IoT device identification

The need

- Day by day the number of IoT devices used in organization specfic networks are increasing
- It is becoming tough to identify what are the IoT devices and what are non-IoT devises connected in the organization network
- This has become key aspect of security

Problem statement

- To distinguish between IoT devices and non-IoT devices by classification
- For a specific IoT device to model its network behavior and detect the device’s presence in the network

Current Scenario

- One possible way is to use the prefixes of MAC addresses to identify the manufacturer of the devices
  - There is no standard to identify brands
  - Aswell types of devices

Proposal

- To identify malicious traffic in network communications using network features like
  - Ratio between incoming and outgoing bytes
  - Average time to live
- Using network traffic analysis

Approach / Plan

- To collect traffic data from local IoT devices
- Convert theTCP packets to some standard form using some feature extractor
- To classify the datasets using machine learning techniques

What Next

- Identify / Study different network traffic extractors (feature extractors)
- To classify using machine learning algorithms

Traffic features in a Network

&

Network Traffic Analysis Tools

Traffic Features

- Include
  - ✓ Port number
  - ✓ Packet interval time
  - ✓ Different bytes of the data packet and so on
    - ✓ have a total of more than 200 features

- Used to describe and measure network traffic
- Used as an input of traffic classification algorithms

Traffic Features contd...

- Traffic features are clasified into:
  - packet header feature
  - load feature and
  - flow feature

NTA : Network Traffic Analysis

- Network traffic analysis involves examining packets passing in the network
- This is intended to investigate the sources of all traffic and
- The volumes of throughput for the capacity analysis

NTA : Network Traffic Analysis contd...

- Now a days NTA includes
  - deep packet inspection
    - » used by firewalls
  - traffic anomaly analysis
    - » used by intrusion detection systems

NTA Tools: Features required

- NTA tools required to perform the following
  - Copy passing traffic into files
  - Analyze traffic patterns
  - Sample traffic from several points of the network simultaneously
  - Consolidate the source material to discover unusual behavior

NTA Tools: Features required Contd...

- NTA tools need not have to operate at rapid speeds
  - As the security applications can not recgnize threats unless they have streams of data to work on
  - So there is less urgeny
  - But more accuracy is desired

NTA Tools: Features required Contd...

NTA tools have to operate at the Application Layer and not at the Network Layer

- As the Application Layer gives the NTA tool a better overview of network activity

NTA Tools

- Few best NTA tools
  - 1.SolarWinds NetFlow Traffic Analyzer
  - 2.ManageEngine OpManager Plus
  - 3.Elastic Stack
  - 4.Plixer Scrutinizer
  - 5.Open WIPS-NG

SolarWinds NetFlow Traffic Analyzer

- Features:
  - 1.Includes the Network Performance Monitor
  - 2.Packet analysis utilities built into network equipment to get packet samples and throughput metrics
  - 3.Displays the collected data live on the screen
  - 4.Able to identify Virtual LANs
  - 5. Alerts if traffic starts to push to the limit of the network’s capacity

SolarWinds NetFlow Traffic Analyzer Contd...

- Features:
  - 6.Can segment data by source and protocol / port
  - 7. Can display the time based charts with peaks and troughs in traffic volumes
  - 8. Works with Microsoft Windows Servers
  - 9. A 30 Day Free Trial available
- Proproitary Software

WireShark

- Features:
  - 1.Free and Open source software
  - 2.Complete documentation available along with user guide
  - 3.Administrators can use to troubleshoot Network problems
  - 4.Learners can use to understand network protocol internals
  - 5.Developers can use to debug protocol implementations

What next

Planning to study the complete documentation of Wireshark

Wireshark – Features

- It lets us see what's happening in the network at a microscopic level
- Tool that can capture and help us to analyze the packets
- Wireshark is the popular open source graphical user interface (GUI)
- Also provides a powerful utility called TShark for people who prefer to work on Linux command line
- The de facto standard across many commercial and non-profit enterprises
  - Like Government agencies and
  - Educational institutions

Wireshark – Features Contd

Wireshark has a rich feature set which includes the following:

- Deep inspection of hundreds of protocols
- Live capture and offline analysis
- Multi-platform: Runs on Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, and many others
- Captured network data can be browsed via a GUI, or via the TTY-mode Tshark utility

Wireshark – Features Contd

- The most powerful display filters in the industry
- Rich VoIP analysis
- Read/write many different capture file formats like:
  - tcpdump (libpcap)
  - Pcap NG
  - Catapult DCT2000
  - Cisco Secure IDS iplog
  - Microsoft Network Monitor and so on

Wireshark – Features Contd

- Captured files compressed with gzip can be decompressed on the fly
- Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth,USB, Token Ring, Frame Relay, FDDI, and others (depending on the platform)
- Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA
- Output can be exported to XML, PostScript, CSV and plain text