The Christian Science Monitor

Passcode

Modern field guide to security and privacy

Illustration by Alicia Tatone

The hackers trying to build a hack-proof operating system

PRIVACY

A team of Canadian security researchers is set to unveil a computer operating system called Subgraph designed to protect its users from the most common types of digital attacks.

Jack Detsch
Staff writer | @JackDetsch

MARCH 27, 2017 | MONTREAL — As a teenage hacker in the early 1990s, David Mirza Ahmad quickly learned that even the savviest techies can be "owned," old-school computer slang for exposing someone's identity.

After Mr. Ahmad tangled with rival hackers on a local online message board, they discovered his name and quickly found out his phone number at his parent's home in Calgary. They called him from a payphone down the street, and posing as cops, threatened to press charges for his digital trespassing.

It was just a prank, but for Ahmad, who immediately ripped up his printouts and destroyed his floppy disks after the call ended, it provided a wake-up call that eventually led him to pursue a career in security research. Over the past 25 years as he taught himself the ins and outs of breaking computer programs, he became increasingly aware that the systems that people trust with their most sensitive information are inherently untrustworthy.

On a larger scale, the experience with his online foes in early internet forums isn't all that different from what millions of people experience today when cybercriminals break into their emails or take over social media accounts and expose their personal and financial details.

“All of these anxieties have been scaled up,” he says. The importance of secure computing, “is sort of catching up with everyone,” he adds.

Now, along with David McKinney and Bruce Leidl, the two Calgary pranksters who today are his close friends and business partners, Ahmad has set out to build a more secure computer operating system called Subgraph, designed to withstand common hacks and the most sophisticated cyberattacks.

"We're trying to build security that's invisible to the user," Ahmad explains. "There's always going to be some choices to make. We're not going to stop you, but we're going to pause you."

Development is progressing quickly. Backed with more than $300,000 in funding from the US government's Open Technology Fund, Ahmad plans to release a “beta” version of Subgraph later this year.

It also offers a default built-in firewall that gives Subgraph a chance to help users more easily distinguish between trustworthy and malicious software – a task that's becoming increasingly difficult for users. And he's limited the handful of programs that are available on the operating system, and notifies users whenever an application tries to connect to the internet.

Through a technique known as “sandboxing,” Subgraph aims to mitigate damage caused by criminal hackers by keeping files separate from untrusted programs downloaded online. That can help prevent hackers from readily moving across a user's network. It also allows Subgraph to force apps to communicate only using secure connections.

For self-described paranoid hackers like Ahmad, who assumes that users have already been compromised, that provides clarity and security that isn't available on consumer-ready operating systems. "One thing we don't want is a constant barrage of decisions that users have to make."

Subgraph is set to debut as more internet users are turning to encrypted apps. With a suspected Russian campaign of hacks and leaks dominating election season headlines last year, Apple App Store and Google Play users in the US downloaded the encrypted chat app Signal more than 800,000 times in the run-up to the vote, and saw a 400 percent increase in daily downloads soon after the race ended. Months earlier, WhatsApp encrypted the communications of 1 billion users on the platform by default.

Subgraph's firewall even allows users to readily access system logs that show important security events, a feature that's not available to most Apple and Microsoft users. For instance, the Subgraph team even discovered that the calculator application on its system tried to connect to the web to download currency exchange data – without the user knowing.

"People take it for granted that programs connect to the network. But you don't have any visibility over it," says Mr. McKinney, Subgraph's principal developer. "As our desktop systems become more like mobile systems, you don't know, you can't validate that."

The operating systems also limits so-called “system calls” from programs to the core of the operating system – that can be a gateway for nefarious hackers to steal users' intimate secrets or corrupt the memory. According to their research, the web browser Firefox can make as many as 330 calls to the core of the operating system during a session, but less than half of those actions are needed to run the program.

Mozilla declined to comment for this story.

Those features may not make Subgraph as popular as Apple's Mac operating system or Microsoft Windows. Yet Ahmad and his team want Subgraph to allow users to get under the hood and tinker with their software, a feature that more popular operating systems don't offer.

For Ahmad, the ability to customize, transform, and trade software has been one of the biggest joys of computing since he began hacking as a kid two decades ago.

Confined to their houses by freezing winters and spotty public transportation in Calgary, Ahmad, Leidl, and McKinney used shoddy computer modems to dial into early Microsoft operating systems and networking hardware that connected mainframe computers, phone lines, voice networks, and even signal-collecting multiplexers as if they were dialing numbers in the phone book.

Indeed, logging onto the decentralized internet of the early 1990s took more craft than picking the right Wi-Fi network. For Ahmad, who almost failed to graduate high school because he skipped class to hack, users should be able to choose their route.

"One of the decisions we want to have [users] make is how their packets are transmitted over the internet," says Matthieu Lalonde, Subgraph's lead developer. "You should get to choose the highway you want to take."

And that's not just an issue for privacy junkies such as Mr. Lalonde, who's also removed the microphones from his laptop to ward off digital eavesdroppers and has an external physical key he uses to turn the computer on. When Facebook and Google turned off access to an open source communications protocol in 2015, for instance, Subgraph's founders say it cut users off from a key privacy tool that allowed them to encrypt and segment their communications.

What's more, as advertising becomes increasingly targeted on the social networking platform, they're worried that even keeping your information private on Facebook and other networks can be a huge challenge, because security settings aren't easy to find.

"[On Facebook,] there aren't any boundaries. It's meant to be confusing so you don't know," McKinney says. "They're happy that it's an intellectual burden to figure out the privacy settings."

Subgraph isn’t for everyone. The interface seems particularly barren compared with Apple or Microsoft operating systems. In a early version seen at their Montreal headquarters, the developer had only Richochet, an encrypted chat client that keeps no user metadata, the Tor Browser, the anonymizing web browser, and a handful of other programs open on the desktop. And Mr. Lalonde – known as "smurf" to his colleagues since he used to sport a shock of blue hair – is still trying to get Subgraph to allow printing, but he says that's "a big security problem" because it can be difficult to authenticate hardware that's remotely connected to a computer.

Yet the functionality is improving: Subgraph recently figured out how to securely run Spotify on the platform. But for Ahmad, restoring control over software to users is a worthy endeavor.

"It's not a purely ideological project. It's a very practical project," Ahmad says. "We want to try and preserve our control over our internet experience."