INSE6120 - Fall 2016 - Projects

Xavier de Carné de Carnavalet and Mohammad Mannan

September 7, 2016

For this course, students can choose for their project to work either on a high-quality survey, or on the implementation of some security-related idea. See below the the criteria for each option. Projects can be made in groups of at most three students. Important: please keep in mind that the proposals under Option 2 are restricted—the course professor reserves the rights on your development/analysis (but we will also help you achieve academic recognition for your work, if your contribution is significant).

0.1 Option 1: Survey

The purpose of a survey (also called literature review) is to analyze critically a selected topic through summary, classification, comparison and synthesis of prior research studies. Major security venues publish this type of work, e.g., Systematization of Knowledge (SoK) papers at IEEE Security and Privacy Symposium (labelled under "SoK" or "Systematization of Knowledge"), or the ACM Computing Surveys (CSUR) journal.

If you choose to do a survey, you can take an old existing survey (provided it is the latest one on the topic, and relevant to security), and investigate how things have evolved till now. You may also come up with an original topic that has not been surveyed yet. Your survey will be evaluated something close to an SoK or ACM CSUR paper, i.e., we expect high-quality work.

0.2 Option 2: Implementation

For this type of project, students are asked to implement a working solution (in any programming language), to solve a security and/or privacy-related problem. A list of several topics is provided below, however, students may also propose their own idea (to be validated by the professor).

1. **"Follow me" on the road.** When you are driving and following a friend in front of you, traffic may split you both and you may loose sight of them. To avoid this problem, both of your could share your exact location in real-time via an app on your smartphone, but you would need a third-party service to synchronize the information, which will also know where you are. Design and implement the protocol of a privacy-friendly real-time location sharing among friends.

2. **WhatsApp replacement.** WhatsApp is a popular instant-messing app that supports a variety of convenient features, as well as end-to-end encryption. However, it is not open-source, and the mother company may decide to weaken the encryption or implement backdoors at will. The best secure yet open-source alternative to date is arguably Signal (previously known as TextSecure), from Open Whisper Systems. Unfortunately, Signal lacks group messaging, convenient photo album slide-show, video and audio messages. Also, the desktop version works only as a Chrome app and synchronizes only with Android phones. Thus, there are plenty of features that you can implement yourself.

3. **ObPwd for iOS.** (1-person project only) ObPwd is an Android app and browser extension to generate passwords based on an object, e.g., a picture. Resulting passwords can additionally be tied to a given domain, so that the same object can be reused to generate different passwords on two websites. Implement an iOS version of this app.

4. **Open-source counterpart apps.** F-droid.org proposes a list of open-source apps as alternatives to available closed-source apps found in the official Google Play. This initiative proposes more privacy-friendly apps with less or no ads, which is a great advantage for end-users. Some types of application have not been reimplemented

under an open-source license, e.g., health-related apps (cf. Samsung Health), which you can work on. You can take some very popular apps from Google Play, and implement a privacy-friendly version (e.g., with the least number of permissions).

5. **What is my AV doing?** Security applications, such as antivirus and other security suites, need to constantly remain updated as new signatures are pushed every hour. Companies behind these products also gather information from systems where their product is installed, so they can draw some statistics of infections and further analyze suspicious files. But, what else do they gather? Is it possible to inspect network traffic and understand what these products send out?

6. **Free WiFi.** Free WiFi hotspots have blossomed in recent years and are available in virtually every shop where a customer may consume something (e.g., coffee shops and fast-food restaurants), as well as public places (e.g., airports), including those by local projects such as the MtlWiFi project and Île Sans Fil. How secure are these networks? What can a malicious user do? Also, these access points are sometimes privately owned, and owners may like to gather some information on its users. What do they gather? Do they inject content? Can you implement quick tests as an app to launch when connecting to a new hotspot to verify how dangerous it is? This project will require field studies.

7. **IoT toys.** Some of you may know or will know soon: the stuffed animals and plastic figurines we used to play as children are progressively replaced by Internet-connected toys. These can fetch content in real-time, or react is a pseudo-smart way to voice by uploading audio records to the company-owned servers. A recent work identified worrisome problems (see Hide Yo' Kids: Hacking Your Family's Connected Things). If you have access to such toys, analyze the security of their communications, their network configuration, and understand who else can control the toys.

8. **SecureDrop.** (1 or 2-person project) SecureDrop is an open-source whistleblower submission system used by several news organizations. The source code/design of SecureDrop has been audited in the past. In this project, we would like to evaluate SecureDrop deployment across different news sites – are there security problems introduced by misconfiguration? You can also analyze a similar proposal called Darkleaks.