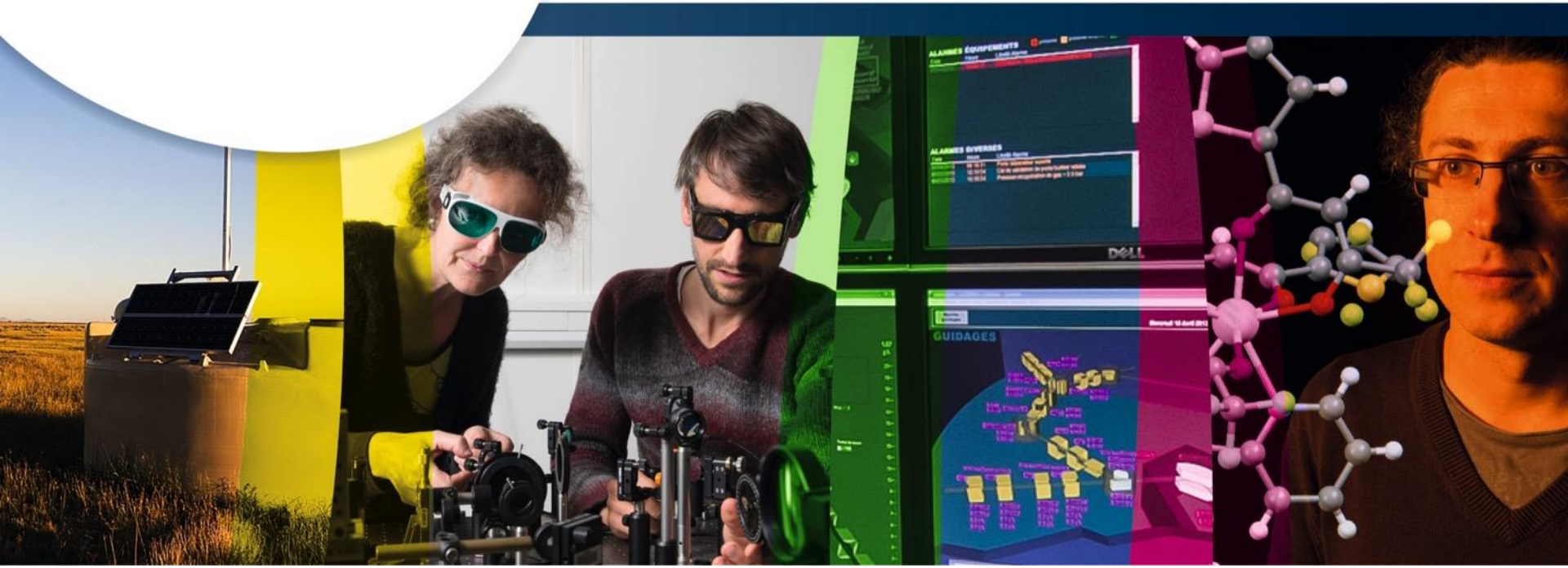
www.cnrs.fr

(In)sécurité des objets connectés ?



Quelques repères historiques

www.cnrs.fr

- Informatique de gestion → *mainframes*
  - IBM 360 (1965), IBM 370 (1970)
  - → *cloud*
- Informatique industrielle, contrôle de processus → mini ordinateur
  - DEC PDP-8 (1965), DEC PDP-11 (1970)
  - → PC, microcontrôleur, Arduino
- Internet
  - Arpanet (1968), Cyclades (1972)
  - Liaisons point à point avec des modems
- Ethernet
  - Xerox PARC (1973)
- WiFi
  - ALOHAnet (1971), 802.11 (1997)
- World Wide Web
  - CERN (1990)

De l'usine à l'objet du quotidien

www.cnrs.fr

- Loi de Moore → faible coût de l'électronique
  - Ubiquité
  - Remplacement par l'informatique de fonctions naguère assurées par
    - mécanique
    - hydraulique
    - pneumatique
- Objet : rien de bien différent dans les principes
  - Capteurs
  - Actionneurs
  - Processeur
  - Connecté
  - IHM
- Comment faut-il considérer un objet connecté ?
  - Un système d'information à part entière
  - Intégré dans un vaste système d'information : Internet, cloud
- Sécurité du monde réel → nécessaire implication du gouvernement

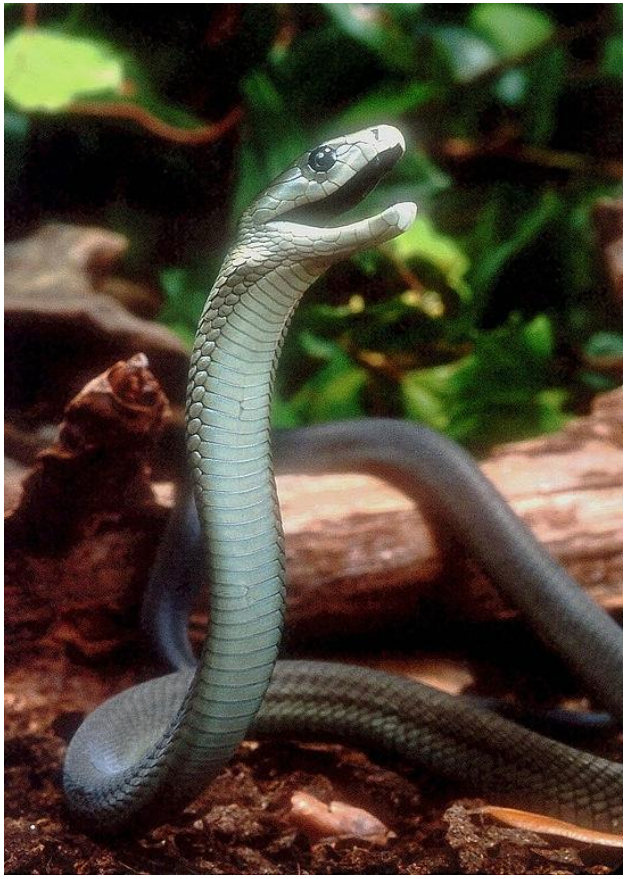
Comment gagner une place à une conférence de sécurité ?

www.cnrs.fr

- Choisir un objet connecté si possible emblématique
- Rechercher et trouver des failles
  - On gagne presqu'à tout coup
    - Radio logicielle pour analyser le protocole réseau
    - Analyse des mises à jour
    - Attaque sur le matériel
- En préparer une exploitation médiatique
- Faire une proposition qui sera acceptée
- Espérer que le fabricant ne fera pas pression pour interdire la présentation

Appréhender le risque

www.cnrs.fr



La peur du serpent (mamba noir) est inscrite dans nos gènes.

Nous avons beaucoup de mal à apprécier les risques liés aux nouvelles technologies.

Sécurité de l'information

- Confidentialité
- Intégrité
- Disponibilité

→ **Quelques exemples de failles de sécurité et raison de ces échecs**

Ukraine BlackEnergy

Ukraine BlackEnergy

www.cnrs.fr

- First known hacker-caused power outage signals troubling escalation
- BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry
- BlackEnergy code malfaisant particulièrement destructif
  - Empêche de redémarrer une machine
  - Détruit le disque
- Imputation ?
- Ukraine: Campagne de spear-phishing BlackEnergy

- **Paralysie du pays**

Stuxnet

www.cnrs.fr

Stuxnet

- To Kill a Centrifuge (Ralph Langner)
- Systèmes industriels
  - Automates programmables industriels (*Programmable Logic Controller, PLC*)
  - SCADA (*Supervisory Control And Data Acquisition*)
    - Windows
    - Attaque passant par une clé USB
- Attaque particulièrement élaborée
  - 0-days
  - Implication de services secrets

- **Destruction de l'outil de production**

Attaque badgeuse RFID par relais

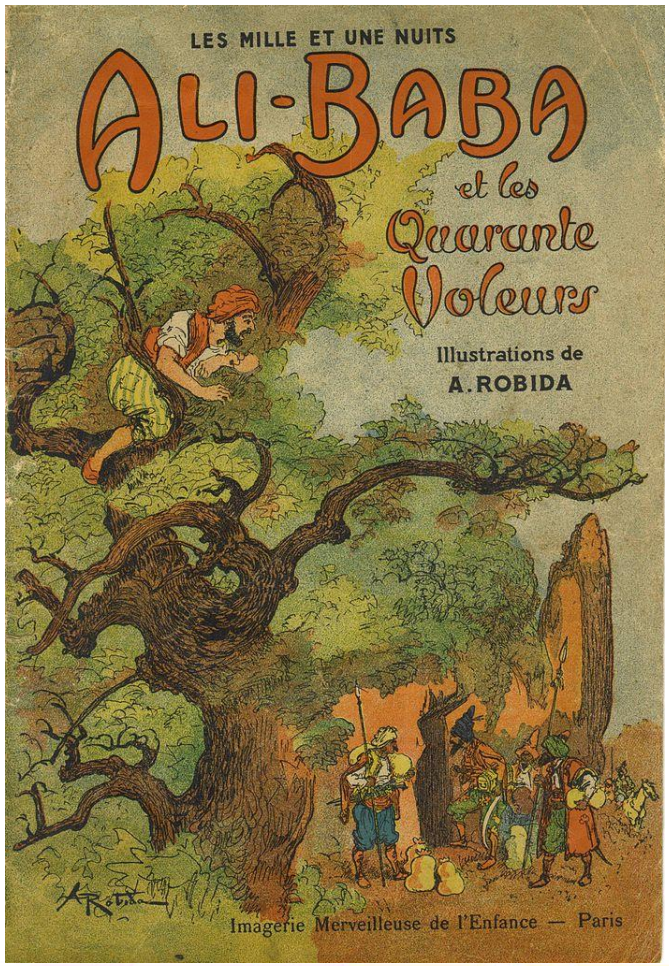
www.cnrs.fr

- Attaque du singe intercepteur ou de l'entremetteur (man in the middle)
- Inhérent à la transmission par des ondes électromagnétiques
- Très difficile de s'en protéger
  - La cryptographie n'y peut rien
  - Mesure du temps mais très délicat
- Brouillage possible

- **La transmission sans fil est intrinsèquement vulnérable**

Antenne accordée sur la fréquence du RFID

Sésame, ouvre-toi !



Un scenario catastrophe : un virus informatique empêche les gens d'entrer !
Des économies mal placées.
Séparer, cloisonner les réseaux est indispensable

De l'utilité de l'audit
découverte d'un Raspberry Pi

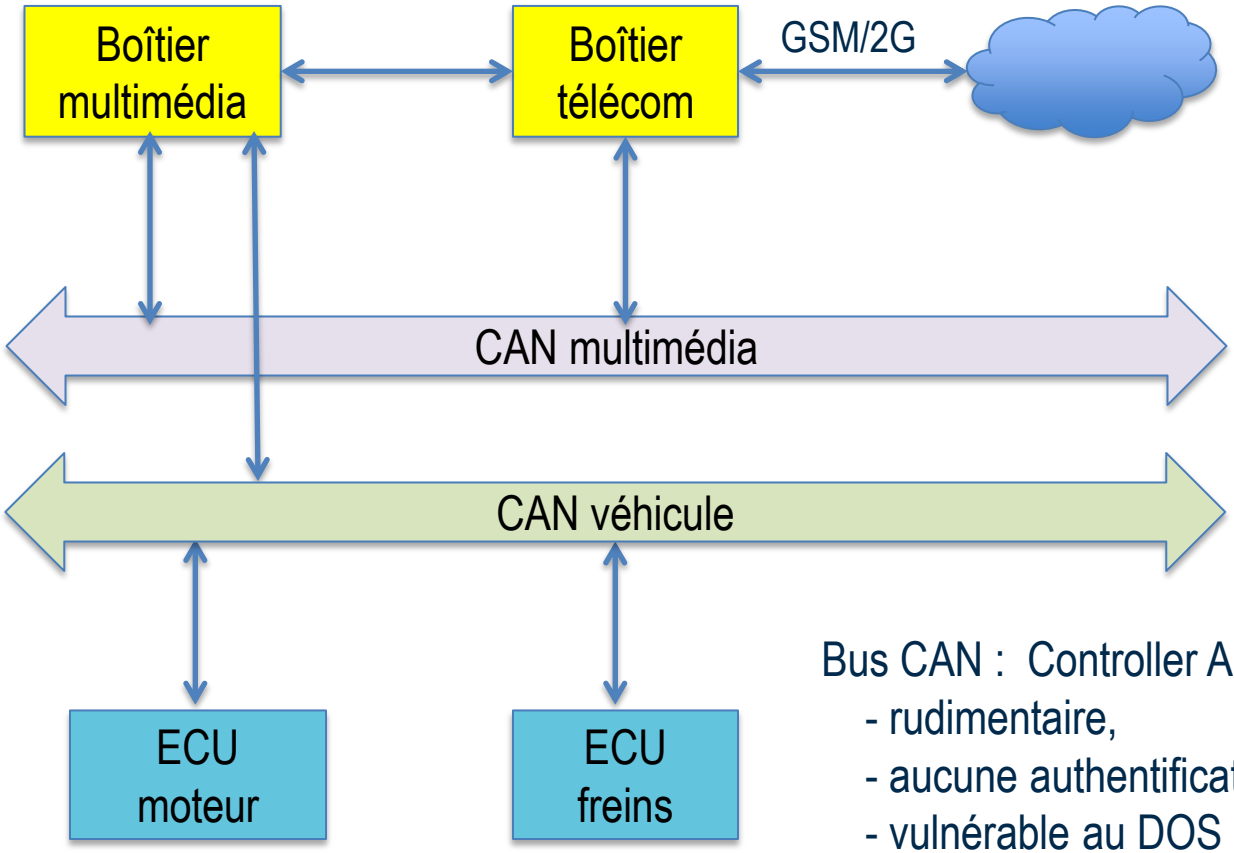
www.cnrs.fr

Un prestataire avait installé discrètement un Raspberry PI pour court-circuiter le pare-feu et administrer à distance le système depuis son domicile.

Découverte chanceuse lors d'un audit.

Un objet connecté peut servir à une attaque discrète.

Voiture : une architecture contestable



Bus CAN : Controller Area network
- rudimentaire,
- aucune authentification
- vulnérable au DOS

ECU : electronic control unit

Voiture

- Évolution et dé-évolution des systèmes multimédia embarqués – François Pollet, Nicolas Massaviol (SSTIC 2016)
- Hackers Remotely Kill a Jeep on the Highway—With Me in It
- Vidéo de la Jeep
- A Tragic Loss (mort du conducteur d'une Tesla en pilotage automatique)

- **Les constructeurs de voitures ne prennent pas suffisamment en compte la possibilité d'actions malveillantes**

Serrure de voitures

www.cnrs.fr

- Clé
  - Communications via radio fréquences
  - Micro contrôleur
  - Envoie un code qui est vérifié par la voiture
- Problématique du rejeu
  - Anciennement code constant → trivial
  - Code tournant
- Analyse de systèmes existants
  - Dispositifs bon marché (radio logicielle, modules RF)
  - Médiocre implémentation de la cryptographie
    - Clés maîtres identiques (VW)
    - Algorithmes faibles (Hitag2)
- Clonage d'une clé
- Dénis de service
- Interférences
  - Enseigne lumineuse

Kettlegate

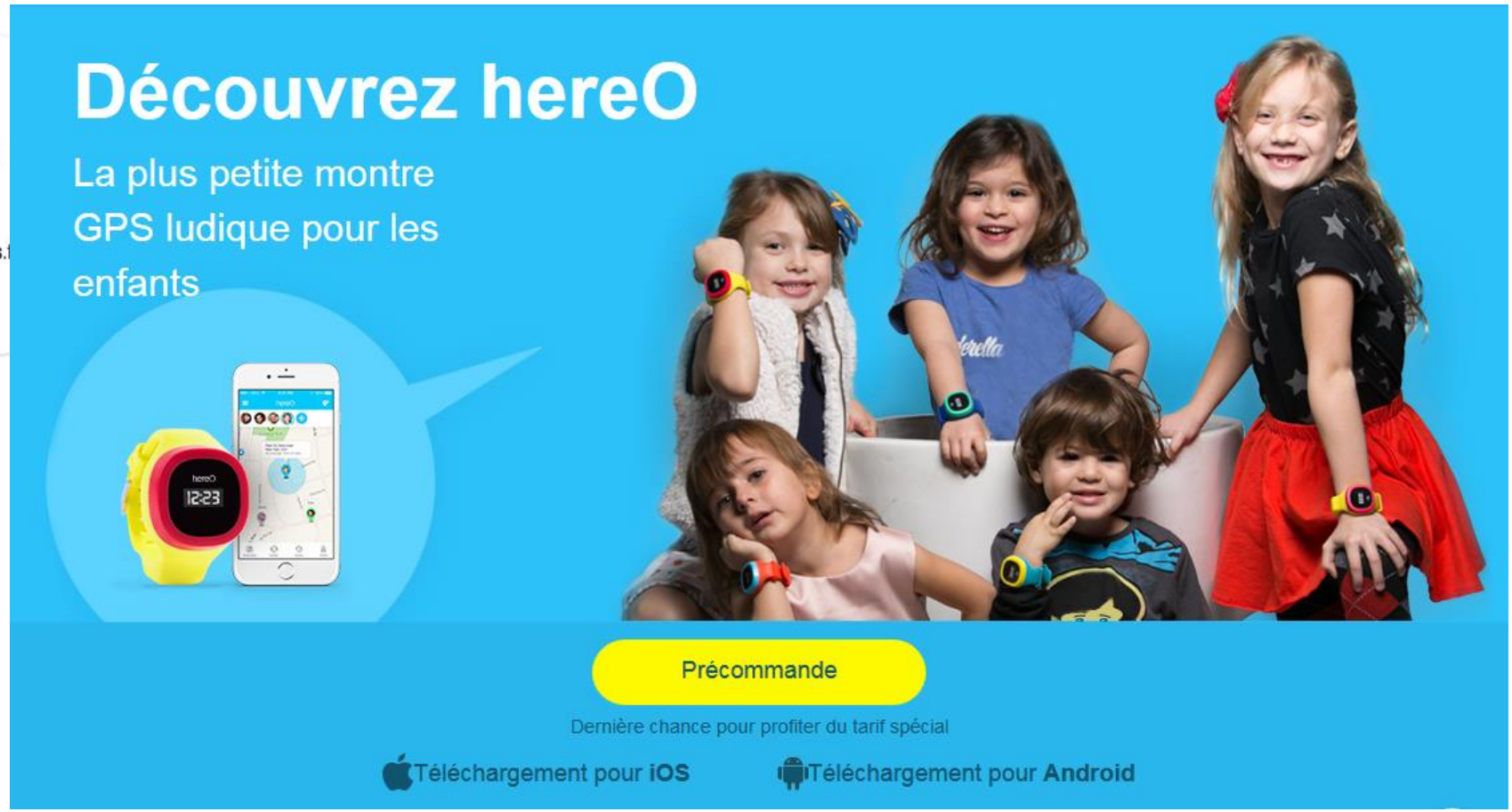
www.cnrs.fr

Kettlegate

- Bouilloires connectées, piratage assuré
- IKettle est conçu pour enregistrer les précieuses secondes passées à attendre l'eau chaude
- Fuite du mot de passe Wi-Fi et pas uniquement de la vapeur
  - Partagé par tous les appareils
- Problème identique avec une ampoule connectée

- **L'attaquant passera par le point le plus faible. Qui va se méfier d'une bouilloire ?**

Les jouets

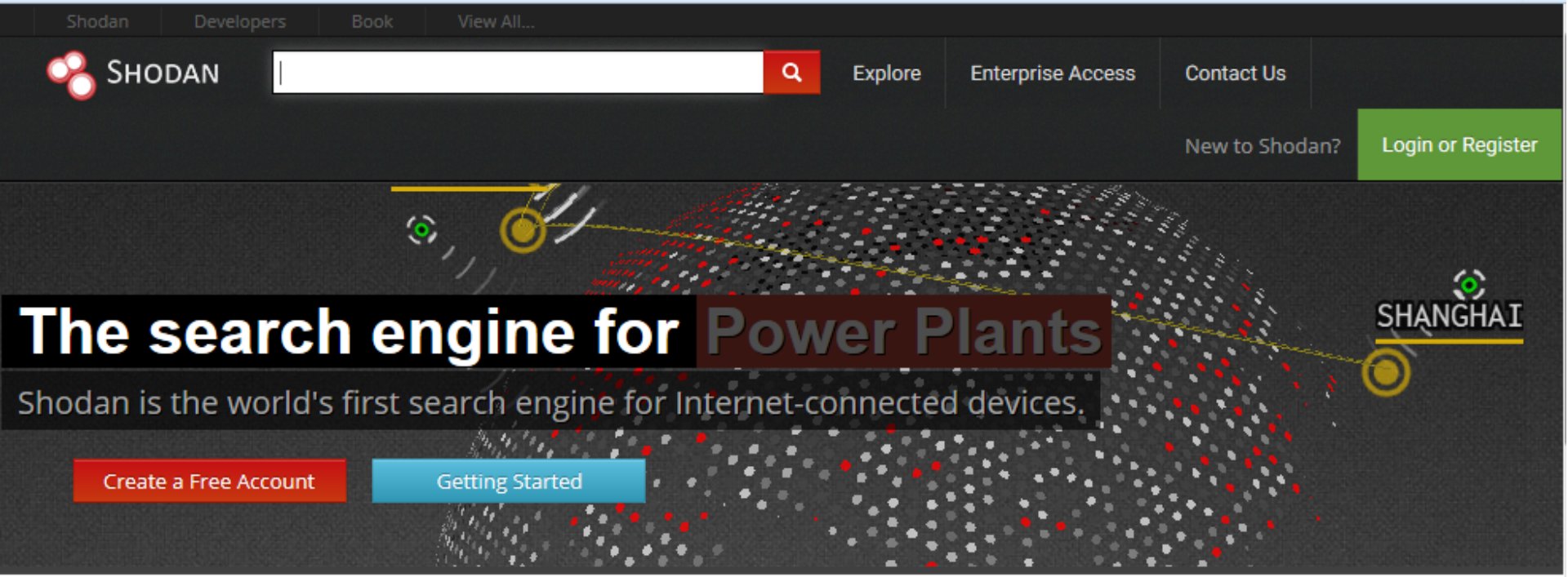

Découvrez hereO
La plus petite montre GPS ludique pour les enfants
Précommande
Dernière chance pour profiter du tarif spécial
Téléchargement pour iOS
Téléchargement pour Android

Les jouets

www.cnrs.fr

- R7-2015-27 and R7-2015-24: Fisher-Price Smart Toy® & hereO GPS Platform Vulnerabilities (FIXED)
  - Fisher-Price : fuites d'informations sur le profil de l'enfant et interaction avec le jouet
  - HereO : l'attaquant était capable de suivre les déplacements de l'enfant
- Vtech toujours confronté à son piratage de Noël
  - Les nom, prénom, âge, adresse, email de plus de 6 millions d'enfants (1,2 en France) et de leurs parents ont été détournés. Les pirates ont même diffusé des photos prises par certains de ces jouets.

- **Parents, vous n'êtes pas les seuls à surveiller vos enfants !**



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

Le bébé qui dort

www.cnrs.fr

Le bébé qui dort

www.cnrs.fr

- "Internet of Things" security is hilariously broken and getting worse
- Shodan
  - Nouvelle rubrique → les webcam librement accessibles sur Internet
  - Des plantations de marijuana aux piscines en passant par la chambre de bébé
- Webcam bon marché sans prise en compte réelle de la sécurité
  - Real Time Streaming Protocol (RTSP, port 554) sans authentification

- **Tout appareil directement connecté sur Internet présente des risques**

Caméra P2P

www.cnrs.fr

FOSCAM

Solutions Products Cloud Service Support Cooperate Login

FI9821P 720P HD IP Camera Make your home & office more safety without changing your lifestyle.

The wireless camera can help you keep an eye on what matters most when you are away from home & office.You can also connect with your family members or pets remotely via smartphone or tablet.

FI9821P

Caméra P2P

- This is Why People Fear the 'Internet of Things'
  - La caméra se connecte à un vaste réseau *peer to peer* géré par le fabricant chinois
- Autre exemple, une prise électrique télécommandé par un smartphone
  - C'était l'application qui était malfaisante et se connectait vers des serveurs en Chine

- **Peut-on faire confiance à certains fabricants ? Il faudrait des normes et des certifications comme il en existe dans d'autres domaines (appareils électriques par exemple)**

DDoS à partir d'objets connectés

Octave Klaba / Oles @olesovhcom · 23 sept.
This botnet with 145607 cameras/dvr (1-30Mbps per IP) is able to send >1.5Tbps DDoS. Type: tcp/ack, tcp/ack+psh, tcp/syn.

Octave Klaba / Oles
@olesovhcom

Suivre

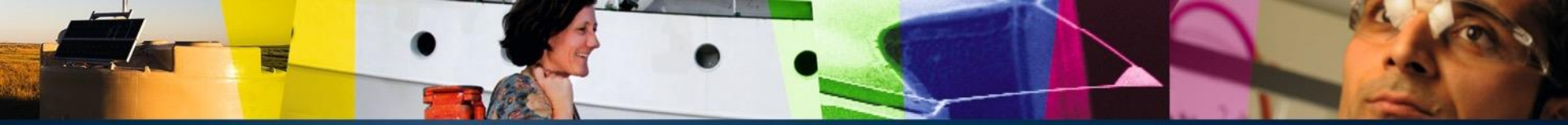
Last days, we got lot of huge DDoS. Here, the list of "bigger that 100Gbps" only. You can see the
simultaneous DDoS are close to 1Tbps !

```
log /home/vac/logs/vac.log-last | egrep "pps\|.....
bps" | awk '{print $1,$2,$3,$6}' | sed "s/ /|/g" | cut -f
1,2,3,7,8,10,11 -d '|' | sed "s/.........bps/Gbps/" | sed
"s/......pps/Mpps/" | cut -f 2,3,4,5,6,7 -d ":" | sort | g
rep "gone" | sed "s/gone|//"
Sep|18|10:49:12|tcp_ack|20Mpps|232Gbps
Sep|18|10:58:32|tcp_ack|15Mpps|173Gbps
```

- DDoS contre le blog de Brian Krebs 620Gb/s
  - Botnet d'objets connectés
  - Suspension de la protection anti DDoS fournie par Akamai

L’attaque du robot aspirateur

www.cnrs.fr



L’attaque du robot aspirateur

www.cnrs.fr

- A robot vacuum tried to eat its sleeping owner's head
- 1ère loi de la robotique d’Asimov
  - Un robot ne peut porter atteinte à un être humain, ni, en restant passif, permettre qu'un être humain soit exposé au danger.

- **Les limites de l’intelligence artificielle ou comment ne pas confondre les poils tombés du chat avec les cheveux de sa maîtresse !**

Problématiques

www.cnrs.fr

- Faible puissance de calcul, consommation électrique
  - Limites sur la cryptographie
- Mises à jour, application de correctifs souvent impossibles
  - Matériel inaccessible
  - Débit réseau insuffisant
- Dépérimétrisation
  - L'objet envoie ses données dans le *cloud*
    - Sécurité du *cloud*
    - *Sécurité du réseau*
  - Quid d'un extincteur connecté ?
- Gestion du cycle de vie : quid des objets abandonnés ou oubliés ?
- Séparation difficile des mondes privé et professionnel
  - Peut-on interdire
    - Montre connectée ?
    - Pacemaker ?
    - Prothèses auditives ?

Problématiques (2)

www.cnrs.fr

- Culture des développeurs de ces objets
  - Peu en informatique
  - Encore moins en sécurité des systèmes d'information
  - Conscient des menaces accidentelles, beaucoup moins de celles résultant d'acteurs malveillants
- Time to market → impasse sur la sécurité
- Changement d'échelles
  - Ce qui est acceptable pour 2 ou 3 ordinateurs en réseau ne l'est plus pour des dizaines d'objets connectés → ex. clé partagée
- Sans fil vulnérable :
  - Brouillage
    - Contre mesure limitée : sauts de fréquence
  - Écoute, *Man in the Middle*
    - Contre mesure : cryptographie

Que faut-il faire ?

www.cnrs.fr

- L'attaque doit toujours être envisagée
- Cloisonner, séparer les réseaux, usages
  - Contre exemple : systèmes industriels
    - Matériel et protocole spécifiques (Modbus sur port série)
    - Composants sur étagères → (Modbus sur Ethernet)
    - Mutualisation des réseaux → même Ethernet pour industriel et bureautique
    - Ouverture à Internet → accessible depuis le monde entier
- La sécurité par l'obscurité est illusoire
  - Kerckhoffs (1883)
  - Rien ne résiste à un chercheur un peu persévérant

Que faut-il faire ? (2)

www.cnrs.fr

- Ne pas réinventer la roue
  - La cryptographie doit être réservée à des spécialistes
  - Un protocole réseau ne s'invente pas sur un coin de table
- Effectuer une appréciation des risques (menaces, exploits, impacts)
  - Il existe des risques létaux (voiture, pompe à insuline, etc.)
  - Obligations : RGS, PSSIE, informatique et libertés
- La sécurité est aussi pour protéger la propriété intellectuelle
  - Prévenir la copie par un concurrent indélicat

En guise de conclusion

www.cnrs.fr

- *Rien de nouveau sous le soleil* (Ec 1:9)
  - Les développeurs reproduisent les mêmes erreurs
  - Mêmes contraintes de *time to market,* pression des MOA
  - Même problématique de suivi des correctifs
- Le CNRS est consommateur mais aussi producteur d'objets connectés comme de systèmes industriels (pilotage d'expériences)
- Introduire la sécurité en amont dans les projets
  - La correction *a posteriori* est très chère voire est impossible
  - La sécurité est un excellent argument pour promouvoir un produit
    - Surtout après la prochaine catastrophe qui arrivera fatalement
- Il faut espérer la mise en place de normes, de certifications, d'homologations comme dans d'autres domaines (électricité, santé, etc.)

Peut-on laisser les développeurs faire n'importe quoi ?

www.cnrs.fr

We need to start making more ethical and political decisions about how our technologies should work. But because the internet has been so benign [until now] we've allowed programmers to have this special light in society to code the world as they see fit, I don't think we can do that anymore. I think this is becoming too critical to allow programmers to do what they want.

Bruce Schneier "Privacy, Trust and the Internet of Things" à infosecurity