PROPOSED 301 PROJECT

EAVESDROPPING PROTECTION IN CONCLAVE

(EPIC)

CLIENT: DEPARTMENT OF DEFENCE, PEACE, SAFETY AND SECURITY, AT THE COUNCIL FOR SCIENTIFIC AND INDUSTRIAL RESEARCH. (DPSS, CSIR)

CONTACT PEOPLE: F. MOUTON (FMOUTON@CSIR.CO.ZA)

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

CONTENTS

PROBLEM STATEMENT

Android is becoming much more prominent in the mobile phone market. Specifically in South Africa it is suspected that about 700,000 android devices are being used. It is mostly the corporate individual or the more upper class communities that have access to these Smartphone devices. They are also the individuals who are most likely to sit in a big corporate meeting where extremely sensitive data can be discussed. It is for these reasons that it has been identified that mobile malware which perform eavesdropping on their phones could cause sensitive data to be easily leaked out.

This project consists of two unique parts, the eavesdropping malware and the protection against this eavesdropping malware. It is required to develop both parts of this project, as it will be much better to demonstrate the defensive software against actual malicious tools.

This project will also make use of a new technology called NFC (Near Field Communication) which is found in most of the mobile phones released during 2012. Tectiles is a NFC application which already has some of the features that this project requires and a demonstration of this can be provided to the group. More information on Tectiles can be found on http://www.samsung.com/us/microsite/tectile/.

OBJECTIVES

The task consists of two main objectives:

- NFC for meeting rooms: Upon entering a meeting room, a person should be able to tap his phone on a NFC tag which should control whether or not he's allowed in the meeting, log his presence at the meeting, turn his mobile device on silent and switch off its WiFi and GSM in order to prevent eavesdropping malware. Upon exiting the meeting room, the person should be able to tap his phone on the NFC tag again in order to restore the device as it was.
  Summarised:
  - Develop a mobile application for android devices
  - The mobile application must have NFC functionality
  - The device will be tapped on a NFC tag at the door of the meeting room
  - The NFC tag will instruct the device to go into silent mode, turn off the Wi-Fi and turn off the GSM communication
  - Upon tapping the NFC tag the mobile device must also perform access control to the meeting by checking in to a centralized server
  - After performing access control, presence at the meeting should be logged on the server
  - After the meeting has been concluded, the participant needs to tap his device on the NFC tag
  - Upon exit the NFC tag will restore all functionality to the device as well as checking out of the centralised server.
- Voice recording and transmission malware: Create a malware application which should be activated by SMS which makes voice recordings and sends it to someone via email.
  Summarised:
  - The malware should be dormant on the phone until it is activated by an attacker
  - The activation of the malware should occur via SMS
  - The SMS should be intercepted by the application and must not be displayed to the victim
  - Upon receiving the SMS, voice recording clips should be taken by the mobile device
  - In order to keep the voice recordings small, the recorded audio must be sent to the attacker at certain time intervals

    - The voice recordings should be sent via e-mail
    - The attacker should be able to disable the malware via SMS
- The web server application: This can also be seen as the central server where all the mobile phone data is logged to.
    - User friendly GUI
    - Displaying on the GUI the list of individuals who attended the meeting

TECHNICAL REQUIREMENTS

- The developed mobile application should include the following:
    - NFC communication
    - NFC tag programming
    - Interaction with the Wi-Fi and GSM when tapping the NFC tag
    - Interaction with the silent mode functionality when tapping the NFC tag
    - Checking in and out to a centralised server
    - Logging presence on the server
- The developed mobile malware should include the following:
    - Covert SMS interception
    - Covert voice recording
    - Covert e-mailing of the voice recording
- The developed web server application should include the following:
    - User friendly GUI
    - Displaying on the GUI the list of individuals who attended the meeting

SIMPLISTIC ACCESS CONTROL OF WHO IS ALLOWED IN THE MEETING WITH THE GUIEXPECTED SCOPE (17)

The maximum score for the scope of the projects proposed by the CSIR is 20. Each of the expected scope fields can be scored to a maximum of 5.

COMPUTER SCIENCE DOMAIN **(5)**

This project focuses on several domains covered by computer science. The focus of this project is in the mobile development and computer networking domain of computer science.

Due to the complexity of the network communication that is required for this project as well as the complex mobile development required in this project, this project is worthy of a score of 5 for the complexity in the computer science domain.

PROGRAMMING **(4)**

The programming behind this project will be fairly complex. The phone application requires to be deployed only on an android platform and it is not required to be cross-platform. This project requires both malware and defensive software to be written. The programming difficulties of both of these tasks are very similar and thus a programming difficulty of 4 has been specified.

SOFTWARE ENGINEERING **(3)**

As this project is developed for the CSIR, as a client, it is required that the software goes through the entire software lifecycle development process. It is very important that the entire software lifecycle is well developed. It is expected at the end of the project that the team is able to present the information gained through the project to staff at the CSIR. The entire software package which will be developed must also be easily deployable by the CSIR. All the source code must also be provided to the CSIR to be used for research purposes.

RESEARCH **(5)**

This project has an extensive research element. The main research area for this project is in both the NFC communication and the malware which has to be developed. The team may be required to provide the client with the research that has been performed in order to establish the NFC communication and to deploy the malware.

ADMINISTRATIVE INFORMATION

The team is welcome to contact Francois Mouton directly for more information on this project. He prefers to only be contacted by email. His email address is:

Email: fmouton@csir.co.za

REQUIRED DELIVERABLES

The final deliverable of the project must have the following features:

- The developed mobile application should include the following:
  - NFC communication
  - NFC tag programming features
  - Automatic disabling of Wi-Fi and GSM when tapping the NFC tag
  - Automatically turning the mobile device to silent mode when tapping the NFC tag
  - Automatically restore settings on the mobile device when existing the meeting and tapping the NFC tag
  - Automatic check in to the centralised server when tapping the NFC tag
  - Automatic check out from the centralised server when tapping the NFC tag
- The developed mobile malware should include the following:
  - Covert SMS interception
  - Covert voice recording
  - Covert e-mailing of the voice recording
- The developed web server application should include the following:
  - User friendly GUI
  - The ability to check who was present in the meeting
  - The ability to specify who should have access to the meeting

The team is also allowed to suggest any additional functionality to both the mobile application and the web application. Any additional functionality will be seen as bonus features and will be examined to such an extent.

SUBMISSION SCHEDULE AND IMPORTANT DATES

The submission schedule will coincide with the dates as is published later on in the COS 301 study guide.

A successful prototype for the Iteration 1 is deemed to at least already have the following features:

- Iteration 1:
    - Prototype of the web server application to demonstrate the user management
    - Simplistic voice recording on mobile phone
    - Basic NFC tag communication
- Iteration 2, 3 and 4: This will be confirmed during the first meeting with the client

CLIENT COMMITMENTS

At least one of the clients will be available, depending on the project's requirements, for consultation. Consultation will take place at the CSIR campus during core business hours, 8 am to 4 pm. Scheduling of meetings is left to the students, but bear in mind that both clients of the project are full time employees and cannot attend meetings on short notice.

The client does however request a meeting with the students one week before or after each of the student's major demos.

Any further requirements from students can be negotiated during contact sessions.