24 NEW ARTICLES ▾

Google releases open-source 2FA security key platform called OpenSK

4 ◢

Ryne Hager

🕐 16 hours ago

GOOGLE | 📰 NEWS | SECURITY | 🎬 VIDEOS

Two-factor security is a basic requirement these days if you want to take your digital responsibilities seriously, but some hardware lacks the sort of public documentation that some privacy advocates feel is truly necessary to provide ideal security. Open source enthusiasts will be glad to hear that Google has just announced the release of OpenSK, an open-source implementation for security keys, supporting both FIDO U2F and FIDO2.

This isn't the sort of thing most of our readers will be able to appreciate immediately, you can't zip out and buy a product running Google's OpenSK just yet. This early, explicitly experimental release is only compatible with a single piece of reference hardware right now: the Nordic chip dongle (for which the project supplies a 3d-printable case). But with this working software platform and reference hardware, Google and participating developers/security researchers may be able to build something new with the benefits of open-source security.

OpenSK demo

▶

FOLLOW ANDROID POLICE ▾

LATEST DEALS ▾

LATEST POLL ▾

RECENT REVIEWS ▾

LATEST ROUNDUPS ▾

RECENT APPS AND GAMES ▾

BLAST FROM THE PAST ▾

A quick demonstration of OpenSK working on a Nordic chip dongle as a security key.

Rust evangelicals — who frequently champion its memory safety/security — will be glad to hear that a good chunk of OpenSK is written in the language, running on top of TockOS. Those interested in learning more can dive right into the GitHub repository and see how it all works.

Source: Google

TAGS	2FA	FIDO U2F	FIDO2	NORDIC CHIP	NORDIC CHIP DONGLE	OPEN SOURCE

OPEN-SOURCE SECURITY	OPENSK	TWO-FACTOR SECURITY	VIDEO

SUBSCRIBE

f   🐦

15

PREVIOUS STORY

You can finally silence notifications in Android Auto

NEXT STORY

Android 10 rolling out to Samsung Galaxy S10 series (Update: T-Mobile 5G variant)

TRENDING

Stable Android 10 starts hitting the Galaxy Note10 and Note10+ (Update: Australia, Hong Kong, more)

158

Jan 16, 2020

Latest WhatsApp beta finally brings dark mode (APK Download)

70

Jan 21, 2020

Google is killing Google One Today, gives supporters only a week's notice

42

Jan 29, 2020

COMMENTS

Android Police Comment Policy

Do: post respectful and insightful comments. Don't: flame, hate, impersonate staff, spam.

---

5 Comments   **Android Police**   ① **Login**

♡ Recommend   🐦 Tweet   f Share   Sort by Best

Join the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ⑦

Name

Leif Sikorski • 14 hours ago

I'm not a big fan of them promoting it as a "replacement" for a password - at least in the video. Having a hardware key to access almost anything is such a horrible idea if it's not used as a second factor authentication combined with a password.

8 ⌃ | ⌄ 1 • Reply • Share ›

> **Marion Stevens** ➜ Leif Sikorski • 9 minutes ago
>
> I agree with you completely, but, just to play devil's advocate, it does eliminate the possibility that some criminal gang in Russia can get into your bank account. Well, assuming that the key can't be cloned somehow.
>
> It kind of poses the question of what's worse: a guy carrying a key on his keyring that can let an attacker into all of his accounts, should that attacker steal the key, or a guy reusing the same password on all his accounts, meaning any attacker in the world who finds the password to one of them now has access to all of them. Obviously, using different passwords on each account, back by a physical 2FA key, is best, but most people can't be bothered to do either. Again, not saying that using a key as the sole authentication method is a good idea, but there are plenty of other security practices out there that people are using right now that may be worse.
>
> ⌃ | ⌄ • Reply • Share ›

> **Colin Richardson** ➜ Leif Sikorski • 7 hours ago
>
> Off-topic, but your comment somehow reminded me to print out my backup codes and leave them at my parents.
>
> ⌃ | ⌄ • Reply • Share ›

WHAT'S HOT ⌄