Prof. Dr.-Ing. habil. Falko Dressler
Data Communications and Networking – TKN

Technische Universität Berlin

Master’s Thesis

Encrypted Traffic Detection: Beyond the Port_number Era

Encryption is introduced to protect the online communication of people all around the world. Nowadays, a significant amount of our online activity is under encryption protection.

However, Internet Network Providers used to sneak into their user data to improve their functionality and identify any security threat. ISPs use expensive but accurate technics like Deep Packet Inspection to extract valuable information from their users’ traffic. Unfortunately, these technics are useless facing with encrypted traffic. Therefore, the ISPs need to identify encrypted traffics and treat them differently. Relying on the port number is the current trend to identify encrypted traffic. E.g. if a network traffic use port number 443, then it will be considered as encrypted data and be treated accordingly. Following, an intruder can switch to a different port number to carry its encrypted traffic and easily bypass the security mechanisms of the network.

Goals of the Thesis

You, as a well-prepared researcher, are in charge of finding a new way that is more robust than the port number to identify encrypted traffic. In your quest, you should read many different papers and documents to identify the unique footprint of encrypted traffic. As the next step, you should develop a tool that looks in the traffic to find the footprint and label it as encrypted or not.

Of course, you will not be alone in your journey and your supervisor will guide you to take each step and will keep a close eye on you to correct any deviation toward your goal. In the end, you will finish your journey by defencing your thesis and introduce yourself to the academic community with (a) valuable publication(s). Besides, you will have a repository to maintain that host a precious tool to protect the online activity of thousands of people

Keywords

Encryption detection, Network Security

Contact:
Hossein Doroud: <h.doroud@tu-berlin.de>

Website:
www.tkn.tu-berlin.de