Research Paper Proposal

Mobile Security

Mobiles have become an increasing target for hackers for adversaries. In this age, when the security for computers by itself poses new risks every day and with more information being collected from the users by social networking sites, companies for recruitments, positional information collected to calculate routes, etc. These devices serve as a perfect point of entry to manipulate user’s information.

Different security counter-measures are being developed and applied to smartphones, from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable apps.

Smartphone users in particular are vulnerable to the following:

There are three prime targets for attackers:

* **Data**: smartphones are devices for data management, therefore they may contain sensitive data like credit card numbers, authentication information, private information, activity logs (calendar, call logs);
* **Identity**: smartphones are highly customizable, so the device or its contents are associated with a specific person. For example, every mobile device can transmit information related to the owner of the mobile phone contract, and an attacker may want to steal the identity of the owner of a smartphone to commit other offenses;
* **Availability**: by attacking a smartphone you can limit access to it and deprive the owner of the service..

The sources of these attacks are the same actors found in the non-mobile computing space:

* **Professionals**, whether commercial or military, who focus on the three targets mentioned above. They steal sensitive data from the general public, as well as undertake industrial espionage. They will also use the identity of those attacked to achieve other attacks;
* **Thieves** who want to gain income through data or identities they have stolen. The thieves will attack many people to increase their potential income;
* **Black hat hackers** who specifically attack availability.[[3]](http://en.wikipedia.org/wiki/Mobile_security#cite_note-3) Their goal is to develop viruses, and cause damage to the device.[[4]](http://en.wikipedia.org/wiki/Mobile_security#cite_note-4) In some cases, hackers have an interest in stealing data on devices.
* **Grey hat hackers** who reveal vulnerabilities.[[5]](http://en.wikipedia.org/wiki/Mobile_security#cite_note-5) Their goal is to expose vulnerabilities of the device.[[6]](http://en.wikipedia.org/wiki/Mobile_security#cite_note-6) Grey hat hackers do not intend on damaging the device or stealing data.

**(Source: Wikipedia)**

This paper is to de-mystify and provide a crystal clear explanation of the actual threats and risks and the security systems in use, with specific emphasis on the android operating systems, and the measures taken to thwart the threats. It attempts to show the reader the level of security measures which are already in use, and which ones are effective and how to improve on it.

The sources for this paper are:

1. The first paper gives an idea about the current state of affairs of phones with advanced operating systems. This is where the foundation for most of the paper will be set.

**Mobile Security Catching Up?**

Revealing the Nuts and Bolts of the Security of Mobile Devices

Michael Becher, Felix C. Freiling

University of Mannheim, Germany

Johannes Hoffmann, Thorsten Holz, Sebastian Uellenbeck, Christopher Wolf

Horst G¨ortz Institute (HGI)

Ruhr-University Bochum, Germany

1. This paper gives a more in depth view about the current state of the art security systems, and discusses in depth about the concepts and challenges in mobile security.

**Emerging Security Technologies for Mobile User Accesses**

Nirav Jobanputra, Vijayendra Kulkarni, Dinkar Rao, and Jerry Gao, Ph.D.

San Jose State University, email: [jerrygao@email.sjsu.edu](mailto:jerrygao@email.sjsu.edu)

1. Investigation about the concepts and more detail about the framework around which modern security systems are built is given in this paper:

**A Hierarchical FrameworkModel of Mobile Security**

Jun-Zhao Sun, Douglas Howie, Antti Koivisto, and Jaakko Sauvola

MediaTeam Oulu, MVMP, Infotech Oulu

Tutkijantie 2 B, FIN-90570 University of Oulu, Finland

Further papers that will be used include:

**WIRELESS HOME SECURITY SYSTEM WITH MOBILE**

Prof. (Dr.) Khanna SamratVivekanand Omprakash

Address for Correspondence

Information Technology Dept, ISTAR, Sardar Patel University, VVNagar, India

**Mobile Phone Threats**

HITBSecConf2005, Kuala Lumpur, Malaysia

Mikko Hypponen , Chief Research Officer F-Secure

Security Comparison of Mobile OSes

Arto Kettula

Helsinki University of Technology

Telecommunications Software and Multimedia Laboratory

Kernel-Level Interception and

Applications on Mobile Devices

Michael Becher and Ralf Hund

Department of Computer Science, University of Mannheim, Germany