Heimdall: Detecting Malicious Behavior in USB Mass Storage Devices

Zlatanov, Ivan (School: National Trade and Banking High School)

USB mass storage devices security has been a leading issue in cybersecurity for decades. Attacks like Stuxnet and Flame and USB exploitation methods like BadUSB and Cottonmouth-I demonstrated the real-life threats that this problem poses. Because of these reasons, multiple government and private entities have restricted the usage of USB mass storage devices in their facilities. Previous researches in the field address this issue by either developing devices that can sanitize data on USB mass storage devices or designing methodologies and systems that provide theoretically safe usage of USB peripheral devices by logical separation. However, these works have their weak points and severe limitations. In this paper we discuss Heimdall - threat evaluation framework, running onto an embedded device that can perform tests on conceivable malicious USB mass storage devices without the risk of compromising or destroying legitimate computer systems.

Awards Won: