# NIST develops experimental validation tool for cell phone forensics

December 2 2009

Viewers of TV dramas don't focus on the technology behind how a forensics crime team tracks a terrorist or drug ring using cell phone data, but scientists at the National Institute of Standards and Technology do. NIST researchers have developed a new technique aimed at improving the validation of a crime lab's cell phone forensics tools. Early experiments show promise for easier, faster and more rigorous assessments than with existing methods.

Cell phones reveal much about our daily communications—the who, when and what of our calls and texts. A small chip card within most phones, called an identity module, stores this and other data for a subscriber. A subscriber identity module (SIM) accommodates phonebook entries, recently dialed numbers, text messages and cellular carrier information. Forensic examiners use off-the-shelf software tools to extract the data, allowing them to "connect the dots" in a criminal case such as identifying affiliations or detecting mobile phone activity around the time of an event.

But for this information to be used as evidence in court or other formal proceedings, the software tools that forensic teams employ are normally validated to determine suitability for use. Currently, preparing test materials for assessing cell phone tools is labor intensive and may require learning new command languages to perform the process.

NIST scientists detail their proof-of-concept research in a NIST Interagency Report, Mobile Forensic Reference Materials: A

Methodology and Reification (available online at http://csrc.nist.gov/publications/nistir/ir7617/nistir-7617.pdf.) They also developed an experimental application, called SIMfill, and a preliminary test dataset that follows the methodology described in the report. SIMfill can be used to automatically upload cell phone data such as phone numbers and text messages to "populate" test SIMs that can then be recovered by forensic cell phone tools. In this way, examiners can use SIMfill as one method to assess the quality of their off-the-shelf tool.

The SIMfill software and dataset may be downloaded for free at http://csrc.nist.gov/groups/SNS/mobile_security/mobile_forensics_software.html.

"In this report," explains coauthor Wayne Jansen, "we document the results of a recent experiment with a number of commonly used mobile phone forensics tools. No tool was found to work perfectly and some worked poorly on fairly simple test cases."

The automated features of the applications and XML representation of test data allow technicians to develop new test cases easily. This offers a simple alternative to using manual means or specialized tools with higher learning curves. The data can be adapted to different languages with alternate character sets.

"Our research was a proof of concept," Jansen says. "Hopefully, forensic examiners will use our work to validate mobile forensics tools thoroughly before they employ them." The next step in the research is open. Scientists could expand the technique for mobile handsets and other types of identity modules, or the forensic community could decide to adopt this dataset and application as an open source project, according to Jansen.

Source: National Institute of Standards and Technology (news : web)