Research finds new channels to trigger mobile malware

May 16 2013

(Phys.org) —Researchers at the University of Alabama at Birmingham (UAB) have uncovered new hard-to-detect methods that criminals may use to trigger mobile device malware that could eventually lead to targeted attacks launched by a large number of infected mobile devices in the same geographical area. Such attacks could be triggered by music, lighting or vibration.

The research, highlighted in a paper entitled "Sensing-Enabled Channels for Hard-to-Detect Command and Control of Mobile Devices," was presented May 10, 2013, at the 8th Association for Computing Machinery (ACM) Symposium on Information, Computer and Communications Security (ASIACCS) in Hangzhou, China. The work

was a joint collaboration between the UAB SECuRE and Trustworthy (SECRET) computing lab and the UAB Security and Privacy in Emerging computing and networking Systems (SPIES) research group.

"When you go to an arena or Starbucks, you don't expect the music to have a hidden message, so this is a big paradigm shift because the public sees only emails and the Internet as vulnerable to malware attacks," said Ragib Hasan, Ph.D., assistant professor of computer and information sciences and director of the SECRET computing lab. "We devote a lot of our efforts towards securing traditional communication channels. But when bad guys use such hidden and unexpected methods to communicate, it is difficult if not impossible to detect that."

A team of UAB researchers was able to trigger malware hidden in mobile devices from 55 feet away in a crowded hallway using music. They were also successful, at various distances, using music videos; lighting from a television, computer monitor and overhead bulbs; vibrations from a subwoofer; and magnetic fields.

"We showed that these sensory channels can be used to send short messages that may eventually be used to trigger a mass-signal attack," said Nitesh Saxena, Ph.D., director of the SPIES research group and assistant professor in the Center for Information Assurance and Joint Forensics Research (CIA|JFR). "While traditional networking communication used to send such triggers can be detected relatively easily, there does not seem to be a good way to detect such covert channels currently."

Researchers were able to trigger malware with a bandwidth of only five bits per second – a fraction of the bandwidth used by laptops or home computers.

Shams Zawoad, a doctoral student and graduate assistant in the SECRET

computing lab presented the paper at the conference in China.

"This kind of attack is sophisticated and difficult to build, but it will become increasingly easier to accomplish in the future as technology improves," said Zawoad. "We need to create defenses before these attacks become widespread, so it is better that we find out these techniques first and stay one step ahead."

The paper was co-authored by Zawoad's fellow UAB graduate student Dustin Rinehart, as well as Tzipora Halevi, a recent doctoral graduate from the SPIES research group. All worked closely with the directors of the two groups to thoroughly test each novel channel.

More information: PDF: students.cis.uab.edu/zawoad/paper/asia03-hasan.pdf

Provided by University of Alabama at Birmingham