C21 Generating a Corpus of Mobile Forensic Images for Masquerading User Experimentation

Marc Brooks, MS, The MITRE Corporation, 7515 Colshire Drive, Mclean, VA 22102; Justin Grover, MS, The MITRE Corporation, 7515 Colshire Drive, Mclean, VA 22102; Mark D. Guido, MS, The MITRE Corporation, 7515 Colshire Drive, Mclean, VA 22102; Eric Katz, 2099 Malibu Drive, West Lafayette, IN 47906; Jared Ondricek, MS, The MITRE Corporation, 7515 Colshire Drive, Mclean, VA 22102; Marcus Rogers, PhD, Purdue University, 401 N Grant Street, West Lafayette, IN 47907; and Lauren Sharpe, MS, The MITRE Corporation, 7515 Colshire Drive, Mclean, VA 22102*

After attending this presentation, attendees will understand the research outcomes and results of a recently conducted experiment identifying masquerading users on mobile devices using traditional and mobile forensic techniques.

This presentation will impact the forensic science community by providing forensic investigators/researchers with an example of successful human subject experimentation used in support of forensic analysis.

Periodic Mobile Forensics is a research project investigating user behavioral measurement on mobile devices by applying both traditional and mobile forensics processes. Forensic techniques have been applied to an enterprise mobile infrastructure where a mobile on-device agent named TractorBeam was utilized. This agent periodically collects changed storage locations from each device to allow for later image reconstruction and analysis. TractorBeam operates silently in the background during the normal use of the device. TractorBeam provides its collected data periodically to an enterprise infrastructure, which consists of a cloud- or server-based queuing service, a relational database, an analytical framework for running forensic processes, and a Mongo database for storing the analytic output.

Collaborating with Purdue University, a three-month experiment was performed where TractorBeam's operation in a simulated operational setting to identify masquerading users (i.e., users operating the devices other than the enterprise designated mobile device user) was evaluated. It was surmised that even if a masquerading user on an enterprise mobile device lacked malicious intent; this masquerader would still be undesirable to the enterprise. A set of human-subject volunteers were provided with the following: preconfigured mobile devices with cellular voice and data plans, with the TractorBeam agent pre-installed; a simple acceptable-use policy; and deceptive project background information to stimulate normal behavior. TractorBeam transmitted encrypted incremental backups to an Amazon® Web Services cloud instance. In the relational database, redundant information within the collected data was deduplicated, resulting in a 50-times reduction in storage size of the images. Most of those images were rebuilt and a series of developed forensic processes were executed on them, resulting in a Mongo collection of extracted audit data. As a result of the experiment, enough data was collected to successfully reconstruct 821 forensic images, extract over one million audit events, and perform masquerading user analysis. This study characterizes the collected corpus, the extracted audit events, and the performance of TractorBeam throughout the protocol. For masquerading detection, a set of features from the collected audit data was produced and associated those features to user sessions, or periods of device usage. Those sessions and their associated features are being used to train and evaluate a set of classifiers. This analysis is in progress and will be documented in a future paper.

Mobile, Masquerading, Experiment