Vitamin C for your Smartphone: The SKIMS Approach for Cooperative and Lightweight Security at Mobiles

Matthias Wählisch*, Sebastian Trapp*, Jochen Schiller*, Benjamin Jochheim†,
Theodor Nolte†, Thomas C. Schmidt†, Osman Ugus†, Dirk Westhoff†, Martin Kutscher‡,
Matthias Küster‡, Christian Keil◇, Jochen Schönfelder◇
*Institut für Informatik, Freie Universität Berlin, Berlin, Germany
†Dept. Informatik, Hamburg University of Applied Sciences, Hamburg, Germany
‡escrypt GmbH, Bochum, Germany
◇DFN-CERT Services GmbH, Hamburg, Germany
{first.last}@fu-berlin.de, {first.last}@haw-hamburg.de, {first.last}@escrypt.com, {last}@dfn-cert.de

ABSTRACT

Smartphones are popular attack targets, but usually too weak in applying common protection concepts. SKIMS designs and implements a cooperative, cross-layer security system for mobile devices. Detection mechanisms as well as a proactive and reactive defense of attacks are core components of this project. In this demo, we show a comprehensive proof-of-concept of our approaches, which include entropy-based malware detection, a mobile honeypot, and spontaneous, socio-inspired trust establishment.

Categories and Subject Descriptors

C.2.0 [**Computer-Comm. Networks**]: General—*Security and protection (e.g., firewalls)*

General Terms

Security

Keywords

Mobile security, malware detection, mobile honeypot, ad hoc trust

1. INTRODUCTION

Mobile, wireless-based end devices represent a significant part of our current networks, both with respect to the number of deployed equipment and their economic impact. Limited hardware resources and the per se unprotected transmission medium air turn such devices into attractive targets for attacks. These are additionally motivated because handhelds commonly store or exchange confidential data (e.g., calendar, contact lists).

In contrast to wired end systems, mobile devices exhibit three characteristic differences: (a) they normally are equipped with several different network interfaces; (b) their capabilities are significantly limited, so that they are not able to permanently maintain strong protection mechanisms; (c) physical vicinity with the help of appropriate access technologies allow for the establishment of separate, cooperative delivery structures. Mobile end devices, thus, need a lightweight, environment-adaptive protection mechanism that exploits the heterogeneous technologies available on-board.

In this demo, we present SKIMS, a digital immune system for smartphones. Similar to the biological immune system, our framework tries to protect the mobile device on its own. In cases where this is insufficient, cooperation between neighbors is established. For the detection and defense, SKIMS is guided by the principles of infrastructureless and lightweight approaches.

From a general perspective, we demonstrate a user-friendly security system that independently estimates apparent and existing threats. From a detailed perspective, we show (1) entropy-based malware detection for zero-day shellcode, (2) a mobile honeypot, (3) socio-inspired trust-establishment for reliable ad hoc communication to protect the mobile, and (4) secure data distribution using fountain coding.

SIGCOMM'12, August 13–17, 2012, Helsinki, Finland.
ACM 978-1-4503-1419-0/12/08.

2. SKIMS IN A NUTSHELL

The SKIMS protection system consists of multiple components that allow for detection as well as proactive and reactive defense of attacks. These are controlled by the mobile sandbox. Mobiles are consumer devices. We therefore hide most of the inherent complexity from the end user.

Detection—Malware Identification We employ a statistical analysis of the information content obtained from network streams to detect potential anomalies in real-time. Unlike previous work, our time-frequency analysis extracts the non-stationary properties of entropy signals. From this context-adaptive technique, we obtain a clear signature of binary instructions and can also detect embedded shellcode. Preliminary details of our approach are sketched in [2].

Detection—Mobile Honeypot A low-interaction honeypot collects suspicious connections. It emulates multiple network services (FTP, POP3, etc.) and collects valuable information from the observed attacks. It allows for universal deployment on mobiles as well as on common Linux systems, which enables a comprehensive analysis of attacks on multiple platforms.

Defense—Ad hoc Trust Establishment This component evaluates spontaneous trust between peers to establish reliable ad hoc communication. Compared to other approaches, our scheme [3] applies only data inherent at mobiles and does not require any central component. Using a commutative encryption protocol two peers exchange their address books in a privacy-friendly way and find mutual contacts without

(a) SKIMS GUI reduces complexity and presents different threat levels and details in a user-friendly way

(b) Demonstrator with mobiles and control screen

Figure 1: Deployment and demonstration of the SKIMS application

revealing different entries. Mutual entries will be weighted locally using data from communication logs [4]. An overall, transitive trust value is derived from sociological principles (tie strengths).

Defense—Secure Data Transmission This component allows for a secure and reliable data broadcast between the mobiles. It is achieved by adapting the techniques which are originally proposed in [1] to mobile devices. The communication is based on fountain coding to increase the efficiency in places where the connectivity is unreliable due to high amount of wireless interferences. It enables the encrypted distribution of any kind of data such as security logs and programs to adjacent mobile devices running the SKIMS app.

Controlling—SKIMS App Each component for detection reports its current threat level to the SKIMS app, which calculates an overall state. Depending on the severity, the SKIMS app activates autonomously defense strategies or interacts with the end user.

A core design objective while developing the SKIMS app was the lightweight integration and interaction of the different building blocks. We implemented the internal signaling based on a content provider.

3. DEMONSTRATION

Setup An attendee can test all SKIMS components, either by itself or in combination. A typical procedure is the following: The user starts with the threat level "no attacks" (green) and may choose to download an uninfected or malicious file via a QR code. The user observes the live entropy analysis. In case of embedded malware, the SKIMS app switches to yellow. From an external PC we emulate an attack by connecting to the mobile and poke the local file system. This is handled by the mobile honeypot, which changes the current state to red. The user is asked to cancel its current Internet connection and to establish an ad hoc link. The SKIMS app visualizes the spontaneous trust calculation with an adjacent mobile.

On-Site Requirements For our demonstration, we will need a connection for power supply and a table. An Internet connection is not required. We will bring an access point, a notebook, multiple Android smartphones, and a tablet, which will communicate among each other via 802.11.

Acknowledgements

We would like to thank the students who helped in the implementation and testing of the SKIMS application. This work is supported by the German BMBF within the project SKIMS (http://skims.realmv6.org).

4. REFERENCES

[1] Bohli, J. M., Westhoff, D., Hessler, A., and Ugus, O. Security Enhanced Multi-Hop over the Air Re-programming with Fountain Codes. In *Proc. of the 34th IEEE LCN. 4th IEEE International Workshop on Practical Issues in Building Sensor Network Applications (SenseApp)* (Piscataway, NJ, USA, October 2009), IEEE Press.

[2] Schmidt, T. C., Wählisch, M., Jochheim, B., and Gröning, M. WiSec 2011 Poster: Context-adaptive Entropy Analysis as a Lightweight Detector of Zero-day Shellcode Intrusion for Mobiles. *ACM SIGMOBILE Mobile Computing and Communications Review (MC2R) 15*, 3 (July 2011), 47–48.

[3] Trapp, S., Wählisch, M., and Schiller, J. Short Paper: Can Your Phone Trust Your Friend Selection? In *Proc. of the 1st ACM CCS Workshop on Security and Privacy in Mobile Devices (SPSM)* (New York, 2011), ACM, pp. 69–74.

[4] Trapp, S., Wählisch, M., and Schiller, J. Bridge the Gap: Measuring and Analyzing Technical Data for Social Trust between Smartphones. Technical Report arXiv:1205.3068, Open Archive: arXiv.org, May 2012.