Institut Mines-Télécom

COMBINER ATTAQUES LOGICIELLES ET MATÉRIELLES

SOMMAIRE

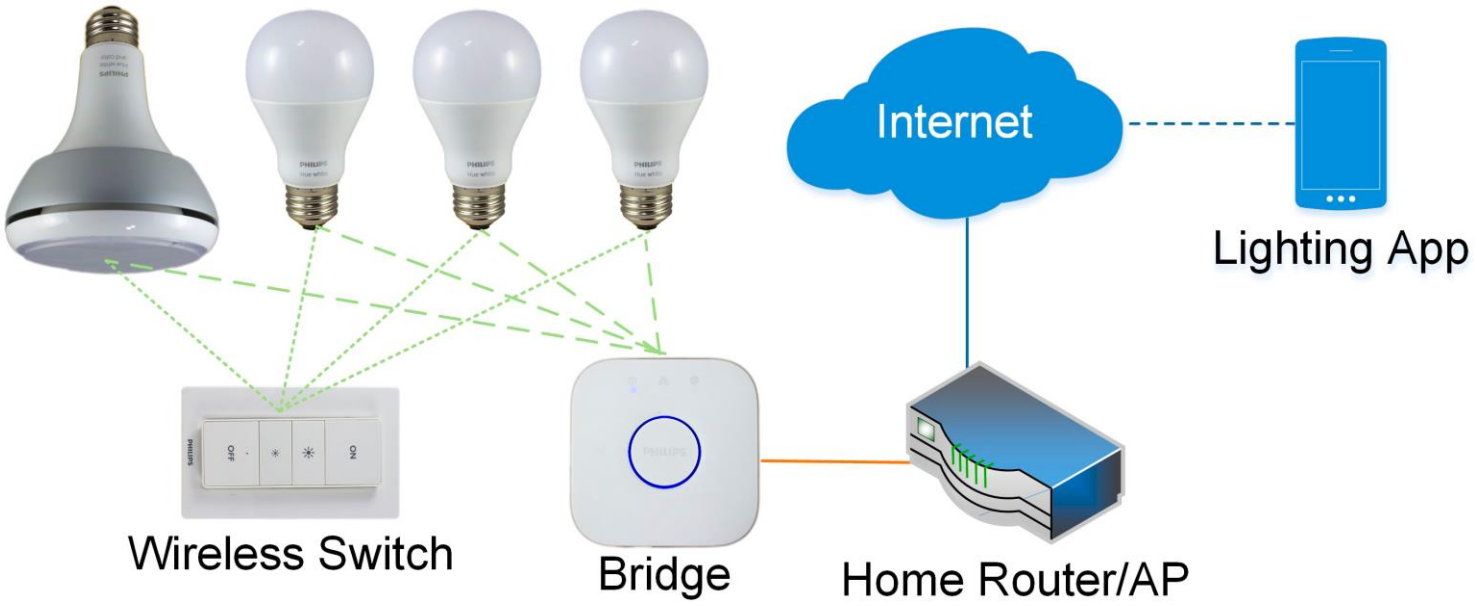
Institut Mines-Télécom

CHAPITRE 1
#IOT

Institut Mines-Télécom

Ampoules connectées Philips Hue
Protocol : Zigbee Light Link (ZLL)

« IoT Goes Nuclear: Creating a ZigBee Chain Reaction », Ronen and al, 2016



La sécurité est le 1er frein au développement de l'IoT dans le monde professionnel

(Etude KPMG, livre blanc IoT, mai 2016)

Nature de la menace

- Données personnelles de l'utilisateur
- Propriété intellectuelle du fabricant
- Réputation commerciale du fabricant
- Constitution de **botnets** mettant en danger internet
  - distribution de pourriels
  - attaques par déni de service (DDoS)

Particularités

- Effet d'échelle (internet), accès physique, objets bas coût

Historique de la sécurité des objets connectées

- Ignorance/Absence de toute politique de sécurité

Caméra IP :
Mot de passe par défaut : **default**

- Prise en compte → mise à jour logicielle à distance
  - Failles protocolaires et Attaques logicielles
- Utilisation de la cryptographie
  - Mathématique sûr
  - Attaques matérielles

Temps

CHAPITRE 2
ATTAQUE DE LA LAMPE PHILIPS

Institut Mines-Télécom

Contre-mesures de la mise à jour Over the Air (OtA)

- Protocole sécurisé (Test de proximité)
- Utilisation de la cryptographie : Firmware chiffré et signé par AES

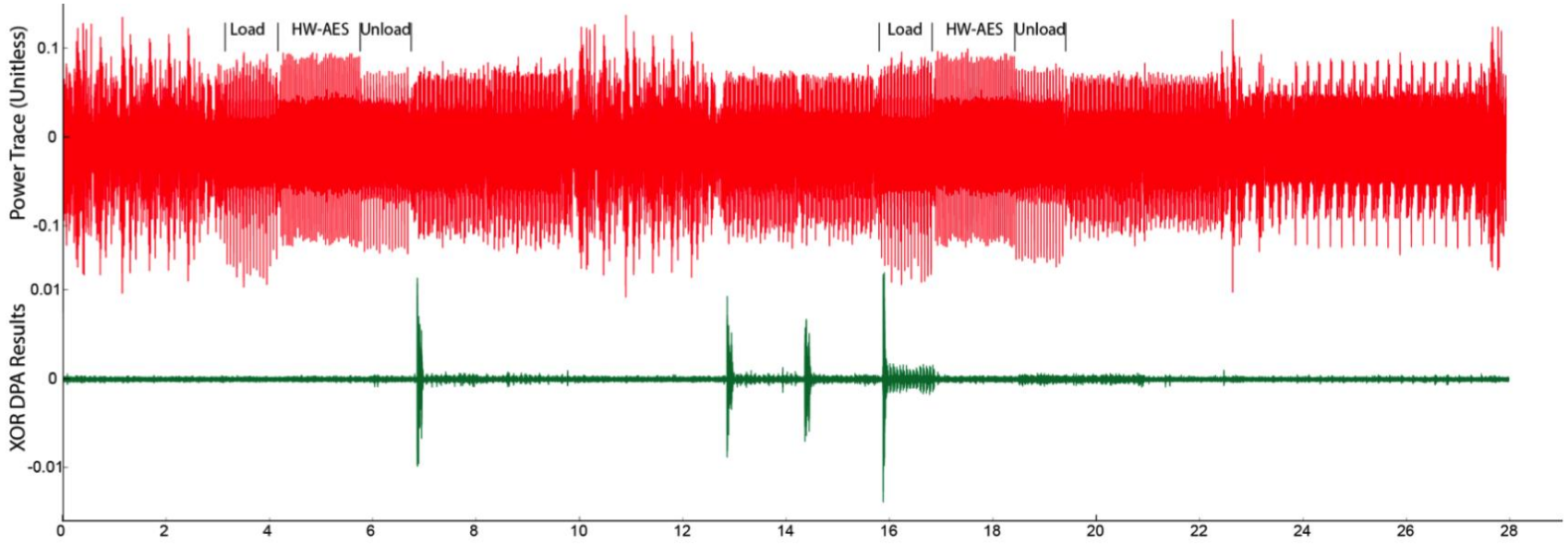
Attaque mixte (protocole & physique) en deux étapes :

- Exploitation d'une faille protocolaire :
  - Défaut du test de proximité lors du « Factory New Reset Request »
    → Possibilité de mise à jour OtA à 50-70m

- Attaque physique par observation du chiffrement AES

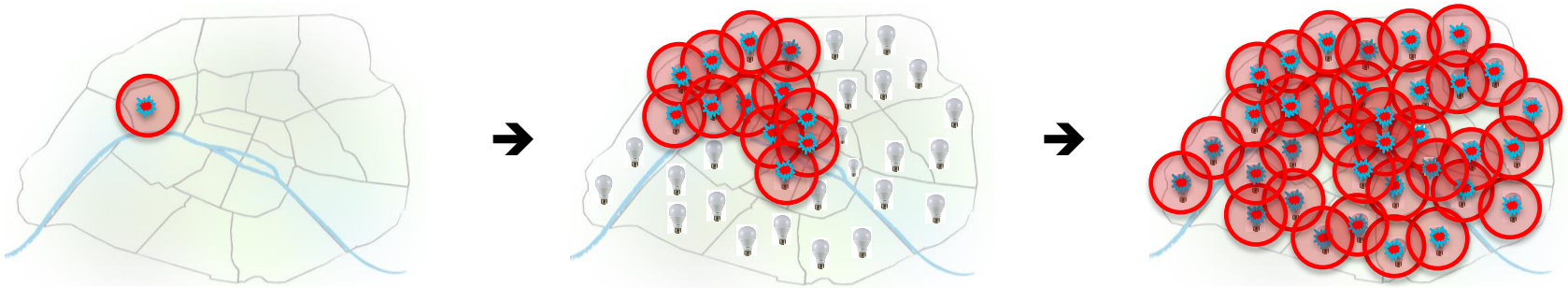
Attaque physique par observation :
Ecoute de l'activité électrique pendant le chiffrement

- Fuite d'informations et traitement statistique



Attaque physique par observation :
Ecoute de l'activité électrique pendant le chiffrement

- Fuite d'informations et traitement statistique
- Obtention de la clé secrète
  - → Clé **commune** à toutes les lampes !!!
  - → Création du **Firmware corrompu** pour la prise de contrôle
  - → Propagation aux autres lampes à proximité



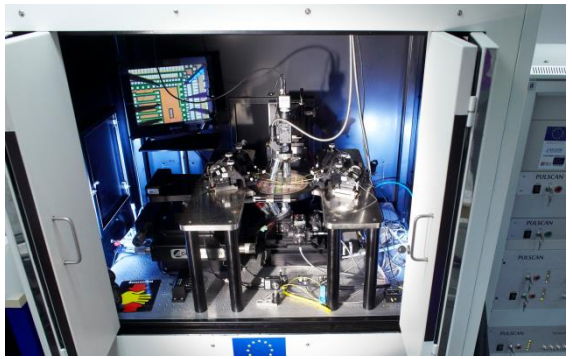
CHAPITRE 3
QUE FAIRE ?

Institut Mines-Télécom

Département SAS – Mines Saint-Etienne

« Systèmes et Architectures Sécurisées »

- Evaluation des menaces et réalisation d'attaques physiques
  - Banc d'écoute EM
  - Banc d'injection EM et Laser



- Modélisation d'attaques
- Conception de circuits sécurisés (ST 65nm…)
  - Contre-mesures logicielles / matérielles
  - Capteurs d'intrusion