Sécurité et recueil de données protégées sur plateformes mobiles grand public

Les téléphones mobiles et les tablettes interactives contiennent de plus en plus de données sur leur propriétaire, personnelles et professionnelles. Ils embarquent également d'ores et déjà *des infrastructures d'identité mobile* avec à court terme des *fonctions de capture biométrique*. Ces données s'avèrent capitales, tant dans le domaine de l'expertise judiciaire que pour le monde du renseignement. Elles peuvent également faire l'objet de vols ou de compromissions.
Ainsi, la sécurité de ces plateformes devient un élément essentiel, intégré de manière disparate selon les fabricants et les fournisseurs de systèmes d'exploitation. Certaines (ie Apple) deviennent très sécurisées, même si la confidentialité des données reste non prouvée. Cependant ce niveau de sécurité empêche le recueil de renseignement ou de preuves. C'est pourquoi l'analyse en profondeur des terminaux mobiles grands publics en vue de détecter des failles ou des moyens d'accès aux données utilisateurs, systèmes et physiques s'avère nécessaire. Cette étude permettra de montrer si des données sont récupérables ou non, d'un point de vue quantitatif et qualitatif.

La réussite de cette récupération dépend de plusieurs facteurs :

- la manière dont l'OS gère l'écriture, l'effacement et la réécriture des données ;
- la structure et le format des données concernées (notamment la quantité de redondance présente dans ces données) ;
- la quantité d'information pouvant être récupérée ;
- la présence ou l'absence de mécanismes de chiffrement et/ou d'effacement physique des données;

La thèse approchera ce problème de manière théorique et pratique aussi bien sous l'angle de l'attaque que sous l'angle de la défense.

Etat de l'art

Sécurité matérielle - TrustZone

TrustZone est une fonctionnalité processeur développée par ARM. Elle permet de séparer matériellement deux systèmes d'exploitation. Ainsi, il est possible d'avoir sur le même appareil, un OS riche, comme Android et un petit OS sécurisé (Trusted Execution Environment - TEE) qui prendra en charge les fonctions d'authentifications (credentials, biométrie, bancaire, etc). Le TEE peut également héberger l'exécution du *secure boot,* requis notamment par le protocole TPM MOBILE.
Cette sécurité empêche l'exécution de code non approuvé et est donc un obstacle à la récupération des données, notamment si l'utilisateur a protégé ses données par mot de passe.
Nous voyons que la plupart des plateformes ont été la cible d'attaques et des failles ont permis aux attaquant d'exécuter du code arbitraire et accéder aux données systèmes. Quelles sont les plateformes réellement sécurisées ?

Sécurité matérielle - Cryptoprocesseur

Certaines plateformes embarquent un chiffrement matériel des données. Ainsi, les mémoires des appareils Apple, sont pour la grande majorité chiffrées par le processeur avec une clé « gravée dans le silicone » et donc accessible que par lui seul.
Ce chiffrement matériel garantit une stérilisation rapide de la mémoire, peut augmenter les performances, mais empêche l'accès aux données par lecture directe du composant.

Sécurité logicielle - Chiffrement

Le chiffrement logiciel est utilisé à plusieurs niveaux. Sur Android par exemple, il est possible de chiffrer au niveau d'un volume logique (via dm-crypt).
WindowsPhone 8 utilise le logiciel BitLocker et propose un chiffrement du système d'exploitation et pour les fichiers de données.
Enfin, sur iOS(>5), plusieurs chiffrement logiciels sont utilisés par défaut : un chiffrement de chaque partition logique et un chiffrement de chaque fichier. La suppression des fichiers s'opère donc par suppression de la clé.
Cependant, sur une plate-forme iOS 6, nous avons pu, en accédant au niveau physique de la NAND (après le chiffrement matériel), retrouver des clés de fichiers effacés.
En effet, nous nous sommes appuyés sur la redondance des données, inhérente à la gestion des mémoire flash. Ainsi, l'effacement des clés de chiffrement est-il maîtrisé ? Garantit-il une parfaite sécurité ?

Code de verrouillage

Les terminaux mobiles de type smartphones protègent l'accès aux données et aux fonctionnalités par code de verrouillage indépendant du code PIN de la carte SIM. Ce code est liés aux fonctions de chiffrement évoquées au paragraphe précédent et sa connaissance est souvent fondamentale pour l'accès aux données. Les dernières plateformes Apple de type iPhone ou iPad, qui n'ont pas de faille matérielle dans le bootloader, ne permettent pas l'accès aux données sans connaissance de ce code. Que ce soit dans le domaine criminalistique ou du renseignement, beaucoup de cas de figure font que ce code n'est pas connu (personne décédée, milieu hostile, etc).
Est-il possible de récupérer ce code sur ces plateformes ?

Plan de travail

Le travail de recherche couvrira les aspects suivants:

1. Acquérir une compréhension complète des propriétés de sécurité des systèmes d'exploitation principaux utilisés en téléphonie mobile tels qu'iOS, Android, Windows 8 et leurs frameworks associés (e.g. Java JEM2, OKL4 etc).

2. Étude détaillée de l'architecture iOS (>6) en vue de récupérer des données effacées.

3. Recherche de failles matérielles et logicielles dans cette architecture permettant d'accéder aux données protégées par code de verrouillage.

4. Mettre au point une méthodologie pratique permettant aux acteurs de la criminalistique et du renseignement d'extraire, de manière aussi automatisée que possible, le contenu de plateformes mobiles. Imaginer, breveter et prototyper toute solution innovante d'extraction ou d'anti-extraction de données et toute idée tirant avantage des capacités des plateformes mobiles de nouvelle génération..

Nous souhaitons orienter les recherches du doctorant de manière relativement libre dans ce vaste champ thématique afin de créer et proposer des algorithmes, protocoles et solutions dans le cadre des volets que nous venons d'exposer.

Laboratoires

Département informatique-électronique de l'Institut de Recherche Criminelle de la Gendarmerie Nationale
Département informatique de l'ENS (équipe cryptologie)