arXiv.org > cs > arXiv:1805.04850

Computer Science > Cryptography and Security

Title: Shattered Trust: When Replacement Smartphone Components Attack

Authors: Omer Shwartz, Amir Cohen, Asaf Shabtai, Yossi Oren
(Submitted on 13 May 2018)

Abstract: 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. In contrast to 'pluggable' drivers, such as USB or network drivers, the component driver's source code implicitly assumes that the component hardware is authentic and trustworthy. As a result of this trust, very few integrity checks are performed on the communications between the component and the device's main processor.
In this paper, we call this trust into question, considering the fact that touchscreens are often shattered and then replaced with aftermarket components of questionable origin. We analyze the operation of a commonly used touchscreen controller. We construct two standalone attacks, based on malicious touchscreen hardware, that function as building blocks toward a full attack: a series of touch injection attacks that allow the touchscreen to impersonate the user and exfiltrate data, and a buffer overflow attack that lets the attacker execute privileged operations. Combining the two building blocks, 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.

Comments: Presented in WOOT 17', 11th {USENIX} Workshop on Offensive Technologies ({WOOT} 17) - 2017
Subjects: Cryptography and Security (cs.CR)
Cite as: arXiv:1805.04850 [cs.CR]
(or arXiv:1805.04850v1 [cs.CR] for this version)

Submission history

From: Omer Shwartz [view email]
[v1] Sun, 13 May 2018 10:01:23 GMT (4202kb,D)