

Researchers

Prof. Yossi Oren
yos@bgu.ac.il

Yehonatan Tsionov
Anatoly Shusterman
Rom Ogen
Adar Ovadya
Liron Avraham
Amir Cohen
Benyamin Farshteindiker
Omer Shwartz
Hen Hayoon

Publications

Y. Oren, "Side-channel Attacks Pose Growing Threat to Secrecy," IHS Jane's Intelligence Review Volume 29, Issue 9, September 2017.

O. Shwartz, et al., "Opening Pandora's Box: Effective Techniques for Reverse Engineering IoT Devices," 17th Smart Card Research and Advanced Application Conference [CARDIS], 2017.

O. Shwartz, et al., "Shattered Trust: When Replacement Smartphone Components Attack," 11th USENIX Workshop on Offensive Technologies [WOOT], 2017.

B. Farshteindiker, et al., "How to Phone Home with Someone Else's Phone: Information Exfiltration Using Intentional Sound Noise on Gyroscopic Sensors," 10th USENIX Workshop on Offensive Technologies [WOOT], 2016.

Patent Applications

Y. Oren, A. Shabtai, O. Shvartz, A. Cohen, "Protecting a Device from Malicious Field Replaceable Units," US Patent Application.

Y. Oren, A. Grosz, N. Hasidim, and B. Farshteindiker, "Acoustic Security Code Transmission," US Patent Application.

When Replacement Smartphone Components Attack

Goals

The group at the Implementation Security Lab are researching side-channel attacks: cyber-attacks that allow the extraction of secret information from various devices by exploiting their precise physical behaviors (such as power consumption, electromagnetic emanations, heat or vibrations). Most recently they are looking at the threats posed by phone touchscreens and other hardware components, such as orientation sensors and NFC readers, where third-party driver source code to support these components is integrated into the vendor's source code with very few integrity checks.

Description

The research conducted in the lab is grounded in knowledge attained as part of the EU-funded ECRYPT project and uses precise measurement equipment and techniques to assess the impact of side-channel attacks by measuring the leakage of target devices under tests. This allows the researchers to obtain an upper bound on the potential performance of attacks carried out using less sensitive measurement devices such as compromised phones or malicious aftermarket peripherals.

In recent testing, they were able to 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. Their results make the case for a hardware-based physical countermeasure.

In addition, Dr. Oren plans to use this lab to find creative and unexpected uses for the sensors found on modern mobile phones, such as the gyroscope, touch screen, and magnetic compass.