Cybersécurité des objets connectés

Risques, bonnes pratiques et opportunités

Vincent Strubel

Agence Nationale de la Sécurité des Systèmes d'Information

17 juin 2015

Agence dépendant du Premier Ministre, avec une double mission

- Prévention des cyberattaques
  - Référentiels et guides
  - Politique industrielle et labellisation
  - Assistance technique
- Réaction aux cyberattaques
  - Détection et analyse
  - Remédiation

Contexte : menaces "cyber" multiples

- "Cyber-racket" et fraude *(particuliers, entreprises)*
  - *Cryptolocker*, menaces d'attaque
- Déstabilisation *(institutions, entreprises)*
  - Défigurations, dénis de service, *Sony*, *TV5Monde*
- Espionnage *(entreprises, administrations)*
  - Une réalité quotidienne
- Sabotage *(infrastructures critiques)*
  - Peu de cas concrets, des scénarios réalistes

Un enjeu majeur de souveraineté et de développement économique

Cybersécurité et objets connectés

Des cibles de haute valeur (1/2)

Des cibles de choix pour la captation de données

Des cibles de haute valeur (1/2)

Des cibles de choix pour la captation de données

- Manipulation de données sensibles à haute valeur
  - Données personnelles et de santé
  - Moyens de paiement et identité numérique
  - Stockées localement ou transmises vers le cloud

Des cibles de haute valeur (1/2)

Des cibles de choix pour la captation de données

- Manipulation de données sensibles à haute valeur
  - Données personnelles et de santé
  - Moyens de paiement et identité numérique
  - Stockées localement ou transmises vers le cloud
- Capteurs intégrés détournables de leur usage
  - Caméra, micro, etc. + accès réseau

Des cibles de haute valeur (2/2)

Des conséquences potentiellement dramatiques en cas de sabotage

Des cibles de haute valeur (2/2)

Des conséquences potentiellement dramatiques en cas de sabotage

- Impact potentiel sur la vie humaine
  - Objets connectés à usage médical : *pacemaker*, etc.
  - Moyens de transport, voiture connectée

Des cibles de haute valeur (2/2)

Des conséquences potentiellement dramatiques en cas de sabotage

- Impact potentiel sur la vie humaine
  - Objets connectés à usage médical : *pacemaker*, etc.
  - Moyens de transport, voiture connectée
- Usage croissant dans les infrastructures critiques
  - Comme capteurs voire comme actionneurs
  - Mais également pour assurer la sécurité physique : serrures, caméras, etc.

Problèmes de sécurité (1/3)

Des objets peu supervisés

- Pas ou peu de mises à jour de sécurité
- Peu de moyens de supervision / détection des attaques
- Objets peu surveillés ou perdables : accès physique de l'attaquant
  - Vol de données sensibles
  - Risques d'attaques physiques : piégeage, etc.

Problèmes de sécurité (2/3)

Des environnements contraints

- Peu de ressources à consacrer à la sécurité
  - Recours limité à la cryptographie
  - Environnements d'exécution peu sécurisés
- Peu de ressources dans l'absolu
  - Traitement complexes dans le Cloud
  - Transmission de données sensibles

Problèmes de sécurité (3/3)

Des objets hétérogènes

- Hétérogénéité des architectures
  - Matériel, logiciel
  - Pas de plateforme unifiée (même Android)
- Hétérogénéité des protocoles
  - Protocoles radio multiples et complexes
  - Cryptographie "artisanale"

Il est quasi-impossible d'avoir une vue d'ensemble

Principaux risques de sécurité

- Attaques destructives ou revendicatives
  - Potentiellement à grande échelle (ex. : *Shodan*)
  - Potentiellement ciblées : destabilisation d'un concurrent

Principaux risques de sécurité

- Attaques destructives ou revendicatives
  - Potentiellement à grande échelle (ex. : *Shodan*)
  - Potentiellement ciblées : destabilisation d'un concurrent
- Espionnage
  - Captation de données personnelles
  - Espionnage de l'environnement (ex. : entreprise)
  - Porosité entre les environnements "pro" et "perso"

Principaux risques de sécurité

- Attaques destructives ou revendicatives
  - Potentiellement à grande échelle (ex. : *Shodan*)
  - Potentiellement ciblées : destabilisation d'un concurrent
- Espionnage
  - Captation de données personnelles
  - Espionnage de l'environnement (ex. : entreprise)
  - Porosité entre les environnements "pro" et "perso"
- Sabotage
  - Villes intelligentes, transports, énergie, santé, etc.

Principaux risques de sécurité

- Attaques destructives ou revendicatives
  - Potentiellement à grande échelle (ex. : *Shodan*)
  - Potentiellement ciblées : destabilisation d'un concurrent
- Espionnage
  - Captation de données personnelles
  - Espionnage de l'environnement (ex. : entreprise)
  - Porosité entre les environnements "pro" et "perso"
- Sabotage
  - Villes intelligentes, transports, énergie, santé, etc.
- Détournement pour mener d'autres attaques
  - *Botnets* : DDoS, Spam ou *Command & Control*

Bonnes pratiques et axes de recherche

Prise en compte globale de la sécurité

Au juste niveau...

Intégrer l'objectif de sécurité tout au long du projet

- Au même titre que la fiabilité
  - i.e. pas la veille de la commercialisation...
- Des réflexes simples mais systématiques
  - Valider les *inputs*
  - Tester les comportements anormaux
  - Vérifier la qualité du code
- Sensibiliser, former et outiller les développeurs

On peut obtenir un bon niveau de sécurité
sans efforts démesurés

Points d'attention particuliers

Couvrir les principaux risques

- Mises à jour de sécurité
  - *Sécurisées*, c'est mieux
- Chiffrement et authentification des communications
  - Pas de clés partagées par tous les équipements
  - Protocoles standards et éprouvés
- Sécurité locale
  - Intégrité du code, confidentialité des données
  - Limiter et brider les interfaces locales

Des axes de recherche

- Primitives et protocoles cryptographiques
  - Cryptographie légère, cryptographie pour le cloud
- Sécurité logicielle
  - Outils de production ou de validation de code sécurisé
- Sécurité matérielle
  - Résistance aux attaques *side-channel* ou injection de faute
- Intégrité d'exécution
  - *Boot* sécurisé, *remote attestation*

Des axes de recherche

- Primitives et protocoles cryptographiques
  - Cryptographie légère, cryptographie pour le cloud
- Sécurité logicielle
  - Outils de production ou de validation de code sécurisé
- Sécurité matérielle
  - Résistance aux attaques *side-channel* ou injection de faute
- Intégrité d'exécution
  - *Boot* sécurisé, *remote attestation*

Autant de secteurs d'excellence en France

Opportunités

De bonnes raisons d'investir dans la cybersécurité

Protéger son *business*, mais aussi le développer

- Se protéger de risques significatifs
  - Impact commercial d'une vulnérabilité publicisée

De bonnes raisons d'investir dans la cybersécurité

Protéger son *business*, mais aussi le développer

- Se protéger de risques significatifs
  - Impact commercial d'une vulnérabilité publicisée
- Mais aussi rendre ses produits plus attractifs
  - Un vrai différentiateur dans certains domaines
  - Sensibilisation croissante des clients

De bonnes raisons d'investir dans la cybersécurité

Protéger son *business*, mais aussi le développer

- Se protéger de risques significatifs
  - Impact commercial d'une vulnérabilité publicisée
- Mais aussi rendre ses produits plus attractifs
  - Un vrai différentiateur dans certains domaines
  - Sensibilisation croissante des clients
- Et capitaliser sur des points forts nationaux
  - Cryptographie, composants sécurisés
  - Evaluation de la sécurité

Initiatives majeures en cybersécurité

Nouvelle France Industrielle

- Plan cybersécurité, piloté par l'ANSSI
  - Développer et valoriser l'industrie de la cybersécurité (produits et services)
- Mais aussi prise en compte dans les autres plans

Initiatives majeures en cybersécurité

Nouvelle France Industrielle

- Plan cybersécurité, piloté par l'ANSSI
  - Développer et valoriser l'industrie de la cybersécurité (produits et services)
- Mais aussi prise en compte dans les autres plans

Loi de Programmation Militaire

- Sécurisation des systèmes d'information critiques
- Obligations légales des OIV : prévention, détection, notification
- Effet structurant sur le marché

Un cadre favorable

Investissements d'avenir

- Accélérateur de R&D industrielle
- Appels à projets cybersécurité et domaines connexes : Cloud, IoT, données personnelles, etc.

Un cadre favorable

Investissements d'avenir

- Accélérateur de R&D industrielle
- Appels à projets cybersécurité et domaines connexes : Cloud, IoT, données personnelles, etc.

Schémas de labellisation

- Evaluations de sécurité, label *France Cybersecurity*
- Un bon moyen de valoriser la sécurité d'un produit

Le rôle de l'ANSSI

Aider les développeur à sécuriser leur produits

- Guides et recommandations : `http://www.ssi.gouv.fr`
- Echanges techniques et collaborations de recherche
- Orientation de la R&D
- Evaluation et labellisation de sécurité

Le rôle de l'ANSSI

Aider les développeur à sécuriser leur produits

- Guides et recommandations : `http://www.ssi.gouv.fr`
- Echanges techniques et collaborations de recherche
- Orientation de la R&D
- Evaluation et labellisation de sécurité

Mais aussi les aider à vendre leurs produits sécurisés

- Référencement de produits labellisés
- Intégration dans les recommandations
- Sensibilisation des utilisateurs

Conclusion

- Des risques significatifs
  - Pour les éditeurs comme pour les utilisateurs
  - Souvent insuffisamment pris en compte
- Mais aussi de réelles opportunités de développement
  - La cybersécurité devient un vrai différentiateur sur le marché
  - Forte mobilisation des acteurs publics et privés
- Et des manques à combler par des travaux de recherche
  - Verrous technologiques à lever
  - Mais aussi transferts à effectuer vers l'industrie

Merci