Issued 8/21/17

Replacement Touch Screens Found Embedded with a Malicious Chip

A new study has found that when replacement touch screens are embedded with a malicious chip, they can be used to compromise your smartphone. Ars Technica reports that a new paper, published by the Ben-Gurion University of the Negev, includes simulated attacks on two Android devices: a Huawei Nexus 6P and LG G Pad 7.0. Researchers were able to take control of the devices by using a malicious chip embedded into a third-party touch screen.

Phones with a malicious touch screen could essentially record your photos and app data, or direct users to phishing websites to exploit vulnerabilities and gain control of the device. The attack is very difficult to detect, as anti-virus programs can't flag it and the hardware survives operating system updates and factory resets. In the study, researchers used a hot air blower on the phone's touch controller connection to access and solder on their malicious chips. "Our attack assumes that the phone's touch controller had been replaced with a malicious component, but that the rest of the hardware and software on the phone is authentic and trusted," the researchers wrote.

"A well motivated adversary may be fully capable of mounting such attacks in a large scale or against specific targets. System designers should consider replacement components to be outside the phone's trust boundary, and design their defenses accordingly."

More than half of people who own a smartphone have damaged their phone screen at least once, so the idea of exploiting third party touch screens is pretty conceivable. However, most modern smartphones are compact, making it difficult to access the devices' innards for manipulation. Apple's iPhones also have secure modules to block features like Touch ID from being tampered with.