C25 Detecting Causality Through Fine-Grain Logging in Digital Investigations

Golden G. Richard III, PhD, University of New Orleans, Dept of Computer Science, New Orleans, LA 70148; and Aisha Ali-Gombe, MS, University of New Orleans, Computer Science, 308 Mathematics Bldg, 2000 Lakeshore Drive, New Orleans, LA 70148*

After attending this presentation, attendees will understand the impact of attribution on multi-app systems such as Android™. Storage and access of sensitive system data like contacts on SQLite databases by applications does not leave any trace of the causal relationships that will attribute the target app to the database object(s). Attendees will also learn how this problem can be solved by enforcing fine-grained access control on the SQLite database using static bytecode rewriting. The methodology is backed by a practical experiment that analyzed the 64 most-downloaded free apps on Google® Play™ and evaluated them based on application crashes, static, and runtime overhead.

This presentation will impact the forensic science community by discussing how fine-grained logging mechanisms can aid investigations by providing clear causal relationships between apps and database objects. Practical scenarios will be illustrated on how these casual relationships can be vital in supplementing memory and disk forensics to enhance digital investigations.

In a digital forensics investigation, how data gets written onto a device is as important as who writes the data. Often, research has shown that malicious software can write incriminating evidence on digital devices, thereby putting users at risk, as in the child pornography case against Michael Fiola.[1] The problem presented in this study illustrates how data written onto SQLite databases via the Android™ native providers cannot be linked to any specific application. While READ/WRITE accesses on the database are restricted and granted based on exclusive user permissions, general log files and typical digital evidence sources do not affiliate any app to the written data at any time.

With WRITE permission for instance, update, insert, and delete database operations can be performed by an application with very little data available to support attribution. This is primarily because SQLite is a single-user system and is not designed to keep track of who performs what operations on a system. For forensics investigation, this makes it very difficult to ascertain if a particular entry in the database is added or updated by the user or by a malicious application.

Thus, to aid digital investigation, a fine-grain logging technique that uses bytecode weaving to statically weave in extra auditing code after the return of specific Android™ database Create, Read, Update, and Delete (CRUD) functions (insert, update, delete, and query) is presented. The presented technique uses aspect-oriented programming to instrument Android apps. This instrumentation process does not require any modification to the operating system and/or framework code, thereby making it easily adoptable by average users. The experiment also revealed the system incurs an average of 15 seconds of static overhead and 58 nanoseconds runtime overhead across a range of test apps.

References:

1. AP. Framed for child porn - by a pc virus. Online. http://www.nbcnews.com/id/33778733.U2Ana l tLV.

Causal Relationships, Fine-Grain Logging, Bytecode Weaving

Copyright 2017 by the AAFS. Unless stated otherwise, noncommercial *photocopying* of editorial published in this periodical is permitted by AAFS. Permission to reprint, publish, or otherwise reproduce such material in any form other than photocopying must be obtained by AAFS.