Enjeux, évolution et conséquences de la sécurité dans monde mobile

Guillaume Bouffard <guillaume.bouffard@ssi.gouv.fr>

Agence nationale de la sécurité des systèmes d'information

Workshop SERTIF - 11 Octobre 2016

ANSSI ? Késako ?

- ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) dépend 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

Agenda

- Introduire la notion de racine de confiance :
  - Qu'est ce que c'est ?
  - Comment garantir un niveau de sécurité ?.
  - Présentation rapide d'un élément sécurisée : la carte à puce.

Agenda

- Introduire la notion de racine de confiance :
  - Qu'est ce que c'est ?
  - Comment garantir un niveau de sécurité ?.
  - Présentation rapide d'un élément sécurisée : la carte à puce.
- Présentation de la sécurité des ordiphones et des objets intelligents :
  - Les objets intelligents sont partout,
  - Peut-on garantir un niveau de sécurité comme pour une carte à puce ?

1. Introduction

La Racine de Confiance

Pourquoi les racines de confiance sont elles nécessaires ?

- Plusieurs fonctionnalités ont besoin d'un environnement de confiance où il est possible :
  - de stocker des données sensibles :
    - en protégeant la confidentialité/intégrité des données ;
  - exécuter des opérations sensibles (cryptographie) :
    - sans aucune fuite.

Pourquoi les racines de confiance sont elles nécessaires ? (cont.)

- La racine de confiance est un environnement d'exécution sécurisé.
- **Traditionnellement** c'est un composant sécurisé.

Pourquoi les racines de confiance sont elles nécessaires ? (cont.)

- On voit apparaître des implémentations logicielles de composant sécurisé :
  - Émulation de composant sécurisé matériel :
    - remplacement de TPMs physiques par des enclaves sécurisées, (type ARM TrustZone)
    - **ce n'est pas un composant sécurisé**.
  - whitebox cryptographique :
    - c'est **fondamentalement** moins sécurisé,
    - cette tendance est de plus en plus importante,
    - comment garantir le niveau de sécurité de ces implémentations ?
    - comment et sous quelles conditions mener ces évaluations ?

1. Introduction

Évaluation d’un composant sécurisé

Comment garantir le niveau de sécurité ?

- Les développeurs spécifient les recommandations de sécurité.
- Les vendeurs implémentent les recommandations de sécurité dans leurs produits.
- Les CESTIs évaluent le niveau de sécurité des produits.
- Le centre de certification certifie les produits en vérifiant chaque étapes du processus d'évaluation.

Quel schéma ?

- Critère Commun pour l'évaluation Sécuritaire des Technologie de l'information, (Abrégé comme Critère Commun ou CC)
- Standard international (ISO/IEC 15408) pour la certification des produits de sécurité.

Niveau d'évaluation

- Plusieurs classes de certification existent :

Level	Description
EAL 1	Testé fonctionnellement
EAL 2	Testé structurellement
EAL 3	Testé et vérifié méthodiquement
EAL 4	Méthodiquement conçu, testé et le code est relu
EAL 5	Semi-formellement conçu et testé
EAL 6	Semi-formellement conçu, vérifié et testé
EAL 7	Semi-formellement conçu, vérifié et testé

- À chacune de ces classes, un niveau exigence d'évaluation est défini et peut être *augmenté* :
  - Par exemple : une carte à puce peut-être évaluée :
    `EAL4 + ALC_DVS.2 + AVA_VAN.5`

Reconnaissance Mutuelle

- SOG-IS (*Senior Official Group Info. Systems Security*) :
  - Accord européen de reconnaissance (10 membres),
  - Audits périodiques entre centres de certification (procédures and compétences techniques).

Reconnaissance Mutuelle

- SOG-IS (*Senior Official Group Info. Systems Security*) :
  - Accord européen de reconnaissance (10 membres),
  - Audits périodiques entre centres de certification (procédures and compétences techniques).
- CCRA (*Common Criteria Recognition Arrangement*) :
  - Reconnaissance internationale (27 membres),
  - Audits périodiques entre chaque centre de certification (seulement la procédure),
  - Limitation sur le niveau maximum de reconnaissance :
    - `AVA_VAN` $\Rightarrow$ `AVA_VAN.2` maximum

D'autre schémas ?

- Schéma EMVCo

- Schéma Global Platform (Java Card, TEE)

D'autre schémas ?

- Schéma EMVCo
  - Spécifications pour l'intéropérabilité dans les transactions bancaires,
  - schéma certification privé,
  - échanges réguliers avec les groupes de travail du SOG-IS.
- Schéma Global Platform (Java Card, TEE)

D'autre schémas ?

- Schéma EMVCo
  - Spécifications pour l'intéropérabilité dans les transactions bancaires,
  - schéma certification privé,
  - échanges réguliers avec les groupes de travail du SOG-IS.
- Schéma Global Platform (Java Card, TEE)
  - Spécifications du cycle de vie et des communications vers la plate-forme Java Card et, récemment pour les TEE (Trusted Execution Environment),
  - Nouveau schéma de certification privée pour les TEE,
  - Échanges réguliers avec le SOG-IS
    Le profil de protection (PP) pour le TEE a été élaboré par l'ANSSI.

1. Introduction

La carte à puce : un système évalué

La carte à puce

- La carte à puce est le plus répandu des composants de confiance.

La carte à puce

- La carte à puce est le plus répandu des composants de confiance.
- Utilisée dans :
  - le monde bancaire,
  - la TV à péage,
  - l'identité,
  - la santé,
  - votre téléphone,
  - ...

La carte à puce : une racine de confiance

- La carte à puce est un système sécurisé avec :
  - juste quelques protocoles d'entrée/sortie :
    - ISO/IEC 7816,
    - ISO/IEC 14443.
  - protection contre les attaques physiques,
  - durcissement du code logiciel.

2. L’ordiphone

L'ordiphone : le réveil de la force

(Martin Cooper avec le premier téléphone mobile.)

La sécurité des ordiphones

- La sécurité des ordiphones est un problème difficile avec de nombreux chemins d'attaque.

La sécurité des ordiphones

- La sécurité des ordiphones est un problème difficile avec de nombreux chemins d'attaque.
- Quelques fonctions de sécurité :
  - Chiffrement des données
  - Protection de l'intégrité du code (et des données)
  - Cloisonnement applicatif et contrôle d'accès
  - ...

La sécurité des ordiphones

- La sécurité des ordiphones est un problème difficile avec de nombreux chemins d'attaque.
- Quelques fonctions de sécurité :
  - Chiffrement des données
  - Protection de l'intégrité du code (et des données)
  - Cloisonnement applicatif et contrôle d'accès
  - ...
- Quelques chemins d'attaques :
  - Corruption de la phase de démarrage et/ou du matériel,
  - Installation d'applications malveillantes,
  - Corruption des échanges extérieurs. (les mises à jour peuvent être corrompues.)

Quelques contre-mesures implémentées

- Fonctionnalités de sécurités présentes :
  - Phase de démarrage sécurisée,
  - Chiffrement des partitions,
  - Exécution sécurisée d'applications :
    - Contrer les attaques d'applications malveillantes.
    - L'utilisateur peut installer uniquement les applications mises à disposition dans une boutique et validées. (sauf dans les appareils de développement)

Quelques contre-mesures implémentées

- Fonctionnalités de sécurités présentes :
  - Phase de démarrage sécurisée,
  - Chiffrement des partitions,
  - Exécution sécurisée d'applications :
    - Contrer les attaques d'applications malveillantes.
    - L'utilisateur peut installer uniquement les applications mises à disposition dans une boutique et validées. (sauf dans les appareils de développement)
- Ces contre-mesures sont implémentées entre le monde logiciel et le monde matériel.

Quelques contre-mesures implémentées

- Fonctionnalités de sécurités présentes :
  - Phase de démarrage sécurisée,
  - Chiffrement des partitions,
  - Exécution sécurisée d'applications :
    - Contrer les attaques d'applications malveillantes.
    - L'utilisateur peut installer uniquement les applications mises à disposition dans une boutique et validées. (sauf dans les appareils de développement)
- Ces contre-mesures sont implémentées entre le monde logiciel et le monde matériel.
- Apple maîtrise complètement les composants embarqués dans ses ordiphones.

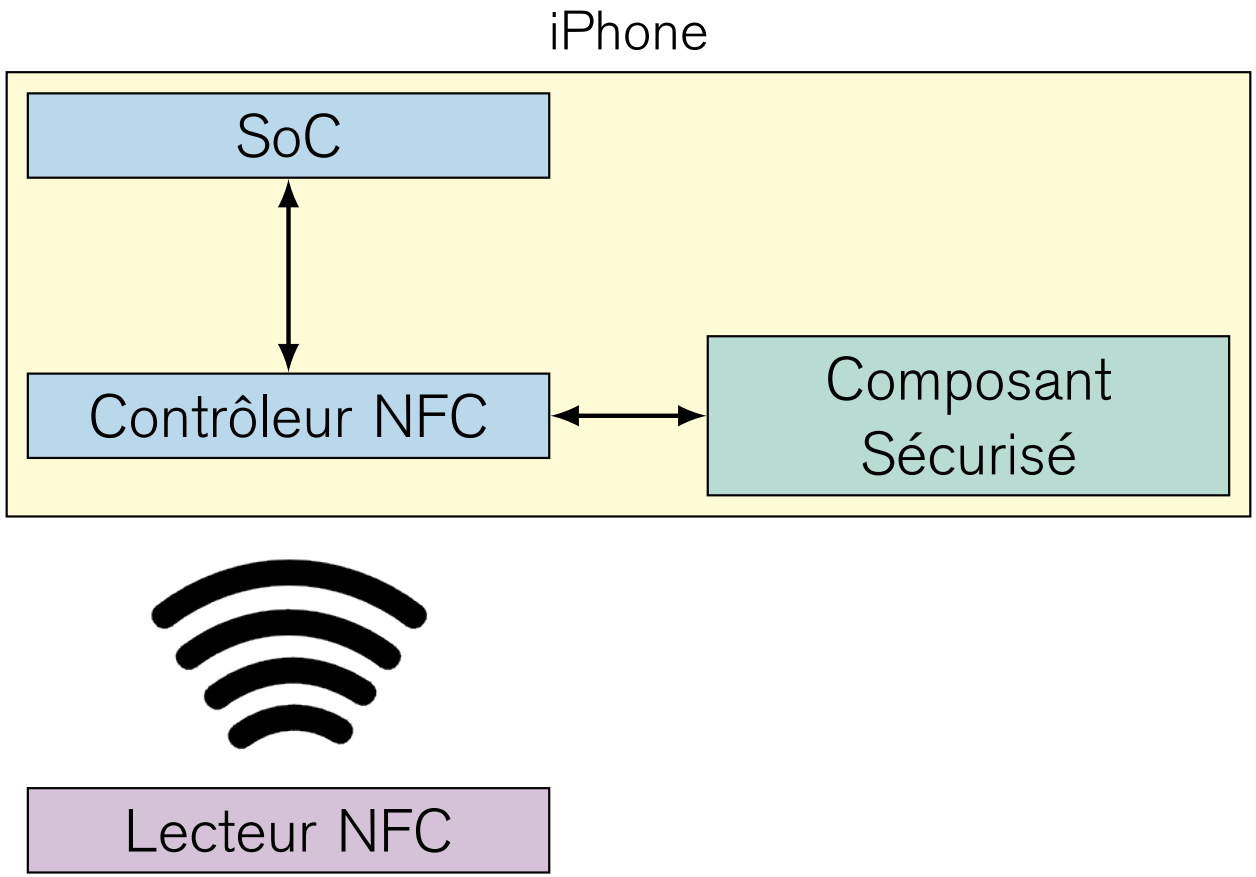
« Un grand pouvoir implique de grandes responsabilité »

- Un composant sécurisé est utilisé pour des fonctionnalités sensibles :
  - ce composant sécurisé doit être évalué,
  - la plupart ont le même niveau d'évaluation qu'une carte à puce,
    - pour payer, le composant doit respecter le schéma d'évaluation EMVCo.
- Pour les opérations nécessitant plus de ressources :
  - les opérations doivent être faites sur un SoC (Système sur une puce),
  - Les SoCs récents ont un Environnement d'Exécution Sécurisé.
    (comme *ARM TrustZone*)

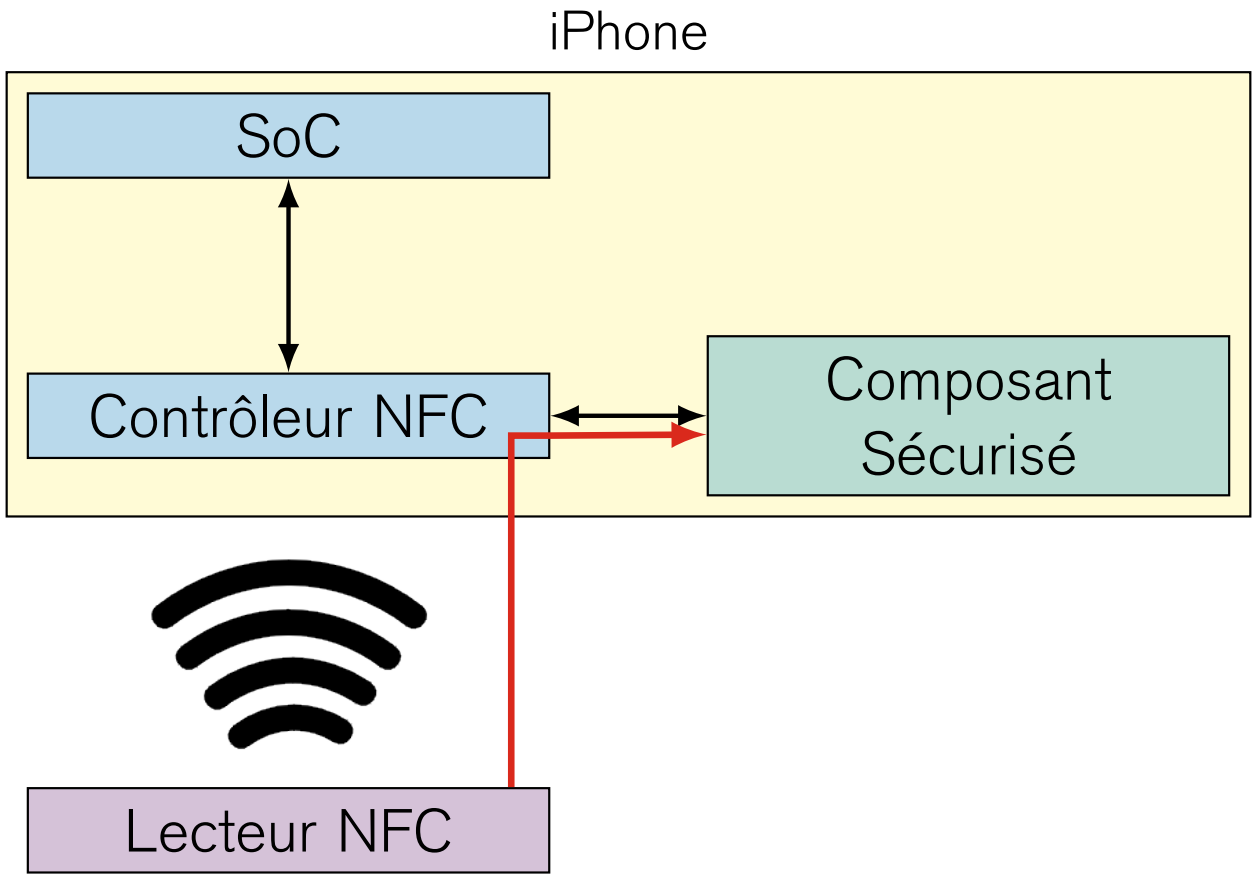
2. L’ordiphone

Utilisation des composants sécurisés dans les ordiphones

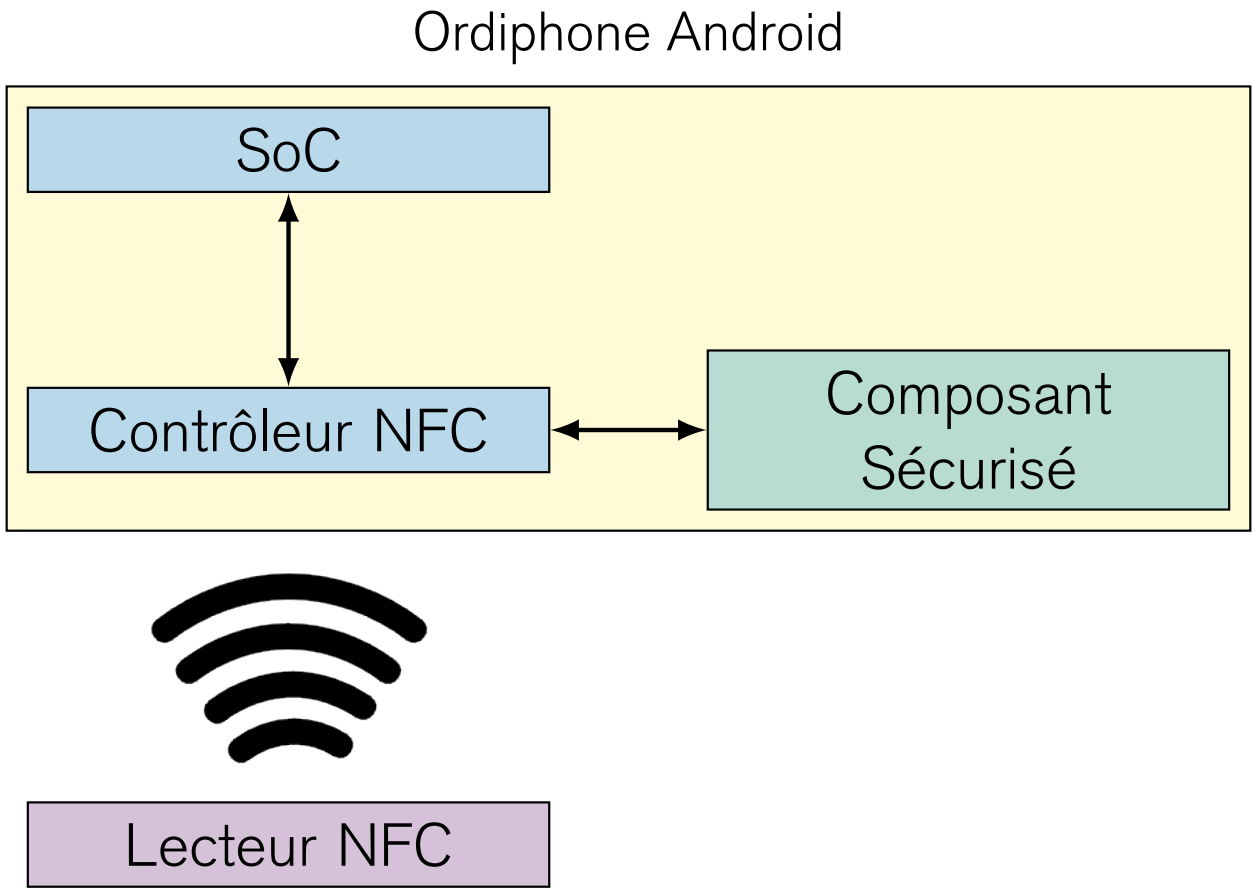
Utilisation du composant sécurisé pour Apple Pay



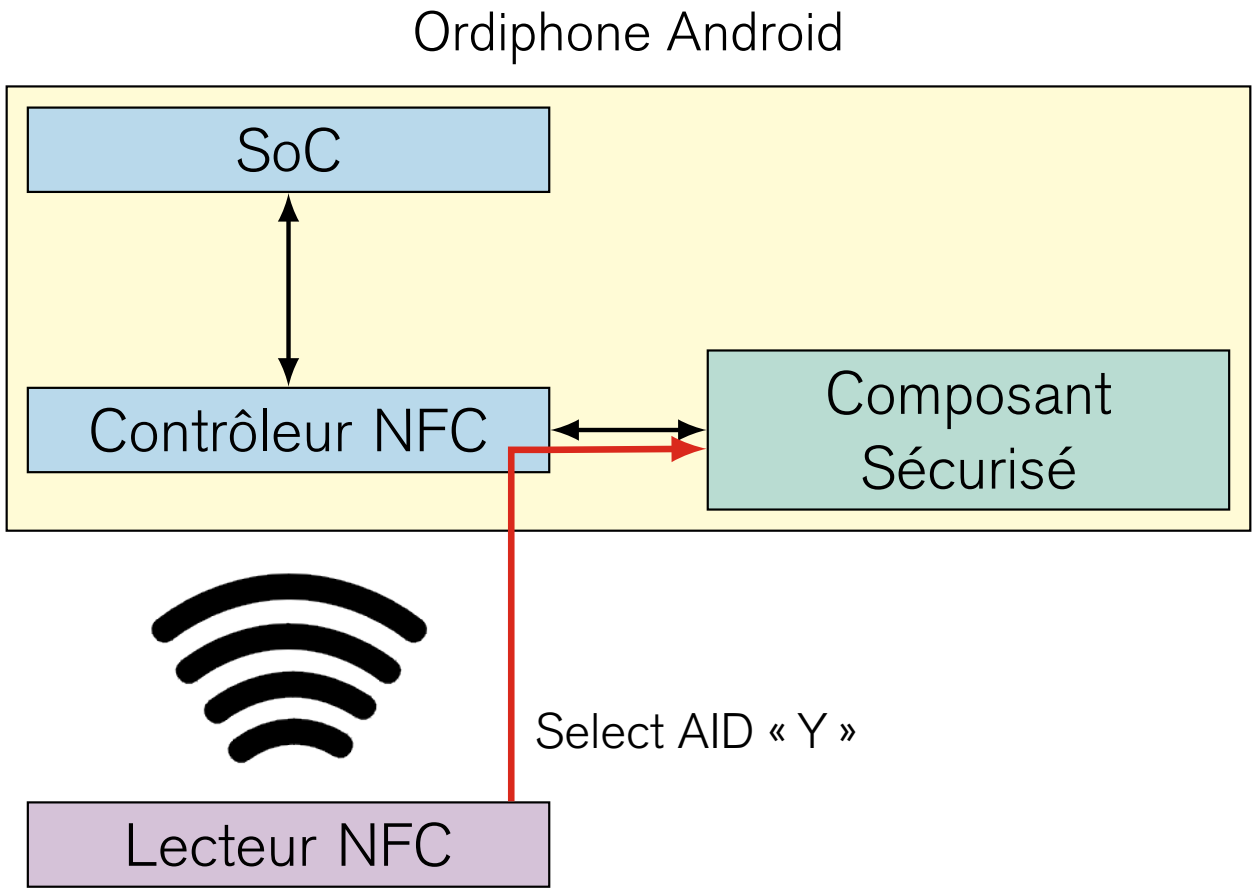
Utilisation du composant sécurisé pour Apple Pay



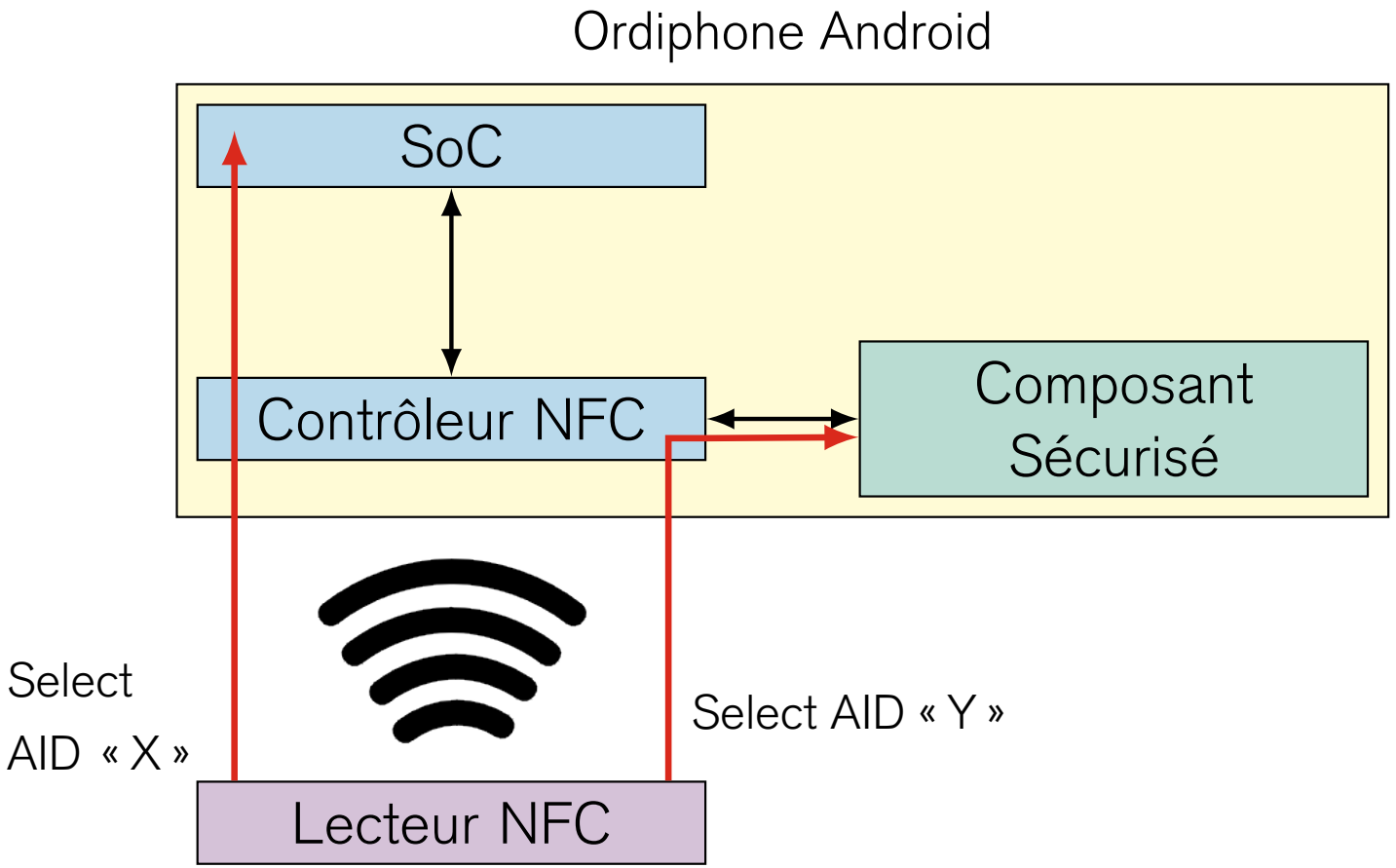
Utilisation du composant sécurisé pour Google Pay



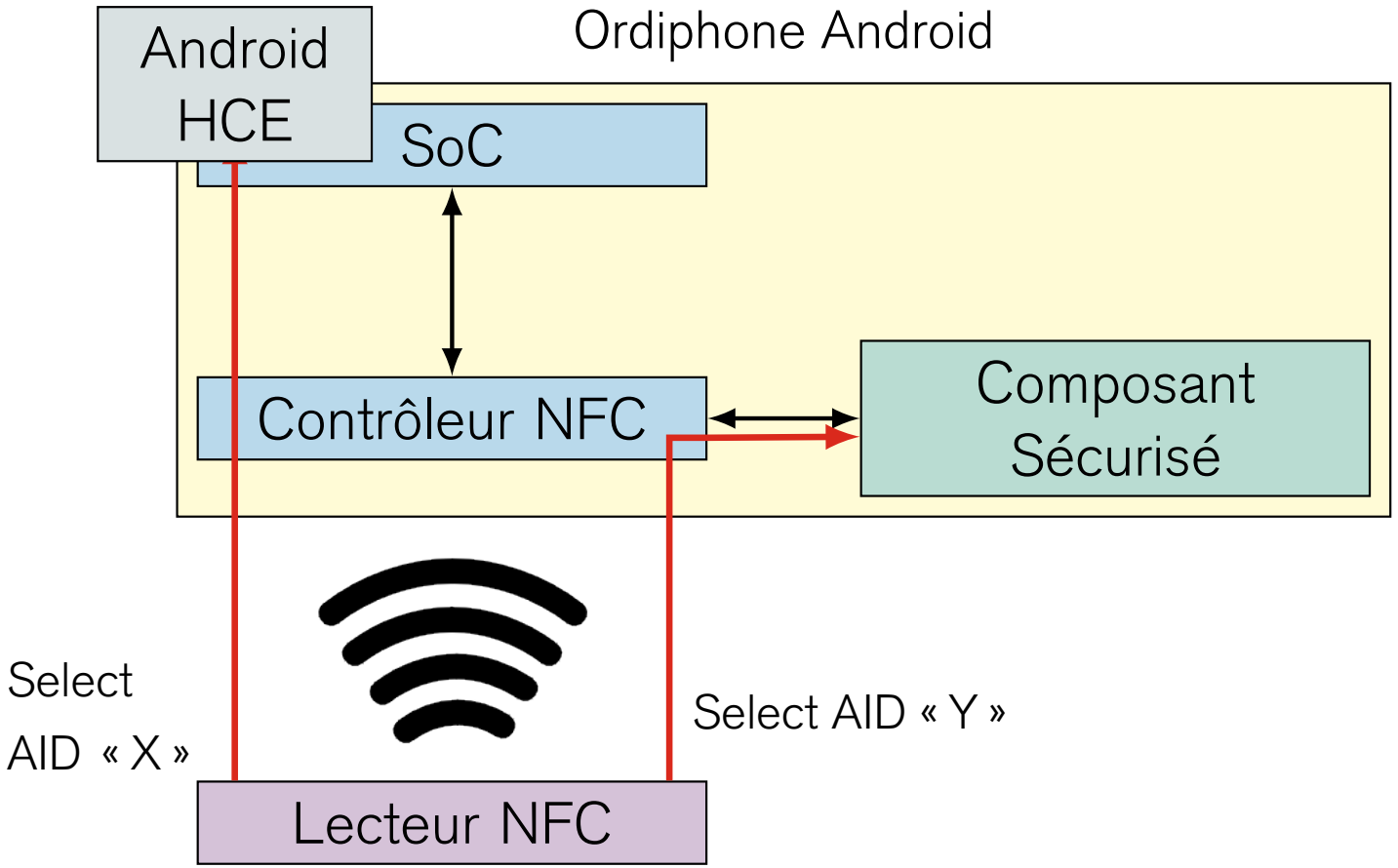
Utilisation du composant sécurisé pour Google Pay



Utilisation du composant sécurisé pour Google Pay



Utilisation du composant sécurisé pour Google Pay



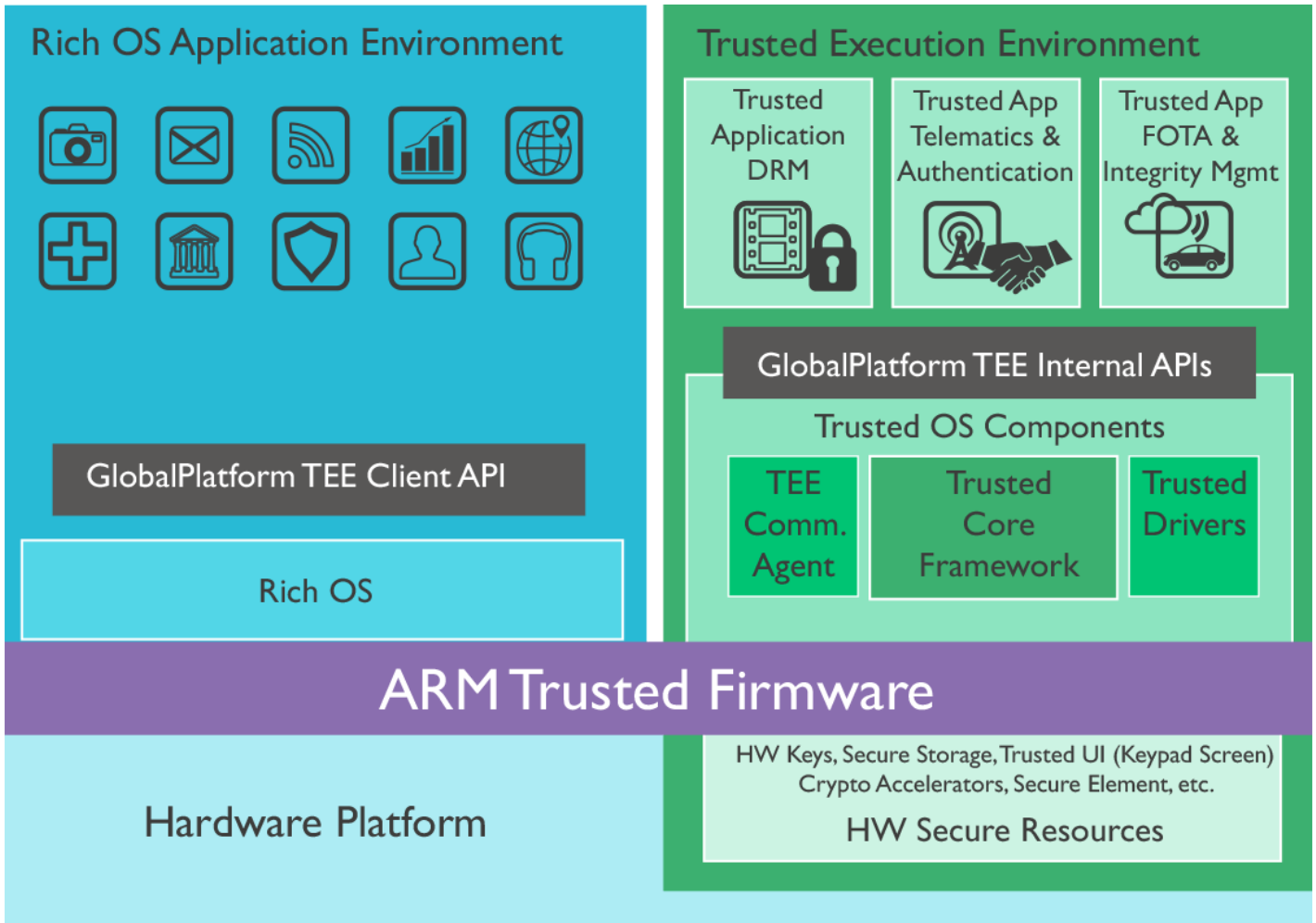
2. L’ordiphone

Sécurité des SoCs

Fonctionnalités des SoCs

- Les SoCs sont des micro-processeurs complexes,
- Majoritairement basés sur des ARM 32/64-bits,
- Les SoCs haut de gamme ont :
  - au moins 4-cœurs,
  - au moins 4 Go de RAM,
  - Wi-Fi,
  - 3G/LTE,
  - Bluetooth,
  - GPS,
  - NFC,
  - support de USB,
  - support des caméras,
  - GPU,
  - support des extensions mémoires (type SD, eMMC, etc.).

Architecture ARM TrustZone



(Source : `https://developer.arm.com/technologies/trustzone`)

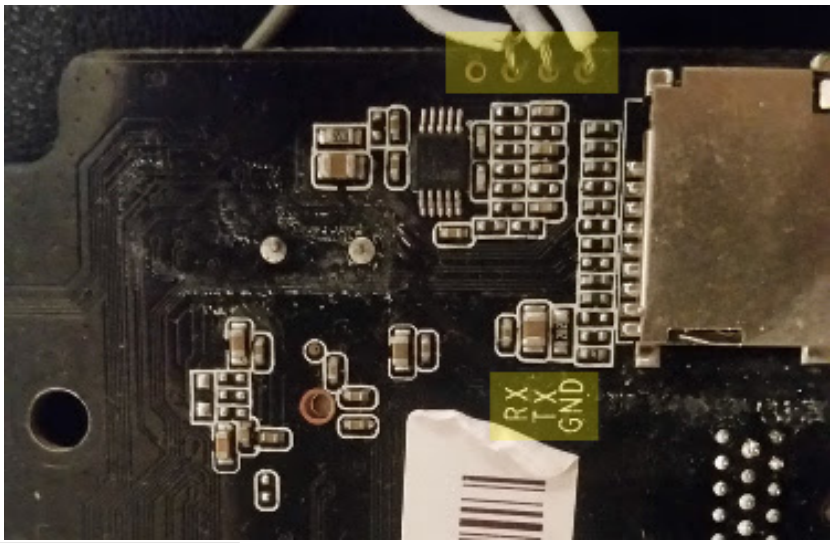
Exemple d'attaque sur ARM TrustZone

- Étude de cas : démarrage sécurisé d'un boîtier Android multimédia vidéo [1].
- Le SoC contient un mécanisme de démarrage sécurisé afin de vérifier l'image de l'OS avant de la charger en TrustZone.
- Partie TrustZone non documentée.

1. `http://www.fredericb.info/2016/10/amlogic-s905-soc-bypassing-not-so.html`

Exemple d'attaque sur ARM TrustZone

- Étude de cas : démarrage sécurisé d'un boîtier Android multimédia vidéo [1].
- Le SoC contient un mécanisme de démarrage sécurisé afin de vérifier l'image de l'OS avant de la charger en TrustZone.
- Partie TrustZone non documentée.
- Accès *root* disponible (côté non sécurisé) via une connexion UART.



1. `http://www.fredericb.info/2016/10/amlogic-s905-soc-bypassing-not-so.html`

Exemple d'attaque sur ARM TrustZone (cont.)

- Impossible de lire la *BootROM* depuis le monde non sécurisé.
  (fonctionnement attendu)

Exemple d'attaque sur ARM TrustZone (cont.)

- Impossible de lire la *BootROM* depuis le monde non sécurisé.
  (fonctionnement attendu)
- La chaîne de démarrage sécurisé ne permet pas de charger du code non autorisé.

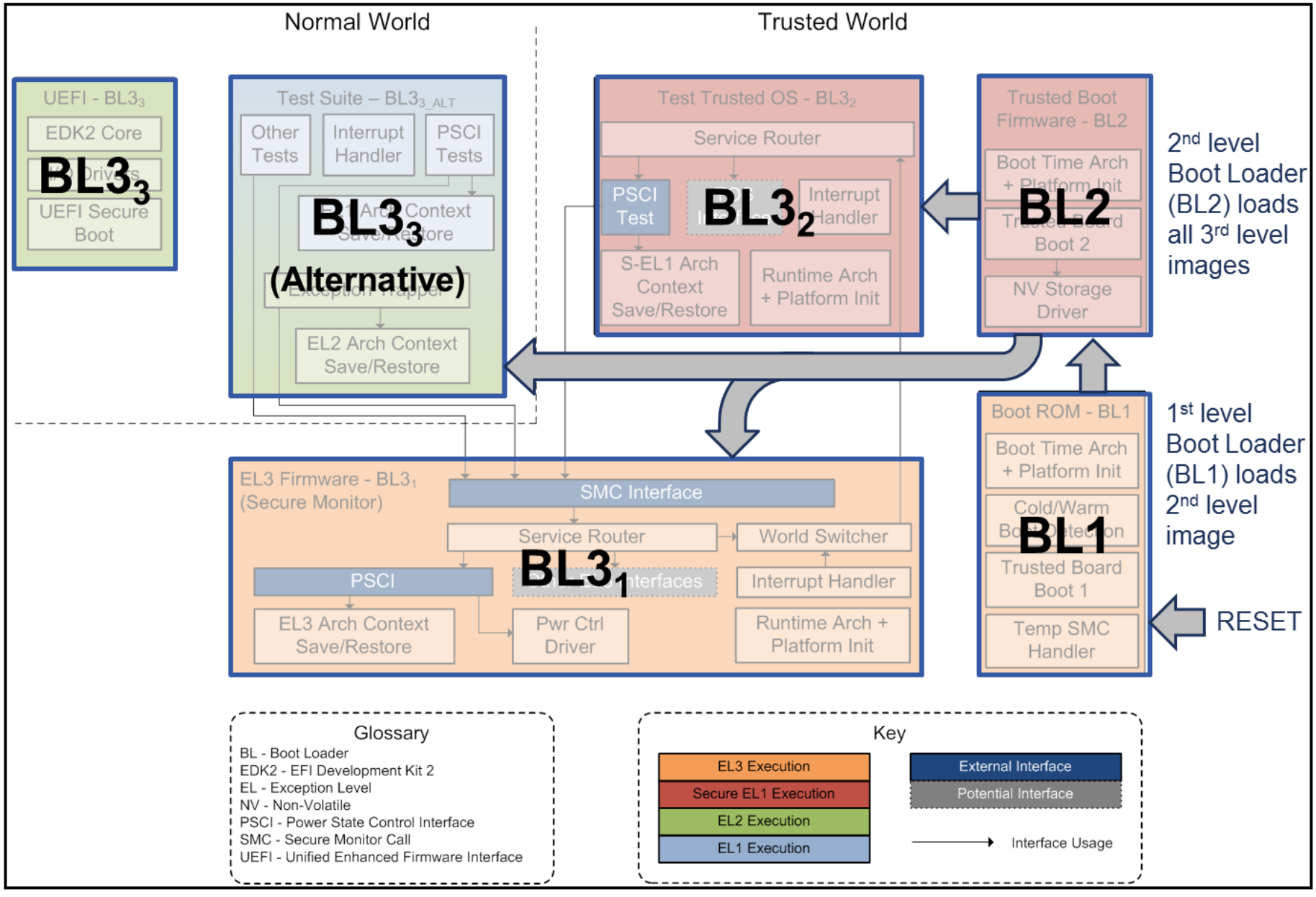


FIGURE – ARM Trusted Firmware Design.

Exemple d'attaque sur ARM TrustZone (cont.)

- À partir de là, deux chemins d'attaque ont été découverts.
- Grâce à la liaison UART, il est possible d'envoyer des commandes U-Boot.

1. La communication entre le Monde Non Sécurisé et le Monde Sécurisé se fait via des instructions SMC (Secure Monitor Call).
   - Corruption non trivial du plan mémoire via une interruption SMC.
   - Lecture du code binaire du BL2
2. Corruption de la phase de chargement du niveau 2.
   - Seulement l'intégrité de le BL3 est vérifié, pas d'authentification.
   - Chargement d'un BL3 corrompu.

Exemple d'attaque sur ARM TrustZone (cont.)

- À partir de là, deux chemins d'attaque ont été découverts.
- Grâce à la liaison UART, il est possible d'envoyer des commandes U-Boot.

1. La communication entre le Monde Non Sécurisé et le Monde Sécurisé se fait via des instructions SMC (Secure Monitor Call).
   - Corruption non trivial du plan mémoire via une interruption SMC.
   - Lecture du code binaire du BL2
2. Corruption de la phase de chargement du niveau 2.
   - Seulement l'intégrité de le BL3 est vérifié, pas d'authentification.
   - Chargement d'un BL3 corrompu.
   - **Bingo !**

Exemple d'attaque sur ARM TrustZone (cont.)

- À partir de là, deux chemins d'attaque ont été découverts.
- Grâce à la liaison UART, il est possible d'envoyer des commandes U-Boot.
  1. La communication entre le Monde Non Sécurisé et le Monde Sécurisé se fait via des instructions SMC (Secure Monitor Call).
     - Corruption non trivial du plan mémoire via une interruption SMC.
     - Lecture du code binaire du BL2
  2. Corruption de la phase de chargement du niveau 2.
     - Seulement l'intégrité de le BL3 est vérifié, pas d'authentification.
     - Chargement d'un BL3 corrompu.
     - **Bingo !**
- Attaque purement logicielle.

Enclave Sécurisée d'Apple

- Introduit avec iPhone 5S et iOS 7 en 2013.
- coprocesseur intégré au processeur A7 ou supérieur.
  - Mémoire chiffrée.
  - générateur de nombres aléatoires matériel.
  - Système d'exploitation durci.
  - Identifiant matériel unique inconnu d'Apple.
  - Opérations de chiffrement et déchiffrement en boite noire.
  - Les clés ne peuvent pas être lues hors de l'enclave sécurisée.
  - Communications entre l'enclave sécurisée et le processeur applicatif via une « boite aux lettres ».
- Protège les données d'authentification et les clés de déchiffrement des partitions.

Peut-on attaquer physiquement un SoC ?

- Un SoC n'est pas un composant sécurisé contre les attaques physiques,
  - Actuellement, un système d'exploitation TrustZone est évalué via le schéma CC en France (EAL2 + ALC_DVS.2 + AVA_VAN.5),
  - ANSSI a fourni un profil de protection à propos de l'évaluation des TEE.

Peut-on attaquer physiquement un SoC ?

- Un SoC n'est pas un composant sécurisé contre les attaques physiques,
  - Actuellement, un système d'exploitation TrustZone est évalué via le schéma CC en France (EAL2 + ALC_DVS.2 + AVA_VAN.5),
  - ANSSI a fourni un profil de protection à propos de l'évaluation des TEE.
- *Théoriquement*, un SoC peut être perturbé par une attaque par injection de faute,

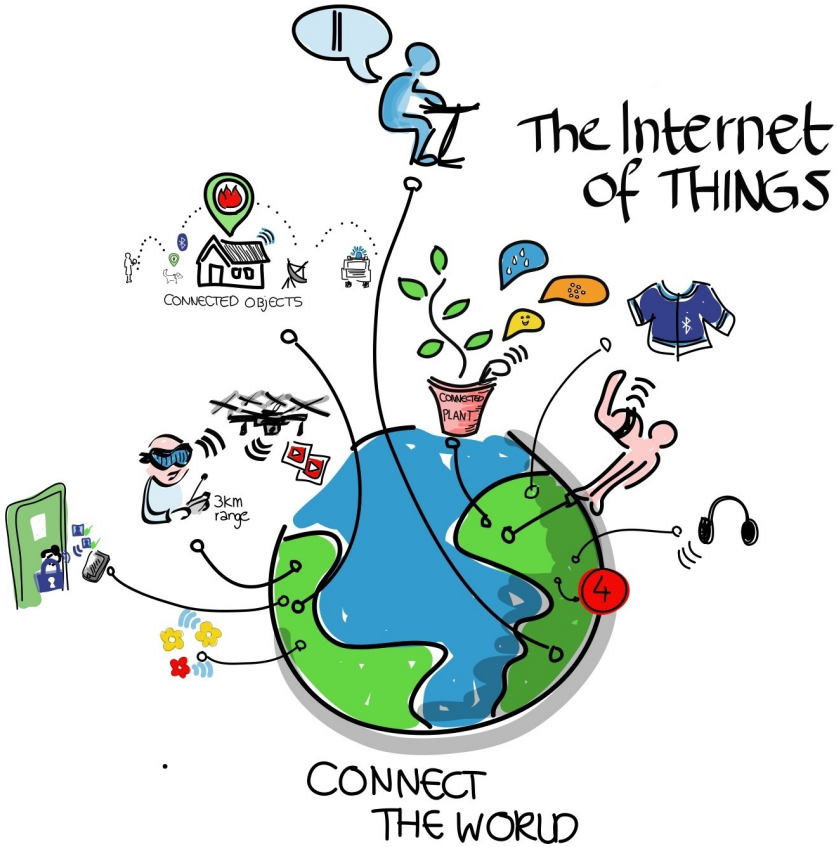
Peut-on attaquer physiquement un SoC ?

- Un SoC n'est pas un composant sécurisé contre les attaques physiques,
  - Actuellement, un système d'exploitation TrustZone est évalué via le schéma CC en France (EAL2 + ALC_DVS.2 + AVA_VAN.5),
  - ANSSI a fourni un profil de protection à propos de l'évaluation des TEE.
- *Théoriquement*, un SoC peut être perturbé par une attaque par injection de faute,
- **Mais**, un SoC est :
  - un processeur multitâche,
  - avec une CPU haute fréquence.

Peut-on attaquer physiquement un SoC ?

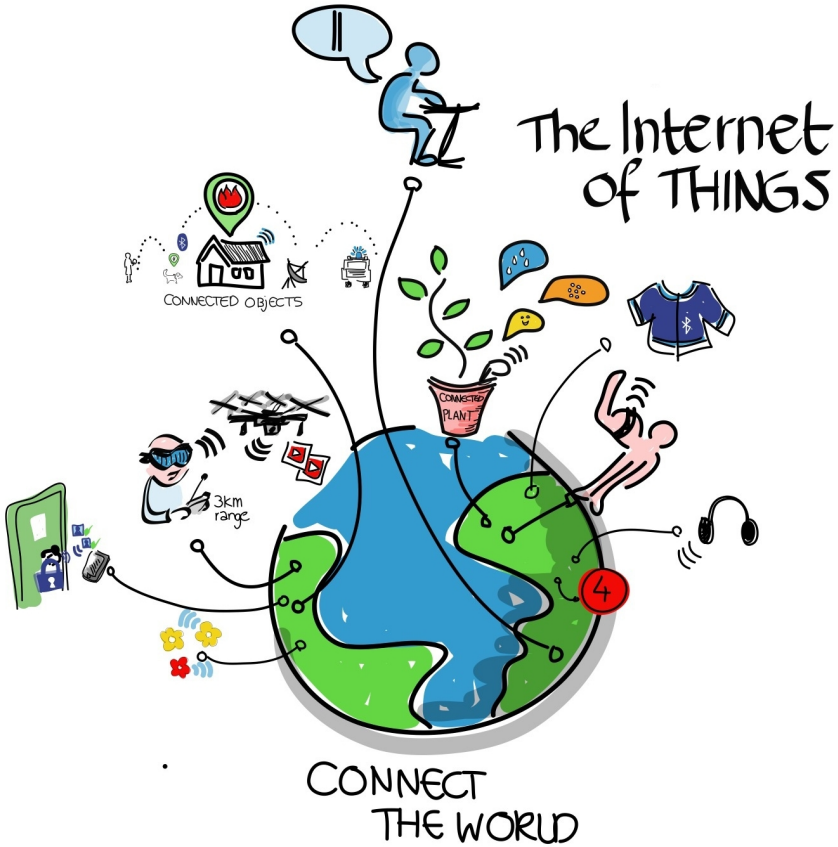
- Un SoC n'est pas un composant sécurisé contre les attaques physiques,
  - Actuellement, un système d'exploitation TrustZone est évalué via le schéma CC en France (EAL2 + ALC_DVS.2 + AVA_VAN.5),
  - ANSSI a fourni un profil de protection à propos de l'évaluation des TEE.
- *Théoriquement*, un SoC peut être perturbé par une attaque par injection de faute,
- **Mais**, un SoC est :
  - un processeur multitâche,
  - avec une CPU haute fréquence.
- . . . ce qui complexifie le succès d'attaques physiques.

Et l'IoT dans tout ça ?



(Source : `flickr.com/wilgengebroed/`)

Et l'IoT dans tout ça ?



(Source : `flickr.com/wilgengebroed/`)

- Comme pour les ordiphones, l'IoT a un cycle de développement très rapide,
- La plupart des systèmes IoT n'ont pas de composants de sécurité.

Comment certifier l'Iot ?

- Actuellement aucun standard n'est établi pour évaluer des objets intelligents,
- des initiatives privées semblent émerger,
- il faut des schémas de certification adaptés :
  - on n'évalue pas une brosse à dent comme un pacemaker,
  - la méthode d'évaluation doit être adaptée aux cycles rapides de développement de ces objets.

Conclusion

- Pour l'instant, les attaques physiques ne sont pas/très peu utilisées pour attaquer les ordiphones.
- Peut-on attaquer physiquement un SoC ? Oui, mais ce n'est pas trivial.
- Pour l'instant, les attaques sont principalement logicielles.
- Comment garantir le niveau de sécurité d'un SoC ?
  - Évaluer ce SoC,
  - Il n'existe pas encore de schéma d'évaluation sûr et rapide,
  - C'est à faire !

Questions ?

Guillaume Bouffard
<guillaume.bouffard@ssi.gouv.fr>