Researchers develop toolkit to test Apple security, find vulnerability

13 September 2021, by Matt Shipman

Credit: Pixabay/CC0 Public Domain

Researchers from North Carolina State University have developed a software toolkit that allows users to test the hardware security of Apple devices. During their proof-of-concept demonstration, the research team identified a previously unknown vulnerability, which they call iTimed.

"This toolkit allows us to conduct a variety of fine-grained security experiments that have simply not been possible on Apple devices to this point," says Aydin Aysu, co-author of a paper on the work and an assistant professor of electrical and computer engineering at NC State.

Apple is well known for creating integrated devices. The design of the devices effectively prevents people from seeing how the devices function internally.

"As a result, it has been difficult or impossible for independent researchers to verify that Apple devices perform the way that Apple says they perform when it comes to security and privacy," says Gregor Haas, first author of the paper and a recent master's graduate from NC State.

However, a hardware vulnerability was uncovered in 2019 called checkm8. It affects several models of iPhone and is essentially an unpatchable flaw.

"We were able to use checkm8 to get a foothold at the most fundamental level of the device—when the system begins booting up, we can control the very first code to run on the machine," Haas says. "With checkm8 as a starting point, we developed a suite of software tools that allows us to observe what's happening across the device, to remove or control security measures that Apple has installed, and so on."

The researchers stress that there are practical reasons for wanting to have third parties assess Apple's security claims.

"A lot of people interact with Apple's tech on a daily basis," Haas says. "And the way Apple wants to use its platforms is changing all the time. At some point, there's value in having independent verification that Apple's technology is doing what Apple says it is doing, and that its security measures are sound."

"For example, we want to know the extent to which attacks that have worked against hardware flaws in other devices might work against Apple devices," Aysu says.

It didn't take the researchers long to demonstrate how useful their new toolkit is.

While conducting a proof-of-concept demonstration of the toolkit, the researchers reverse-engineered several key components of Apple's hardware and identified a vulnerability to something they named an iTimed attack. It falls under the category of so-called "cache timing side channel attacks," and effectively allows a program to gain access to cryptographic keys used by one or more programs on an Apple device. With the relevant keys, outside users would then be able to access whatever

information the other affected program or programs on the device had access to.

"We haven't seen evidence of this attack in the wild yet, but we have notified Apple of the vulnerability," Aysu says.

The NC State team is sharing much of the toolkit as an open-source resource for other security researchers.

"We also plan to use this suite of tools to explore other types of attacks so that we can assess how secure these devices are and identify things we can do to reduce or eliminate these vulnerabilities moving forward," Aysu says.

The paper, "iTimed: Cache Attacks on the Apple A10 Fusion SoC," is co-authored by Seetal Potluri, a postdoctoral researcher at NC State. The paper will be presented at the IEEE International Symposium on Hardware Oriented Security and Trust, which is being held Dec. 12-15 in Washington, D.C.

More information: Paper: Gregor Haas, Seetal Potluri and Aydin Aysu, "iTimed: Cache Attacks on the Apple A10 Fusion SoC," in IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2021, eprint.iacr.org/2021/464.pdf

Toolkit: github.com/iTimed-Toolkit/

Provided by North Carolina State University