Preventing Sensitive Data Being Shared With 3rd Party Servers

Initial Plan

Jake Williamson – C1433282

Supervisor: *Eirini Anthi*
Moderator: *George Theodorakopoulos*
Module: *CM3203*
Module Title: *One Semester Individual Project*
Credits: *40*

1 The Problem

Gibler showed that [1] almost 10% of *Android* applications, from a pool of 24,350 applications, forward sensitive user data to third party servers. This data includes information that can personally identify a user, such as: phone information, GPS location, WiFi data, and audio recorded with the microphone. Even though each application explicitly states what data is going to be taken, it is not clear to a user how the data will be used, or who it will be sent to.

Furthermore, a study by Boyels et al. [2] showed that 54% of app users decided to not install an app when they discovered how much personal information they had to share to use the app. Also, 30% of users uninstalled an app that was already installed on their phone, when they learned it was collecting personal information that they did not want to share.

Finally, due to the high percentage of apps sharing identifiable information, and identity theft increasing in the UK [3], this project will design and develop a mobile application that will inform users if their data is being shared, and who it is being shared with.

To combat these issues, I will be designing, and developing, an application that will can monitor a phone's network traffic and alerting the user if the data is going to a third-party server. If the application detects that sensitive data is being shared, then the user will have the option to block the connection to that server, preventing personal information from being shared.

2 Project Description

This application will monitor all outgoing network connections and analyse each packet to see if it contains any information that goes to a third-party server. If the application detects that information is being shared, the user will be notified, and will be asked whether they want this information to be sent, or if they want to stop it from being sent. If the user decides to allow the data, then the application will allow the packet to continue as normal. If the user decides to stop the data being sent, then the application will block that packet. This will require the application to be able to monitor the operating system's network card, so that it can determine what information is being sent.

This application is initially going to be made for *Android* devices, due to the open-source nature of the operating system. Also, I do not have access to an iPhone that can be used for testing the application. However, if time permits and Cardiff University can provide a suitable environment, the application will be extended to work on *iOS* devices as well. By doing this, the project will cover a greater number of users. Furthermore, if time permits, the user should have

the option of selecting which installed applications this application monitors

3 Project Objectives

The objectives for this project have been separated into "essential" and "time-permitting." The essential objectives are those that need to be implemented in the working application, whereas the time-permitting objectives will only be implemented if there is time at the end of the project.

3.1 Essential Objectives

- Application will be developed for a mobile platform
- Application will be able to monitor outgoing network traffic
- The user must be able to turn this application on and off
- Alert the user when personal information is being shared with third-party servers
- Provide an option to the user to block or allow this information
- Test the application and its usability with real-world applications

3.2 Time-Permitting Objectives

- Extend the application to work with *iOS* devices
- Allow the user to select which apps to monitor

4 Work Plan

Frequent discussions with my project supervisor and their feedback, will inevitably cause the plan to change as the project progresses; taking this into consideration, an Agile approach is being taken to allow me to adapt to these changes as they occur. Testing of this project will be carried out on an ongoing basis, to ensure that all the requirements are met

There are going to be two main deliverables for this project:

- Final report
- Fully developed application

Week 2 – Preparation

- Set up development environment and version control system
- Write up the justification for my chosen tools

Milestone: All preparation done

Week 3 - Week 7 – Backend Implementation

- Able to capture all network packages
- Decrypt all decryptable data
- Create regex for sensitive data
- Implement algorithm to check regex against data
- Write up the justification for how I implemented the backend
- Book meeting with project supervisor for 1^{st} March 2018

Milestone: Backend implemented
Milestone: First major review with supervisor done

Week 8 - halfway through Easter break – Frontend Implementation

- Design all aspects of user interface
- Implement user interface
- Write up the justification for how I implemented the frontend

Milestone: Frontend implemented

Remainder of Easter break - Week 10 – Testing and Report Writing

- Testing the completed application in a real-world scenario
- Compile report using write-ups from other weeks
- Proof-read report
- Book meeting with project supervisor for 18^{th} April 2018

Milestone: All testing completed
Milestone: Report completed, and proof read
Milestone: Second major review with supervisor done

Week 11 – Submit Report

- Ensure project is ready for submission
- Submit report and implementation

Milestone: Report submitted
Deliverable: Report
Deliverable: Application

From the plan above, 8 notable milestones have been identified:

- End of week 2: All preparation done
- 1^{st} March 2018: First major review with supervisor done
- End of week 7: Backend implemented
- Halfway through Easter break: Frontend implemented
- End of Easter break: All testing done
- 18^{th} April 2018: Second major review with supervisor done
- End of week 10: Report completed, and proof read
- End of week 11: Report submitted

Task ID	Description	05/02/2018 Week 2	12/02/2018 Week 3	19/02/2018 Week 4	26/02/2018 Week 5	05/03/2018 Week 6	12/03/2018 Week 7	19/03/2018 Week 8	26/03/2018 - 13/04/2018 Easter Break	16/04/2018 Week 9	23/04/2018 Week 10	30/04/2018 Week 11	07/05/2018 Week 12	11/05/2018 Deadline
1	**Preparation**													
1.1	Set up development environment, version control system, and required devices													
1.1.1	Write-up for report: justification for chosen tools													
1.2	Ethics Research													
1.2.1	Apply for ethical approval (if required)													
1.2.2	Write-up for report: justification for ethical approval required													
2	**Backend Implementation**													
2.1	Able to capture all network packets													
2.2	Decrypt all decryptable data													
2.3	Create Regex for sensitive data													
2.4	Implement algorithm to check regex against data													
2.5	Write-up for report: justification regarding backend implementation													
3	**Frontend Implementation**													
3.1	Design all aspects of user interface													
3.2	Implement user interface													
3.3	Write-up for report: justification regarding design of frontend													
4	**Testing**													
4.1	Ongoing testing whilst implementing code													
4.2	User testing with a completed system													
5	**Build report**													
6	**Submit report**													
7	**Supervisor meeting 1**													
8	**Supervisor meeting 2**													

5 References

[1] C. Gibler, J. Crussell, J. Erickson and H. Chen, "AndroidLeaks: Automatically Detecting Potential Privacy Leaks in Android Applications on a Large Scale", *Trust and Trustworthy Computing*, pp. 291-307, 2012.

[2] J. Boyles, A. Smith and M. Madden, "Privacy and Data Management on Mobile Devices", *Pew Research Center: Internet, Science & Tech*, 2012. [Online]. Available: http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/. [Accessed: 31- Jan- 2018].

[3] R. Jones, "Identity fraud reaching epidemic levels, new figures show", *The Guardian*, 2017. [Online]. Available: https://www.theguardian.com/money/2017/aug/23/identity-fraud-figures-cifas-theft. [Accessed: 31- Jan- 2018].