Secret chips can be hidden in the device to spy on and hijack smartphones

Called an intermediate chip, this attack uses poisonous replacement parts to attack the device.

At a recent security conference, experts from Israeli universities presented new research describing the scenario in which attacks could be carried out through replacement parts to contain broken parts. (spare part) on the phone and other smart devices.

The form of attack - described as an intermediate chip - is based on the assumption that a third party produces excess replacements in large numbers containing additional chips to interfere with internal communication. set of devices, and still capable of executing poisoning commands.

An attacker can hide the infected chip on the replacement part of the phone

Researchers demonstrate their hypothesis by creating a poisoning replacement and using them to gain control of a test phone.

Although the attack looks complicated, the researchers say these available electronic devices cost only about $ 10. There must be certain skills with electronic devices, but to perform the attack is not as complicated as many people think.

Two ways to attack through replacement parts on the device

When creating toxic replacements, the researchers discovered two ways to perform this type of attack.

1. The first way is to insert the basic command into the communication between the device and the replacement parts. This works best with touch screens because it allows an attacker to impersonate a user by mimicking touch gestures, thereby stealing information.
2. The second way is to attack the buffer overflow type in the vulnerability of the touch device driver inside the operating system kernel. The attacker exploits this error to hijack the device and perform an attack on the OS without mimicking the touch operation. The second type of attack is suitable for some device drivers but not for all.

The team - which includes experts from Ben-Gurion University of the Negev, Israel - offers a variety of ways to prevent attacks by replacing hardware with their research reports. These methods can be found on the report 'Shattered Trust: When Replacement Smartphone Components' at the following addresses *https://iss.oy.ne.ro/Shattered.pdf* and *https: // www .usenix.org / system / files / conference / woot17 / woot17-paper-shwartz.pdf* . These researchers presented their results at the WooT '17 USENIX conference. The videos below describe the process by which the group performs the attack through the intermediate chip on the phone

that contains the infected replacement.