OpenSK research platform cheered as boost for adoption of security keys

2 February 2020, by Nancy Cohen

Credit: CC0 Public Domain

An implementation for security keys was in the news recently. The spotlight was on OpenSK.

Elie Bursztein, security and anti-abuse research lead and Jean-Michel Picod, software engineer, Google, wrote the announcement about OpenSK as a research platform, in their Jan. 30 post in the Google Security Blog.

It is open source; its reason for being is to improve access to FIDO authenticator implementations.

Who can benefit? Researchers, security key manufacturers and enthusiasts can use it to help develop innovative features. They can also accelerate security key adoption, they said.

"You can make your own developer key by flashing the OpenSK firmware on a Nordic chip dongle. In addition to being affordable, we chose Nordic as initial reference hardware because it supports all major transport protocols mentioned by FIDO2: NFC, Bluetooth Low Energy, USB, and a dedicated hardware crypto core."

(FIDO2 refers to the FIDO Alliance's set of specifications. According to the FIDO Alliance, "FIDO2 cryptographic login credentials are unique across every website, never leave the user's device and are never stored on a server. This security model eliminates the risks of phishing, all forms of password theft and replay attacks.")

ZDNet affirmed that hardware vendors needing to build hardware security keys would have help in the form of OpenSK. Catalin Cimpanu said this was going to make it easier for hobbyists and hardware vendors to build their own security key.

The first versions of the OpenSK firmware were created for Nordic chip dongles, said Cimpanu.

"With this early release, developers will be able to flash OpenSK on a Nordic chip dongle," said *XDA Developers*.

it is written in Rust. The Google Security Blog authors said that "Rust's strong memory safety and zero-cost abstractions makes the code less vulnerable to logical attacks."

It runs on TockOS. The latter is "a secure embedded operating system for microcontrollers," according to GitHub. Adam Conway in *XDA Developers* said that "TockOS offers a sandboxed architecture for better isolation of the security key applet, drivers, and kernel."

The GitHub page for OpenSK, meanwhile, stated: "This project is proof-of-concept and a research platform. It's still under development and as such comes with a few limitations." The authors made some points about the limitations and the points included the following.

First, FIDO2. "Although we tested and implemented our firmware based on the published CTAP2.0 specifications, our implementation was not reviewed nor officially tested and doesn't claim to be FIDO Certified." Second, Cryptography. They

implemented algorithms in Rust as a placeholder; the implementations were research-quality code and haven't been reviewed. "They don't provide constant-time guarantees and are not designed to be resistant against side-channel attacks."

The blog post noted that "this release should be considered as an experimental research project to be used for testing and research purposes."

What's on the authors' wish list? "With the help of the research and developer communities, we hope OpenSK over time will bring innovative features, stronger embedded crypto, and encourage widespread adoption of trusted phishing-resistant tokens and a passwordless web," they stated.

Cimpanu in *ZDNet*: "Google is also hoping that the project is also broadly adopted by hardware vendors that have not yet invested R&D into security key products."

More information: Say hello to OpenSK: a fully open-source security key implementation, security.googleblog.com/2020/0 … lly-open-source.html

APA citation: OpenSK research platform cheered as boost for adoption of security keys (2020, February 2) retrieved 22 October 2021 from https://techxplore.com/news/2020-02-opensk-platform-boost-keys.html