Chapitre 3
Les différents types d'attaques

1. Introduction

Dans ce chapitre, nous allons nous concentrer sur les différents types d'attaques les plus courantes existant sur les appareils mobiles Android, mais également sur les divers types de menaces mettant en danger la sécurité des appareils mobiles. Ces différentes menaces venant généralement de pirates, escrocs, hackers, black hat, etc., peuvent perturber le fonctionnement d'un appareil mobile, modifier les données d'un utilisateur et également transmettre des données, comme le ferait un logiciel malveillant. Nous allons voir que les escrocs et hackers ne manquent pas d'imagination pour mettre à mal la sécurité des utilisateurs et de certaines entreprises.

– La disponibilité : il s'agit de priver l'utilisateur de l'utilisation de son appareil mobile ou d'en limiter l'accès. Nous appelons cela les attaques par déni de service (*denial of service*). Elles sont très répandues.
– L'identité : il s'agit d'usurper l'identité d'un utilisateur pour commettre d'autres infractions sans être inquiété. Tous les appareils mobiles sont capables de transmettre des informations relatives au propriétaire du contrat d'abonnement de leur opérateur.

– Les données : comme dit précédemment, notre smartphone contient énormément de données sensibles telles que des informations d'authentification, des informations privées, des numéros de cartes bancaires, des applications gérant le système d'alarme domestique, des journaux d'activité, comme par exemple le journal d'appels, la liste de contacts, les réseaux sociaux, etc. La récupération de données est très prisée non pas uniquement par les pirates, car elles peuvent intéresser des professionnels commerciaux peu scrupuleux. Avec ce type de données, un attaquant peut facilement vous voler de l'argent, faire un crédit à votre nom, violer la sécurité de votre habitation, etc.

2. Les attaques physiques

Les attaques physiques sont aussi dangereuses et même pires que les attaques ciblées, car un attaquant peut facilement avoir accès à toutes les données de votre appareil mobile. Il est très simple de contourner et même casser les mécanismes de protection quand on dispose d'un accès physique à l'appareil. Un attaquant peut également déverrouiller ou débloquer (nous parlerons de *rootage* en anglais ou de jail-break sur iOS) l'appareil et ainsi s'attribuer tous les droits (lecture, écriture, exécution) sur le système (y compris l'installation d'un nouveau système d'exploitation). En bref, il pourra tout faire avec l'appareil.

Il est donc très important de rester vigilant et de ne pas se faire voler son appareil mobile, car les conséquences vous seront bien évidemment préjudiciables.

Une attaque physique connue est le Juice Jacking, qui est une attaque spécifique aux plateformes mobiles et qui consiste à exploiter leur port USB, qui permet de recharger l'appareil mais également de transférer des données vers celui-ci ou depuis celui-ci. De nombreux périphériques sont ainsi susceptibles de voir leurs données volées ou de se faire installer des applications malveillantes via les plateformes de charge se trouvant par exemple dans des lieux publics. Il existe également des applications malveillantes cachées dans certains adaptateurs de charge nomades. Nous l'avons compris, il est donc impératif de ne pas laisser traîner son téléphone mobile ou sa tablette pour éviter qu'ils soient piratés.

3. Les attaques locales

Les attaques locales sont moins courantes. Dans ce type d'attaque, le pirate doit se trouver à proximité de l'appareil. Par exemple, un pirate peut très facilement récupérer les données d'un utilisateur (identifiant, mot de passe) transmises en clair sur un réseau Wi-Fi public, qui est non sécurisé et sur lequel les données ne sont pas cryptées. Des attaques par Wi-Fi sont également présentes parmi les attaques à distance.

Parmi ces attaques locales, nous pouvons citer les deux suivantes :

– Les attaques par Bluetooth : ces attaques consistent à exploiter certaines failles de sécurité permettant à un attaquant de se connecter sur le port Bluetooth afin de prendre le contrôle total du périphérique et donc de l'appareil. Cette attaque était rendue possible car les services qui ne sont pas configurés et enregistrés ne nécessitent aucune authentification particulière ; de plus, les applications vulnérables à ce type d'attaque disposent d'un port série virtuel permettant de contrôler l'appareil mobile. Il est également possible, si votre Bluetooth est activé en mode découverte et donc détectable par n'importe qui, de recevoir automatiquement un fichier venant d'un attaquant contenant un virus, une application malveillante ou un ver. Le Bluetooth dispose de privilèges élevés sur la plupart des systèmes d'exploitation, ce qui rend l'attaque invisible aux yeux de l'utilisateur. Ces attaques ont déjà posé des problèmes par le passé sur de nombreux appareils mobiles. Des protections sont sans cesse mises en place par Google mais de nouvelles vulnérabilités voient le jour constamment.

Remarque

En 2004, le premier virus informatique qui se propageait grâce à la technologie Bluetooth a été découvert. Ce ver se chargeait de rechercher des appareils mobiles en mode détectable à proximité et envoyait un fichier infecté, en espérant que l'utilisateur accepte le fichier et l'installe sur l'appareil.

– Les attaques par ondes électromagnétiques : ce type d'attaque est moins connu du grand public et assez complexe à mettre en place, car il nécessite d'avoir du matériel parfois coûteux. Des chercheurs ont découvert en 2015 qu'il était possible de déclencher à distance (mais pas trop loin de l'appareil quand même) l'interface vocale de certains appareils mobiles vulnérables en utilisant des formes d'ondes électromagnétiques bien spécifiques. L'attaque consiste à exploiter les propriétés des antennes de fils de casque audio lorsque le casque est branché sur les prises de sortie audio ; le but est d'usurper une entrée audio afin de pouvoir injecter du code et des commandes via l'interface audio. Des chercheurs ont également découvert en 2016 qu'il était possible de récupérer des clés privées d'Android basées sur des algorithmes de courbes elliptiques.

Remarque

Il y a déjà quelques années, un drone américain a été détourné et a pu être amené au sol par une équipe israélienne militaire de chercheurs en sécurité. Il se dit, sans que nous en soyons sûrs, que cet exploit a pu être possible grâce à ce type d'attaque. Intéressant, non ?

4. Les attaques à distance

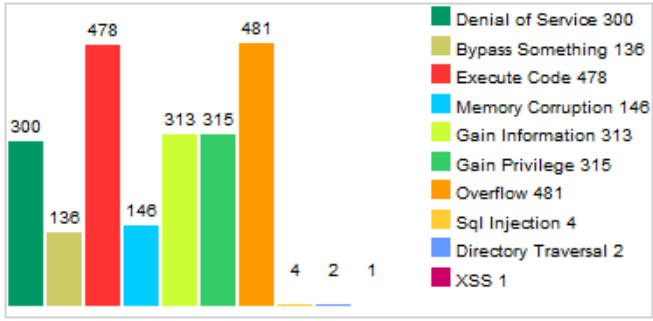
Les attaques à distance sont très répandues, comme sur tout autre système. Qui n'a jamais reçu un e-mail indésirable, un SMS contenant un lien suspect, des appels indésirables, des MMS contenant une pièce jointe vérolée, etc. ? Il faut savoir qu'en plus de ces attaques menées par des kackers, des sociétés peu scrupuleuses vendent vos données comme d'autres entreprises en achètent, à des fins commerciales, mais pas seulement.

En effet, outre les voleurs de données personnelles, les hackers black hat, etc., il y a aussi des organismes soi-disant sérieux, qui sont susceptibles de vendre vos données personnelles à des entreprises commerciales. Dans ce cas, il est impossible pour un utilisateur de remédier à ce problème (nous reviendrons sur ce sujet plus en détail dans le dernier chapitre de cet ouvrage).

Les liens malveillants sur les réseaux sociaux sont une attaque à distance très prisée des hackers. Ils utilisent cette technique car elle est très efficace et il est très facile de propager des logiciels malveillants contenant des chevaux de Troie, des logiciels espions, etc. Ces derniers permettront au pirate de suivre votre position, de consulter vos SMS et e-mails, d'écouter vos conversations téléphoniques. Ils peuvent également placer des backdoors, des portes dérobées qui permettent au pirate de revenir facilement se connecter au système qu'il a infecté. Il ne faut pas oublier le téléchargement d'application malveillante, par exemple si l'utilisateur télécharge un jeu (ou une autre application) qui contient en réalité un code malveillant capable de voler vos données personnelles à votre insu ou d'ouvrir d'autres canaux de communication pour installer par exemple une autre application malveillante complémentaire de la première afin de communiquer plus efficacement. Via les Botnets (réseaux de robots connectés à Internet, souvent utilisés pour mener des attaques par déni de service), les hackers infectent plusieurs machines avec des applications malveillantes (généralement en envoyant des pièces jointes vérolées) et peuvent alors se servir du réseau infecté à des fins néfastes et dangereuses pour la victime. Le Wi-Fi constitue également une menace pour la sécurité, car un pirate peut intercepter le trafic en menant une attaque de type Man-in-the-Middle (que nous verrons un peu loin dans cette section) et ainsi récupérer tout ce que l'utilisateur transmet sur le réseau.

Pour résumer les différents types d'attaques à distance, nous pouvons citer les attaques via les SMS, MMS, e-mails, les attaques basées sur les réseaux GSM, les réseaux Wi-Fi, les attaques par Bluetooth, les attaques sur le système d'exploitation et bien évidemment les attaques sur les navigateurs web, dont la sécurisation devient un enjeu majeur, les applications web étant en pleine expansion.

Nous avons vu dans le premier chapitre un diagramme représentant les failles de sécurité sur les appareils mobiles ainsi qu'un petit schéma qui illustre les différentes attaques subies par le système Android. Nous allons reprendre ce schéma pour détailler les différents types d'attaques à distance.



Parmi ces attaques à distance nous pouvons citer les attaques par :

- Injection SQL : cette attaque consiste à injecter du code et des requêtes SQL (comme son nom l'indique). Elle met l'accent sur l'exploitation et la manipulation d'une application qui interagit avec une base de données. Il existe plusieurs types d'injections SQL.
  - *Blind SQL* (injection SQL à l'aveugle) : elle consiste à interroger la base de données par des requêtes vraies ou fausses, qui détermine la réponse en fonction de l'application.
  - *Error-based* (basée sur les erreurs) : dans cette attaque, une application affiche une erreur pour extraire des informations de la base de données. Normalement, lorsque vous interrogez de manière incorrecte la base de données, celle-ci répond par une erreur. Ici, cela consiste à détourner le message d'erreur généré par le système de gestion de la base de données, erreur qui aura bien évidemment été provoquée par l'attaquant afin qu'il puisse récupérer certaines informations, comme par exemple la version de la base de données utilisée, etc.
  - *Union-based* (méthode basée sur l'UNION) : cette attaque consiste à utiliser l'instruction UNION pour obtenir certaines données de la base de données. Certains hackers utilisent cette méthode pour récupérer des tables entières de la base de données et donc de grandes quantités d'informations.