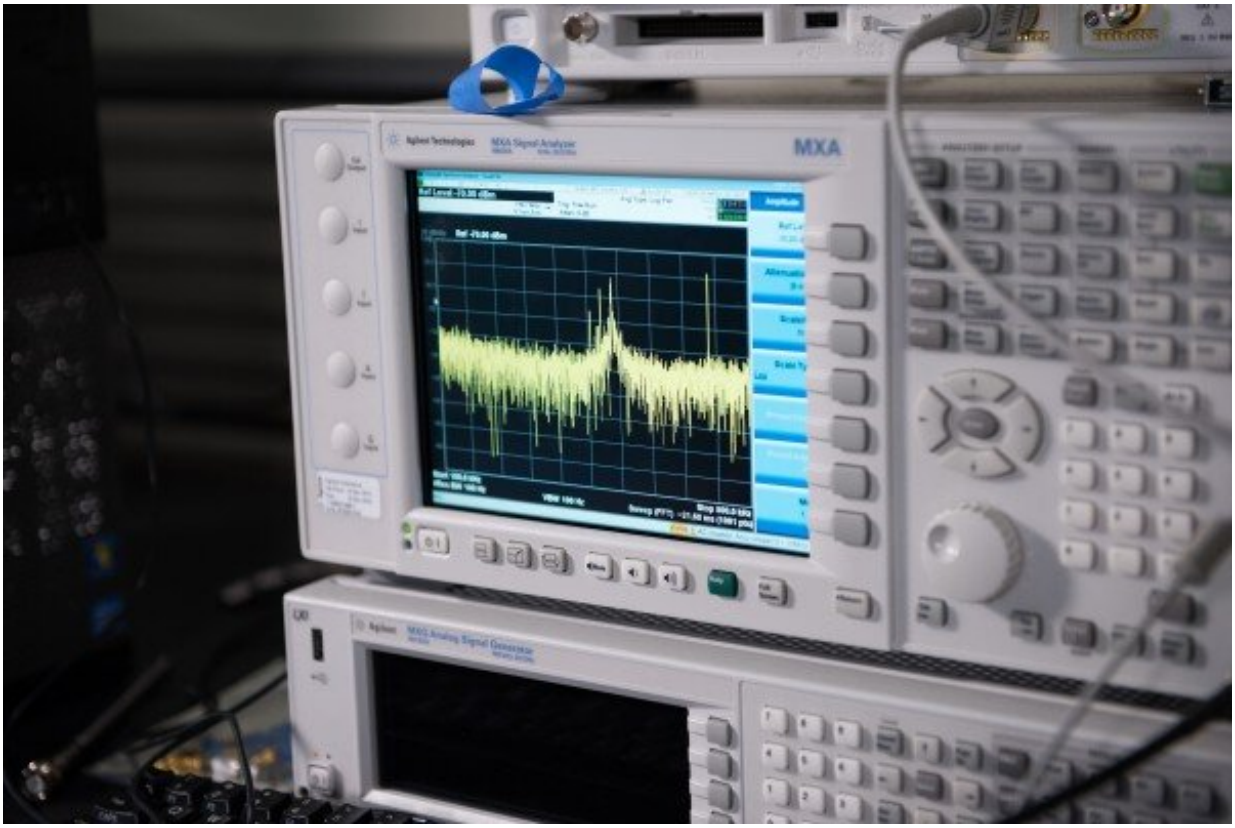
Researchers discover new side channel attack on low-end phones

September 28 2021



Credit: Georgia Institute of Technology

Georgia Tech Researchers have now shown that one of the very measures meant to keep data secure on a low-end phone can enable attackers to steal it.

Their paper, presented on September 10 at the 6th IEEE European Symposium on Security and Privacy, demonstrates successful attacks on two different types of low-end Android phones, a ZTE Zfive and an Alcatel Ideal. In accordance with standard practice, the researchers reported their findings to software developers before releasing their results so that the problem could be fixed.

The attack relies on placing a radio sensor within a few centimeters of a device, close enough to detect the weak radio waves that are inadvertently emitted by a phone's processor. By witnessing a single secure web transaction transmitted in these signals, an attacker can figure out a user's secret key, a form of numerical password that is used to encrypt their data.

"It demonstrates that a really powerful attack, one that can actually steal the key, can be done under realistic conditions," said Milos Prvulovic, professor of Computer Science at Georgia Tech and coauthor of the study. "How many times have you put your phone down on a desk at the airport and not checked what's under the desk?"

Fortunately, the researchers found a relatively straightforward fix. Implementing this fix is currently in progress, and will be important. If researchers can figure out how to make the attack work on high-end phones, then the same vulnerability will occur on billions of the most widely-used modern devices.

Hacking a phone from the side

Secret keys or encryption keys are often used for securing user data. Once the attacker has access to a user's encryption keys, they can forge their "digital signature" and gain access to banking data, for example. Because the newly discovered attack should work on a wide variety of phones in everyday use, it is expected to require prompt amendment to

the relevant security standards, RFC 7748.

The attack targets a standard encryption process employed in a wide range of online activities, such as logging into a virtual private network (VPN), creating a secure web connection with a bank, or e-signing a digital document. During this process, two endpoints on a network, such as two phones, must exchange a series of messages to verify each other's identity. If they cannot verify that they are who they say they are, then they know not to send private data.

Proving one's identity amounts to carrying out a certain kind of encryption algorithm. This algorithm involves a series of operations on a secret key called a "nonce," which can be represented as a binary number, a sequence of ones and zeroes or "bits." For each operation that a phone's processor carries out, it emits a weak radio signal, thousands of times weaker than the signal of a Wi-Fi transmitter. These signals are called "side-channel" emissions since they do not come from the primary channels that the phone uses to communicate.

Years ago, researchers realized that these side-channel emissions can leak the value of the nonce. For example, an encryption algorithm might require additional processing steps when a bit of the nonce is a one, making the processor emit a longer lasting signal for those bits. By tracking the pattern of longer and shorter emissions that come from the phone while it is processing the nonce, an attacker can reconstruct the value of each of its bits. From there, they can break a user's encryption.

Other researchers invented a solution for this problem known as a "constant-time" algorithm. This algorithm ensures that a processor carries out the same sequence of operations for each bit. The radio emissions are therefore indistinguishable for each bit and the nonce cannot be reconstructed. This algorithm was codified in encryption standards like RFC 7748 and widely adopted.

Breaking the constant-time algorithm

In the new work, the researchers discovered a problem with the constant-time algorithm. One particular operation that is carried out for each bit, called a "conditional swap," has a tell-tale trait. When the operation is performed on a bit with the value of one, the processor emits a slightly stronger radio signal. The researchers realized that if an attacker could listen in on the emissions during this operation, each time it occurs, they could determine the nonce.

The hard part was to figure out whether they could focus in on the specific radio signature of the conditional swap, buried within a sequence of many other emissions. Also, because of the high processing speed of modern phones, the radio signature of the conditional swap only lasts for a brief duration. But, it turns out, it is the constant-time algorithm—meant to be a countermeasure to side-channel attacks—which allows the attack to work in the first place.

The key for the researchers was to carefully observe a phone's emissions. Because of the constant-time algorithm, these emissions are extremely regular. Each time the phone processes a bit, the same general pattern of emissions takes place. The researchers could therefore automate the process of picking out the tiny piece of emissions corresponding to the conditional swap, like learning to spot a small logo on a fast-moving train car by watching enough train cars passing by. From there, the researchers could measure the strength of the emissions to determine whether each bit was a zero or one, and thereby reconstruct the entire nonce.

The attack works so effectively that researchers found they only needed to listen in on a single secure transaction to steal a phone's secret key.

"As long as somebody can put a probe or antenna close enough," said

Prvulovic, "We can have your key now."

To fix the issue, the researchers modified the constant-time algorithm so that the signal corresponding to the conditional swap has the same strength regardless of the value of the bit. After developers implement this fix into cryptographic libraries like OpenSSL, the constant-time algorithm should be secure once again.

More information: A Single-Trace EM Side Channel Attack on Several Constant-Time Elliptic Curve Implementations in Mobile Platforms. Monjur Alam, Baki Yilmaz and Frank Werner (Georgia Tech); Niels Samwel (Radboud University); Alenka Zajic (Georgia tech); Daniel Genkin (University of Michigan); Yuval Yarom (University of Adelaide and Data61); Milos Prvulovic (Georgia Tech). 6th IEEE European Symposium on Security and Privacy, September 6-10, 2021.

Provided by Georgia Institute of Technology

Citation: Researchers discover new side channel attack on low-end phones (2021, September 28) retrieved 31 March 2023 from https://techxplore.com/news/2021-09-side-channel-low-end.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.