New firewall protects cellphones from security threat

June 29 2017

Cellphone parts harboring malicious code can be surreptitiously placed in various replaceable phone components, compromising user data and security. Ben-Gurion University of the Negev researchers areThe researchers are seeking to further test the patent-pending technology with phone manufacturers. Credit: Ben-Gurion U.

Cyber security researchers at Ben-Gurion University of the Negev (BGU) developed an innovative firewall program that adds a missing layer of security in Android cellphones and monitors for malicious code.

Earlier this year, Dr. Yossi Oren and his team of researchers in the BGU Department of Software and Information Systems Engineering (ISE), discovered a security vulnerability in the internal communications between Android cellphone components and a phone's central processing unit (CPU). They alerted Android developer Google and helped the global company address the problem.

"Our technology doesn't require device manufacturers to understand or modify any new code," says Dr. Oren. "It's a firewall that can be implemented as a tiny chip, or as an independent software module running on the CPU."

Some 400 million people change their phone's components, such as touchscreens, chargers, and battery or sensor assemblies, which are all susceptible to significant security breaches and attacks. These components, referred to as "field replaceable units (FRUs)," communicate with the phone CPU over simple interfaces with no authentication mechanisms or error detection capabilities. A malicious vendor could add a compromised FRU to a phone, leaving it vulnerable to password and financial theft, fraud, malicious photo or video distribution, and unauthorized app downloads.

"This problem is especially acute in the Android market with many manufacturers that operate independently," the researchers say. "An attack of this type occurs outside the phone's storage area; it can survive phone factory resets, remote wipes and firmware updates. Existing security solutions cannot prevent this specific security issue."

Researcher Omer Schwartz adds, "There is no way for the phone itself to discover that it's under this type of an attack. Our solution prevents a malicious or misconfigured FRU from compromising the code running on the CPU by checking all the incoming and outgoing communication."

The research team used machine learning algorithms to monitor the phones' internal communications for anomalies that may indicate malicious code. Their software allowed them to identify and prevent hardware-generated data leaks and hacks.

A paper on the discovery and the new software will be presented at the prestigious Workshop on Offensive Technologies in Vancouver, Canada this August. Dr. Oren and Dr. Asaf Shabtai collaborated on the paper along with research students Omer Shwartz and Amir Cohen.

"The work of Dr. Oren's team is the latest invention from ISE at BGU," says Zafrir Levi, senior vice president of business development at BGN Technologies, the University's commercialization and technology transfer company. "In the last decade, ISE has spawned many inventions that have been used worldwide through patents sold to international corporations and by start-up companies."

The researchers are seeking to further test the patent-pending technology with phone manufacturers.

More information: Paper: iss.oy.ne.ro/Shattered.pdf

Provided by American Associates, Ben-Gurion University of the Negev