PHYS.ORG

Forensics: A call for evidence

January 21 2011, By Lee Swee Heng

Credit: cottonbro studio from Pexels

Many people today rely heavily on instant messaging services such as AIM, Windows Live Messenger and Google Talk for communications, and an increasing number of users are accessing these online chat services from their mobile phones. For forensic investigators, such conversations may provide valuable evidence, but retrieving the instant messages from mobile phones remains a great challenge.

Vrizlynn Thing and co-workers at the A*STAR Institute for Infocomm Research have now developed an automated system to extract volatile application data such as incoming and outgoing instant messages from mobile phones running on Google's Android mobile operating system. The forensic system and methodology, in theory, could extend to other mobile operating systems.

Previous experimental groups have used state-of-the-art forensic systems to extract call logs, SMS messages, contacts, emails and images from mobile phones, but attempts to retrieve instant messages have met with no success. The reason for the difficulty is that unlike computers, mobile phones tend to store application data in volatile memory, which is overwritten whenever the user types or sends a new message.

Thing and her co-workers have developed a memory acquisition tool called Memgrab and a memory dump analyzer called MDA for collecting and analyzing volatile information on the Android platform. The Memgrab tool connects to an Android phone and retrieves a bit-by-bit copy of the volatile memory, while the MDA tool decodes and extracts useful information from the retrieved data.

The researchers conducted an experiment to examine the performance of Memgrab and MDA in automatically retrieving and analyzing data during a chat session. They used the Android phone to send 15 messages to a computer and receive 15 messages from the computer in return. They found that, depending on the typing speed and waiting time, the acquisition rate for incoming messages could vary from 75.6% to 100%. However, in all of their tests, their acquisition rate for outgoing messages was consistently 100%.

Based on their statistics, the researchers are confident that their system is capable of capturing close to 100% of instant messages in real-life situations. “Digital forensics is a very important area and technology is advancing at an exponential rate. However, without a more sophisticated mobile device forensics tool, potentially important evidence could be lost forever,” says Thing. “To the best of our knowledge, our study represents the first work in the modeling and analysis of dynamic evidence on a mobile phone.” The researchers are now applying the methodology and porting the system to other mobile operating systems.

More information: Thing, V.L.L., Ng, K.Y. & Chang, E.C. Live memory forensics of mobile phones. *Digital Investigation* 7, S74–S82 (2010).

Provided by Agency for Science, Technology and Research (A*STAR)

Citation: Forensics: A call for evidence (2011, January 21) retrieved 9 April 2024 from https://phys.org/news/2011-01-forensics-evidence.html