Are virtual private networks actually private?

October 12 2022, by Annelise Krafft

Associate Professor Jedidiah Crandall hopes his research will help inform users that the networking fundamentals of virtual private networks, or VPNs, do not provide the security properties people expect. He wants to illuminate a path forward to building a better VPN. Credit: Shutterstock

In countries where internet censorship and surveillance are government policy, online security is crucial for at-risk users. Journalists, activists, politicians and others with a prominent online presence can face dire consequences for even the websites they browse.

Virtual private networks, or VPNs, are designed to keep users' data protected from surveillance, but whether they do what they claim is of utmost importance to those whose lives can depend on their effectiveness. The ability of VPNs to protect users also inspires the research of Jedidiah Crandall, an associate professor of computer science at Arizona State University.

Crandall explains that VPNs conceal your internet protocol, or IP, address by linking it to a different server than your own and making it seem as though you're accessing the internet outside of your normal network.

"VPNs were originally designed to get into a secure network, but companies have repurposed them so you can escape a restrictive internet service provider that you don't trust and access a free and safe one instead," Crandall says. "So, the way that people use VPNs today is kind of backwards."

Crandall notes that this access is helpful when users are worried about their browsing data being monitored though their internet service provider, or ISP, or when users are in a country that censors their internet content.

Resources like OpenVPN, a leading global private network and cybersecurity company, and the most popular resource for commercial VPN services, boast access to tools that quickly and easily connect to private networks and safeguard assets. But Crandall's research aims to debunk claims of privacy and expose whether VPNs may create a false sense of security for their users.

"We're really just asking fundamental questions like 'When you repurpose VPNs in this way, do they actually have the security properties that people expect?'," he says, reiterating his work's focus on at-risk

users who face severe consequences from censorship and surveillance policies. "The first part of the research we did was looking at the VPN tunnel itself, which is an encrypted tunnel between the VPN server and the client, to see what kind of damage attackers can do from there."

To discover how attacks can be made, Crandall and a group of researchers simulated a series of attacks from two potential threat paths: client-side, or direct attacks on the user's devices, and server-side, or attacks on the VPN server accessed by the user's device. The group detailed their findings in a paper titled "Blind In/On-Path Attacks and Applications to VPNs."

The team concluded that traffic can still be attacked from the tunnel in the same ways as if a VPN were not being used, with attackers able to redirect connections and serve malware from which users believe a VPN protects them.

Now looking at the threat of an attack as possible and not just hypothetical, Crandall collaborated with a team of researchers—including experts from the University of Michigan and Merit Network—on a paper titled "OpenVPN is Open to VPN Fingerprinting" for the 2022 USENIX Security Symposium.

The research addresses how VPN adoption has seen steady growth due to increased public awareness of privacy and surveillance threats and how some governments are attempting to restrict access by identifying connections using deep packet inspection, or DPI, technology, which is commonly used for online eavesdropping and censorship.

"A lot of the credit goes to the team at the University of Michigan, who really spearheaded this research," Crandall says. "A big part of this work is trying to set the standards of how to bring together different stakeholders so that everyone, from the VPN providers to the users, has

the same expectations. But we're also trying to define what those expectations should be."

"For people around the world, there can be a lot at stake when VPN providers market with false claims about their services. Our research exposed how VPN-based services, including ones marketing thier VPN service as 'invisible' or 'unblockable' can be effectively blocked with little collateral damage," says Ensafi, an assistant professor of electrical engineering and computer science. "Jed is one of the leading internet censorship researchers who has been focusing on network interference since 2005, so he has been instrumental in moving this research forward."

More information: Blind In/On-Path Attacks and Applications to VPNs

OpenVPN is Open to VPN Fingerprinting

Provided by Arizona State University