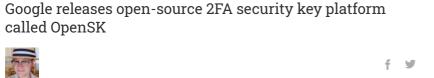




Ryne Hager 16 hours ago



GOOGLE INEWS SECURITY



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.

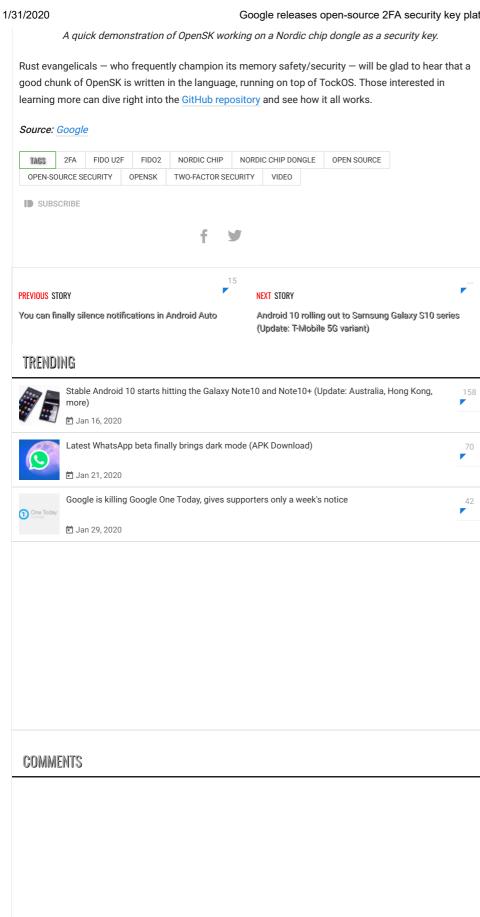
This isn't the sort of thing most of our readers will be able to appreciate immediately, you can't zip out and buy a product running Google's OpenSK just yet. This early, explicitly experimental release is only compatible with a single piece of reference hardware right now: the Nordic chip dongle (for 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 -



Android Police Comment Policy

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



5 Comments Android Police	1 Login ▼
У Tweet f Share	Sort by Best
ssion	
VITH	
UP WITH DISQUS ②	
	¥ Tweet f Share



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 >



Name

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 -

Notice a bug? Let us know here. Link monetization by Skimlinks Privacy Policy | Change Consent | DMCA Disclaimer | About | Advertise | Contact 101 aueries | 0.419s | forge Android is a trademark of Google Inc. | © Illogical Robot LLC, 2009-2020