TOR PHONE MEGA SECURE PHONE IS HERE!

Tor phone is antidote to Google “hostility” over Android, says developer

An Android phone hardened for privacy and security that plays Google at its own game.

J.M. Porup -

Enlarge / Tor-on-mobile prototype goes from mission impossible to merely improbable.
Mission Impossible
27

The Tor Project recently announced the release of its prototype for a Tor-enabled smartphone—an Android phone beefed up with privacy and security in mind, and intended as equal parts opsec kung fu and a gauntlet to Google.

The new phone, designed by Tor developer Mike Perry, is based on Copperhead OS, the hardened Android distribution profiled first by Ars earlier this year.

Further Reading

Building a new Tor that can resist next-generation state surveillance

"The prototype is meant to show a possible direction for Tor on mobile," Perry wrote in a blog post. "We are trying to demonstrate that it is possible to build a phone that respects user choice and freedom, vastly reduces vulnerability surface, and sets a direction for the ecosystem with respect to how to meet the needs of high-security users."

To protect user privacy, the prototype runs OrWall, the Android firewall that routes traffic over Tor, and blocks all other traffic. Users can punch a hole through the firewall for voice traffic, for instance, to enable Signal.

The prototype only works on Google Nexus and Pixel hardware, as these are the only Android device lines, Perry wrote, that "support Verified Boot with user-controlled keys." While strong Linux geekcraft is required to install and maintain the prototype, Perry stressed that the phone is also aimed at provoking discussion about what he described as "Google's increasing hostility towards Android as a fully Open Source platform."

It’s about the software backdoors, stupid!

Apple's iOS is famously more secure than the Android security garbage fire, right?

But Android security will eventually improve, and when that happens, Perry told Ars in an e-mail, "then the next measure will be the ability of the platform to resist backdoors of various kinds."

Further Reading

iPhone exploit bounty surges to an eye-popping £1.2 million

A closed source platform, such as Apple's mobile operating system, is at much greater risk of being compelled to deploy software backdoors, he added.

Enlarge

Tim Ellis

"I think the best argument against backdoors is that they are technically impossible to deploy at all, due to the security properties of the system and people's ability to remove or avoid the backdoor. That argument is stronger for open source than it is for closed source."

Perry also worried aloud about targeted backdoors delivered to specific users.

"The iOS App Store is at a significant disadvantage there even compared to Google Play," he told us. "Each iOS app is re-encrypted specifically for the user with Apple's DRM, making it technically impossible to verify that the package you installed matches the official one."

He said that Apple has "created the perfect platform for delivering targeted backdoors to specific users. I don't like banking on iOS for those reasons."

Google hostile to freedom

In order to solve the Android security mess, Google is taking steps that hurt user freedom, and make Android vulnerable to compelled backdoors, Perry argued.

The fragmentation of the Android ecosystem into multiple OEMs, who distribute their own versions of the operating system, has resulted in rampant insecurity. Without financial incentives to push security updates to users' phones, OEMs by and large abandon users to their fate.

Further Reading

Fix for critical Android rooting bug is a no-show in November patch release

Under pressure from many quarters to solve this problem, Google is working to improve Android security, but Perry criticised Google's release and development process as increasingly opaque.

Android platform is effectively moving to a 'Look but don't touch' Shared Source model that Microsoft tried in the early 2000s," Perry wrote in his blog post. "However, instead of being explicit about this, Google appears to be doing it surreptitiously.

"It is a very deeply disturbing trend."

Copperhead to the rescue

Copperhead OS was the obvious choice for the prototype's base system, Perry told Ars.

Further Reading

Copperhead OS: The startup that wants to solve Android’s woeful security

"Copperhead is also the only Android ROM that supports verified boot, which prevents exploits from modifying the boot, system, recovery, and vendor device partitions," said Perry in his blog post.

"Copperhead has also extended this protection by preventing system applications from being overridden by Google Play Store apps, or from writing bytecode to writable partitions (where it could be modified and infected)."
He added: "This makes Copperhead an excellent choice for our base system."
Daniel Micay, Copperhead's lead developer, welcomed Perry's prototype. "It will be nice to have somewhere to direct technical users that cannot live without Google Play," he told Ars in an e-mail. By default, Copperhead eschews Google Play, and Micay himself refuses to use any Google Apps.

Enlarge / A general outline of Copperhead's main features.
"Mike Perry is interested in doing things properly which is why [the prototype] goes through the effort of not breaking verified boot or depending on leaving an insecure recovery image," Micay said. "The rough edges can be smoothed out over time."

Mission Improbable, but useable today

The prototype, nicknamed "Mission Improbable," is now ready to download and install. Perry said he uses the prototype himself for his personal communications: "E-mail, Signal, XMPP+OTR, Mumble, offline maps and directions in OSMAnd, taking pictures, and reading news and books."
He suggests leaving the prototype in airplane mode and connecting to the Internet through a second, less-trusted phone, or a cheap Wi-Fi cell router.

Further Reading

Double-dip Internet-of-Things botnet attack felt across the Internet

Further Reading

FBI demands Signal user data, but there’s not much to hand over
The prototype is the second of its kind. Back in April, 2014, Perry proposed his first Android device optimised for privacy and security—then nicknamed Mission Impossible. The earlier prototype consisted of a 2013 Google Nexus tablet running Cyanogenmod.
Perry emphasised that the Tor Project has no plans to get into the hardware business, but hopes the prototype will provoke discussion and innovation. He pointed to the Neo900, which bills itself as "The truly open smartphone that cares about your privacy"—a project, he said, that came about in part due to the "Mission Impossible" blog post two years ago.
"What I’ve found is that posts like this one energise the Android hobbyist/free software ecosystem, and make us aware of each other and common purpose," Perry told Ars. "It also shows Google and others what gaps there are in Android for Tor support, and raises awareness about the dangers the ecosystem faces."
Ars readers looking for a weekend project will find the complete Mission Improbable installation instructions on GitHub.
J.M. Porup is a freelance cybersecurity reporter who lives in Toronto. When he dies his epitaph will simply read "assume breach." You can find him on Twitter at @toholdaquill.