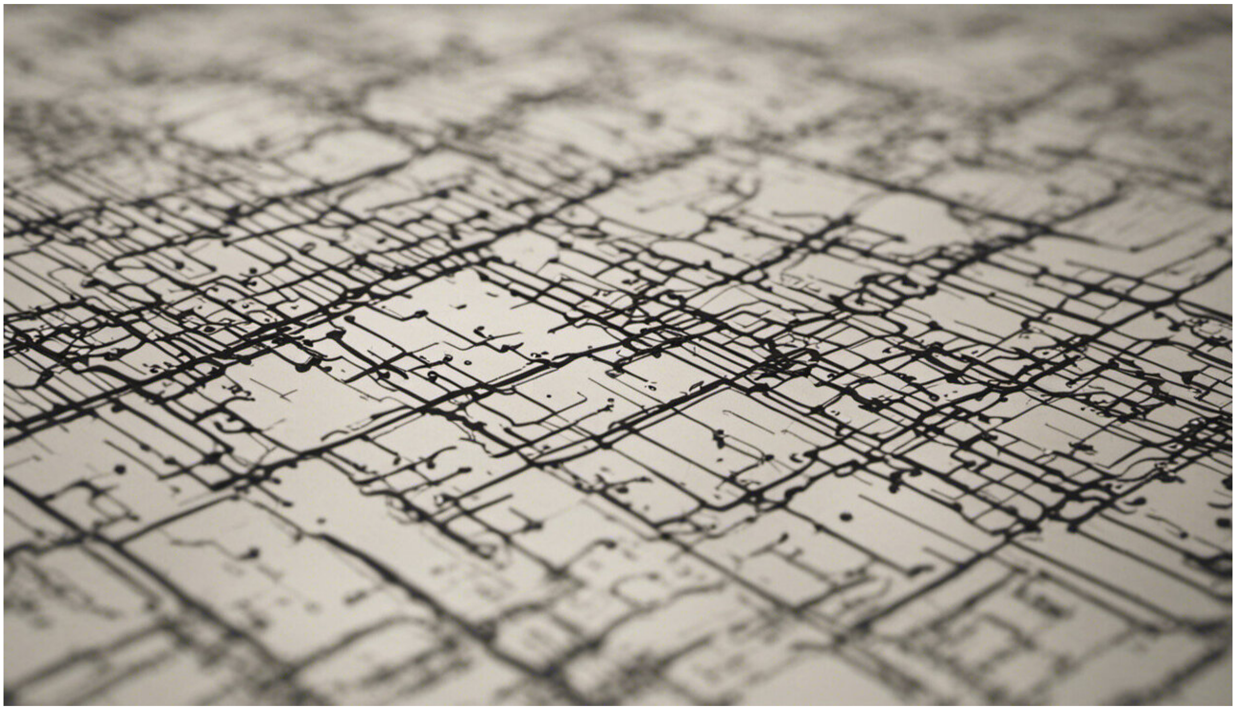
End-to-end encryption isn't enough security for 'real people'

August 14 2017, by Megan Squire



Credit: AI-generated image (disclaimer)

Government officials continue to seek technology companies' help fighting terrorism and crime. But the most commonly proposed solution would severely limit regular people's ability to communicate securely online. And it ignores the fact that governments have other ways to keep an electronic eye on targets of investigations.

In June, government intelligence officials from the Five Eyes Alliance nations held a meeting in Ottawa, Canada, to talk about how to convince tech companies to "thwart the encryption of terrorist messaging." In July, Australian Prime Minister Malcolm Turnbull called on technology companies to voluntarily ban all systems that totally encrypt messages in transit from sender to recipient, an approach known as "end-to-end encryption." British Home Secretary Amber Rudd made global headlines with her July 31 newspaper opinion piece arguing that "real people" don't need end-to-end encryption.

These claims completely ignore the one billion real people who already use secure messaging apps like Signal and WhatsApp. And it leaves no room for people who may decide they want that security in the future. Yet some technology companies look like they might be considering removing end-to-end encryption – and others installed backdoors for government access years ago. It's been two decades since the Clipper chip was in the news, but now a revival of the government-business-consumer "crypto-wars" of the 1990s threatens.

One thing is very clear to computer scientists like me: We real people should work on improving security where we are most vulnerable – on our own devices.

Endpoints are the weakest link

For the moment at least, we do have good, easy-to-use solutions for secure communication between computers, including end-to-end encryption of our messages. End-to-end encryption means that a message is encrypted by the sender, and decrypted by the recipient, and no third party is able to decrypt the message.

End-to-end is important, but security experts have warned for years that the most vulnerable place for your data is not during transit from place to place, but rather when it's stored or displayed at one end or the other – on a screen, on a disk, in memory or on some device in the cloud.

As the WikiLeaks release of CIA hacking tools highlighted, if someone can gain control of a device, they can read the messages without needing to decrypt them. And compromising endpoints – both smartphones and personal computers – is getting easier all the time.

Why are we most vulnerable at the endpoint? Because we don't like to be inconvenienced, and because adding more protection makes our devices harder to use, the same way putting multiple locks on a door makes it harder to get in, for both the homeowner and the burglar. Inventing new ways to protect our digital endpoints without reducing their usefulness is very challenging, but some new technologies just over the horizon might help.

Next-generation solutions

Suppose a criminal organization or bad government, EvilRegime, wants to spy on you and everyone you communicate with. To protect yourself, you've installed an end-to-end encryption tool, such as Signal, for messaging. This makes eavesdropping – even with a court's permission – that much more difficult for EvilRegime.

But what if EvilRegime tricks you into installing spyware on your device? For example, they could swap out a legitimate upgrade of your favorite game, "ClashBirds," with a compromised version. Or, EvilRegime could use a malware "network investigative technique" as a backdoor into your machine. With control of your endpoint, EvilRegime can read your messages as you type them, even before they are encrypted.

To guard against either type of EvilRegime's trickery, we need to improve our endpoint security game in a few key ways, making sure that:

- EvilRegime isn't masquerading as the company that makes "ClashBirds" when we install our software.
- No one has tampered with our "ClashBirds" app before or after installation.
- The app doesn't have any backdoors or security holes that could be exploited by EvilRegime after we install it.

In addition, it would be ideal if users could control their apps' security themselves, rather than having to rely on app store security provided by yet another vulnerable corporation.

Computer security experts are excited about the idea that blockchain technology might be able to help us secure our own endpoints. Blockchain, the technology that underpins Bitcoin and other cryptocurrencies, creates a verifiable, unchangeable public record of information.

What this means for endpoint security is that computer scientists might be able to create blockchain-based tools to help us verify the origin of our apps. We could also use blockchains to confirm our data haven't been tampered with, and to ensure our privacy. And as long as the source code for these programs is also free for us to inspect – as Signal is today – the security community will be able to verify that there are no secret backdoors.

As with any new technology, there is an enormous amount of hype and misinformation around blockchain and what it can do. It will take time to sift through all these ideas and develop secure tools that are easy to use. In the meantime, we all need to continue to use end-to-end encryption apps whenever possible. We should also stay vigilant about password hygiene and about what apps we install on our machines. Finally, we must demand that real people always have access to the best security mechanisms available, so we can decide for ourselves how and when to resist surveillance.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: End-to-end encryption isn't enough security for 'real people' (2017, August 14) retrieved 12 July 2024 from https://phys.org/news/2017-08-end-to-end-encryption-isnt-real-people.html