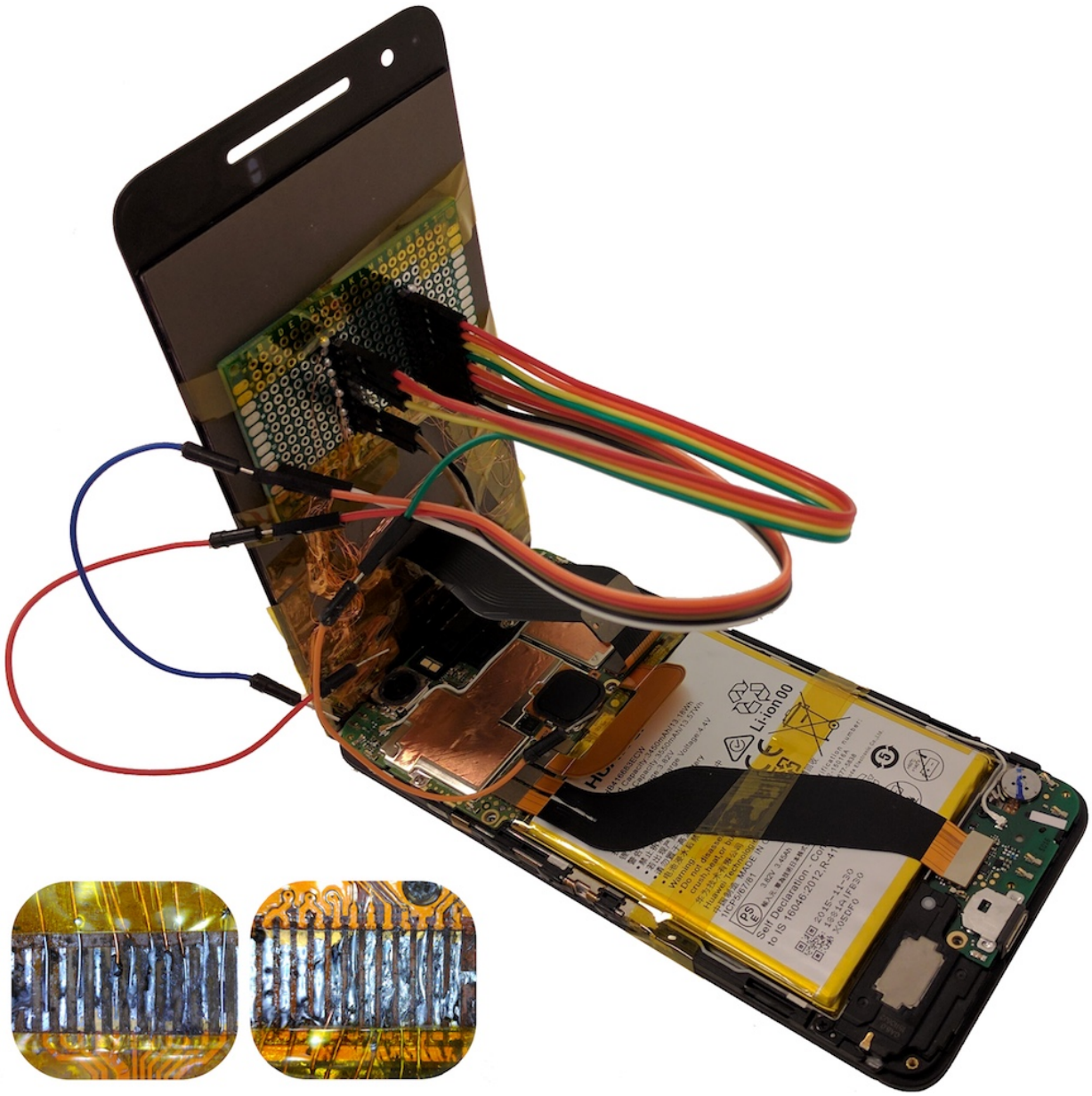
Researchers explore how phone replacement screens could trigger attacks

August 23 2017, by Nancy Owano



People with cracked phone touch screens? What else is new? Many people drop their phones, shatter their screens and either put up with their cracked screens or run to shops for replacements. Now there is something to worry about other than just inconvenience.

As *Ars Technica* and other sites reported, there is "the possibility the replacement parts installed by repair shops contain secret hardware that completely hijacks the security of the device."

The reports coming in said that malicious code on replacement screens could serve up attacks on your Android phone. The team relaying this wake-up call are from Ben-Gurion University of the Negev.

Dan Goodin in *Ars Technica* elaborated on what the hijackers can do; replacement screens can be used "to surreptitiously log keyboard input and patterns, install malicious apps, and take pictures and e-mail them to the attacker."

The screens are in a sense booby-trapped.

And it's not quite a simple picture of service technicians being up to no good. Goodin said, "the booby-trapped parts could be indistinguishable from legitimate ones, a trait that could leave many service technicians unaware of the maliciousness. There would be no sign of tampering unless someone with a background in hardware disassembled the repaired phone and inspected it."

Secret chips in replacement parts can do the smartphone mischief. "Booby-trapped touchscreens can log passwords, install malicious apps,

and more," said *Ars Technica*.

In these devices, where are the integrity checks on communications between components and main processors? That is a good question.

The researchers—Omer Shwartz, Amir Cohen, Asaf Shabtai and Yossi Oren—wrote about their work in "Shattered Trust: When Replacement Smartphone Components Attack."

The paper was presented earlier this month at the 2017 Usenix Workshop on Offensive Technologies (WOOT).

Let the researchers explain: "Phone touchscreens, and other similar hardware components such as orientation sensors, wireless charging controllers, and NFC readers, are often produced by third-party manufacturers and not by the phone vendors themselves. Third-party driver source code to support these components is integrated into the vendor's source code...the component driver's source code implicitly assumes that the component hardware is authentic and trustworthy."

The authors called this trust into question. They said in their work, "we present and evaluate a series of end-to-end attacks that can severely compromise a stock Android phone with standard firmware. Our results make the case for a hardware-based physical countermeasure."

The authors wrote, "System designers should consider replacement components to be outside the phone's trust boundary, and design their defenses accordingly."

They were able to simulate a chip-in-the-middle scenario in which "a benign touchscreen has been embedded with a malicious integrated chip that manipulates the communication bus."

Shaun Nichols in *The Register*: "Too much stuff in the phone trusts other electronics to be legit, which means an evil part, replaced during a repair or inserted if the handheld was seized, could cause all sorts of mischief." He referred to "rogue physical hardware, allowing photos and other files to leak or be tampered with."

Additional protections would be in order to guard against tampering.

The authors in their paper noted that mobile phones are often dropped, shattering screens. They pointed to a 2015 study, with more than 50% of global smartphone owners having damaged their phone screen at least once.