Computer memory leaks a turn off

August 11 2012

When you switch off your computer any passwords you used to login to web pages, your bank or other financial account evaporate into the digital ether, right? Not so fast! Researchers in Greece have discovered a security loophole that exploits the way computer memory works and could be used to harvest passwords and other sensitive data from a PC even if it is in standby mode.

Writing in a forthcoming issue of the *International Journal of* Electronic Security *and Digital Forensics*, Christos Georgiadis of the University of Macedonia in Thessaloniki and colleagues Stavroula Karayianni and Vasilios Katos at the Democritus University of Thrace in Xanthi explain how their discovery could be used by information specialists in forensic science for retrieving incriminating evidence from computers as well as exploited by criminals to obtain personal data and bank details.

The researchers point out that most computer users assume that switching off their machine removes any data held in random access memory (RAM), this type of fast memory is used by the computer to temporarily hold data currently used by a given application. RAM is often referred to as volatile memory, because anything contained in RAM is considered lost when a computer is switched off. Indeed, all data is lost from RAM when the power supply is disconnected; so it is volatile in this context.

However, Georgiadis and colleagues have now shown that data held in RAM is not lost if the computer is switched off but the mains electricity supply not interrupted. They suggest that forensics experts and criminals

might thus be able to access data from the most recently used applications. They point out that starting a new memory-intensive application will overwrite data in RAM while a computer is being used, but simply powering off the machine leaves users vulnerable in terms of security and privacy.

"The need to capture and analyse the RAM contents of a suspect PC grows constantly as remote and distributed applications have become popular, and RAM is an important source of evidence," the team explains, as it can contain telltale traces of networks accessed and the unencrypted forms of passwords sent to login boxes and online forms.

The team tested their approach to retrieving data from RAM after a computer had been switched off following a general and common usage scenario involving accessing Facebook, Gmail, Microsoft Network (MSN) and Skype. They carried out RAM dumps immediately after switch off at 5, 15 and 60 minutes. They then used well-known forensic repair tools to piece together the various fragments of data retrieved from the memory dumps.

The team was able to reconstruct login details from the memory dumps for several popular services being used in the Firefox web browser including Google Mail (GMail), Facebook, Hotmail, and the WinRar file compression application. "We can conclude that volatile memory loses data under certain conditions and in a forensic investigation such memory can be a valuable source of evidence," the team says.

More information: "A framework for password harvesting from volatile memory" in *Int. J. Electronic Security and Digital Forensics*, 2012, 4, 154-163.

Provided by Inderscience