

Smartphone Security: New Applications and Challenges

Doctoral Thesis

Author(s):

Marforio, Claudio

Publication date:

2016

Permanent link:

<https://doi.org/https://doi.org/10.3929/ethz-a-010608037>

Rights / license:

[In Copyright - Non-Commercial Use Permitted](#)

Diss. ETH No. 23154

Smartphone Security: New Applications and Challenges

A thesis submitted to attain the degree of

DOCTOR OF SCIENCES of ETH ZURICH
(Dr. sc. ETH Zurich)

presented by

CLAUDIO MARFORIO

Master of Science in Computer Science,
ETH Zurich

born on 10.03.1986

citizen of Italy

accepted on the recommendation of

Prof. Dr. Srdjan Čapkun, examiner

Prof. Dr. N. Asokan, co-examiner

Prof. Dr. David Basin, co-examiner

Prof. Dr. Patrick Traynor, co-examiner

2016

Abstract

Smartphones have become daily companions and are carried around by billions of people. They are used for the most diverse tasks and users trust them with both private and business data. As with any technology that reaches such a scale and holds so much information about its users, smartphones enable new applications but also pose new challenges. On the one hand, the power and versatility of these platforms can be used to enhance the security of our day to day activities. On the other hand, smartphones are becoming more and more the targets of attacks.

In this thesis we look at both aspects of smartphone security. We first propose two ways in which smartphones can enhance the security of daily life operations. Then, we look at sophisticated attacks that can circumvent the security mechanisms deployed on smartphones.

In the first part of this thesis, we introduce Sound-Proof, a two-factor authentication mechanism for the web. Sound-Proof uses short audio recordings to verify the proximity of the user's smartphone and computer. Only when the two are close to each other is the login attempt authorized. This solution is transparent to the user, who does not have to interact with his smartphone, thus matching the experience of password-only authentication. It is also easily deployable, as no extra software is required on the computer from where the user is logging in. We then propose a secure location-based two-factor authentication system for payments at points of sale. In this case we consider a strong adversary that can compromise the user's mobile operating system. To overcome this adversary, we propose novel secure enrollment schemes for the trusted execution environment of the user's smartphone.

In the second part of this thesis, we first investigate application phishing attacks. We look at various countermeasures and identify personalized security indicators as an attractive solution. We perform the first user study to assess their effectiveness in the new context of mobile application phishing. Our results show an increase in attack detection rates compared to previous studies on the web and give reason to believe that personalized security indicators can be used effectively on smartphones. We then look at application collusion attacks. In particular, we implement and evaluate various overt and covert communication channels that two applications can use to exchange information on smartphones. We provide evidence as to why some channels cannot be easily prevented and conclude that application collusion attacks remain an open problem.

Sommario

Da qualche anno a questa parte, miliardi di persone portano sempre con sé e interagiscono con uno smartphone. Questi dispositivi hanno molteplici utilizzi, da quelli lavorativi a quelli più personali. Come spesso accade con tecnologie che raggiungono tali livelli di utilizzo e che gestiscono una grande quantità di informazioni private, gli smartphone possono essere utilizzati per nuove operazioni ma pongono anche nuove sfide nell'ambito della sicurezza. Da una parte, le capacità di questi apparecchi fanno sì che possano essere utilizzati per migliorare la sicurezza delle nostre operazioni giornaliere, dall'altra essi vengono presi di mira dai criminali informatici con sempre maggior frequenza.

In questa tesi approfondiamo i seguenti aspetti della sicurezza degli smartphone: in primo luogo proponiamo due modalità con cui gli smartphone possono migliorare la sicurezza delle operazioni di ogni giorno; in seguito analizziamo alcuni sofisticati attacchi che aggirano le misure di sicurezza implementate su questi apparecchi.

Nella prima parte della tesi introduciamo Sound-Proof, un sistema di autenticazione a due fattori per il web. Sound-Proof usa due brevi registrazioni audio per verificare che il computer e lo smartphone dell'utente siano vicini tra di loro. Solo quando questi dispositivi sono vicini il sistema autorizza l'accesso. Questa soluzione risulta pratica per l'utente in quanto quest'ultimo non deve interagire con il proprio smartphone, ma semplicemente inserire l'identificativo e la password come d'abitudine; allo stesso tempo, non deve installare alcun software sul proprio computer. Proseguiamo questa prima parte della tesi introducendo un sistema di autenticazione a due fattori per i pagamenti con carta di credito presso i negozi, basato sulla posizione GPS dello smartphone. In questo contesto consideriamo un attaccante potente che sia in grado di compromettere il sistema operativo dello smartphone dell'utente. Per combattere questo tipo di attaccante proponiamo due nuovi sistemi di inizializzazione per la modalità sicura del dispositivo.

Nella seconda parte della tesi investighiamo le truffe di tipo "phishing" perpetuate contro applicazioni per smartphone. In particolare analizziamo diverse contromisure e identifichiamo le immagini personali di sicurezza come una soluzione accattivante al problema. Conduciamo il primo studio di usabilità atto a capire l'effettiva efficacia di questo sistema nel nuovo ambito degli smartphone. I risultati dimostrano un miglioramento nella rilevazione degli attacchi da parte degli utenti quando comparati con si-

stemi simili utilizzati sul web. Per questo motivo le immagini personali di sicurezza possono essere utilizzate con successo sugli smartphone. In seguito analizziamo gli attacchi di applicazioni che colludono tra loro: in particolare, implementiamo e valutiamo diversi canali di comunicazione, sia palesi che occulti, che due applicazioni possono utilizzare per scambiarsi informazioni. Dimostriamo come alcuni di questi canali non possano essere facilmente bloccati e concludiamo che gli attacchi portati avanti da tali applicazioni rimangono un problema aperto.

Zusammenfassung

Smartphones sind zum ständigen Begleiter von Milliarden von Menschen geworden. Sie werden für die verschiedensten Aufgaben eingesetzt und Benutzer vertrauen ihnen private wie auch geschäftliche Daten an. Wie bei jeder Technologie mit derartiger Verbreitung und derartigem Informationsgehalt, ergeben sich auch durch Smartphones neue Möglichkeiten aber auch neue Herausforderungen. Einerseits kann die Funktionalität und Vielseitigkeit dieser Plattformen genutzt werden um die Sicherheit unserer alltäglichen Aktivitäten zu erhöhen. Andererseits, werden Smartphones mehr und mehr zum Ziel von Angriffen.

In dieser Dissertation betrachten wir beide Sicherheitsaspekte von Smartphones. Zuerst schlagen wir zwei alltägliche Sicherheitsverbesserungen mit der Hilfe von Smartphones vor. Dann behandeln wir zwei komplizierte Angriffe, die die Sicherheitsmechanismen auf Smartphones umgehen können.

Im ersten Teil dieser Dissertation zeigen wir Sound-Proof, eine Zwei-Faktor-Authentifizierung für Webseiten. Sound-Proof nutzt kurze Audio-Mitschnitte, um die räumliche Nähe des Smartphones zum Computer des Benutzers zu verifizieren. Nur wenn beide Geräte nah beieinander sind, wird die Anmeldung autorisiert. Die Lösung ist für den Benutzer unsichtbar, da er sein Smartphone nicht aktiv benutzen muss und daher die gleiche Vorgehensweise, wie bei einem rein Passwort-gestützten Verfahren, hat. Die Lösung ist auch leicht einsetzbar, da keine zusätzliche Software auf dem verwendeten Computer installiert werden muss. Zudem schlagen wir eine sichere, ortsbasierte Zwei-Faktor-Authentifizierung für Zahlungen an Verkaufsstellen vor. In diesem Fall nehmen wir an, dass ein starker Angreifer das mobile Betriebssystem eines Nutzers kompromittieren kann. Um Sicherheit gegen einen solchen Angreifer zu gewährleisten, schlagen wir neue, sichere Registrierungsverfahren für die gesicherte Ausführungsumgebung des Benutzer-Smartphones vor.

Im zweiten Teil dieser Dissertation, analysieren wir zunächst Phishing Angriffe durch mobile Anwendungen. Wir betrachten verschiedene Gegenmassnahmen und stellen fest, dass personalisierte Sicherheitsindikatoren eine ansprechende Lösung sind. Wir führen die erste Benutzerstudie durch, in der die Wirksamkeit dieser Sicherheitsindikatoren, im neuen Kontext von Phishing Angriffe durch mobile Anwendungen, getestet wird. Unsere Ergebnisse zeigen einen Anstieg in erkannten Angriffen, verglichen mit vorherigen webbasierten Studien, und somit den möglichen Nutzen von

personalisierten Sicherheitsindikatoren auf Smartphones. Wir zeigen ausserdem, dass Kollusion zwischen mobilen Anwendungen möglich ist. Genauer entwickeln und bewerten wir verschiedene offene und verdeckte Kommunikationskanäle, die von zwei Anwendungen genutzt werden können, um auf Smartphones Informationen auszutauschen. Wir zeigen warum manche dieser Kanäle nicht einfach geschlossen werden können und folgern, dass Kollusion zwischen Anwendungen ein offenes Problem bleibt.