Etude de la sécurité sous Android - Analyse et audit

Type de contenu : Texte

Titre(s) : Etude de la sécurité sous Android - Analyse et audit ; ELHAJJI, Said ; PARRAUD, Patrice ; SLT FOUCHEROT, Thomas

Autre(s) responsabilité(s) : ELHAJJI, Said (Directeur de thèse)
PARRAUD, Patrice (Directeur de thèse)
SLT FOUCHEROT, Thomas Promotion Chef de bataillon Bulle (2010-2013) (Secrétaire)

Editeur, producteur : Ecoles Militaires de Saint-Cyr Coëtquidan

Description matérielle : 1 CD

Note sur le contenu : mémoire

Note de thèses et écrits académiques : Filière Scientifique - Option Informatique Promotion Chef de bataillon Bulle Date de soutenance : 01/01/2013

Résumé ou extrait : ETUDE : Position du problème Nous proposons une étude de la sécurité Android, et notamment de sa sécurité applicative, sans perdre de vue ses spécificités techniques de système embarqué. En faisant un état de l'art, nous pouvons mieux appréhender les mécanismes de sécurité du système d'exploitation embarqué Android et ainsi comprendre les faiblesses de ce système. Il faut savoir que le plus grand danger pour un téléphone utilisant Android est l'infection dûe à une application malveillante. Il existerait près de 25000 malwares pour Android. Google est en pleine réflexion pour élaborer de nouvelles sécurités pour Android. Nos travaux ETUDE DES SMARTPHONES Tout d'abord, nous étudions le contexte dans lequel s'inscrit le téléphone Android, à savoir celui des smartphones. Une étude comparative économique, technique et sécuritaire permet de justifier notre choix de s'intéresser à ce système embarqué : il est le plus utilisé, le plus ouvert et le plus vulnérable. Modèle de sécurité sur la plateforme Android Ensuite, nous nous attachons à étudier plus spécifiquement l'implémentation de la sécurité sur la plateforme Android. Cela passe par une présentation du système d'exploitation embarqué Android, utilisant un noyau Linux et open-source, puis par un exposé du modèle de sécurité retenu par Google. Cela passe par sept points clé : signature des applications, permission des applications, séparation des application, l'unité de gestion de mémoire, l'utilisation d'un langage typé pour écrire les applications, le verrouillage du terminal et la maintenance à distance de Google. Nous évoquons le cas d'une faille réseau en lien avec ce dernier point. SECURITE APLLICATIVE SOUS ANDROÏD Enfin, nous exposons nos recherches sur la sécurité applicative. Après une introduction dans ce domaine particulier grâce à l'analyse du code du malware iCalendar, nous développons notre propre application malveillante afin de bien comprendre la méthodologie d'un pirate, puis nous effectuons un audit de sécurité complet, statique et dynamique, sur l'application malveillante LuckyCat, qui est une porte dérobée. DEMARCHE Notre démarche a évolué au fur et à mesure de nos travaux. Partis d'une vision universitaire du problème, nous nous sommes peu à peu orientés vers une vision d'ingénieur. Ainsi, notre mémoire présente des parties techniques, très utiles à un ingénieur chargé par son entreprise de monter le projet d'audit de

sécurité de malware. Nous nous inscrivons dans le cadre d'une prestation de service, ce qui est très actuel. Notre position a donc été la suivante : nous recevons une application à auditer. Nous effectuons un audit statique et un audit dynamique sur cette application, ce qui nous permet de statuer sur son caractère malveillant. Enfin, nous livrons au client un rapport d'audit de sécurité avec nos conclusions et nos préconisations. RESULTATS OBTENUS Nous avons réussi à mettre en place un protocole d'audit de sécurité. Nous avons pu auditer de manière statique l'application iCalendar et de manières statique et dynamique l'application LuckyCat, cette dernière étude débouchant sur la publication d'un rapport type d'audit de sécurité. Nous avons également pu étudier de façon annexe une faille réseau permettant l'installation et la désinstallation à distance d'application. Nous n'avons pu exploiter cette faille réseau. Nous avons utilisé Androguard, sur lequel nous donnons notre avis, ainsi qu'Eclipse pour la programmation en Java. PERSPECTIVES Les perspectives d'amélioration de ce mémoire sont regroupées dans un mot d'ordre : l'automatisation. En effet, nous avons exposé les moyens et la méthodologie en cours dans l'univers de la sécurité Android, mais il est possible de développer des programmes pour automatiser les processus. Cette automatisation peut concerner deux volets. Tout d'abord, la veille sécuritaire est ciblée. Elle protège l'utilisateur en temps réel et s'apparente aux anti-virus que nous connaissons sur les ordinateurs. Ainsi, les détect

Sujet(s) : Androïd
Google
Linux
innovation technologique
protocole
système embarqué
sécurité informatique
téléphone intelligent