CS 858 – Mobile Privacy and Security (MoPS)

Fall 2016

Introduction

WATERLOO
CHERITON SCHOOL OF
COMPUTER SCIENCE

CrySP


1 OUT OF 2
PEOPLE
DON'T HAVE A
PASSCODE
ON THEIR PHONE.
Lookout | Sprint

Tenth Symposium On Usable Privacy and Security

It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception

Marian Harbach[1], Emanuel von Zezschwitz[2], Andreas Fichtner[2],
Alexander De Luca[2], Matthew Smith[3]

Some of our key findings are that users spend up to 9.0 % of the time they use their smartphone on dealing with unlock screens, that a secure lock screen is considered unnecessary in 24.1 % of the situations we sampled, and that shoulder

Research Challenges

Evaluate usability of deployed smartphone authentication schemes

Develop authentication schemes better suited for smartphones

OPEN USA TODAY
A GANNETT COMPANY

Search

SUBS
to get

NEWS | SPORTS | LIFE | MONEY | TECH | TRAVEL | OPINION | 39° | CROSSWORDS | YOUR TAKE | INVESTIGATIONS | VIDEO | STOCKS | APPS | MORE

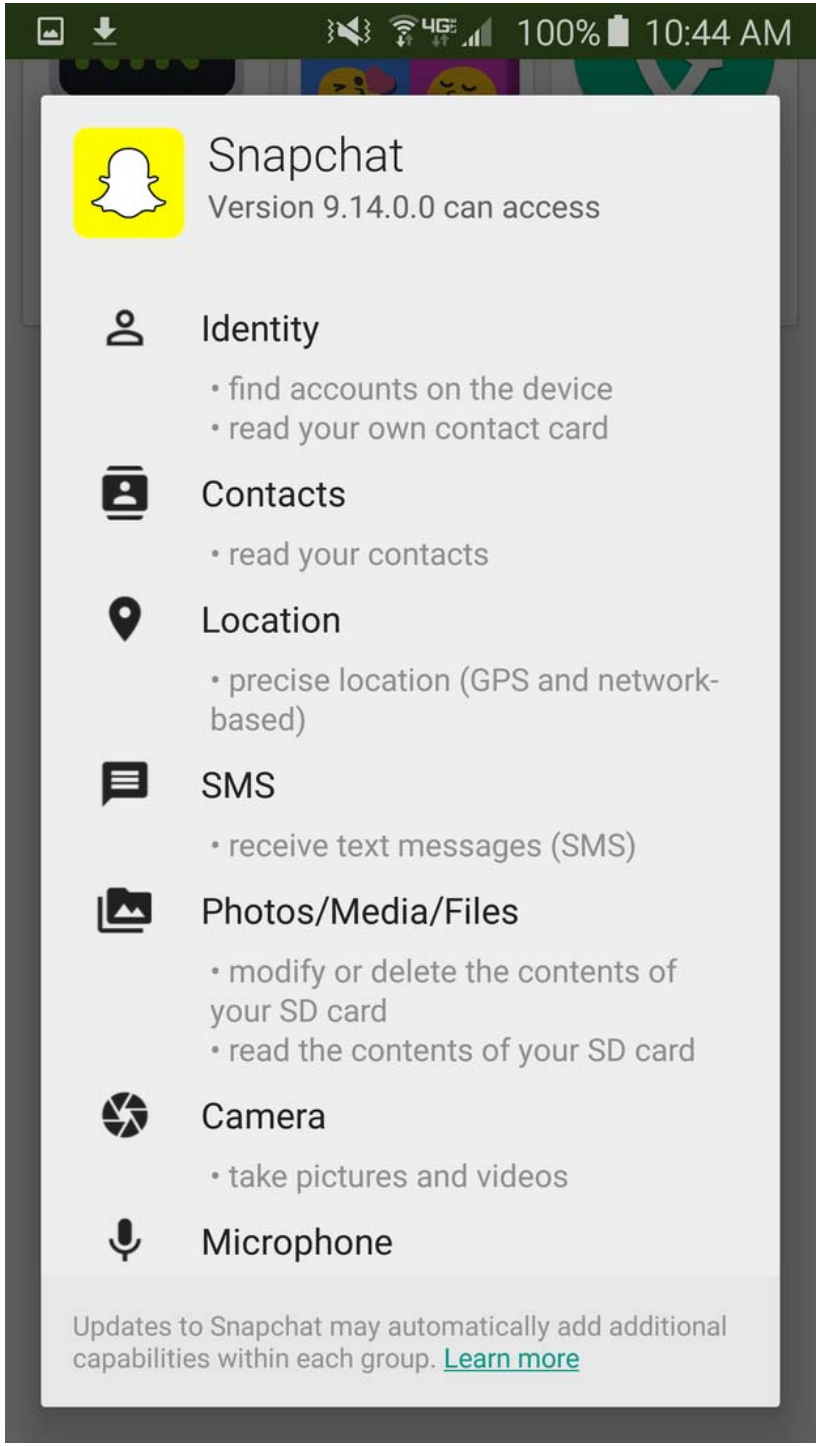
Is your flashlight app stealing data from your phone?


FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS
Contact | Stay Connected | Privacy Policy | FTC en español
Search
ABOUT THE FTC | NEWS & EVENTS | ENFORCEMENT | POLICY | TIPS & ADVICE | I WOULD LIKE TO...
Home » News & Events » Press Releases » Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission
Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission
Company Will Pay $950,000 For Tracking Children Without Parental Consent
FOR RELEASE
June 22, 2016
EVENTS CALENDAR
Related Cases
InMobi Pte Ltd.

Research Challenges

Detect when apps leak sensitive information

What can be inferred from (arguably) non-sensitive sensor data?


100% 10:44 AM
Snapchat
Version 9.14.0.0 can access
Identity
• find accounts on the device
• read your own contact card
Contacts
• read your contacts
Location
• precise location (GPS and network-based)
SMS
• receive text messages (SMS)
Photos/Media/Files
• modify or delete the contents of your SD card
• read the contents of your SD card
Camera
• take pictures and videos
Microphone
Updates to Snapchat may automatically add additional capabilities within each group. Learn more

Research Challenges

Do users pay attention to permission screens?

Do users understand permission screens?

Overview

Goals

Organization

Topics

Goals

Becoming familiar with state-of-the-art in research on mobile privacy and security

Undertaking novel research in a course project

Learning to read and review technical papers

Learning to give good technical presentations

Organization

Goals

Organization

Topics

Meetings

Time: Mondays and Wednesdays 3:00-4:20pm

Location: DC 2568

Office hour: Mondays and Wednesdays 10-11am or by appointment

Prerequisites

No formal prerequisites

No familiarity with security or cryptography required

Basic knowledge of computer systems and networks helpful

Wide range of papers (applied cryptography, economics, human computer interaction, machine learning, networking, programming languages, systems)

Course Website

Reachable from my own website

Has reading list, schedule, policies,...

Keep track of announcements posted there

Lectures

First week:

Introduction, advice on giving presentations, background

Second week:

Guest lectures by Dr. Hassan Khan, Erinn Atwater, and Prof. Ian Goldberg

Following lectures:

Two students will each present and lead a discussion on a research paper

Course project presentations at the very end

Grading

Paper presentations: 25%

Paper reviews: 20%

Class participation: 15%

Includes presentation feedback

Research project : 40%

Discussion Forum

On Piazza

Link on course website

Paper Reviews

Goal: learn what makes a good paper
So that you can write your own good papers ☺

Every student should read the two papers discussed in a lecture beforehand

See Keshav's How to Read a Paper

Every student should submit a review for one of the two papers before class

Using submission system, see later

You will see each others' (anonymized) reviews

Paper Presentations

Goal: practice your presentation skills

Every student should present two research papers during the term

Workshop/conference-style presentation

Present the paper as if it were your own

You can re-use figures and animations (with attribution)

Carefully prepare your slides (will give advice on Wednesday)

At most 25 minutes

Send me your slides before the lecture

Paper Discussion

After each paper presentation, the presenter leads a discussion about his/her paper

Suggested outline:

- Presenter answers clarification questions from the audience
- Presenter gives his/her opinion about the paper and audience chimes in
- Presenter has some backup questions to stimulate discussion if necessary

About 15 minutes

Presentation Feedback

Feedback is essential for training speaking skills

Every student should submit a review for each presentation by 12pm the day after a presentation
Using submission system, see later

Look at review form in system before preparing your presentation

Presenter will see (anonymized) feedback

HotCRP

We will use HotCRP, which is used by many CS workshops/conferences to manage the review of submitted papers

Three different instantiations of HotCRP, reachable from course website

1) Bidding for papers to present
2) Submitting paper reviews
3) Submitting presentation reviews

Bidding for Papers

I will create an account in the bidding system for all students registered in the course

Go to the bidding system and retrieve your password

Log in, click on “Review Preferences”, and bid for papers; instructions are in the system

The bidding deadline is Sept 18, 11:59pm; students who submit their bids late will likely not get any papers assigned

Course Project

Goal: novel research in the area of mobile privacy and security

Might lead to workshop/conference submission

Possible topics will be discussed later

Typically in groups of two

Proposal: Oct 16

Presentation: Nov 30 and Dec 5 (tentative)

Write-up: Dec 11 (tentative)

See course website for details

Overview

Goals

Organization

Topics

Survey of Topics

Reading list is on the course website

More topics/papers may be added/removed

Order is subject to change

Not all research areas in mobile privacy and security are included

Implicitly Authenticating Smartphone Users

Existing smartphone authentication schemes are not well suited for smartphones (see later)

Instead authenticate users continuously and transparently based on their typical behaviour

Overview of our research in this area

Is touch-based implicit authentication susceptible to mimicry attacks? (Guest lecture by Dr. Hassan Khan)

Distributing Security Tasks among Multiple Collaborating Devices

Assume a single device is able to perform a security task (e.g., authenticating to a website or signing an instant message)

Dangerous if this device is lost/gets stolen

Instead distribute security task among multiple devices owned by the same person such that loss of a single device has no impact (Guest lectures by Erinn Atwater and Prof. Ian Goldberg)

Analyzing Network Traffic for Information Leaks

Information leaks typically happen over the network

Detect leaks through analyzing network traffic

Analysis can be done locally [Song and H., SPSM 2015] or remotely [Ren et al., MobiSys 2016]

Distinguishing Between Legitimate and Illegitimate Information Leaks

Some information leaks are required for an app to function

How can we distinguish between legitimate and illegitimate leaks?

Illegitimate if blocking leak has no impact on user interface [Rubin et al., ASE 2015]

Consider semantics in app source code [Wang et al., Ubicomp 2015]

Studying Users (Un)Locking Smartphones

Why do users choose (not) to lock their smartphones [Egelman et al., CCS 2014]

How often do users unlock? How long does it take them? How many errors to they make [Harbach et al., CHI 2016]

Studying Deployed Smartphone Authentication Schemes

Do users like Touch ID or Face Unlock better than PINs? [Bhagavatula et al., USEC 2015]

Are passwords created on smartphones weaker than desktop passwords? Are they really less usable? [Melicher et al., CHI 2016]

Improving Smartphone Authentication

Users choose weak PINs for usability reasons

It would be more secure to have smartphone assign PIN to user

Can we help user learn this assigned PIN [Schechter and Bonneau, SOUPS 2015]

Smartphones enable new ways of authentication, for example, gesture-based [Sherman et al., MobiSys 2014]

Giving Up on All-or-Nothing Authentication

Not every task executed on a smartphone requires authentication

Some tasks are very sensitive, others less

Use multiple authentication techniques and combine them in confidence level

Different apps require different levels [Riva et al., USENIX Security 2012]

Allow users to use their phone without explicit authentication for 30 secs

Blacklist sensitive apps [Buschek et al., CHI 2016]

Attacking Geo-Social Services

There are many widely used geo-social services (Waze, Swarm/Foursquare, Tinder,...)

Sharing your location with strangers is potentially dangerous

Therefore most geo-social services have some protection mechanisms

However these defenses can be often be circumvented [Polakis et al., CCS 2014]

Many of these attacks rely on deploying Sybil (i.e., fake) devices [Wang et al., MobiSys 2016]

Tracking People and their Devices

A person's location trajectories reveals lots of information (home, work, sexual/political orientation,...)

Location trajectory could be established by sighting her smartphone's MAC address at several places

A company in London actually put WiFi scanners into garbage bins to do this

Therefore smartphone have started to use random MAC addresses

Unfortunately this is not sufficient [Vanhoef et al., AsiaCCS 2016]

Tracking People and their Devices (cont.)

As it turns out we don’t necessarily need device identifier to link different location sightings to the same device and establish trajectory

Having a mobility model that typical users follow is good enough [Tsoukaneri et al., EuroS&P 2016]

More Tracking and Defending Against Tracking

Some smartphone sensors, like accelerometer or gyroscope, do not require any permissions and can be used by any app

A malicious app can use information from these sensors to learn user's location trajectory [Narain et al., Oakland 2016]

For apps that use location information, how often do they access this information? Only when app is in foreground? Provide mock locations to overly nosy apps [Fawaz et al., USENIX Security 2015]

Inferring User Input using Side Channels

Accelerometer and gyroscope cannot only be used for tracking people

They can also leak the text that people enter using the soft keyboard [Shrestha et al., WiSec 2016]

Other public information, like number and timings of interrupts, still leaks user input [Simon et al., PETS 2016]

Studying and Helping App Developers

Developers are notoriously bad when it comes to implementing cryptography and authentication

Is the situation better for banking apps? [Reaves et al., USENIX Security 2015]

Previous research has shown that app developers often misuse SSL/TLS libraries when trying to authenticate servers

Why? Can we help developers by making it harder to misuse these libraries? [Fahl et al., CCS 2013]

Studying Users Interacting with Permissions

Android has displayed permission screens to users upon app installation

Do users pay attention to them and understand them? [Felt et al., SOUPS 2012]

At the time an app accesses a resource protected by a permission, do users think that this access is justified? Or should it be blocked? [Wijesekera et al., USENIX Security 2015]

Developing Better Ways to Inform Users

iOS and Android are moving towards asking for permissions on a fine-grained basis

Many users may not be able to make a decision

Develop an assistant that suggests initial settings and ongoing nudges [Liu et al., SOUPS 2016]

Many apps come with privacy notices but users don't pay attention to them

When is the best time to display this notice? [Balebako et al., SPSM 2015]

Introducing Android and Android Security

Historically interesting papers and reasonable introductions to Android and its security mechanisms

Are there dangerous combinations of permissions, potentially used by malware? The first Android security paper published in a major security venue [Enck et al., 2009, CCS 2009]

The first large-scale study of Android apps for security and privacy vulnerabilities [Enck et al., USENIX Security 2011]

Developing Taint Analysis for Android

Taint analysis tracks (sensitive) information while it's flowing through an app from a source (e.g., GPS sensor) to a sink (e.g., network)

Analysis can be done dynamically, i.e., while app is running [Enck et al., OSDI 2010], or statically, i.e., by analyzing source/intermediate code [Arzt et al., PLDI 2014]

Analyzing Android Inter-Component Communication

Static analysis on Android is hard due to Android's component model

Make static analysis work across apps [Octeau et al., USENIX Security 2013]

Make it scale [Octeau et al., POPL 2016]

Sandboxing Libraries and Apps

Sandboxing is a classic security mechanism to defend against malicious software

Android's permission model is arguably too coarse grained

Sandbox an app for more fine-grained control [Backes et al., USENIX Security]

On Android many apps have third-party libraries embedded, which get the same permissions as the app

Sandbox libraries within app for better protection [Seo et al., NDSS 2016]

Studying Mobile, Targeted Advertising

Many apps have advertisement libraries embedded that send targeting information to advertisement networks

What kind of targeting information is sent? Do ad networks actually use this information? [Nath, MobiSys 2015]

Ads are correlated with a user's profile. This allows an app that displays ads to learn its user's profile [Meng et al., NDSS 2016]

Developing Context-Aware Privacy Mechanisms

Smartphone users that take pictures and publish them may violate the privacy of bystanders

Bystanders should be able to inform picture taker of their privacy policy [Aditya et al., MobiSys 2016]

Data collected by an app from smartphone sensors data may enable inferencing of sensitive information

Inform user of inferences that an app could make [Chakraborty et al., NDSI 2014]

Hacking the OS and Below

Notify the user whenever a sensor is accessed by an app

This notification must be trustworthy, e.g., malware shouldn't be able to override it (Mirzamohammadi et al., MobiSys 2016]

In a cold-boot attack, memory is cooled down, physically removed from a computer, and searched for sensitive information

Protect smartphones against cold-boot attacks [Colp et al., ASPLOS 2015]