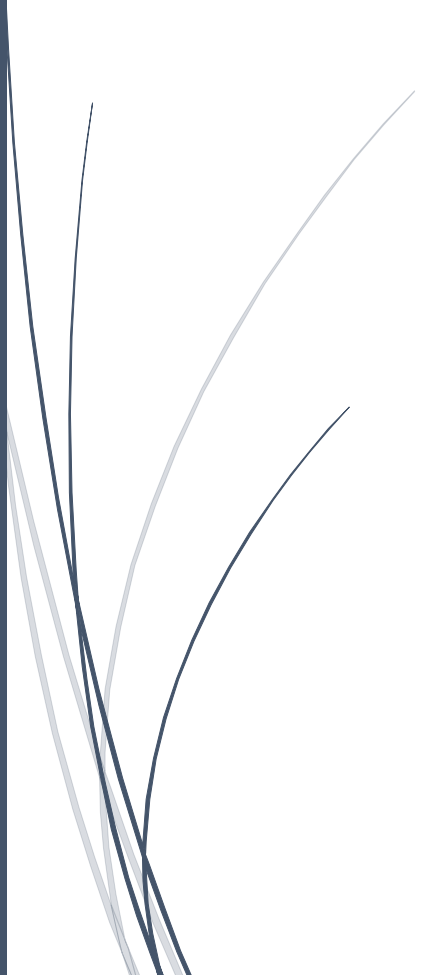
Exploration and analysis of smartphone Wi-Fi and Bluetooth data.

By: Eirini Sofia Anthi, Supervisor: George Theodorakopoulos



Cardiff University 2016

Background/The problem

In the last decade the amount of smartphone users has increased dramatically [1]. Smartphones are internet-enabled devices, with an operation system (iOS, Android, Windows), in which they can run various applications. Usually they are also equipped with voice control functionality, a Wi-Fi antenna, Bluetooth, and GPS [4]. People not only use their smartphones to communicate, but they also use them to help perform everyday important life activities, from researching a health condition to accessing educational resources and managing their money [2]. As a result, many security issues related to smartphones have arisen including: data leakage, unintentional disclosure of data, attacks on decommissioned smartphones, spyware attacks etc. [3].

According to ENISA (European Union Agency for Network and Information Security), the number one threat is data leakage [3]. Data leakage can happen in various ways. One way is when the smartphone is stolen or lost and its memory or removable media are unprotected, allowing an attacker to access the data stored on it [3]. Additionally, most of the applications used on a smartphone, will require the user to allow them to access and change their privacy settings and even share sensitive information with third parties. Researches have proven that during these processes, there is a significant percentage of data leak [5]. Finally, there is data loss that can happen when the smartphone is connected to the Wi-Fi or Bluetooth, and in this case we refer to possible unencrypted or badly encrypted data that gets transmitted [6].

Project description

The purpose of this project is to examine in depth the data leakage that happens in the background, when the mobile is connected to the Wi-Fi or Bluetooth and discover further possible vulnerability issues. Using various techniques and tools, we will try to sniff the data that gets broadcasted from the phone, when specific applications that use sensitive data or not, are running. More specifically to sniff the Wi-Fi packets, we can use the following methods [7]:

- **For Android phones**: We can root the phone and then use *Shark for root* app, which will install *tcpdump* and allow us to start capturing packets. Additionally, there is the *Android PCAP from Kismet app,* which uses the USB OTG interface to support packet capture without requiring root. Last but not least, there is the *tPacketCapture* that uses the Android VPN service to intercept packets and capture them.
- **For iOS phones:** There is mainly available a remote virtual interface (RVI) facility that allow us to use Mac OS X packet trace programs to capture traces from an iOS device.
- **For all the phones:** We can set up the PC as a *wireless access point*, then run *wireshark* on it, or use a capture device that can sniff Wi-Fi. The advantage with it is that it can also give us *802.11x header,* but it can miss some packages.
- **Capture using a VPN server**: We can set up a VPN server using OpenVPN. Then we can route the traffic through the server by setting up the mobile device as a VPN client and capture the traffic on the server end.

On the other hand, to track and decrypt the data transmitted via Bluetooth, the most accurate and effective way seems to be just one and this involves the usage of UbertoothOne device and Kali Linux [8].

Afterwards we will analyse the collected data and try to see if any of it was unencrypted. We will also analyse the kind of encryption that has been used on the encrypted data that was broadcasted. This way we can check how secure the data is.

These processes will be performed in both android and iOS devices. As they have different operation system, it is expected that there will be different kinds of data that gets leaked, therefore it would be interesting to compare the results. Additionally, for both types of smartphones, more than one method to sniff the data will be used, to ensure that the observations are as accurate as possible.

Aims and Objectives

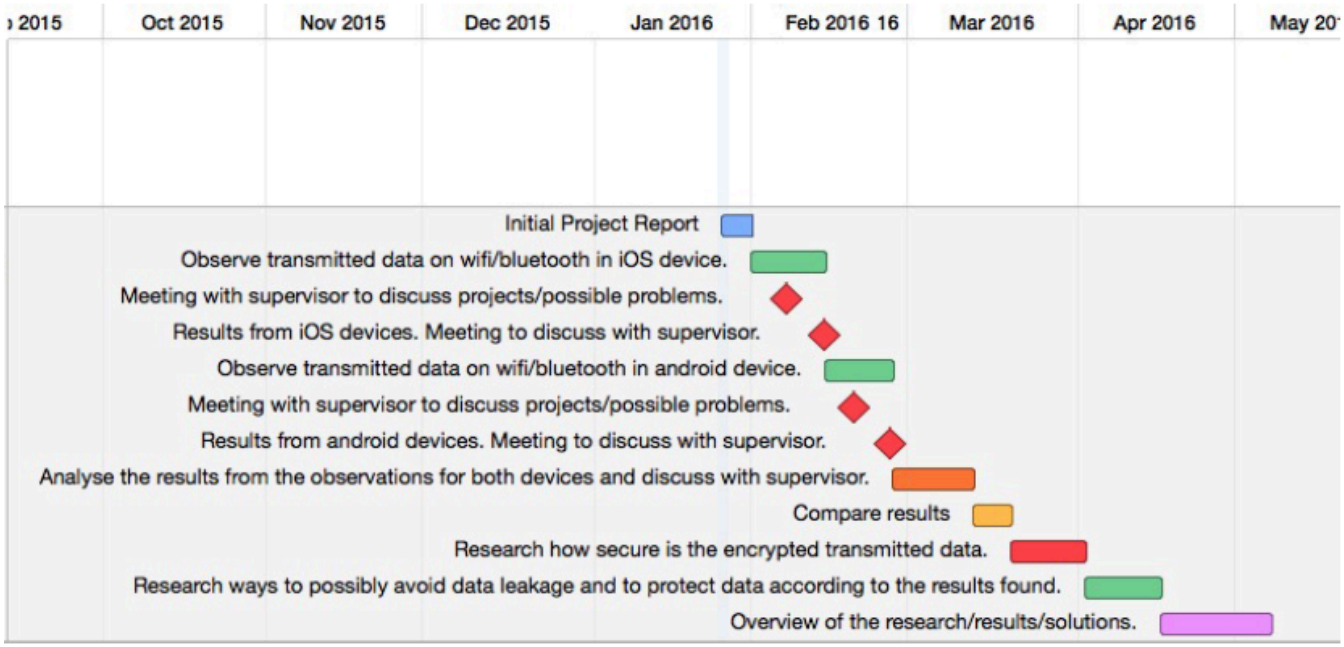
The project aims to research the data leakage security issue on smartphones, that happens when they are connected to Wi-Fi or Bluetooth.

The objectives are:

- To observe the transmitted data, using a variety of methods in both android and iOS.
- To analyse the type of data that was broadcasted and identify any unencrypted sensitive information.
- To analyse the encryption methods used on the encrypted data that was transmitted.
- To determine how secure is the encrypted data.
- To possibly research methods to protect sensitive data while its transmitted.

Work Plan

A detailed work plan, including arranged meetings with the supervisor to discuss progress and possible problems, can be found in the timeline below:



Resources

[1]I. Lunden, "6.1B Smartphone Users Globally By 2020, Overtaking Basic Fixed Phone Subscriptions", *TechCrunch*, 2016. [Online]. Available: http://techcrunch.com/2015/06/02/6-1b-smartphone-users-globally-by-2020-overtaking-basic-fixed-phone-subscriptions/#.frs3oqh:RPIH. [Accessed: 25- Jan- 2016].

[2]A. Smith, "U.S. Smartphone Use in 2015", *Pew Research Center: Internet, Science & Tech*, 2015. [Online]. Available: http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/. [Accessed: 25- Jan- 2016].

[3] Enisa.europa.eu, "Data leakage resulting from device loss or theft — ENISA", 2016. [Online]. Available: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks/data-leakage-resulting-from-device-loss-or-theft. [Accessed: 25- Jan- 2016].

[4]B. Gerneglia, "The Rise of Smartphones and Related Security Issues", *Ciozone.com*, 2016. [Online]. Available: http://www.ciozone.com/index.php/Security/The-Rise-of-Smartphones-and-Related-Security-Issues.html. [Accessed: 25- Jan- 2016].

[5]A. Kingsley-Hughes, "99.7% of all Android smartphones vulnerable to serious data leakage | ZDNet", *ZDNet*, 2011. [Online]. Available: http://www.zdnet.com/article/99-7-of-all-android-smartphones-vulnerable-to-serious-data-leakage/. [Accessed: 26- Jan- 2016].

[6]M. Cooney, "10 common mobile security problems to attack", *PCWorld*, 2016. [Online]. Available: http://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html. [Accessed: 26- Jan- 2016].

[7]C. wireshark, "Capturing mobile phone traffic on wireshark", *Stackoverflow.com*, 2016. [Online]. Available: http://stackoverflow.com/questions/9555403/capturing-mobile-phone-traffic-on-wireshark. [Accessed: 31- Jan- 2016].

[8]N. Kraljevic, "Now I wanna sniff some Bluetooth: Sniffing and Cracking Bluetooth with the UbertoothOne", *The Security Sleuth*, 2015. [Online]. Available: http://www.security-sleuth.com/sleuth-blog/2015/9/6/now-i-wanna-sniff-some-bluetooth-sniffing-and-cracking-bluetooth-with-the-ubertoothone. [Accessed: 31- Jan- 2016].