SOUTENANCE DE THESE

Mohamed SABT

Unité de Recherche : **UMR 7253 Laboratoire Heudiasyc**

soutiendra sa thèse de **Doctorat**

sur le sujet :

Outsmarting Smartphones – Trust based on Provable Security and Hardware Primitives in Smartphones Architectures

A l'Université de technologie de Compiègne
Le mardi 13 décembre 2016 à 14h
Amphi L200 – Centre Pierre Guillaumat

Devant le jury composé de :

M. ACHEMLAL Mohammed, Maître de Conférences, ENSICAEN, Caen
M. BOUABDALLAH Abdelmadjid, Professeur des Universités, Université de technologie de Compiègne, Laboratoire Heudiasyc
M. CHRISMENT Isabelle, Professeur des Universités, LORIA, Vandoeuvre-Lès-Nancy
M. DRITAN Nace, Professeur des Universités, Université de technologie de Compiègne, Laboratoire Heudiasyc
M. FRANCILLON Aurélien, Maître de Conférences, Campus SophiaTech, Eurecom, Biot
M. GILBERT Henri, Responsable du Laboratoire de Cryptographie, Agence nationale de la sécurité des systèmes d'information, Paris
M. TRAORE Jacques, Ingénieur de Recherche, Orange Labs, Caen
M. URIEN Pascal, Professeur des Universités, Telecom ParisTech, Département de réseaux & Informatique, Paris

Abstract:
The landscape of mobile devices has been changed with the introduction of smartphones. Since their advent, smartphones have become almost vital in the modern world. This has spurred many service providers to propose access to their services via mobile applications. Despite such big success, the use of smartphones for sensitive applications has not become widely popular. The reason behind this is that users, being increasingly aware about security, do not trust their smartphones to protect sensitive applications from attackers. The goal of this thesis is to strengthen users trust in their

devices. We cover this trust problem with two complementary approaches: provable security and hardware primitives.

In the first part, our goal is to demonstrate the limits of the existing technologies in smartphones architectures. To this end, we analyze two widely deployed systems in which careful design was applied in order to enforce their security guarantee: the Android KeyStore, which is the component shielding users cryptographic keys in Android smartphones, and the family of Secure Channel Protocols (SCPs) defined by the GlobalPlatform consortium. Our study relies on the paradigm of provable security. Despite being perceived as rather theoretical and abstract, we show that this tool can be handily used for real-world systems to find security vulnerabilities. This shows the important role that can play provable security for trust by being able to formally prove the absence of security flaws or to identify them if they exist.

The second part focuses on complex systems that cannot cost-effectively be formally verified. We begin by investigating the dual-execution-environment approach. Then, we consider the case when this approach is built upon some particular hardware primitives, namely the ARM TrustZone, to construct the so-called Trusted Execution Environment (TEE). Finally, we explore two solutions addressing some of the TEE limitations. First, we propose a new TEE architecture that protects its sensitive data even when the secure kernel gets compromised. This relieves service providers of fully trusting the TEE issuer. Second, we provide a solution in which TEE is used not only for execution protection, but also to guarantee more elaborated security properties (i.e. self-protection and self-healing) to a complex software system like an OS kernel.

Résumé

Le paysage du monde des téléphones mobiles a changé avec l'introduction des ordiphones (de l'anglais smartphones). En effet, depuis leur avènement, les ordiphones sont devenus incontournables dans des différents aspects de la vie quotidienne. Cela a poussé de nombreux fournisseurs de services de rendre leurs services disponibles sur mobiles. Malgré cette croissante popularité, l'adoption des ordiphones pour des applications sensibles n'a toujours pas eu un grand succès. La raison derrière cela est que beaucoup d'utilisateurs, de plus en plus concernés par la sécurité de leurs appareils, ne font pas confiance à leur ordiphone pour manipuler leurs données sensibles. Cette thèse a pour objectif de renforcer la confiance des utilisateurs en leur mobile. Nous abordons ce problème de confiance en suivant deux approches complémentaires, à savoir la sécurité prouvée et la sécurité ancrée à des dispositifs matériels.

Dans la première partie, notre objectif est de montrer les limitations des technologies actuellement utilisées dans les architectures des ordiphones. À cette fin, nous étudions deux systèmes largement déployés et dont la sécurité a reçu une attention particulière dès la conception : l'entrepôt de clés d'Android, qui est le composant protégeant les clés cryptographiques stockées sur les mobiles d'Android, et la famille des protocoles sécurisés SCP (de l'anglais Secure Channel Protocol) qui est définie par le consortium GlobalPlatform. Nos analyses se basent sur le paradigme de la sécurité prouvée. Bien qu'elle soit perçue comme un outil théorique voire abstrait, nous montrons que cet outil pourrait être utilisé afin de trouver des vulnérabilités dans des systèmes industriels. Cela atteste le rôle important que joue la sécurité prouvée pour la confiance en étant capable de formellement démontrer l'absence de failles de sécurité ou éventuellement de les identifier quand elles existent.

Quant à la deuxième partie, elle consacrée aux systèmes complexes qui ne peuvent pas être formellement vérifiés de manière efficace en termes de coût. Nous commençons par examiner l'approche à double environnement d'exécution. Ensuite, nous considérons le cas où cette approche est instanciée par des dispositifs matériels particuliers, à savoir le ARM TrustZone, afin de construire un environnement d'exécution de confiance (TEE de l'anglais Trusted Execution Environment). Enfin, nous explorons deux solutions palliant quelques limitations actuelles du TEE. Premièrement, nous concevons une nouvelle architecture du TEE qui en protège les données sensibles même quand son noyau sécurisé est compromis. Cela soulage les fournisseurs des services de la contrainte qui consiste à faire pleinement confiance aux fournisseurs du TEE. Deuxièmement, nous proposons une solution dans laquelle le TEE n'est pas uniquement utilisé pour protéger l'exécution des applications

sensibles, mais aussi pour garantir à des grands composants logiciels (comme le noyau d'un système d'exploitation) des propriétés de sécurité plus complexes, à savoir l'auto-protection et l'auto-remédiation.