Software Vulnerabilities: Exploitation and Mitigation

—

Lab 10

Alexandre Bartel

The report for the lab should consist of a single pdf file and a zip file containing the source code of the applications. Please use the following filename for the pdf:

`lab10_FIRSTNAME_LASTNAME.pdf`

Do not forget to add your name on the first page of the report. Do not forget to comment your code. Send the report to alexandre.bartel@uni.lu with the following subject:

`MICS2019SVEM Lab10 FIRSTNAME_LASTNAME`

The deadline is the 26^{th} of May 2019 at 23:59.

1 Lab 10 (32 P.)

1.1 Android SDK

In this lab you will play with Android Studio to write Android applications to illustrate the concept of confused deputy. According to the official website, "Setting up Android Studio takes just a few clicks." See for yourself if this statement is true by following the instructions here.

Question 1.1 How many clicks did it take to install Android Studio? 2 P.

1.2 Application1: Dave's Confused Deputy

Service components are explained here. How to retrieve the contact list is explained here.

Question 1.2 Write an application which offers as a service component the list of all contacts. The service must not be protected by any security check. This application has the READ_CONTACTS permission. The AndroidManifest.xml must be modified to allow other application to acess the service component. Put the source code of 10 P.

the service and the manifest in your report.

1.3 Application2: Attacker's Application

Toasts are described here.

Question 1.3 Write an application which connects to the service component of Application1, retrieves the contact, converts the list to a string representation and simulates that the string is sent the remote host "hutelohu8942138534890peotnusheotunheotnuhsno.lu" on the Internet by notifying the user with a toast. This application only has the INTERNET permission. Put the source code of the service and the manifest in your report. 10 P.

At this point the two applications should run in the Android emulator. Launching Application2 should automatically get the list of contact using the confused deputy (Application1) and notify the user with a toast.

1.4 Patch

The developer Dave of Application1 wants to share the contacts but only with the applications signed with the same private key he owns.

Question 1.4 Explains how Dave can protect the service component of Application1 to only share the contact information with applications signed with Dave's private key. Implement your solution by updating the code of Application1. 10 P.

Note on plagiarism

Plagiarism is the misrepresentation of the work of another as your own. It is a serious infraction. Instances of plagiarism or any other cheating will at the very least result in failure of this course. To avoid plagiarism, always properly cite your sources.