Electromagnetic emissions from smartphones analyzed for security vulnerability

December 20 2017

This study of the UC3M and the CSIC analyzes the vulnerabilities of smartphones. Credit: UC3M

A platform to improve smartphone security and that of other electronic devices was recently presented in Canada in an international conference on security and privacy, the Workshop on Security and Privacy on Internet of Things. The research focuses on "lateral movement attacks,"

which happen when "someone tries to take advantage of an electric current producing a magnetic field for illicit purposes—in this case, the attacker tries to extract the private password from the encryption, to which he theoretically should not have access," explained researcher José María de Fuentes, UC3M Computer Security Lab (COSEC).

Traditionally, hackers have tried to attack the encrypted algorithm, the process that protects data, which normally has a complicated mathematical base. Later, they sought other ways of breaching security without having to "break" the math upon which it is based. "When the devices are on, they use energy and generate electromagnetic fields. We try to capture their traces to obtain the encryption key, and at the same time, decipher the data," explained Lorena González, also from the UC3M COSEC.

Digital vulnerability

"We want to make it known that these types of devices have vulnerabilities, because if an adversary attacks them, that is, if someone calculates the password on a cell phone, it will make people vulnerable, and data will no longer be private," said Luis Hernández Encinas from the Institute for Physical and Information Technologies.

The basic aim of this research is to detect and make known the vulnerabilities of electronic devices and their chips so that software and hardware developers can implement appropriate countermeasures to protect user security. "Our work is to verify whether this has been carried out correctly and try to attack again to check for any other types of vulnerabilities," added Hernández Encinas.

The most relevant aspect of the project, according to the researchers, is that an architecture and work environment is being developed in which this type of lateral movement attack can be explored. In fact, it is

possible to extract encrypted information from other data, such as variations in temperature of the device, power consumption, and the time it takes a chip to process a calculation.

More information: A Framework for Acquiring and Analyzing Traces from Cryptographic Devices. A. Blanco Blanco, J.M. de Fuentes, L. González Manzano, L. Hernández Encinas, A. Martín Muñoz, J.L. Rodrigo Oliva, I. Sánchez García. Workshop on Security and Privacy on Internet of Things (SePrIoT) 2017. 13th EAI International Conference on Security and Privacy in Communication Networks. 25th October 2017, Niagara Falls, Canada.
www.seg.inf.uc3m.es/~lgmanzan/docs/SCAP.pdf

Provided by Carlos III University of Madrid