Detection of Malicious Network Traffic Behavior

Student: Mgr. Pavel Novák *Advisor: Ing. Václav Oujezský Ph.D.* *Faculty of Informatics MU*

Encrypted traffic in today's networks is an indispensable attribute. It is a valuable tool to protect users' data against eavesdropping or modification. However, encryption also opened new opportunities for malware developers because it makes hiding malicious communication more effortless. Encrypted traffic is much harder to analyze because of privacy issues and performance demands. This inevitably leads to massive research in this area and the development of techniques to classify encrypted traffic without decrypting it.

One of the used methods is called fingerprinting method. TLS fingerprint is a set of metadata about the TLS connection. These data might be arbitrary. For example, it might be the supported TLS version by the client or supported ciphers. The important thing is that all this information is sent during the TLS handshake in plaintext.

The fingerprinting method is currently being used to detect malware, for example, in the Suricata IDP system. Detection is typically based on the direct match with the known "bad" TLS fingerprint. However, this means the problem when dealing with an unknown, new or unexpected threat. When the malware uses the TLS fingerprint we didn't see before, we can no longer detect the traffic as malicious.

The method proposed and tested during the research tries to invert the detection mechanism approach inside out. Instead of detecting the known "bad" TLS fingerprint, we learn the expected "good" traffic for our application and then detect deviations from this traffic. In the first step, clean traffic was simulated, and TLS fingerprints were collected. These fingerprints were clustered together in the second step. Three different clustering algorithms were compared here. The detection has been based on the comparison and deviations between clusters' areas of clean and mixed traffic. This idea is depicted in Figure 1. Green dots and the green line represent the area of clusters containing the known "good" TLS fingerprints. The red dots represent malicious TLS fingerprint clusters, and the red line represents the traffic containing a mix of clean and malicious clusters in the unknown mixed traffic. The detection is based on the fact that these two areas are significantly different if the unknown traffic contains malware.

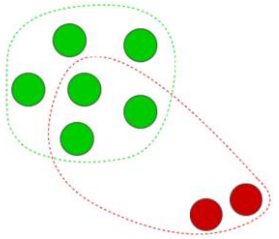

Figure 1: Comparison of the Cluster Areas

During the practical part of the research, we proved that this detection mechanism could detect malware in the network traffic. Moreover, this mechanism is much more universal because it can detect any unknown and thus potentially malicious behavior.