FORENSIC ANALYSIS OF M-BANKING APPS ON ANDROID PLATFORMS

RAJCHADA CHANAJITT 5738689 ITCY/M

M.Sc. (CYBERSECURITY AND INFORMATION ASSURANCE)

THESIS ADVISORY COMMITTEE: WANTANEE VIRIYASITAVAT, Ph.D., KIM-KWANG RAYMOND CHOO, Ph.D.

ABSTRACT

In technology advancement, smartphones play a crucial role and are in widespread use in the business and personal domains. Among the large number of available mobile apps and transactions made for such devices, mobile banking (i.e., m-banking) apps are one of the top app categories that are gaining popularity. Based on a study of mobile money trends in 2015, approximately 69% of mobile users from 15 countries carried out their banking activities via mobile devices. Even though most of these activities are balance checking, many banking institutions offer a mobile app which allows their customers to conveniently perform other banking activities (e.g., check deposit, money transfer) without having to be present at the bank branch office. Despite the available features, there has been increasing concern, especially, regarding insufficient security measures in the m-banking apps (i.e., roughly 10% of mobile users do not trust in m-banking app security.) Since these m-banking apps usually require and store sensitive customer data, the apps have become prime targets for criminals and this has led to a substantial increase in the likelihood of data breaches associated with the use of such apps. In addition to user private information, the record of banking transactions made through the m-banking apps may be stored on the device even after the user has closed the apps. While the amount and type of sensitive information stored and remaining on the mobile devices vary from one to another, the information about how much and how data is stored (or deleted) is not available to the users or public. It therefore becomes important to assess the security mechanisms of these m-banking apps and, more importantly, for users and developers to be aware of any critical security risks associated with the m-banking apps.

Among the m-banking apps available today, we focused on the apps developed for the Android platform partly because Android apps may be downloaded from websites where malicious apps usually reside. Due to these reasons, in this thesis, forensic taxonomy for m-banking apps was proposed for the collection and analysis of data from mobile devices that use m-banking apps. Guidelines to determine the security level of the m-banking apps in Thailand were used as an example to demonstrate how the guidelines may be used to assess mobile app security. In this study, m-banking apps from the seven financial institutions in Thailand were analyzed: (1) SCB EASY from the Siam Commercial Bank, (2) Krungsri from Bank of Ayudhya, (3) K-Mobile Banking from Kasikornbank, (4) Bualuang mBanking from Bangkok Bank, (5) MyMo from Government Savings Bank, (6) KTB netbank from Krung Thai Bank, and (7) TMB Touch from Thai Military Bank. All seven apps were installed on two different Android devices. Typical financial transactions, such as balance inquiry, money transfer, calendar, ATM/branch search location, and bill payment, were made on both devices for the duration of one month. Afterwards, the data in two devices were extracted both logically and physically through JTAG pins. The obtained data and image were then analyzed in order to assess the security performance of the seven m-banking apps. To be specific, we analyze the data stored and or remaining on the phone (either in the data folder, cache, or SD card) after the user had closed using the apps.

To the best of our knowledge, this thesis is the first study that proposes using forensic taxonomy to analyze the security level of the m-banking apps from the user's point of view. While this thesis emphasizes the forensic activity, it is our hope that the results presented in this thesis could raise concerns for both users to be aware of the potential impact of security and privacy of the m-banking apps and for the app developers to take into account the security issues during the design and testing phase to detect and resolve any security vulnerabilities before releasing the apps to the users.

KEY WORDS: ANDROID APP FORENSICS / PHYSICAL ACQUISITION PROCESS / ANDROID FORENSIC TAXONOMY / ANDROID APP REPACKAGING

98 pages