Lecture 32: Security Vulnerabilities of Mobile Devices

Lecture Notes on "Computer and Network Security"

by Avi Kak (kak@purdue.edu)

April 20, 2017
4:17pm

Goals:

- What makes mobile devices less vulnerable to malware (to the extent that is the case) and Android's "Verify Apps" security scanner
- Protection provided by sandboxing the apps
- Security (or lack thereof) provided by over-the-air encryption for cellular communications **with a Python implementation of A5/1 cipher**
- Side-channel attacks on specialized mobile devices
- Examples of side-channel attacks: fault injection attacks and timing attacks
- **Python scripts for demonstrating fault injection and timing attacks**
- USB devices as a source of deadly malware
- Mobile IP

CONTENTS

32.1: MALWARE AND MOBILE DEVICES

- Mobile devices — cellphones, smartphones, smartcards, tablets, navigational devices, memory sticks, etc., — have now permeated nearly all aspects of how we live on a day-to-day basis. While at one time their primary function was only communications, now they are used for just about everything: as cameras, as music players, as news readers, for checking email, for web surfing, for navigation, for banking, for connecting with friends through social media, and, Ah!, not to be forgotten, as boarding passes when traveling by air.

- A unanimous ruling by the Supreme Court of the United States not too long ago is indicative of how integral and central such devices have become to our lives. In a 9-0 decision on June 25, 2014, the justices ruled that police may not search a suspect's cellphone without a warrant. Normally, police is allowed to search your personal possessions — such as your wallet, briefcase, vehicle, etc. — without a warrant if there is "probable cause" that a crime was committed. Regarding cellphones, Chief Justice John Roberts said: **"They are such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human**

anatomy.” Justice Roberts also observed: “Modern cellphones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee’s person.”

- The justices obviously based their decision on the fact that people now routinely store private and sensitive information in their mobile devices — the sort of information that you would have stored securely at home in the years gone by.

- Given this modern reality, it is not surprising that folks who engage in the production and propagation of malware are training their guns increasingly on mobile devices.

- In a report on the security of mobile devices submitted to Congress, the United States Government Accountability Office (GAO) stated that the number of different malware variants aimed at smartphones had increased from 14,000 to 40,000 in just one year (from July 2011 to May 2012). You can access this report at `http://www.gao.gov/assets/650/648519.pdf` [The same report also mentions that the worldwide sales of mobile devices increased from 300 million to 650 million in 2012. One might therefore guess that the worldwide sale of mobile devices in 2015 would amount to over 1 billion. This makes mobile devices the fastest growing consumer technology ever.]

- Mobile devices have become a magnet for malware producers because they can be a source of sensitive information that an attacker may be able to use for monetary gain, to seek political advantage, to use as a means to break into a corporate network, and so on.

- As you would expect, many of the attack methods on mobile devices are the same as those on the more traditional computing devices such as desktops, laptops, etc., — **except for one very important difference:** Unless it is in a private network, a *non-mobile* host is usually directly plugged into the internet where it is constantly exposed to break-in attempts through software that scans large segments of IP address blocks for discovering vulnerable hosts. That is, in addition to facing targeted attacks through social engineering and other means, a non-mobile host connected to the internet also faces un-targeted attacks by cyber criminals who simply want to discover hosts (regardless of where they are) on which they can install their malware.

- **On the other hand**, in general, mobile devices when they are plugged into cellular networks can only be accessed by outsiders through gateways that are tightly controlled by the cellphone companies. [Consider the opposite situation of a mobile device being able to access the internet directly through, say, a WiFi network. When on WiFi, the mobile device will be in a private network (normally a class C private network) behind a wireless router/access-point. So the mobile device would not be exposed directly to IP address-block scanning. However, now, a mobile device could be vulnerable to eavesdropping and man-in-the-middle attacks if, say, you are exchanging sensitive information with a