Institut Mines-Télécom

Objets connectés : enjeux de sécurité et de vie privée

Maryline LAURENT,
Institut Mines-Télécom/Télécom SudParis
Resp. Equipe R3S, CNRS SAMOVAR UMR5157
Cofondatrice de la chaire Valeurs et politiques des informations personnelles

Agenda

- Qu’est ce qu’un objet connecté ?
- Enjeux de sécurité
- Enjeux sur la vie privée
- Différents points de réflexions
- Les tendances pour le futur

Qu’est ce qu’un objet connecté ?

- **Objet : équipement électronique doté de capacités très hétérogènes en communication, traitement, mémoire, énergie et collecte de données**
- **Exemples : smartphone, smartwatch, smartTV, capteur, voiture connectée**

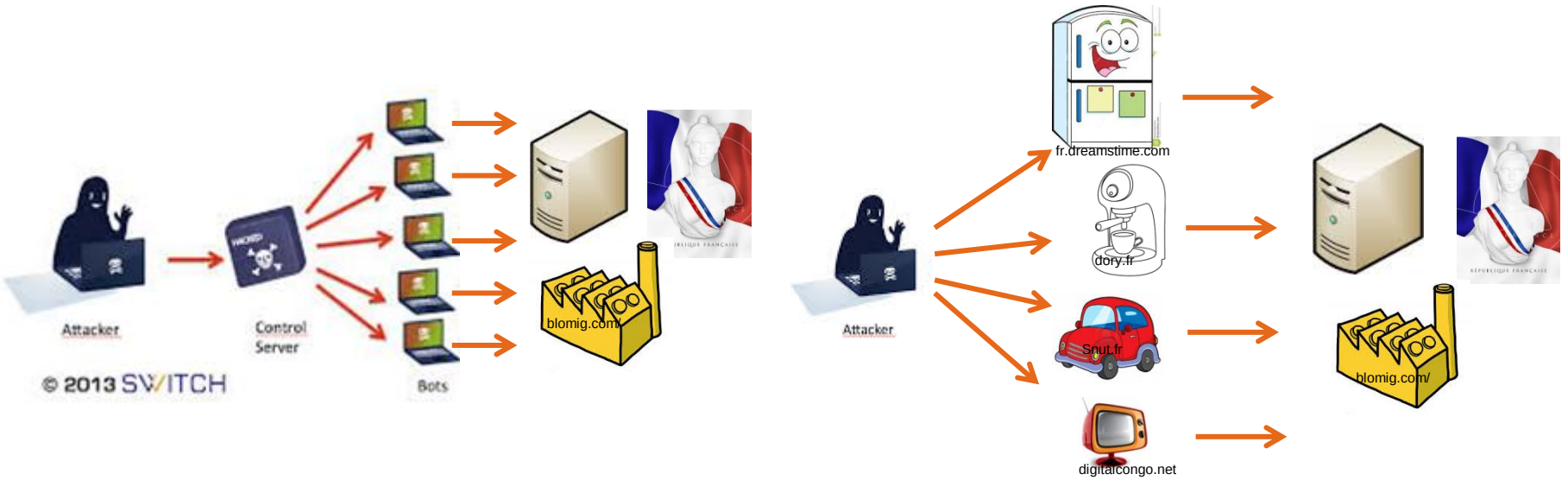
Caractéristiques d'un objet connecté

- Faible niveau de sécurité (mots de passe, système d'exploitation)
- Volume conséquent en forte croissance des objets connectés (6 milliards vs qq 100 millions d'ordinateurs)
- Besoin de connectivité des objets (maintenance ou collecte de données)
- Collecte massive de données personnelles

Enjeux de sécurité

Faible niveau de sécurité + Volume conséquent

Avant ..... Après



Attaque de grande ampleur sur un serveur cible

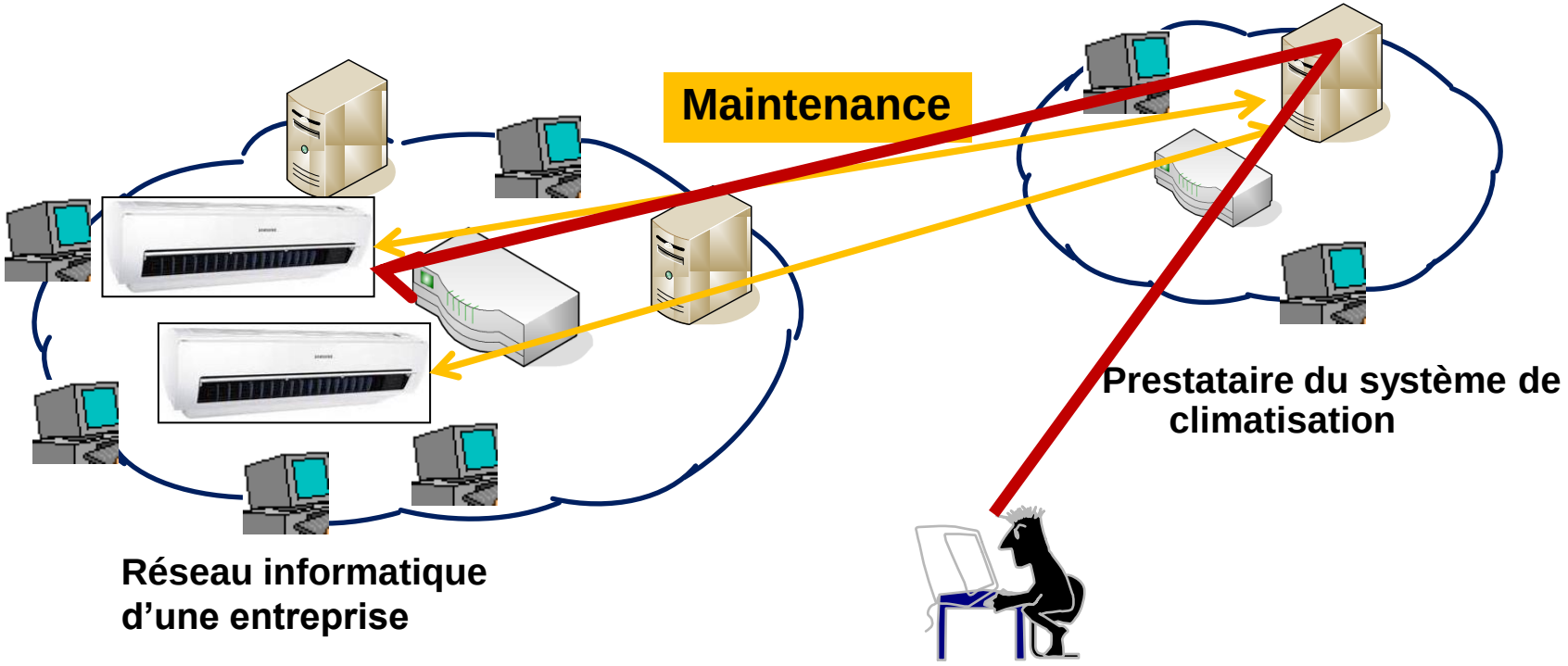
Attaque de déni de service distribuée

Ex : hébergeur OVH sept. 2016 - Pointe à 1Tbps – indisponibilité du service

145.000 caméras IP mal sécurisées impliquées

Enjeux de sécurité

Besoin de connectivité – cas 1 – objets statiques

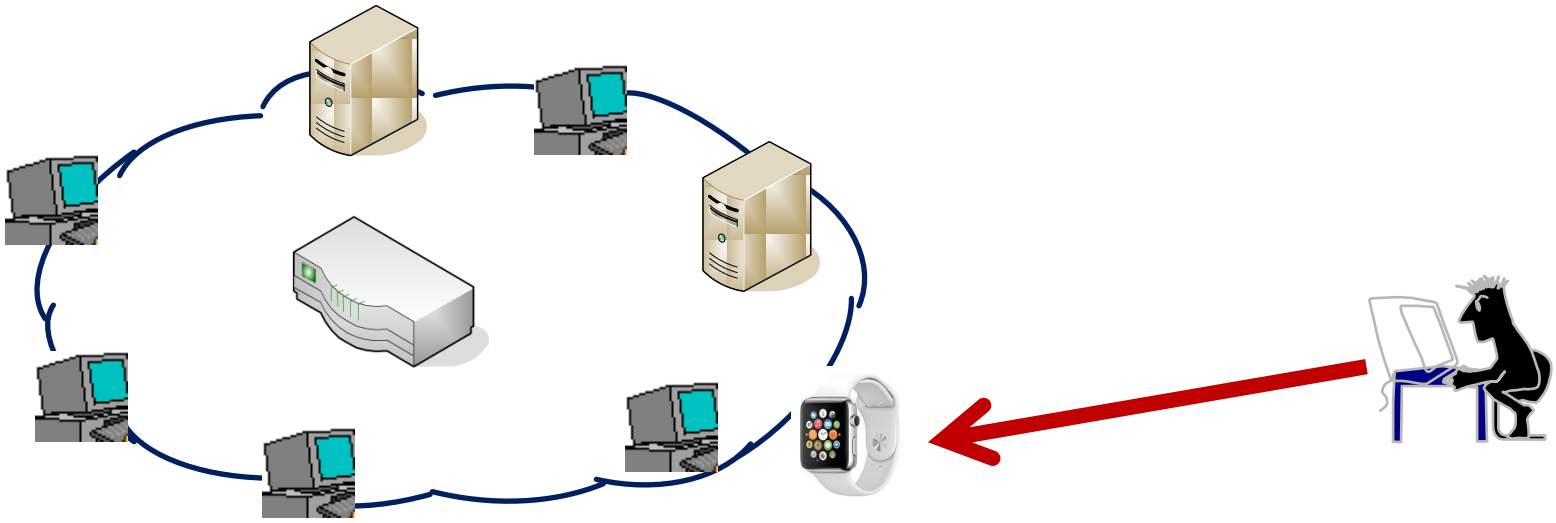


Intrusion dans le système d'information d'une entreprise

Ex : TARGET en décembre 2013 par son système de climatisation - attaque de son prestataire de services

Résultats : 40 millions de comptes clients volées

Enjeux de sécurité
Besoin de connectivité – cas 2 – objets personnels



Réseau informatique d'une entreprise

Besoin de recharger une smartwatch (port USB d'un ordinateur)

Objet = vecteur d'infection d'un réseau d'entreprise

Enjeux de sécurité
Niveau de sécurité insuffisant

Avant ..... Après


w12.fr


fr.123rf.com


Pelagie46.wordpress.com

Piratage d'un véhicule connecté en 2015 par 2 chercheurs - prise de contrôle à distance de plusieurs équipements (autoradio, coupure du moteur…)

Ex : Tesla et Jeep Cherokee

Danger : intégrité physique du conducteur et des passagers menacée

Enjeux sur la vie privée
Faible niveau de sécurité

Avant ..... Après


fr.123rf.com

Cambriolage


juste1oeil.com


depositphotos

Renseignement

Vandenborre.be

Cloud

SmartTV de Samsung (micro activé à des fins de reconnaissance vocale)

Intrusion sur les objets du foyer ou dans le service cloud

Hackers ou cybersurveillance

Enjeux sur la vie privée
Faible niveau de sécurité du cloud

Avant ..... Après

Baisse de chauffage

Consommation électrique minimale

⇒ ***Aucune personne au domicile***

Intrusion dans le service cloud

Hackers ou cybersurveillance

Sécurité nationale vs vie privée

Glissement progressif vers plus de cybersurveillance de masse

<u>En France</u> : Loi de la programmation militaire , loi du renseignement de 2015, allouent de plus de droit à l'Etat pour autoriser la cybersurveillance de masse

<u>En Chine</u> : <u>Service de crédit social</u> en cours d'élaboration pour 2020 pour donner un score à chaque citoyen chinois :

- score décroit : écarts au code de la route, les propos politiquement incorrects sur les réseaux sociaux…

- pénalités : interdiction de sortie du territoire, d'inscrire ses enfants dans telle école, d'accéder à une promotion…

<u>Aux USA</u> : Révélations de Snowden en 2012 (surveillance de masse), révélations de Wikileaks en 2017 sur la CIA (outils permettant de pirater des produits Apple, Samsung, Microsoft, des logiciels Linux ou encore Android)

Sécurité nationale vs vie privée

Glissement progressif de la société par facilité, par attrait du gain

Acceptation d'un bracelet connecté ou d'une télésurveillance

VS

remise de prix par les assureurs

Le droit à la vie privée…
Et vous, que pensez- vous de la surveillance de masse ?

- A : Je n'ai rien à cacher, donc cela ne m'inquiète pas d'être surveillé(e)

- B : Je veux conserver mon intimité numérique pour préserver ma vie privée

… Réfléchissons ensemble…

- **Un besoin naturelle d'opacité dans nos relations :**
  - Nous cachons des choses à nos amis à notre famille (maladie, homosexualité, maternité…)
  - Nous cachons tous un grand nombre de choses sans rien faire de mal

  ➢ C'est cela la « vie privée »

- **Nuisances possibles de l'utilisation des données personnelles par des tiers :**
  - Banquiers : liste des achats en boutiques, leur fréquence…
    => refuser un crédit jugé trop risqué pour la banque
  - Assureurs : informations de santé, données de conduite…
    => refuser d'assurer une personne
  - …

… Réfléchissons ensemble…

- **<u>Etes-vous sûrs</u> de n'avoir rien à vous reprocher ?**
  - Des lois complexes et en constante évolution

  <u>Le pouvoir de la justice et des lois :</u>

  « Qu'on me donne six lignes écrites de la main du plus honnête homme, j'y trouverai de quoi le faire pendre » (Le cardinal de Richelieu)

  Qui connaît suffisamment bien la loi pour affirmer qu'il n'a rien à se reprocher ?

- **Evolution du droit et de la société rendus possibles par :**
  - Combats politiques, débats d'idées (associations, syndicats…) : comment organiser en secret des réunions pour défendre des causes, pour lutter contre des lois illégitimes … sans préservation de la vie privée ?
  - Légalisation de pratiques interdites (cannabis aux USA, homosexualité dépénalisé en France en 1791, avortement légalisé en France en 1975…)

Source : « De l'intimité et de sa nécessité », la Quadrature du Net, mars 2016

Conclusions

- **Enjeux sociétaux et économiques des objets connectés :**
  - Plus grand confort apporté par les technologies (santé, domotique, énergie)
  - Croissance du marché des objets connectés jusque 1,7T US$ d'ici 2020 *(IDC Directions, 2016)*
  - Marché des données personnelles estimé à 1000 milliards d'euros d'ici 2020 en Europe *(Boston Consulting Group, 2014)*
  - Problématique du time-to-market, de la compétitivité entre entreprises dans l'offre => protection des données personnelles et sécurité des objets jusque là plutôt au second plan

VS

- **Enjeux juridiques (+ éthiques) :**
  - Problématique de responsabilité et de cybersurveillance
  - Une législation à la page pour encadrer la sécurité et la vie privée

Conclusions – Tendances à venir

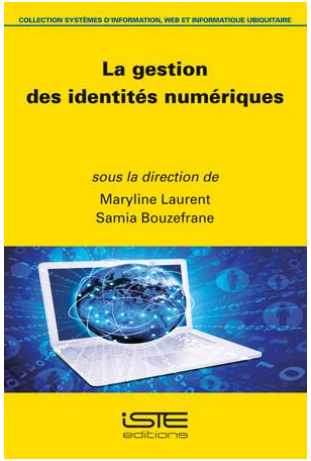
- **Beaucoup de travail reste à accomplir pour un Internet des objets de confiance**
- **Nécessité de :**
  - Former/sensibiliser des consommateurs aux problématiques de sécurité et de vie privée
  - Une législation plus stricte pour limiter les risques

- **Nouveau règlement européen GDPR adopté en 2016 et mis en application en 2018 :**
  - S'applique à tout responsable de traitement des données personnelles (situé UE, hors UE), dès lors que l'objet émetteur (réveil connecté, smartphone…) se trouve dans un pays membre
  - Principes d'importance : Consentement de l'utilisateur ; finalités déterminées, explicites et légitimes ; minimisation des données ; délai de conservation
  - Responsabilité plus grande des entreprises qui doivent garder des preuves des traitements
  - Sanction : jusque 4% du chiffre d'affaire mondial d'une société en cas de manquement

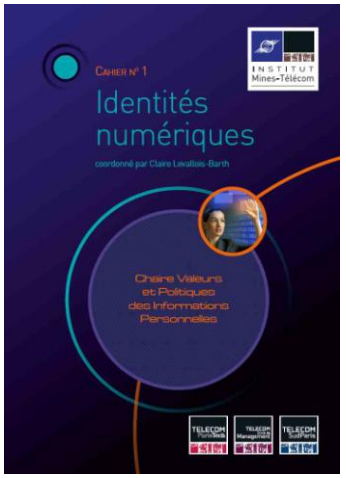
- **Vers une labellisation / certification européenne garante du niveau de sécurité et de la préservation de la vie privée**
  - Bonne idée pour le consommateur, mais périmètre à définir (objet matériel, sous-partie du matériel, du service, de la plate-forme) ?

Conclusions

- **Ces travaux prennent place au sein de la chaire multidisciplinaire Valeurs et politiques des informations personnelles de l'Institut Mines Télécom**



http://cvpip.wp.mines-telecom.fr/



Merci pour votre écoute