Radio waves for the detection of hardware tampering

June 7 2022

The radio signal is as unique as a fingerprint. Credit: Michael Schwettmann

As far as data security is concerned, there is an even greater danger than remote cyberattacks: namely tampering with hardware that can be used to read out information—such as credit card data from a card reader.

Researchers in Bochum have developed a new method to detect such manipulations. They monitor the systems with radio waves that react to the slightest changes in the ambient conditions. Unlike conventional methods, they can thus protect entire systems, not just individual components—and they can do it at a lower cost. The RUB's science magazine *Rubin* features a report by the team from Ruhr-Universität Bochum (RUB), the Max Planck Institute for Security and Privacy and the IT company PHYSEC.

Paul Staat and Johannes Tobisch presented their findings at the IEEE Symposium on Security and Privacy, which took place in the U.S. from 23 to 25 May 2022. Both researchers are doing their Ph.D.s at RUB and conducting research at the Max Planck Institute for Security and Privacy in Bochum in Professor Christof Paar's team. For their research, they are cooperating with Dr. Christian Zenger from the RUB spin-off company PHYSEC.

Protection through radio waves

Data is ultimately nothing more than electrical currents that travel between different computer components via conductive paths. A tiny metallic object, located in the right place on the hardware, can be enough to tap into the information streams. To date, only individual components of systems, such as a crucial memory element or a processor, can be protected from such manipulations. "Typically, this is done with a type of foil with thin wires in which the hardware component is wrapped," explains Paul Staat. "If the foil is damaged, an alarm is triggered."

The radio wave technology from Bochum, however, can be used to monitor an entire system. To this end, the researchers install two antennas in the system: a transmitter and a receiver. The transmitter sends out a special radio signal that spreads everywhere in the system

and is reflected by the walls and computer components. All these reflections cause a signal to reach the receiver that is as characteristic of the system as a fingerprint.

Technology reacts to the slightest changes

Tiny changes to the system are enough to have a noticeable effect on the fingerprint, as the team demonstrated in experiments. The IT experts equipped a conventional computer with radio antennas and punctured its housing with holes at regular intervals. Through these holes, the researchers let a fine metal needle penetrate the inside of the system and checked whether they notice the change in the radio signal. In the process, they varied the thickness of the needle, the position and the depth of penetration.

With the computer running, they reliably detected the penetration of a needle 0.3 millimeters thick with their system from a penetration depth of one centimeter. The system still detected a needle that was only 0.1 millimeters thick—about as thick as a hair—but not in all positions. "The closer the needle is to the receiving antenna, the easier it is to detect," explains Staat. "Therefore, in practical applications, it makes sense to think carefully about where you place the antennas," adds Tobisch. "They should be as close as possible to the components that require a high degree of protection."

Basically, the technology is suitable for both high-security applications and everyday problem. The IT company PHYSEC already uses it to prevent unauthorized manipulation of critical infrastructure components.

More information: Anti-tamper radio: System-level tamper detection for computing systems, IEEE Symposium on Security and Privacy, San Francisco, USA, 2022. Conference Proceedings, DOI:

10.1109/SP46214.2022.00067. www.computer.org/csdl/proceedi … 1600b150/1A4Q40AvPRm

Provided by Ruhr-Universitaet-Bochum