Analyzing privacy leakage from used electronic devices in second-hand market

Soheil Ehsani Banafati, Jay Ghurye, Kookjin Lee, and Doowon Kim
{jayg, klee, doowon}@cs.umd.edu

Overview: Privacy leakage from resold devices by extracting sensitive data is a growing threat as more users buy second-hand electronic devices. Due to [1], the used smartphone market is expected to grow from 53 million to 257 million units over the next 5 years. Many people may not be aware that their smartphones should be wiped out before selling it to another user. Even for users who are advised to use the built-in sanitization functions such as “Factory Reset” in Android to wipe out private and sensitive data in their mobile devices, the threat of privacy leakage exists. Those sanitization attempts could be unsuccessful due to unreliable deletion methods used, leaving sensitive information exposed [2]. Moreover, full-disk encryption could be compromised by an unreliable sanitization attempt. Therefore, we propose to address this problem through two phases: 1) user-behavior study on the second-hand smartphone market and 2) comprehensive study on sanitization process of mobile devices. In the first year, we will conduct the user-behavior study. A study on the sanitization functions of mobile devices will be conducted in the second year. In the final year, we will develop a new guideline to help users sanitize their devices and recommendations for mobile device vendors.

Intellectual Merit: Our proposed research aims to study users’ sanitization behaviors on their smartphones and the sanitization process of Android devices. First, we will investigate whether sellers know the necessity of wiping out their sensitive data before selling on market, and investigate on which sanitization methods (e.g., built-in factory reset) they rely. This can be achieved by collecting data through user survey. In the second study, we will explore Android’s built-in factory reset function. Many of previous researchers have focused on storage devices such as hard disk, and flash memory. In particular, they have studied data recovery from second-hand storages and secure sanitization of those storages. However, there have been little efforts on understanding data recover and sanitization process of Android mobile devices. The process of sanitization on Android devices will be better understood through this second study. Based on results from the two studies, we can develop a new framework to help users sanitize their personal sensitive data on smartphones.

Broader Impact: Hundreds of millions of devices are expected to be traded by 2018 [1]. Unfortunately, due to their remained sensitive personal data on devices, sellers of second hand electronic devices may hesitate trading their old devices. Moreover, people who want to sell their devices would be unwilling to use personal information-related services like online banking or healthcare. These can lead to slowing down innovations on mobile devices because of lack of mobile users. Our research will propose interventions which will help people securely sanitize personal data on their devices before trading. That increases participation of users in the second-hand device markets and make this market more transparent.

References: