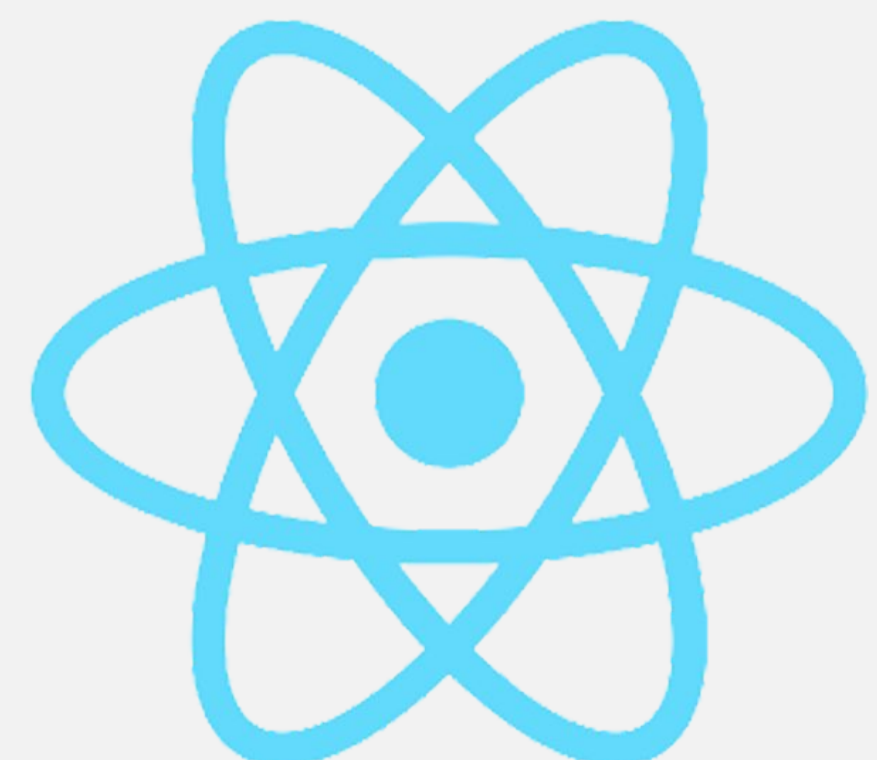


AmiLeaked

Students: Fabian Roman, Lucas Garcia, Javier Bautista, Austin Navas, Noah Fernandez

Instructor/Faculty: *Masoud Sajadi*, Florida International University



React



WHAT IS AMILEAKED?

AmiLeaked is a VPN leak detector web extension that uses observed network behavior to monitor data leaks in a user's VPN connection. Built with React and JavaScript, it periodically scans for changes in IP data while a VPN connection is active and compares it against a baseline fingerprint of the user's real data to detect leaks. Captured vectors include IPv4, IPv6, DNS, and WebRTC. All data is stored temporarily within the program; nothing is sent to a 3rd party service.

SYSTEM DESIGN

AmiLeaked utilizes a baseline comparison technique to enable the detection of VPN leaks. At the extension's startup, a no-VPN network fingerprint is recorded in a first-time setup. This fingerprint is then stored in the extensions local database as a reference point used to compare against future IP detections.

During operation, present IP data is periodically compared against the baseline fingerprint. If any of the users current IP data matches that of the baseline, a leak is flagged.

VERIFICATION

The extension was subjected to tests through several VPN scenarios, along with forced leaks to test its efficiency. In these scenarios, typical VPN usage behaviors were employed, such as turning it off/on and changing VPN related settings like location and connection method. IP leaks were also forced through the usage of html scripts in a controlled environment, and AmiLeaked was able to successfully pick up on these leaks.

PROBLEM

Many people depend on a Virtual Private Network (VPN) to stay private on the internet. However, they may still be leaking their real IP information through intermittent breaks in these private connections. Critical details such as ISP provided public IPs, DNS information, or WebRTC information can be leaked through unannounced VPN leaks that happen in the background.

OBJECT DESIGN

There are various jsx files within the build that each handle different tasks. The ipService module captures the data of common network protocols such as IPv4, IPv6, DNS, and WebRTC data. The baseline storage module takes care of storing the data collected from the network protocols in Chromes persistent storage. The comparison script compares the baseline data with the new data to detect any changes, and the notification system uses extension badges and the Chrome notification API to send leak notifications.

SUMMARY

AmiLeaked was capable of offering a timely and privacy-conscious method of determining whether a user's private network connection is experiencing a leak while using the Internet. It aims to stand out from the other VPN leak detectors on the internet by providing local processing, background detection scans, and no reliance on private VPN sourced IP records.

CURRENT SYSTEM

The current services used for detecting leaks in VPNs have some disadvantages. Most of these tools don't carry out continuous monitoring, only conducting one-off tests of current network traffic. These programs also tend to use history-based records of VPN IPs given to them by private companies. These IPs may fall out of use or be replaced by new ones, which may not be updated concurrently.

IMPLEMENTATION

AmiLeaked is implemented as a lightweight browser-based extension that operates in real time while the user browses. It utilizes network fingerprinting through public APIs to capture and analyze user connection data without relying on other complex 3rd party services. All processing is performed locally on the user's device, ensuring privacy and security.

REFERENCES

IEEE. (2020). IEEE Standard for Virtual Private Network (VPN) Security.

NordVPN. (2023). What is a VPN leak? Retrieved from <https://nordvpn.com>

Mozilla. (2024). WebRTC and IP Address Privacy. Retrieved from <https://developer.mozilla.org>

Cloudflare. (2023). What is DNS and how does it work? Retrieved from <https://www.cloudflare.com>

Khan, R., & Smith, J. (2021). Network Fingerprinting and Privacy Risks. Journal of Cybersecurity, 12(3), 45-58.