C37 Unlocking Fingerprint Scanner-Enabled Mobile Phones

Christina A. Malone, MSFS, Defense Forensic Science Center, Forest Park, GA 30305; Anthony Koertner, MS, United States Army Criminal Investigation Laboratory, Forest Park, GA 30297; Seth M. Eisenberg, Army Educational Outreach Program, Forest Park, GA 30297; Hillary Lathrop, PhD, Defense Forensic Science Center, Forest Park, GA 30297*

Learning Overview: After attending this presentation, attendees will have an understanding of the efficiency and effectiveness of using recorded fingerprints to unlock fingerprint scanner-enabled mobile phones.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by demonstrating the benefits and limitations of a novel technique of using recorded fingerprints to unlock fingerprint scanner-enabled mobile phones.

This presentation, a research project conducted by the Office of the Chief Scientist (the Research, Development, Testing, and Evaluation arm of the Defense Forensic Science Center [DFSC]), focuses on the benefits and limitations of a novel technique of using recorded fingerprints to unlock fingerprint-scanner-enabled mobile phones.

Mobile devices are frequently submitted as evidence in digital forensic examinations. While law enforcement officials are required to secure a search warrant prior to the examination of mobile devices, there are often issues accessing locked phones even after a search warrant is obtained. While suspects may willingly provide a passcode to a locked mobile phone, there are also numerous occasions when a passcode is not provided (e.g., death, uncooperative suspect or victim, etc.). A suspect cannot be required to provide a passcode; however, to conduct a thorough digital forensic examination, it is imperative that examiners are able to access the mobile device's data in a timely fashion. While there are technologies that may assist an examiner in cracking the passcode, often such solutions are expensive and time-intensive. Furthermore, security features of mobile phones may erase data after failed passcode unlock attempts, so it is essential that an alternate method of unlocking a mobile phone is available.

Recently, several articles have demonstrated the possibility of unlocking fingerprint scanner-enabled mobile phones using printed images of fingerprints. A process using a standard inkjet printer combined with silver, conductive inks, and specialty paper can be used to generate a fingerprint capable of unlocking a mobile phone. While a technique has been roughly outlined and has been demonstrated, the success of this process requires further investigation in order to be standardized and employed with commercially available products for practical applications in a crime laboratory setting.

While the articles cite specific instances where mobile phones have been unlocked, recorded prints have not been used as a part of this process. Furthermore, the mobile phone itself may be host to a latent fingerprint, which could be imaged and used to unlock the phone. Within a criminal investigation laboratory, both of these sources of fingerprints have potential for assisting in a digital forensic examination.

Three fingerprint scanner-enabled mobile phones (Samsung™ S6 Edge+, Samsung™ Galaxy S7, and iPhone® 5S) were selected, based on their availability within the Documents & Digital Evidence Branch at the DFSC. A total of six subjects provided record prints (inked and LiveScan), and each participant enrolled his or her right and left thumb and index fingers in each of the mobile phones. Enrolled fingerprints were removed from each phone between participants. Three male and three female subjects were used to produce a sample set of fingerprints that varied in subtle differences in the ridges (e.g., thickness, widths, etc.). The variation among the donors was used to demonstrate the feasibility of the approach across multiple individuals in the general population.

The recorded prints were scanned and enhanced. An inkjet printer with silver, conductive inks was used to print the fingerprints on the appropriate specialty paper. Each printed fingerprint was used to attempt to unlock the mobile phones using various methods. Multiple image enhancements were also made to test the efficacy of the printed fingerprints. Each print was tested multiple times in a systematic manner to determine the repeatability of the technique. The results of each process were recorded and compared to illustrate the differences between participants, mobile devices, image enhancements, and application of the fingerprint to the scanner (heat and/or pressure).

The opinions or assertions contained herein are the private views of the author and are not to be construed as official or as reflecting the views of the Department of the Army (DA) or the Department of Defense (DoD). Names of commercial manufacturers or products included are incidental only, and inclusion does not imply endorsement by the authors, the DFSC, the United States Army Criminal Investigation Command, the Office of the Provost Marshal General (OPMG), the DA, or the DoD.

Unlocking, Mobile Phone, Fingerprint Scanner

*Presenting Author