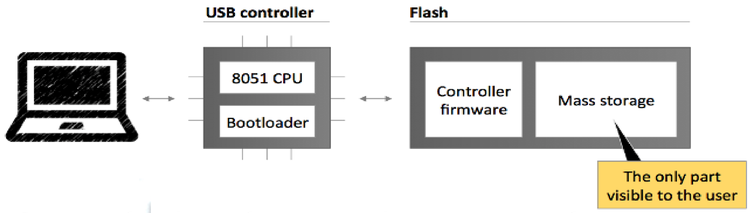
Accurate Fingerprinting of USB Devices to Enable Whitelisting-based Device Security

Hessam Mohammadmoradi
Networked Systems Laboratory, Computer Science Department
University of Houston

Overview

- ✓ There are many devices which use USB port for communication and this popularity is widely abused by hackers to propagate their malicious code
- ✓ Anti-malware solutions usually analyze storage space of USB devices for suspected code signatures
- ✓ New generation of USB malware, instead of hiding on storage space, just update firmware and avoid being detected by anti-malware



- ✓ One of the famous instances of new generation of USB malware is BadUSB
- ✓ There are two possible protection against BadUSB:
  - ✓ Locking Firmware Update
  - ✓ Building Whitelist of Trusted USBs

In Our Research

- ✓ Surveyed current state of the art USB whitelisting solutions
- ✓ Generating unique fingerprint for USB devices is common problem among current solutions
- ✓ Our idea is utilizing features related to USB device to generate a unique identifier
- ✓ We verified accuracy of our model using real data collected from USB devices used by our department's students

Data Collection

Collected Attributes

- ✓ Device Type: Based on USB class code there are different device types such as Mass Storage and Human Interface Devices.
- ✓ Serial Number
- ✓ Firmware Version
- ✓ Driver Filename, Driver Version
- ✓ Last Plug/Unplug Time
- ✓ Vendor ID, Product ID
- ✓ USB Class, USB Sub Class, USB Protocol
- ✓ IP and MAC Addresses
- ✓ User ID

Data Collection Process

- ✓ Lightweight Java Application
- ✓ Fetch Windows registry file (Windows keeps track of devices connected to USB ports in registry file)
- ✓ Extract information regarding devices connected to USB port
- ✓ Send information to central database over the Internet

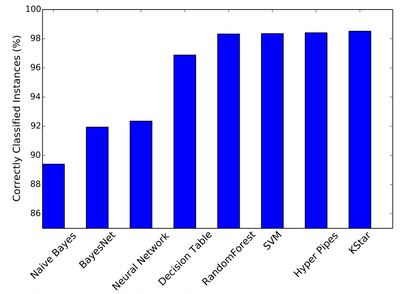
Summary of Dataset

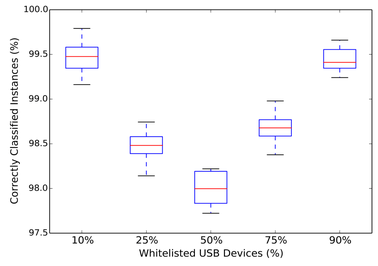
- ✓ We monitored **57** desktop computers located in **2** academic labs
- ✓ Host operating systems were **Windows 7 & 8**
- ✓ Sampling rate was **1** sample per minute
- ✓ Monitoring process was started by **November 2013** and was ended by **December 2014**

Design & Evaluation

Building Model

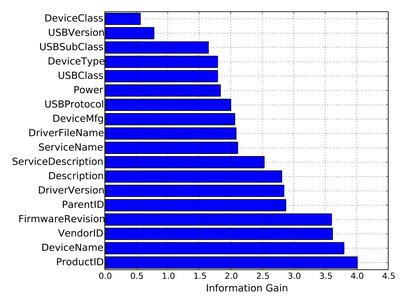
- ✓ Use collected properties to generate unique fingerprint
- ✓ Apply supervised classification techniques to build a model
- ✓ 10 Fold Cross Validation

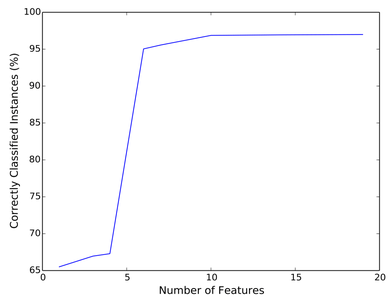




"BadUSB" Detection

- ✓ Randomly divide USB devices to Whitelist and Blacklist Clusters
- ✓ Apply our model to distinguish Whitelisted USBs from Blacklisted ones





Information Gain

- ✓ Sort features based on their Information Gain
- ✓ Top 7 features will generate result with 95% accuracy

We would like to thank Tom Cumpain for logistics support.