jpg
* …

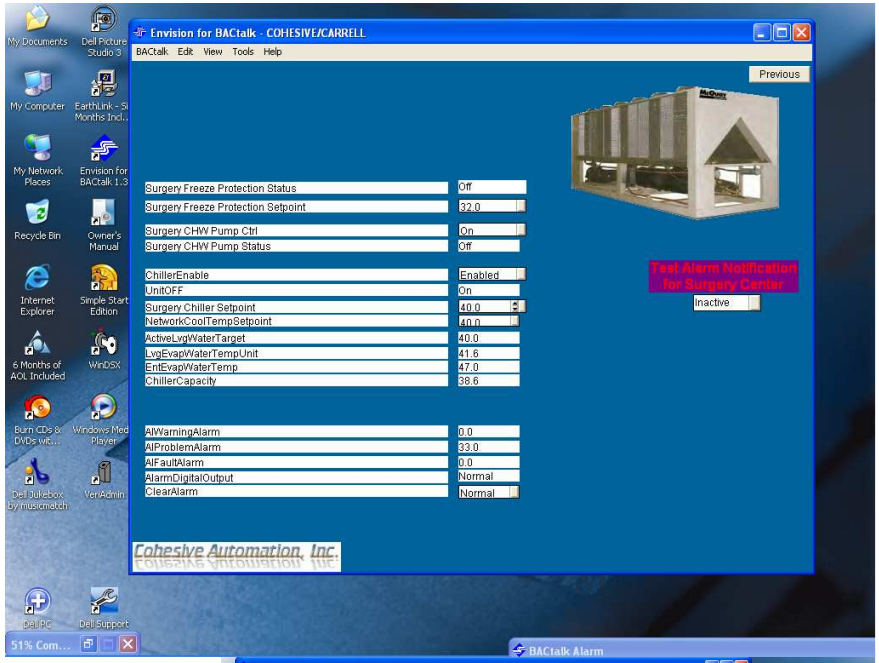


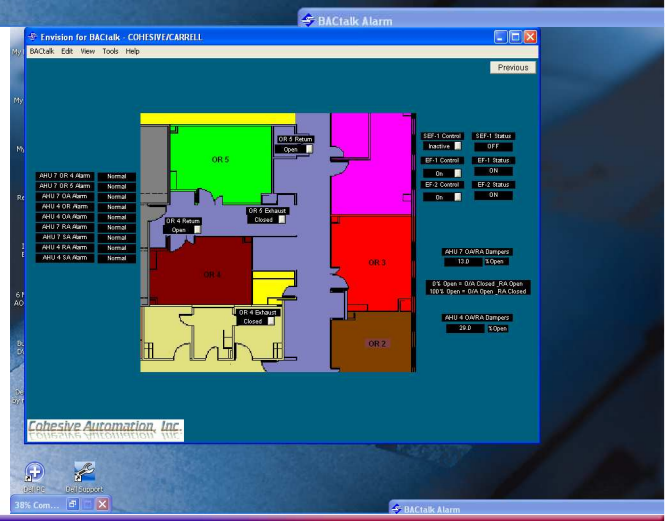
2009 : hacking de la ventilation dans un hôpital

FACTS IN SUPPORT OF AFFIDAVIT

6. On 6/24/2009, The Dallas Division of the FBI was contacted by Special Agent Charles Provine of the FBI in the Jackson Division of the FBI regarding a computer intrusion of a Heating Ventilation and Air Condition (HVAC) computer system at a Dallas, TX hospital, the Carrell Clinic located at 9301 North Central Expressway, Dallas, Texas. This was believed to present a risk to health and safety as the Hospital was a facility that kept patients around the clock who could be adversely affected by the cooling if it were turned off during Texas summer weather conditions and the hospital also maintained drugs which could be adversely affected by the lack of proper cooling if the intruder were to disturb the HVAC system. SA Provine stated that he was in contact with Lieutenant (LT) Lannie Hilbolt, Texas Attorney General's office and CW-1, a network

Page 4 of 18





Absence de ventilation = évacuation

2010, La flotte (auto) est sous contrôle !

Austin, Texas (E-U) : plus de 100 véhicules ont été immobilisés ou leurs klaxons incontrôlables après qu'un individu se soit introduit dans le système web gérant l'immobilisation de véhicules (Webtech Plus) en cas de défaut de paiement

Depuis…

- Brouillage GSM sur convoyage de valeurs
- Contrefac de clé (via OBD2+)
- Altération signaux RDS de navigation
- CarShark, lecteur MP3, sans-fil…

SCADA : malveillances internes (via le S.I.)

- ✓ 2007 : bombe logique d'un employé sur un système de contrôle d'irrigation des eaux de barrage (Californie)
- ✓ 2007 : prise de contrôle et perturbation des feux de signalisation (Californie)
- ✓ 2007 (et 2000 en Australie) : sabotage logique par un administrateur réseau du système d'approvisionnement en eau (Californie)
- ✓ 2008 : prise de contrôle et déraillement de 4 wagons, plusieurs blessés (Pologne)

Pologne (Lodz), déraillement de 4 wagons par un adolescent

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

2010, Stuxnet…

Country	Number of users
india	86258
indonesia	34138
iran, islamic republic of	14171
russian federation	7904
kazakhstan	6316
afghanistan	3081
syrian arab republic	2926
uzbekistan	2798
pakistan	2758
azerbaijan	2566
bangladesh	2489
malaysia	1691
iraq	1593
nepal	1453
belarus	1238
united arab emirates	1206
kyrgyzstan	1097
united states	805
turkmenistan	796
tajikistan	780

source : Aleks, Kaspersky Lab Expert

Publié le 03/10/2010 à 16:09 - Modifié le 03/10/2010 à 16:21 | Le Point.fr

VIRUS

L'Iran assure avoir nettoyé ses ordinateurs industriels de Stuxnet

Source AFP

Les ordinateurs industriels iraniens infectés par le virus Stuxnet ont été nettoyés, a déclaré un responsable iranien,

… Aucune revendication n'a, pour le moment, été formulée. Par ailleurs, le ver a touché d'autres ordinateurs en Chine, en Inde, au Pakistan ou encore en Indonésie. Les experts s'accordent pour considérer que les installations nucléaires iraniennes étaient les cibles prioritaires du ver, notamment celles de Natanz…

(Le Point 20101001)

Plusieurs millions d'ordinateurs infectés par Stuxnet en Chine

LEMONDE.FR avec AFP | 30.09.10 | 14h29

October 2, 2010

Iran Says It Arrested Computer Worm Suspects

By WILLIAM YONG

TEHRAN — Iran has arrested an unspecified number of "nuclear spies" in connection with a damaging worm that has infected computers in its nuclear program, the intelligence minister, Heydar Moslehi, said Saturday.

Une certitude :

virus multiplateformes visant spécifiquement un environnement de production industrielle.

Pour le reste (auteur(s), mobile, cible(s)), à suivre…

Pour les adeptes de *Conspiracy Theory* ou de…

« …As Iran's nuclear assets would probably be isolated from outside computers, hackers would be unable to access them directly, Borg said. Israeli agents would have to conceal the malware software used by the Iranians or discreetly plant it on portable hardware brought in, unknowingly, by technicians. "A contaminated USB stick would be enough," Borg said… ». Scott Borg, director of the US Cyber Consequences Unit (YNetNews (IsraelNews), 20090707)

```
.rdata:00011D95                 db    0
.rdata:00011D96                 db    0
.rdata:00011D97                 db    0
.rdata:00011D98 aBMyrtusSrcObjf db 'b:\myrtus\src\objfre_w2k_x86\i386\guava.pdb',0
.rdata:00011DC4                 db    0
.rdata:00011DC5                 db    0
.rdata:00011DC6                 db    0
.rdata:00011DC7                 db    0
```

Deep inside the computer worm that some specialists suspect is aimed at slowing Iran's race for a nuclear weapon lies what could be a fleeting reference to the Book of Esther, the Old Testament tale in which the Jews pre-empt a Persian plot to destroy them.

That use of the word "Myrtus" — which can be read as an allusion to Esther — to name a file inside the code is one of several murky clues that have emerged… (New York Times, 20100929)

Toutes les théories, même les plus « originales » sont envisageables. 9/11 :

« …Al-Qaida could detonate a Chechen-type building-buster bomb at a federal building. Suicide bomber(s) belonging to al-Qaida's Martyrdom Battalion could crash-land an aircraft packed with high explosives (C-4 and semtex) into the Pentagon, the headquarters of the Central Intelligence Agency (CIA),… » (*Who Becomes a Terrorist and Why*, Library of Congress, 199909)

2011, retour sur *Locks over IP*, le ferroviaire

Stuxnet appliqué aux serrures sur IP : une étude réalisée par 3 chercheurs a montré que les automates de gestion de l'ouverture et de fermeture des portes de prison peuvent être pilotés depuis Internet…

SCADA & PLC VULNERABILITIES IN CORRECTIONAL FACILITIES

White Paper

Teague Newman
Tiffany Rad, ELCnetworks, LLC
John Strauchs, Strauchs, LLC

7/30/2011

28C3 - Version 0.92µ

28th Chaos Communication Congress
Behind Enemy Lines

Can trains be hacked?

Die Technik der Eisenbahnsicherungsanlagen

Warum sind Züge sicher unterwegs? Wie werden Zusammenstöße trotz der Gefahr eines menschlichen Fehlverhaltens vermieden? Und was hat das alles mit IT-Sicherheit zu tun?

Der Vortrag beleuchtet die mehr als 130-jährige Geschichte der Eisenbahn-Sicherungstechnik, diskutiert die Grundbegriffe des sicheren Eisenbahnbetriebs und erklärt die Funktionsweise der verschiedenen Stellwerkstypen, die im Netz der Deutschen Bahn verwendet werden. Neben den ältesten (jedoch immer noch in großer Stückzahl vorhandenen) rein mechanischen Bauformen besprechen wir sowohl die Gleisbildstellwerke, die auf Relaistechnik basieren, als auch die modernen rechnergestützten Stellwerke, die immer größere Verbreitung finden. (Und wir besprechen anhand von Untersuchungsberichten des Eisenbahnbundesamts warum doch hin und wieder Unfälle passieren).

Während mechanische und elektrische Sicherungsanlagen in sich geschlossene Systeme sind, nutzen künftige Anlagen zunehmend drahtlose Kommunikation. Die Sicherheit der Fahrgäste hängt daher auch von der Sicherheit der zugrundeliegenden Kommunikationsinfrastruktur ab. Im Vortrag gehen wir daher der Frage nach, wie die künftige Generation der Sicherungsanlagen abgesichert sein wird, welche neuen Bedrohungsszenarien entstehen und ob daher der "Zug der Zukunft" gehackt werden kann…

SPEAKERS

Stefan Katzenbeisser

SCHEDULE

Day	Day 1 - 2011-12-27
Room	Saal 3
Start time	14:00
Duration	01:00

INFO

ID	4799
Event type	Lecture
Track	Hacking
Language used for presentation	German

<<< >>>

2011, le traitement d'eau comme cible…

Springfield : destruction d'une pompe de distribution d'eau à la suite d'une prise de contrôle de son système SCADA. La destruction est due au fonctionnement à vide de la pompe.

L'intrus met la main sur les données des clients (identifiants, mots de passe,…) du concepteur de la solution.

Il ne reste plus qu'à rendre visite au client… Qui souvent est accessible pour raison de maintenance.

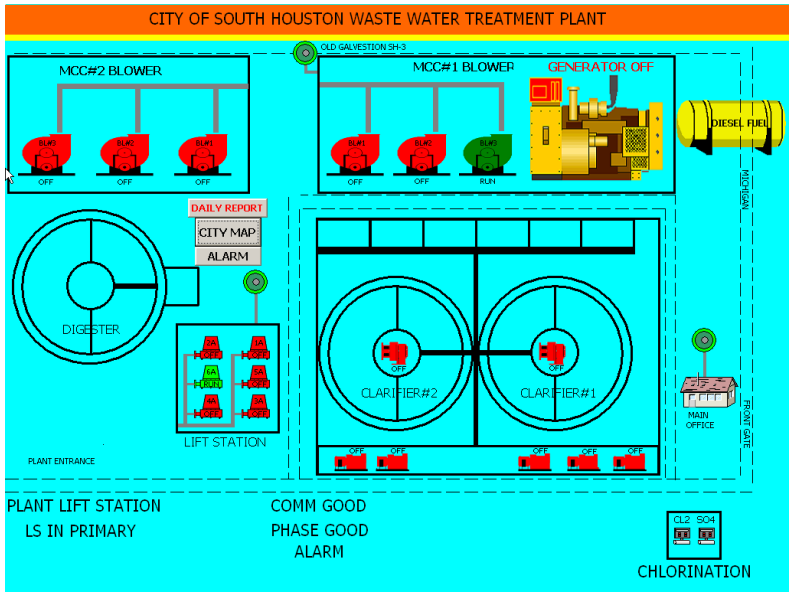
L'adresse IP qui a pu être tracée à conduit vers un pays étranger qui peut n'être qu'un rebond…

L'intrus était présent dans le système depuis 2 mois…

Eau : après Springfield, Houston…

Houston : intrusion dans le système, avec publication de captures d'écran de ce qui semble être le système de supervision de la gestion de l'eau d'une partie de la ville.

L'intrus réagissait aux propos qui minimisaient l'état d'insécurité des installations…



CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

2010 : des botnets de mobiles

Toutes les plateformes sont concernées

Botnet Viruses Target Symbian Smartphones

Nokia, Samsung and Sony Ericsson smartphones are among those running the two Symbian operating systems vulnerable to attack according to NetQin.

By **Mathew J. Schwartz** , InformationWeek
juillet 6, 2010 04:32 PM

New viruses targeting Symbian smartphones have surfaced, according to NetQin, which develops security software for mobile devices.

Two Symbian operating systems are vulnerable: S60 platform 3rd Edition, al S60 5th edition, aka Symbian OS 9.4. The operating systems run a number manufacturers as Nokia, Samsung and Sony Ericsson.

iKee transforme les iPhone jailbreakés en botnet

voter email imprimer Partagez cet article

par **Olivier Chicheportiche**, businessMOBILE.fr. Publié le 23 décembre 2009
Tags: Virus, Apple, iPhone, Sécurité,

Une nouvelle version du ver transforme le smartphone d'Apple en machine zombie afin de détourner des données. Le réseau serait contrôlé depuis la Lituanie.

Il fallait s'y attendre. La multiplication de vers visant les iPhone jailbreakés devait fatalement déboucher sur la constitution d'un réseau de smartphones contrôlables à distance (machines zombies).

La preuve en a été faite par l'institut SRI International Malware Threat Center. Comme on pouvait s'en douter, c'est le ver iKee qui est au centre de l'attaque.

Un réseau de 100 000 smartphones Symbian zombies découvert

voter email imprimer Partagez cet article

par **Guénaël Pépin**, businessMOBILE.fr. Publié le 6 juillet 2010
Tags: Symbian,

Sécurité - L'éditeur de sécurité mobile NetQin a mis au jour un réseau botnet visant les smartphones Symbian S60, se propageant par des jeux à télécharger. 500 plaintes ont déjà été déposées.

Un an après **Sexy Space**, une seconde vague de virus vise les smartphones sous **Symbian** S60 (3.0 et 5.0), l'OS mobile le plus répandu. Les virus ShadowSrv.A, FC.Downsis.A, BIT.N et MapPlug.A ont été identifiés par l'éditeur chinois d'antivirus pour smartphones NetQin, notamment pour l'opérateur China Mobile.

THE LOOKOUT BLOG

DECEMBER 29, 2010

Security Alert: Geinimi, Sophisticated New Android Trojan Found in Wild

By tim 33 Comments

The Threat:
A new Trojan affecting Android devices has recently emerged in China. Dubbed "Geinimi" based on its first known incarnation, this Trojan can compromise a significant amount of personal data on a user's phone and send it to remote servers. The most sophisticated Android malware we've seen to date, Geinimi is also the first Android malware in the wild that displays botnet-like capabilities. Once the malware is installed on a user's phone, it has the potential to receive commands from a remote server that allow the owner of that server to control the phone.

BYOD, installer un pare-feu ?..

L'offre de « sécurité »…

- Du DLP (*Data Leak Protection*) pour un organisme (blocage appareil, effacement contenu)
- De l'*anti-stalking* (filtrage harcèlement) renommé pare-feu pour l'Internaute
- **Peu (pas ?) de mise-à- jour OS** de la part du constructeur et/ou opérateur
- **Pas de suivi (correctifs) pour des versions anciennes** (c.à.d. de plusieurs mois).
  Confer attaques présentées au Chaos Congress, BlackHat 2010, DefCon 2010…

BYOD, installer un pare-feu ?..

Le contrôle des flux sortant de votre téléphone pourrait **s'opposer à une stratégie mercantile**;-)

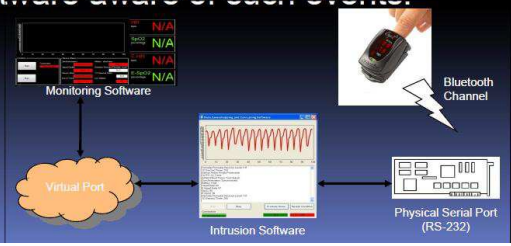
- **Attitudes de consommations**
- Liste de **contacts**
  - Bannière publicitaires ayant une activité spyware à l'insu du développeur d'application
- **Géolocalisation**
- **Liste de mots de passe**
- **Emploi de votre équipement pour envoi de sms, e-mails…**

… et il ne s'agit pas de malwares

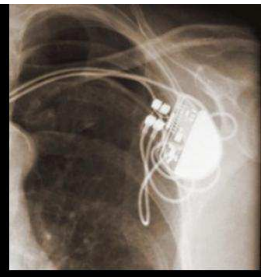
2011, hacking du bio-médical : pacemaker, pompe à insuline, équipements d'hôpitaux…

- Intrusion Technique
  - The intrusion software intercepts the signal that is transmitted from the monitoring device to the computer
  - The interception of the signal is achieve by employing "**Virtual Serial Port**"
  - As a results, we can (i) **eavesdrop** and (ii) **corrupt** the vital signals without letting the Monitoring Software aware of such events.

Security Intrusion Technique



- Researchers had been able to gain wireless access to a combination heart defibrillator and pacemaker. They were able to reprogram it to shut down and to deliver jolts of electricity that would potentially be fatal -- if the device had been in a person
- Also been able to glean personal patient data by eavesdropping on signals.



researchers from Beth Israel Deaconess Medical Center, Harvard Medical School, the University of Massachusetts Amherst, and the University of Washington.
"Security and Privacy of Implantable Medical Devices," Daniel Halperin, Thomas S. Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno, and William H. Maisel, IEEE Pervasive Computing, January 2008.
"Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel, IEEE Symposium on Security and Privacy, May 2008.

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Des actions en région…

RSS/docs CLUSIF
RSS/actus CLUSIF
RSS/actus CLUSIR
RSS/Call For Paper

http://www.clusif.fr/fr/clusir/

http://www.clusif.fr/fr/production/ouvrages/