Recruitment of Volunteers for Research Project

“Implicit User Authentication on Mobile Devices”

Magnum Lab @ Virginia Tech

Purpose of Study

The project is intended to implement and test a system that authenticates users of mobile devices based on user behavior (usage of the device). The main benefit of such system is added security of the user private data stored on the device with no explicit interaction from the users.

For this phase of this research project, it is needed to collect as much information as possible regarding how different users use their mobile devices to build user behavior patterns, to be used in training and testing the authentication system.

Study Procedure

The participant is requested to:

1. **Download and install** the logger application from the Google Play store on his/her Android mobile device
2. **Allow automatic updates** to receive any application updates and bug fixes once released
3. **Launch the application for the first time** once installed (The application won’t run until the user explicitly start it for the first time)
4. **Select three random points** on the map screen of the application (only one time). Please note that if you are not connected to the Internet, the map won’t display, but you can still press any three random points on the gray screen displayed.
5. **Allow the application to run in the background** collecting the required data without any kind of interruption (e.g. force stop, uninstall, or clear data) for a period of at least 6 months
6. **Enable Wi-Fi connection** to the Internet when possible to upload collected data to server
7. Restart the application (by clicking the application icon), in the unlikely cases of application crashes (i.e. if the alert message “Unfortunately, Logger has stopped …” appears)

The participant has the right to uninstall the application from the device at any time, if he/she is not willing to participate in the project anymore. However, all data that has already been uploaded to the server cannot be identified, and hence cannot be erased.

All data will be collected anonymously into a SQLite database file and saved automatically to a secure server. Each device will generate its own random ID that cannot be traced back to the user. In addition, any identifying data, such as phone numbers, email addresses, and URLs will be encrypted locally (hashed and salted on the user device before being sent to the server), in a way that cannot be reverse engineered to the original data. Location is calculated relative to the initially selected points (Points selected on the user device and never sent to the remote server).

All connections to the server will be initiated only when the device is connected to the Internet through a Wi-Fi network (in order not to cost the user any mobile data fees).

Please note that the *anonymous* data collected will be made available publically for related and similar research purposes. Again, the data is collected anonymously in a way that cannot be reverse engineered to identify the sending device or the owner.

The data to be collected include:

- Wi-Fi connections (only encrypted BSSIDs of networks stored)
- Location relative to initially selected points.
- Phone modes (e.g. silent, ringing, vibration, airplane)
- Battery levels and power connections
- Information about accessed mobile networks and cells
- Application installed, removed, and accessed
- Devices connected via Bluetooth, HDMI, USB, and docking
- Bluetooth adapter changes (e.g. enabled, disabled)
- Encrypted visited URLs
- Encrypted source and destination of incoming and outgoing calls, and call durations
- Encrypted source and destination of numbers contacted via SMS/MMS
- Encrypted email addresses of sent and received email messages
- Encrypted names of accessed files

Please note that the permission list of the application on the Google Play Store does not represent the actual functionality of the application. For example, the application will not read, edit, or send text messages. As described above, the application only keeps record of numbers (encrypted) contacted via SMS/MMS, but the permissions required for that are the same permissions required to read, edit, and send messages.

Contact Information

For any more details or inquiries, please feel free to contact:

Amr Abed, PhD Student
Electrical and Computer Engineering Department
Virginia Tech
Durham 369
amrabed@vt.edu
+1-540-4four9-333six