Keio University

Thesis Abstract

No.

Registration Number:	□ "KOU" □ "OTSU" No. *Office use only	Name:	Ferriyan, Andrey

Title of Thesis:

Malicious Traffic Detection In Encrypted Network

Summary of Thesis:

Traditional Network Intrusion Detection Systems (NIDS) practically cannot deal with encrypted data, hence malicious applications, which increasingly use TLS, can freely flow undetected. Therefore, a network intrusion detection system breakthrough is required to prevent and mitigate the risk of malicious applications.

This dissertation aims to detect malicious traffic in an encrypted network that utilizes SSL/TLS traffic. The challenges in detecting malicious applications are a lack of publicly open datasets, NIDS's incapability to detect attacks, and drawbacks of compliance. The dissertation focuses on methods for the detection of the malicious application, the procedures on how to build a new dataset, and determining the compliance of cybersecurity. Among the factors preventing evaluation and comparison are a lack of proper documentation, a lack of comparison technology, a lack of crucial features such as ground-truth labels, and a publicly available, and real-world environment. Two requirements are needed to overcome this. The content requirements focus on the produced dataset, such as complete capture of the traffic, payload, anonymity, ground-truth, up-to-date, labeled dataset, and encryption information. The process requirements focus on how the dataset is built. These requirements produced the HIKARI-2021 dataset and enables future dataset development, which assists security researchers in evaluating network intrusion detection systems.

Existing approaches such as Deep Packet Inspection require traffic decryption and hence potentially breach privacy. Furthermore, the key finding was that the malicious application tends to use weak encryption, offers fewer extensions, and has a specific pattern that differs from the others. The method called TLS2Vec analyzed TLS handshake and the payloads which can be used to take immediate action before the conversation is finished. The evaluation revealed that the detection performance using only TLS handshake information to distinguish between Malicious and Benign with two public datasets reached 99%. The average detection rate was 82% of the total multiclass target. In order to have a comprehensive view in terms of preventing malicious applications, measuring cybersecurity compliance is needed. The evaluation was carried out to identify the potential risk of the data center using COBIT and vulnerability assessment to measure the current condition of the data center. The evaluation focuses on the monitor the infrastructure for security-related events.

Keywords: Privacy Preserving IDS; TLS; Encrypted Malicious Traffic, network intrusion detection systems; network intrusion datasets; encrypted network traffic; https;