blogs.unb.ca

# New dataset from UNB to help detect man-in-the-middle attacks

3 minutes

The Canadian Institute for Cybersecurity (CIC) at the University of New Brunswick has released its first-ever DNS over HTTPS (DoH) dataset funded by CIRA's Community Investment Program. The benchmark cybersecurity dataset, named CIRA-CIC-DoHBrw-2020, will be used to improve privacy of encrypted communication and detect man-in-the-middle attacks.

The dataset has been created by a CIC team led by Dr. Arash

Habibi Lashkari, CIC's research coordinator and assistant professor in UNB Fredericton's faculty of computer science. The project is funded by Canadian Internet Registration Authority's supports initiatives that build a trusted internet for Canadians. The representative dataset contains encrypted DNS packets and traffic flows to detect eavesdropping and tunneling activities and characterize DoH traffic.

This is the first in a series of two datasets of this kind. It collects encrypted DNS queries and responses at web browser, whilst the second dataset will be deployed at a larger level and will be capturing malicious DNS requests and responses at DoH server. It will be named CIRA-CIC-DoHPrx-2020 and will be released soon.

"Since DoH is still an evolving area, a representative dataset can open several research directions for fellow researchers and scholars to identify security issues in DoH and use this dataset to evaluate their new solutions and approaches," says Dr. Lashkari.

Since joining UNB five years ago, Dr. Lashkari has been involved in the generation of several datasets such as VPN Traffic (ISCX-VPN-2016), Malicious and Obfuscated URLs (ISCX-URL-2016), Tor Traffic (ISCX-Tor-2017), Android Adware (ISCX-AAGM-2017), Android Malware (CIC-AndMal-2017 and InvesAndMal2019), Intrusion Detection and Prevention (CIC-IDS-2017 and CSE-CIC-IDS-2018), and DDoS (CICDDoS2019). These datasets have been used by industry and academia around the world to test their algorithms, solutions and techniques.

"CIRA believes in the importance of DNS encryption as the next important internet standard to help protect the personal privacy of Canadians from corporations and hackers," says Byron Holland,

CIRA's president and CEO. "With our goal to build a trusted internet in Canada, we're proud to fund this initiative that contributes to improved cybersecurity for Canadians."

**Media contact:** Kelsey Pye