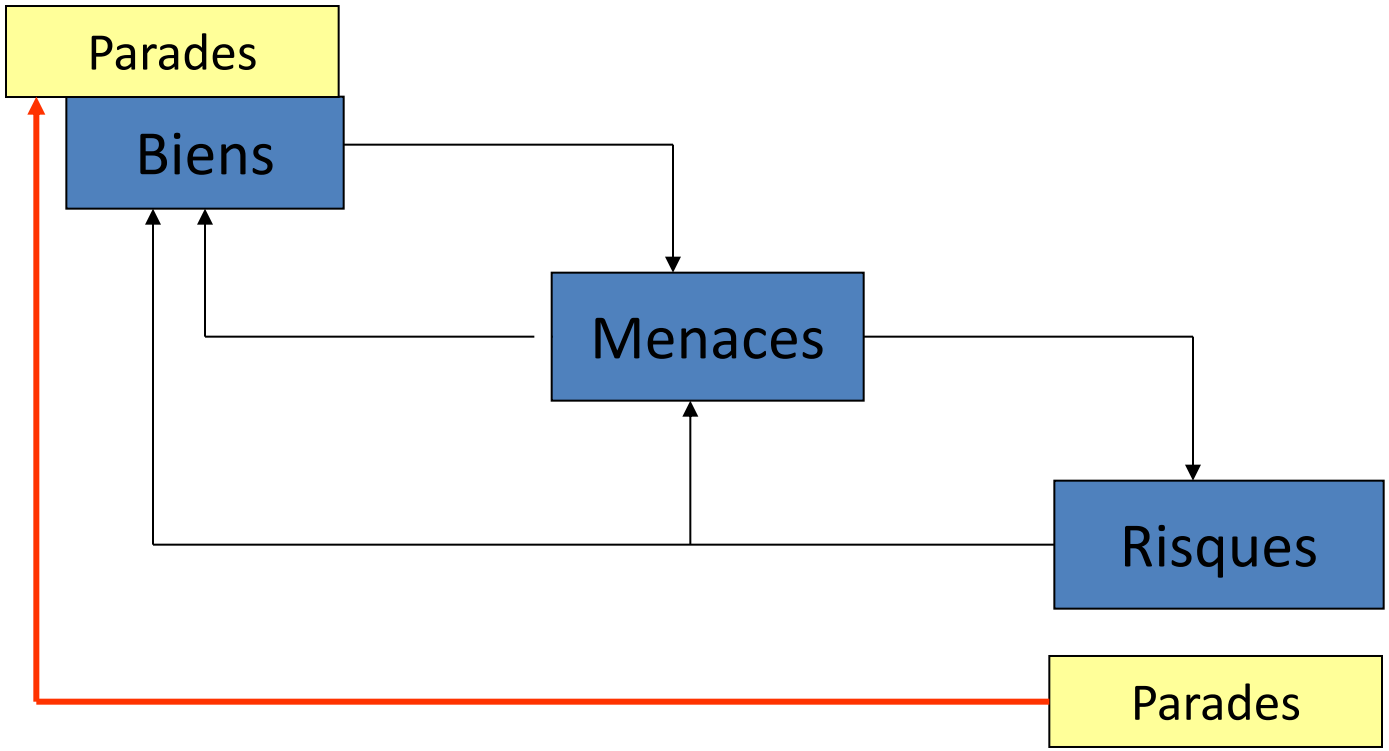
Objets connectés et sécurité

Quels sont les risques ?

Analyse de risques



Les « Biens »

- Des objets physiques : Tags, sondes, transmetteurs, smartphones, serveurs…
- Des données, ou informations : t°, numéro carte CB, nom, code, empreinte…
- Des biens immatériels: nom entreprise, secrets fabrication, réputation…

Les types d'objets

- Objets « passifs » : tags 2D, tags RFID, tags NFC…
- Objets « actifs » : sondes, compteurs, capteurs plus ou moins évolués.
- Objets complexes: smartphones, consoles, PC…
- Serveurs: locaux, par domaine, centraux…

Les informations transmises…

- Données peu sensibles, individuellement: T°, compteur, pression, poids…
- Données sensibles pour l'objet: modification compteur, modification filtre, RAZ, mise hors ou en service, identifiant…
- Données sensibles pour l'utilisateur: modification adresse, données personnelles, modification des droits…

Biens immatériels

- Correspondants.
- Volume de données.
- Secrets de fabrication.
- Informations stratégiques
- Réputation.

Les Menaces/fonctions de sécurité

Menace	Fonction de sécurité
Divulgation information	Confidentialité
Intrusion	Authentification
Modification	Intégrité
Blocage	Disponibilité

Biens → Menaces

BIENS	MENACES
Objets passifs	Intégrité, authenticité
Objets actifs	Intégrité, authenticité, confidentialité, disponibilité
Objets complexes	intégrité, authenticité, confidentialité, disponibilité
Serveurs	intégrité, authenticité, confidentialité, disponibilité

Risques

- Objets passifs : faibles (réputation)
- Objets actifs : moyens à élevés
- Objets complexes : élevés
- Serveurs : graves à majeurs

Connectés comment ?

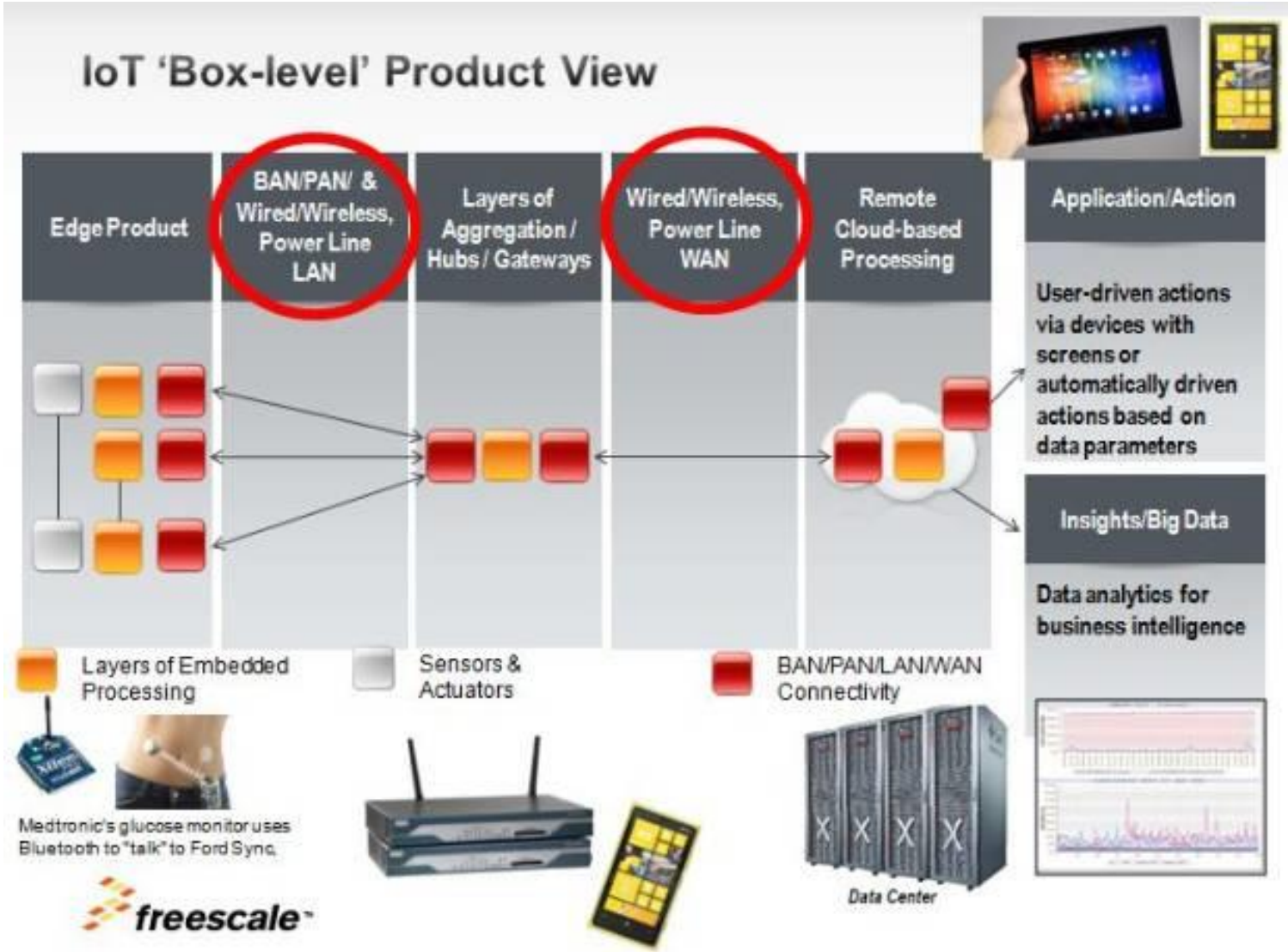
- USB
- IR ?
- RFID ?
- NFC ?
- BT ?
- E-Beacon?
- Zigbee ?
- WiFi ?
- GSM, 3G, 4G?
- …

- GSM, 3G, 4G
- INTERNET

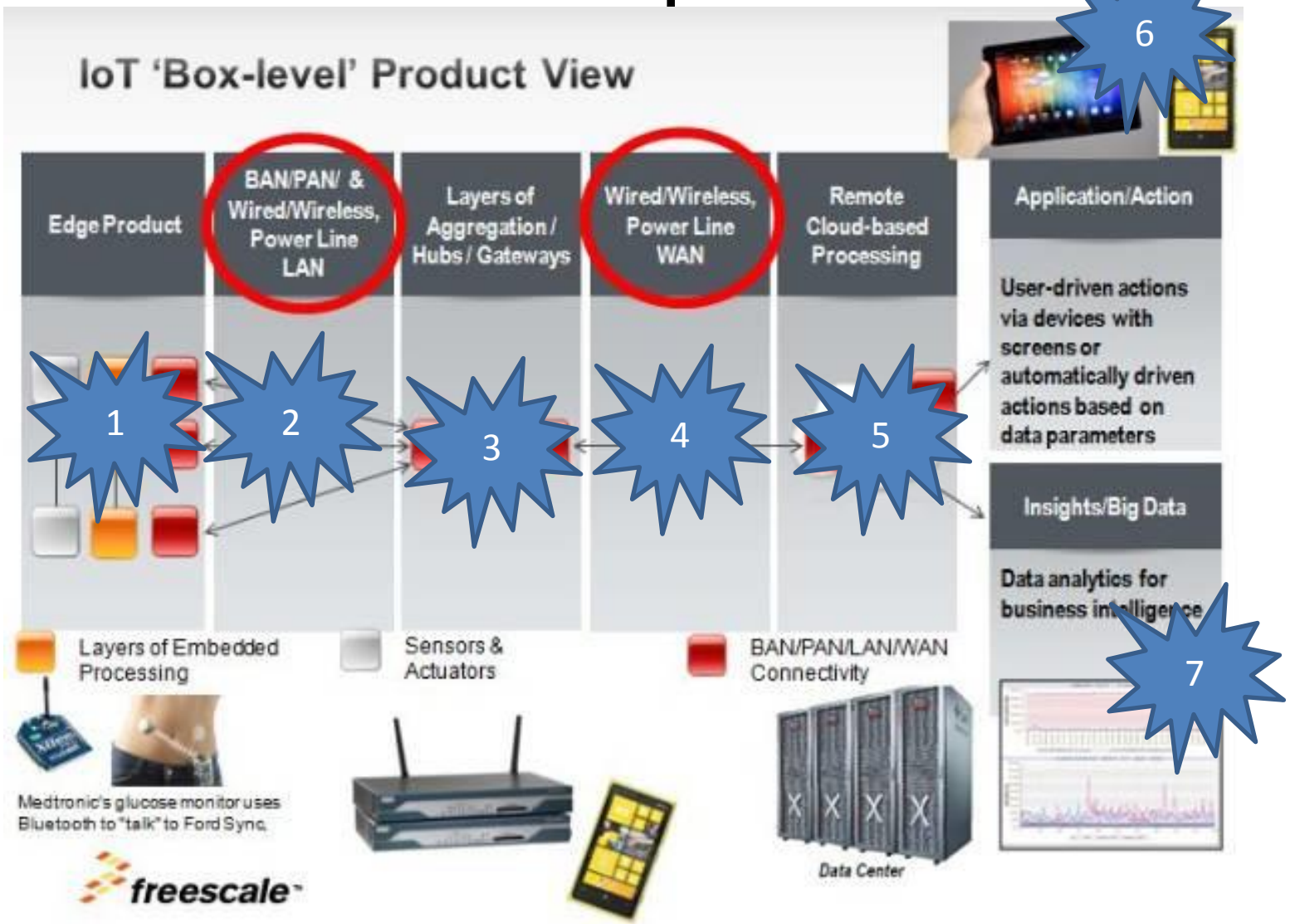
Sécurité des connections ?

- IR : clair, réflexion sur une vitre visible à plusieurs dizaines de mètres…
- BT: chiffré, mais en général identifiant/mot de passe fixes pour beaucoup d'objets…
- RFID: clair, quelques dizaines de cm…
- NFC: clair, une dizaine de mètres
- Wifi: chiffrement correct en WPA2 (**nul sinon)**, quelques dizaines de mètres
- GSM, 3g, 4G: chiffré entre objet et antenne, mais non chiffré sur réseau opérateur
- Internet: si non chiffré, les « grandes oreilles » sont à l'écoute ! (Elles le sont parfois, même si chiffré…)

Sécurité « Cross-domains »

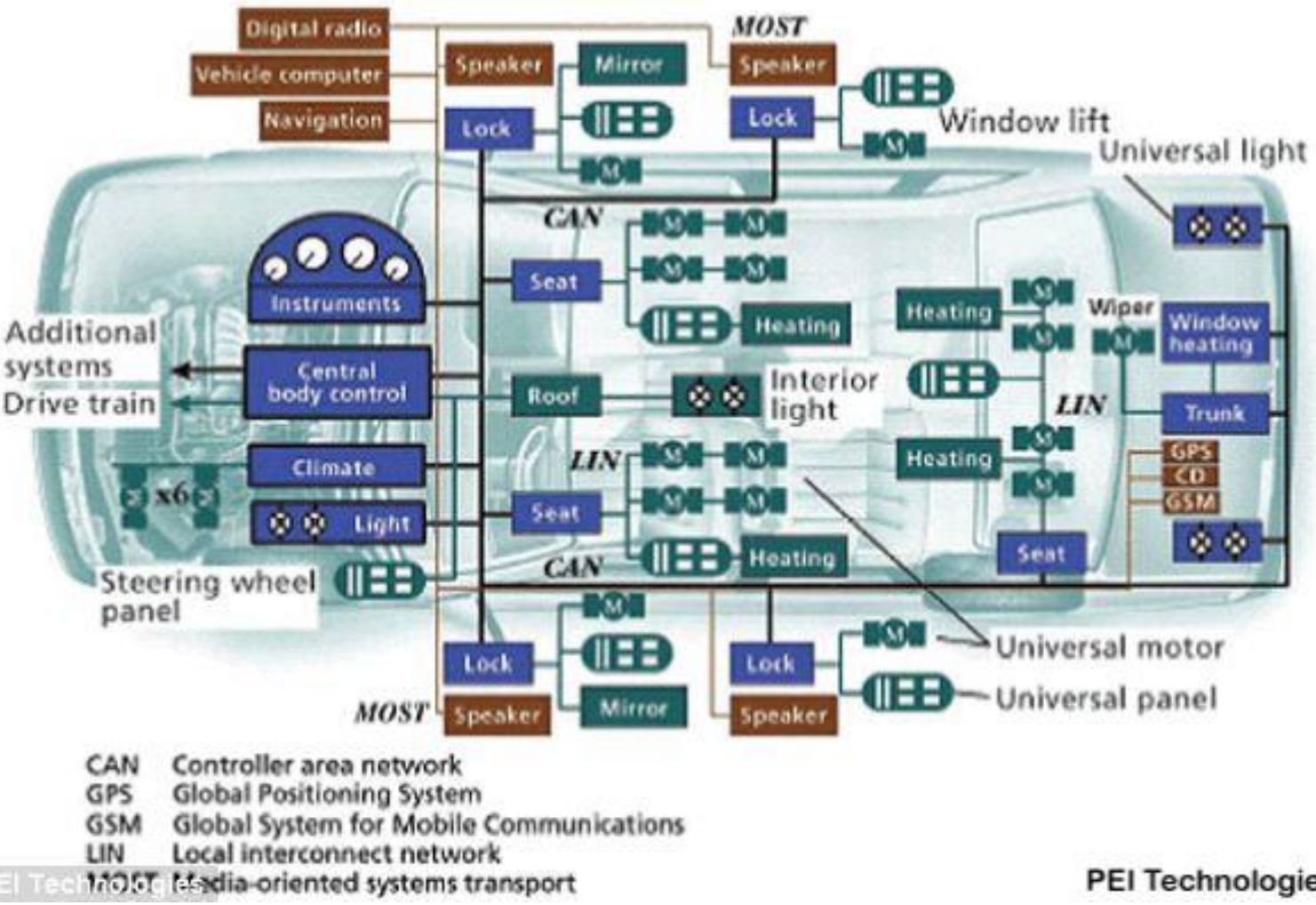


Les attaques ?



Parano ?

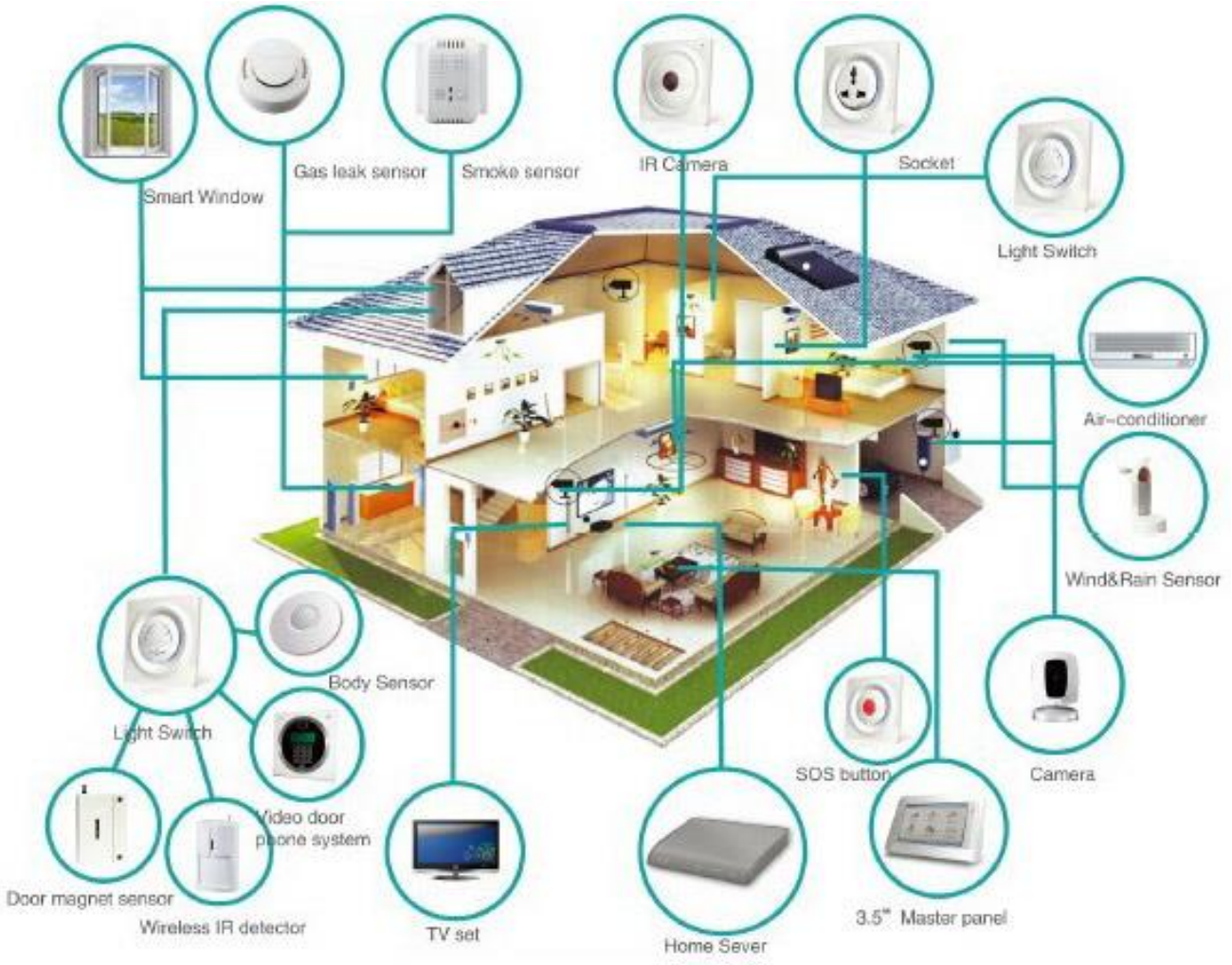
Car Hacking…



Parano 2 ?

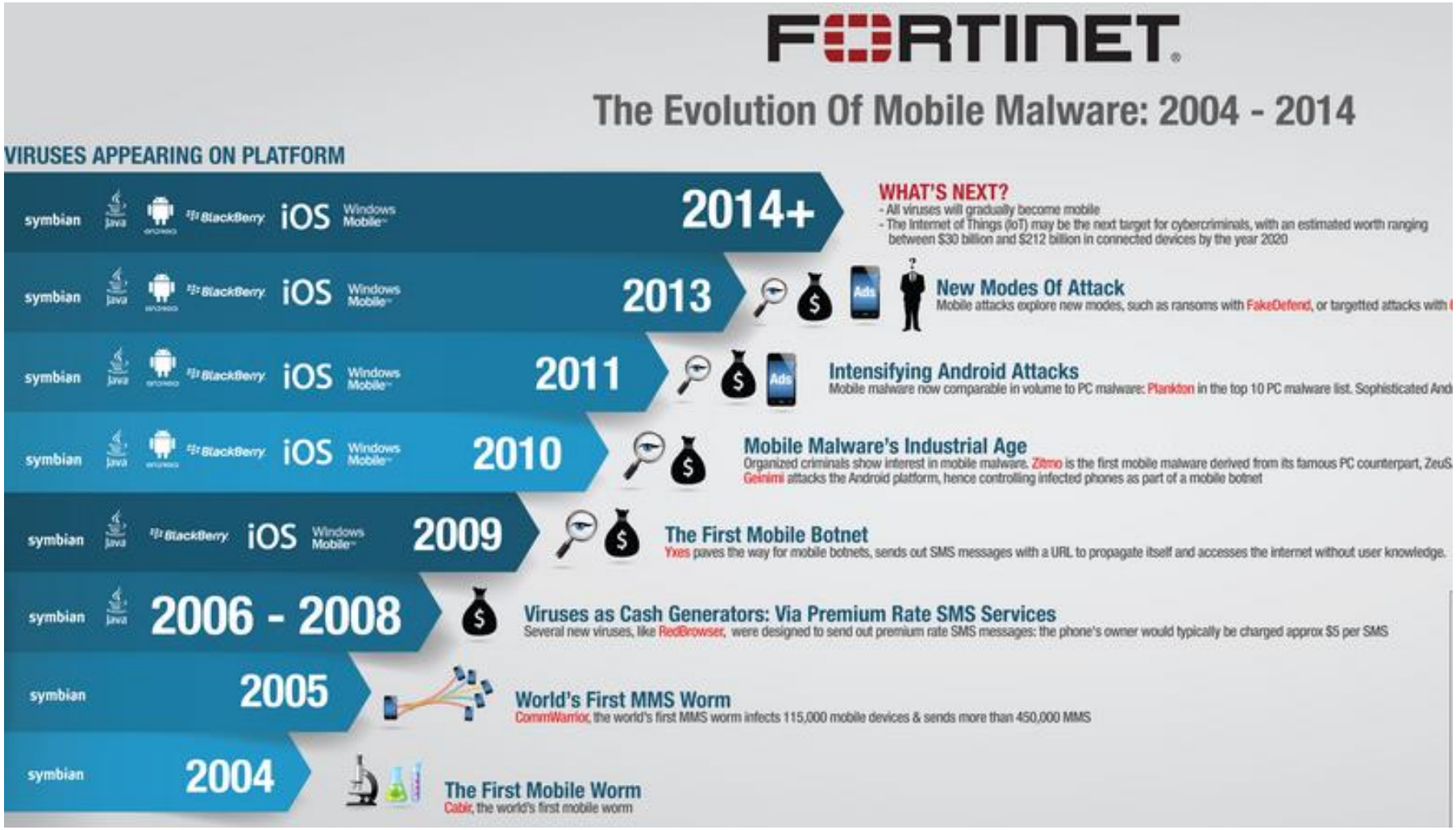
- “I can see all of the devices in your home and I think I can control them,” I said to Thomas Hatley, a complete stranger in Oregon who I had rudely awoken with an early phone call on a Thursday morning.
- He and his wife were still in bed. Expressing surprise, he asked me to try to turn the master bedroom lights on and off. Sitting in my living room in San Francisco, I flipped the light switch with a click, and resisted the Poltergeist-like temptation to turn the television on as well.

« Smart homes »


Smart Window
Gas leak sensor
Smoke sensor
IR Camera
Socket
Light Switch
Air-conditioner
Wind&Rain Sensor
Body Sensor
Light Switch
Video door phone system
Door magnet sensor
Wireless IR detector
TV set
Home Sever
SOS button
Camera
3.5" Master panel

Ooops !

ZITMO ?


FORTINET
The Evolution Of Mobile Malware: 2004 - 2014
VIRUSES APPEARING ON PLATFORM
2014+
WHAT'S NEXT?
- All viruses will gradually become mobile
- The Internet of Things (IoT) may be the next target for cybercriminals, with an estimated worth ranging between $30 billion and $212 billion in connected devices by the year 2020
2013
New Modes Of Attack
Mobile attacks explore new modes, such as ransoms with FakeDefend, or targetted attacks with
2011
Intensifying Android Attacks
Mobile malware now comparable in volume to PC malware: Plankton in the top 10 PC malware list. Sophisticated And
2010
Mobile Malware's Industrial Age
Organized criminals show interest in mobile malware. Zitmo is the first mobile malware derived from its famous PC counterpart, ZeuS. Geinimi attacks the Android platform, hence controlling infected phones as part of a mobile botnet
2009
The First Mobile Botnet
Yxes paves the way for mobile botnets, sends out SMS messages with a URL to propagate itself and accesses the internet without user knowledge.
2006 - 2008
Viruses as Cash Generators: Via Premium Rate SMS Services
Several new viruses, like RedBrowser, were designed to send out premium rate SMS messages: the phone's owner would typically be charged approx $5 per SMS
2005
World's First MMS Worm
CommWarrior, the world's first MMS worm infects 115,000 mobile devices & sends more than 450,000 MMS
2004
The First Mobile Worm
Cabir, the world's first mobile worm

Un bon exemple :

- Terminal entièrement autonome
- Sécurité intérieure
- Sécurité réseau (surcouche SSL sur GSM+ authent mutuelle)

QUE FAIRE ?

- « Security is not a patch »
- Analyse de risques nécessaire
  - Lister les biens
  - Lister les menaces
  - Lister les risques
- La revoir tous les ans !