C12 Fingerprint Replication Utilizing Latent Fingerprints for Conducting Forensic Analysis on Mobile Devices With Biometric Security

Joshua D. Sablatura, SHSU Digital Forensics, 2537 Pine Shadows Drive, Apt 434D, Huntsville, TX 77320; Robert McDown, BS*, Sam Houston State University, 1803 Avenue I, Huntsville, TX 77341; Jorn Chi-Chung Yu, PhD, Sam Houston State University, Dept of Forensic Science, Box 2525, Huntsville, TX 77341; and Lei Chen, PhD, Sam Houston State University, 1803 Avenue I, Huntsville, TX 77341*

After attending this presentation, attendees will have a better understanding of biometric security, specifically fingerprint recognition, in personal digital devices, a technical understanding of the device's specific operations, and of the means for circumventing the device's biometric security to conduct a digital forensics analysis.

This presentation will impact the forensic science community by providing a supplemental means to collect digital evidence from personal devices that are protected with biometric security systems. Current techniques for data extraction on mobile devices include brute forcing pin codes, software security bypass via custom boot-loader, and physical data extraction using a Joint Test Action Group (JTAG) connection; however, these methods are not always implementable under the following conditions: (1) the device allows a limited number of pin code entries before the device locks itself or wipes the data; (2) the operating system does not have a known security bypass; or, (3) the data on the device is encrypted rendering a physical data extraction useless.

The goal of this project is to develop techniques to visualize a latent print from the surface of a mobile device; this print can then be used to develop a mold that can reconstruct the user's print. After using fingerprint powders to lift a print from the device surface, a digital image of the print was created using either a scanner or camera. This image was imported into an image processing software package in order to use the color range selection tool to extract the print from the background. The threshold tool was then used to enhance the print's clarity from the background while converting the image to black and white.

After creating a viable image, a mold was created using either the Printed Circuit Board (PCB) or 3D printing method. Of these two methods, the PCB method is the low-tech, low-cost method to create the mold. This method involves printing the enhanced image with a laser-jet printer to a transfer medium. Using a heat source, the image is transferred from the transfer medium to a copper-clad board. Once the image has been transferred, ferric chloride is used to etch the excess copper from the board, leaving behind the copper concealed by the image transfer. The 3D printing method is more expensive due to the materials and equipment utilized. After the enhanced image is obtained, it must be extruded into a 3D image using a Computer-Aided Design (CAD) program. This is then printed with a 3D printer to create the mold. Using the mold created from either method, the fingerprint can then be reconstructed with a material that mimics the conductivity and pliability of human skin.

This study indicates that the use of gelatin, ballistics gel, and Elmer's® white glue are viable candidates that can be used in the process of reconstructing the fingerprint as each of these substances is recognized by the device's scanner. Currently, research is in progress to refine the methods used to create the molds and to enhance the extracted fingerprint image to produce a more accurate reproduction. This provides additional evidence, not present in the digital examination, but likely to be very useful in an investigation that includes mobile devices.

Biometric Security, Digital Forensics, Fingerprint Reconstruction