Preventing USB Drop Attacks

Abstract:

As USB memory drives become popular, it presents a significant security risk for business: **Abstract** and government agencies for the last few years. The problem arises that adversary who has a physical access to any host computer can loads malicious code onto a USB flash memory to infect that computer which it is plugged in to. In this project, USB signing enforcement approach was proposed which restrict unidentified USBs to be inserted into any host computer only for users who have a valid credentials in order to overcome what is known as USB drop attack.

Worthy to mention, any suspicious or irregular login attempts, the proposed system takes a picture for a person who sitting in front of computer and sends it immediately to administrator email as additional security actions. The experiments showed the effectiveness of the proposed system to restrict various types of USBs from displaying their content using a valid login account registered uniquely based on MAC address of host computer.