Project Topic

Fingerprinting Virtual Private Networks

Background

Virtual private network (VPN) services have become increasingly popular as means of hiding Internet activity, particularly in contexts where Internet censorship and surveillance are prevalent. A VPN tunnels network activity via a secured channel to a VPN server and from the VPN server to the requested websites or services. VPN services are used not only by journalists or activists who may be vulnerable to monitoring or targeting, but also by the general public who value their online privacy while browsing the web over public WiFi networks, connecting remotely to their workplace services, or to access content/services that may be censored in certain parts of the Internet. As VPNs have become more widely used, censorship bodies such as states seeking to control and restrict Internet access that are often motivated by moral or religious values have invested heavily in developing and deploying sophisticated censorship technologies to prevent the dissemination of information, suppress challenges to their official narrative, maintain authority, and prevent disruptions in society.

Project Description

This research program is designed to introduce high school students to the fundamentals of Internet censorship, Network Address Translation (NAT) and VPNs to equip them with the skills needed for future academic and professional pursuits in computer science, computer networks, and network security. The program will involve an investigation of an efficient approach to fingerprint VPN traffic at home routers even when VPN traffic is obfuscated. The key idea behind is that end devices using a VPN connection will, by default, send all their traffic to the same destination (the VPN server) identified by its public IP address. On the other hand, non-VPN traffic is typically sent to a mix of different destinations; e.g. websites, weather widget, OS update server, etc. The model will be tested in a realistic Internet setup.

Prerequisites

- **Grade Level:** 10th grade and above.
- **Interest:** Must have a keen interest in computer science and network security.
- **Skills:** Basic coding skills.
- **Technology:** Access to a computer with internet connection.

Project Outcomes

By the end of the program, students will be able to:
Review of Virtual Private Networks (VPN) fundamentals: Gain knowledge about VPNs, and NAT.
Setup a VPN testbed: Setup a VPN testbed and install necessary tools to conduct a measurement study.
Conduct measurement study: Test access to VPN servers and collect relevant data.
Explore and Visualize Data: Use data visualization tools such as Mathematica or GNUplot.
Enhance Research Skills: Develop essential research skills, including data collection, analysis, and interpretation.
Improve Communication Skills: Enhance written and oral communication skills through a project report and a presentation of the research findings.

Program Structure (Tentative Schedule)

● **Week 1:** Introduction to VPNs and NAT.
o Overview of VPN
o Overview of NAT
o Literature review

● **Week 2:** Setup VPN testbed.
o Installing VPN clients to access popular VPN servers.
o Defining relevant experiments, metrics to be collected and writing relevant scripts.
o Running preliminary experiments.

● **Week 3:** Conduct study, collect and visualize results.
o Complete the experiments and collect results
o Plot the results and draw conclusions
o Propose possible extensions

● **Week 4:** Project report development and presentation
o Research report
o Presentation of project and peer review
o Feedback and refinement of final deliverables

Deliverables

- **Research Report:** A detailed report on the chosen topic, including problem statement, background, research methodology, data analysis, and findings.
- **Presentation:** A PowerPoint presentation summarizing the research project.

References:

[1] A. Thompson, “Buying Silence: The Price of Internet Censorship in China,” Jan. 2021. [Online]. Available: https://cset.georgetown.edu/article/buying-silence-the-price-of-internet-censorship-in-china/

[2] B. Toulas, “Russia’s ’Oculus’ to use AI to scan sites for banned information,” BleepingComputer, Aug. 2022. [Online]. Available: https://www.bleepingcomputer.com/news/security/russias-oculus-to-use-ai-to-scan-sites-for-banned-information/

[3] S. Almutairi, Y. Neumann and K. Harfoush, "Fingerprinting VPNs with Custom Router Firmware: A New Censorship Threat Model," *2024 IEEE 21st Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 2024, pp. 976-981

Tuesday and Thursday 8-9 PM