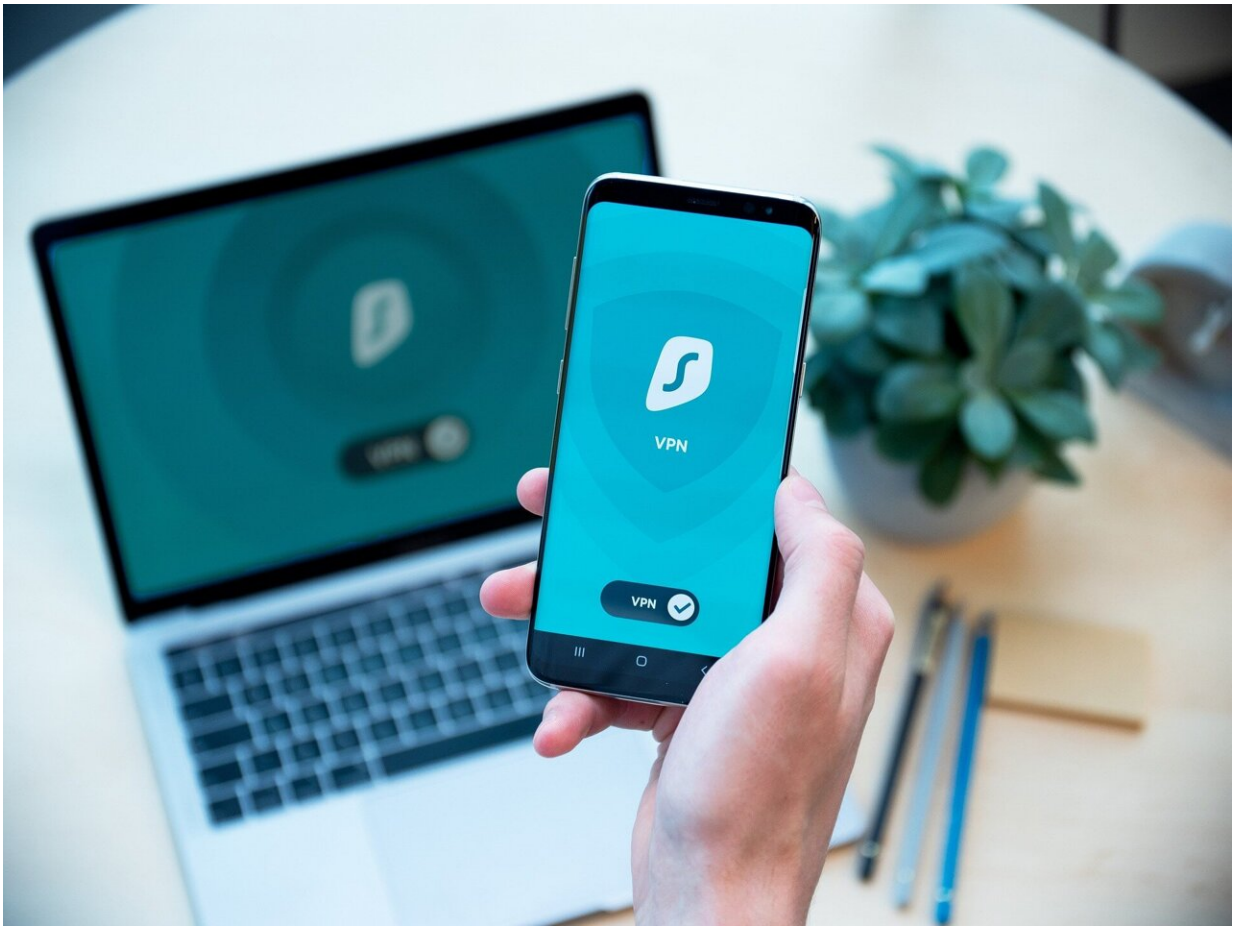
A VPN can be one internet tool but often is not sufficient for all privacy needs

February 8 2023, by Zach Champion



Credit: Pixabay/CC0 Public Domain

Every day, thousands of people turn to VPNs to ensure their privacy and

security while living and working on the internet. A series of recent studies at the University of Michigan have called into question how accurate these expectations can be.

Virtual private networks, or VPNs, allow users to create "tunnels" through their network for purposes of concealing activities and identities and making secure connections to other internet locations. These would appear an ideal tool for evading surveillance or securely accessing blocked content—but new research shows that reliance on VPNs could be exposing users to more surveillance than they realize.

Over the past two years, the U-M researchers have performed a series of research projects under an effort they've called VPNalyzer to expose issues including critical shortcomings in popular currently available commercial VPNs, the ability of network service providers and governments to identify and block the use of VPNs, and issues in user education and gaps in understanding between VPN users and VPN providers

Led by assistant professor of computer science and engineering Roya Ensafi and doctoral student Reethika Ramesh, the research team's expertise spans network measurements, security, privacy, and also qualitative and quantitative study methods.

First, the researchers' efforts were centered around a project building the VPNalyzer tool to bring rigor, scale, and automation to investigating the VPN ecosystem. They tested 80 popular VPN providers using VPNalyzer and uncovered previously unreported vulnerabilities including DNS and IPv6 leaks, data leaks during tunnel failure, and more, which led them to file 29 responsible disclosures to the VPN providers.

VPNalyzer began with a security review of VPNs in collaboration with

Consumer Reports in 2021. The Consumer Reports team used VPNalyzer as part of their efforts to produce a data-driven and reliable recommendation for their millions of users. Their work was quoted in the following articles written by Consumer Reports: Should You Use a VPN? and VPN Testing Reveals Poor Privacy and Security Practices, Hyperbolic Claims. Data from this work with Consumer Reports have also already been cited by members of Congress to call on the FTC to enhance protections for VPN users. Moreover, the researchers' first paper on that project was the largest study of consumer-facing VPNs to date, and won first place in the CSAW '22 Cybersecurity Applied Research Competition that took place at NYU in November 2022.

The U-M team also collaborated with researchers at Arizona State University led by associate professor Jed Crandall, University of Michigan Information and Technology Services, and research scientist Michalis Kallitsis at Merit Network to demonstrate how easy it is for network providers and censors to detect the use of OpenVPN, the most popular VPN protocol in widespread use. In this work, they detailed a technique to challenge VPN anonymity and accurately identify or "fingerprint" over 85% of OpenVPN flows on a one million-user ISP, with negligible false positives.

"We conclude that tracking and blocking the use of OpenVPN, even with most current VPN countermeasures, is straightforward and within the reach of any ISP or network operator," the team wrote in their paper.

VPNs typically promise identity protection, the ability to safeguard planned political action, and the ability to circumvent censorship and geoblocking. The vulnerability the researchers identified calls them all into question. The work won first place in the USENIX/Meta Internet Defense Prize at the 31st USENIX Security Symposium.

"A VPN can be one tool in an Internet user's toolbox but often is not

sufficient as the only solution for all privacy needs," says Ramesh.

Equally valuable, the researchers say, are the insights gathered from their extensive user and provider surveys. With their latest quantitative and qualitative study paper, which has been accepted for presentation at USENIX Security 2023 in August, they advance the understanding of the commercial VPN ecosystem, and illustrate key issues and areas of concern to help security and privacy advocates such as Electronic Frontier Foundation and the Center for Democracy and Technology, technologists, and VPN providers themselves focus their efforts.

From their study of 1,252 users and nine VPN providers, they also present actionable recommendations for the VPN ecosystem including prioritizing user education, oversight on advertisements and marketing surrounding VPNs, coordinated efforts to bring attention to the flawed VPN recommendation ecosystem, and regulations to curb malicious marketing tactics that lead to false mental models and false expectations for users.

Ensafi, Crandall, and Kallitsis are looking ahead to advance VPN ecosystem research and rethink the fundamentals of tunneling technologies for security, privacy, and usability.

"People around the world are using VPNs in hopes of protecting their privacy and gaining security," says Ensafi. "We want them to know that they should not assume that today's VPNs are the complete answer."

More information: "All of them claim to be the best": Multi-perspective study of VPN users and VPN providers.
vpnalyzer.org/assets/VPN_Surve … SENIX23_Preprint.pdf

VPNInspector: Systematic Investigation of the VPN Ecosystem.
www.ndss-symposium.org/ndss-paper/auto-draft-244/

Provided by University of Michigan