SAND2015-3458C

COIN Session

Mobile Forensics: Where Are You Going? Where Have You Been?

Paul Z. Cortez
Sandia National Laboratories

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Mobility in the Complex

Enterprise – BYOD – PED…Oh My!

Mobility Forensics at SNL

- **Implementation of a Mobile Forensic capability is an ongoing, integral part of our overall Mobility strategy.**

- **Began in 2012 with a team put together from Mobility Support and LOFT.**

Mobility Forensics at SNL

- **Requirements:**
  - **Training for both technical proficiencies and forensic methodologies.**
  - **Development of applicable processes.**
  - **Organizational support.**
  - **Identification of organizational impacts, and relational establishment with orgs needing to utilize these capabilities.**

Mobility Forensics at SNL

- **Initial Objectives:**
  - **Provision of prompt and thorough forensic examination, where the need arises, of mobile computing devices.**
  - **Prevention and detection of information-based threats for Sandia-owned mobile computing devices.**
  - **Protection of Sandia-owned or controlled information accessed or stored on mobile devices.**

Mobility Forensics at SNL

- **Requirements:**
  - **Training for both technical proficiencies and forensic methodologies.**
    - **Encase, SANS, H11.**
  - **Development of applicable processes.**
  - **Organizational support.**
  - **Identification of organizational impacts, and relational establishment with orgs needing to utilize these capabilities.**
    - **Cyber Security, Legal Technical Services, et al.**

Mobility Forensics at SNL

- **Expanded Objectives (Capabilities):**
- Provision of a prompt and thorough forensic examination of mobile computing devices.
- Prevention and detection of information-based threats for Sandia-owned mobile computing devices.
- Protection of Sandia-owned or controlled information accessed or stored on mobile devices**.**
- **Provide a deep level understanding of what is happening inside the mobile devices and the management of these devices.**
- **Third-party application assurance.**
- **Provide an understanding of how data is protected on mobile devices.**
- **Mobile device penetration testing.**
- **Incident response involving mobile devices.**
- **Waste, fraud, and abuse detection.**

Examples of Forensics Capability

Logical/File System Analysis: Logical or File System acquisition implies a copy of the logical storage objects (e.g., directories and files) that reside on a logical store (e.g., Flash memory). It essentially presents the same data that one could get from looking at each of the screens on a device. Logical acquisition is easier and quicker for a tool to extract and organize.

Physical Analysis: Physical acquisition implies a bit-for-bit copy of an entire physical store (e.g. flash memory). A physical acquisition has the advantage of allowing deleted files and data remnants to be examined. Physical extraction acquires information from the device by direct access to the flash memory. It is extremely difficult to obtain on most mobile devices.

Password Recovery – The ability to bypass a device password or passcode to analyze the device and extract data from it.

Fixmo Sentinel Desktop – Quickly monitor and verify the configuration and integrity of mobile devices, software, apps and infrastructure. Fixmo Sentinel Desktop is a lightweight desktop product that can be used for manual integrity and compliance scanning of BlackBerry devices.

.

Examples of Forensics Capability

UFED - Cellebrite's UFED enables logical, physical, file system, and password extraction of data from mobile devices. UFED comes with a full complement of cables and accessories for mobile forensic investigations in the field or lab.

AirWatch - AirWatch® Mobile Device Management (MDM) enables businesses to address challenges associated with mobility by providing a simplified, efficient way to view and manage all devices from the central admin console. *AirWatch will indicate whether a device has been jailbroken.

Lantern – Katana Forensics' Lantern is a Mac-based forensic tool that can very quickly perform a logical analysis of an iOS device and present that data in a very user-friendly and reportable interface. *Lantern's physical acquisition requires that the device be jailbroken.

EPPB (Elcomsoft Phone Password Breaker) - Enables forensic access to password-protected backups for smartphones and portable devices based on RIM BlackBerry and Apple iOS platforms.

EnCase - EnCase Forensic lets examiners acquire data from a wide variety of devices, unearth potential evidence with disk level forensic analysis, and craft comprehensive reports on their findings, all while maintaining the integrity of their evidence.

Autopsy - Autopsy™ is a digital forensics platform and graphical interface to The Sleuth Kit™ and other digital forensics tools. The core functionality of TSK allows you to analyze volume and file system data.

Examples of Forensics Capability

Burp Suite - an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Snoop-it is a tool to assist dynamic analysis and blackbox security assessments of mobile Apps by retrofitting existing apps with debugging and runtime tracing capabilities.

idb - a tool to simplify some common tasks for iOS pentesting and research.

Lessons Learned (Thus Far)

Determine investigative priorities and match your capabilities to them.

Leverage MDM whenever possible.

Develop collaborative processes.

Expedite investigative responses appropriately.

Understand chain of custody and other procedural issues.

Broaden scope, but don't forget from where you came.

Table Questions

Who is currently handling your mobile forensics?

What are your current technical capabilities/limitations?

What are your procedural/legal limitations?

What are your plans for expansion?

End