Security: Internet of Things

Based on Trusted Flows

Kyle Haefner

Background - What is IoT Security?

“Security of the Internet of Things is just security at a larger scale”

-- Steve Lovaas Colorado State University IT Manager

This is not the whole picture...

1. Single purpose devices
    a. Less complex to model
2. Effects of poor security implementations more profound.
    a. Pacemaker - stop you heart
    b. Thermostat - burn down your house

Background - IOT DDOS

- Mirai Botnet
  - 1.1 Tbps peak attack
  - 400,000 devices offered for rent
  - 2.5 Million infected devices
- Repear
  - 9 different exploits attacks
  - Checkpoint security says it found the malware on 60% of networks it monitors.
- Hajime
  - Whitehat vigilante botnet
  - Blocks ports other botnets use as vectors
    - TCP/23 (telnet), TCP/7547,TCP/5555,TCP/5358
    - Signed message, "just a white hat, securing some systems."

Top 10 IoT Vulnerabilities 2014

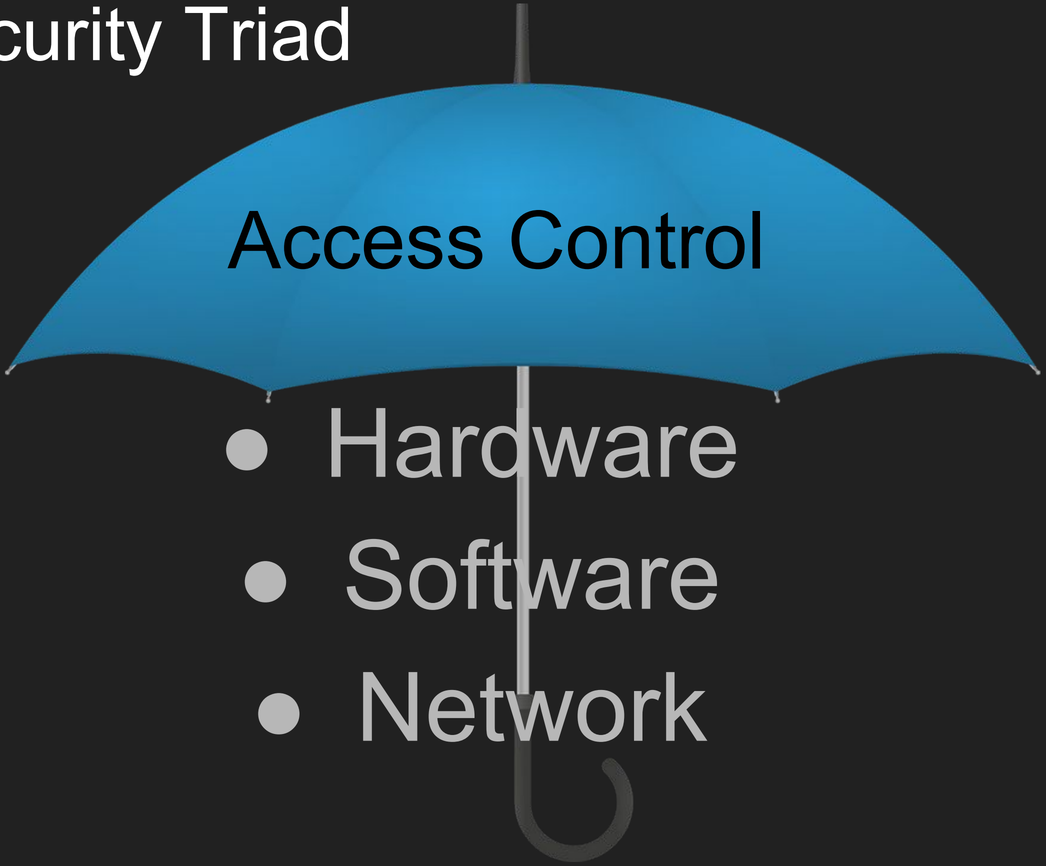
1. Insecure Web Interface
2. Insufficient Authentication/Authorization
3. Insecure Network Services
4. Lack of Transport Encryption/Integrity Verification
5. Privacy Concerns
6. Insecure Cloud Interface
7. Insecure Mobile Interface
8. Insufficient Security Configurability
9. Insecure Software/Firmware
10. Poor Physical Security

Open Web Application Security Project

OWASP Internet of Things Project

https://www.owasp.org

The IoT Security Triad



Access Control

- Hardware
- Software
- Network

Hardwares

- Encryption
  - Elliptic Curve (Smaller Keys, lower power)
- Verifiable Firmware
  - Firmware must be signed
  - Running firmware must be verified.

Software

- Vulnerabilities on device
  - Insecure web interface
  - Buffer overflows
- Vulnerabilities in protocols
  - Unencrypted protocols
  - Protocol Vulnerabilities
- Vulnerabilities in provider's cloud
  - Weak Encryption
  - Weak Authentication

Network

- Fingerprinting of device
  - Clock Skew - Every clock source is unique (unique != identity)
  - Identify a device based on scans (ports, TCP windows etc)
- Behavior of Device
  - Network trends and patterns of a device on a network over time.
  - Theory: It is more important defining what a device does on the network that what a device is.

Trusted Flows - Introduction

- Stage 1:
    - Learn device behavior on the network
    - Develop a trust model based on this behavior (and a few other attributes)
    - Leverage software defined networking to enforce trust model
- Stage 2:
    - Use behavior as a way to classify device type
    - Use semi-supervised machine learning to apply access controls to devices based on device type.

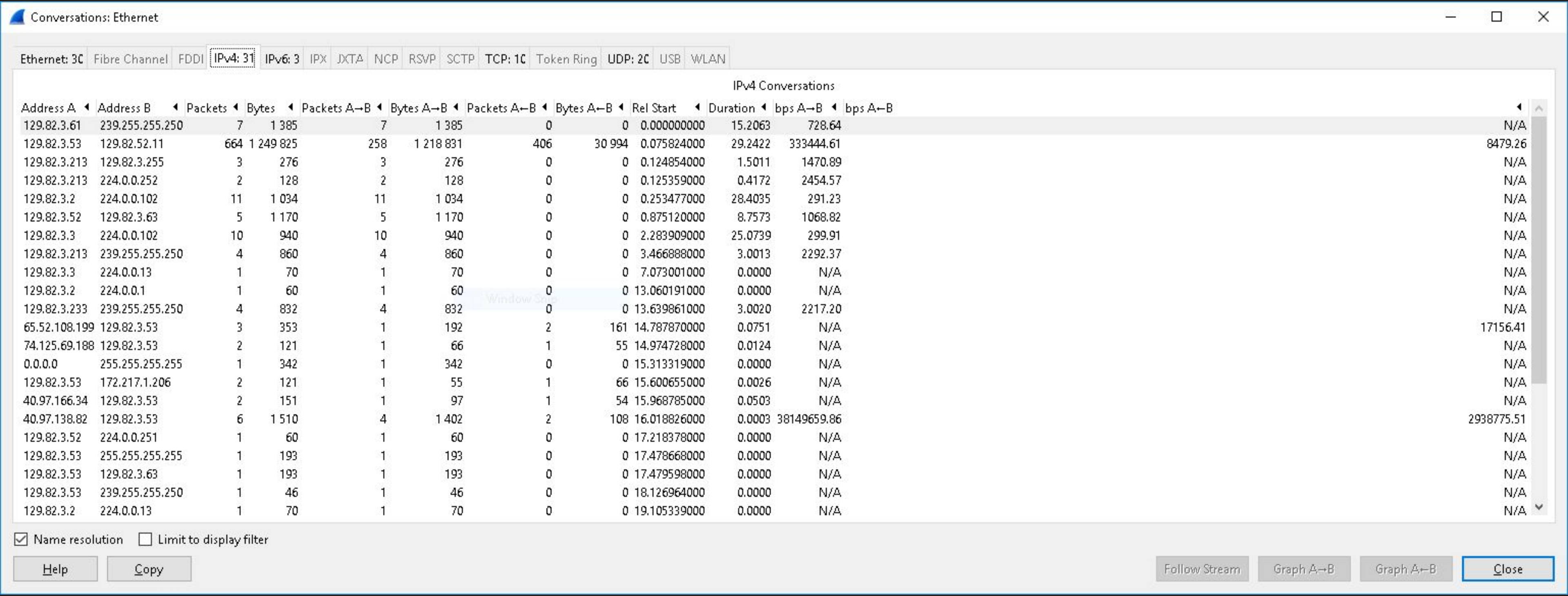
Trusted Flows - Network Flow RFC

RFC 3697 defines traffic flow as “a sequence of packets sent from a particular source to a particular unicast, anycast, or multicast destination that the source desires to label as a flow.”

Trusted Flows - Defining

- Tuple of 5 IP header features (ip_src,ip_dst,ip_protocol,src_port,dst_port)
- Flow statistics (number of packets, bytes, packets per second, bytes per second,duration)
- Direction (Packets A->B, Bytes A->B, bps A->B)

Example of Network Stats

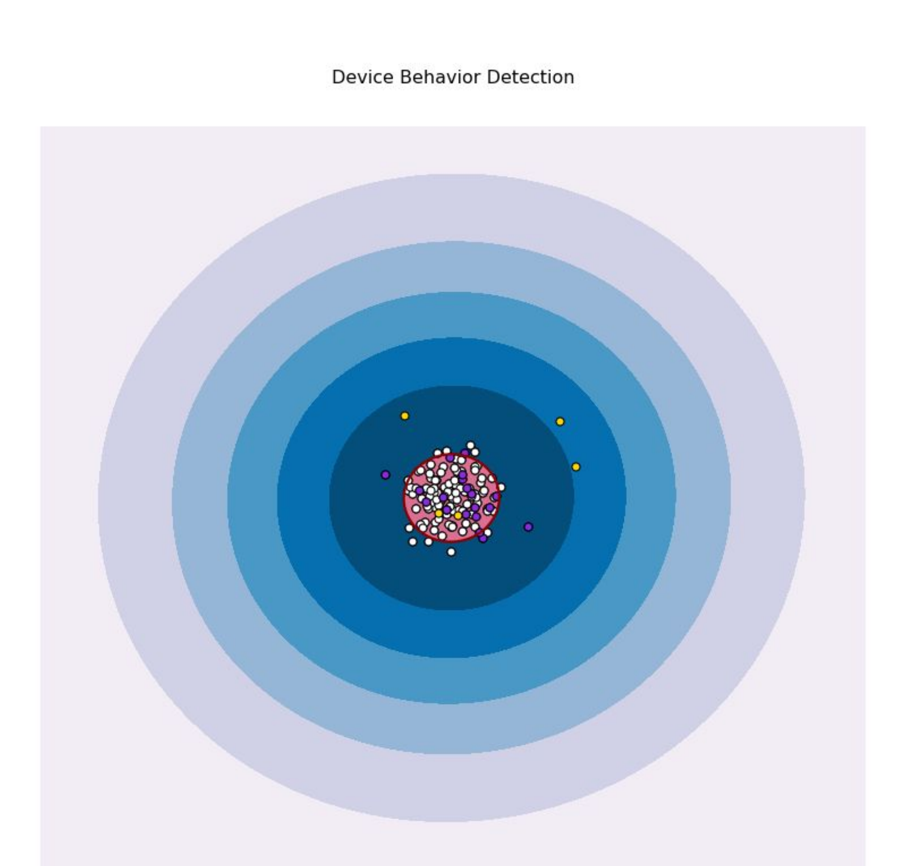


IPv4 Conversations

Address A	Address B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B	Rel Start	Duration	bps A→B	bps A←B
129.82.3.61	239.255.255.250	7	1 385	7	1 385	0	0	0.000000000	15.2063	728.64	N/A
129.82.3.53	129.82.52.11	664	1 249 825	258	1 218 831	406	30 994	0.075824000	29.2422	333444.61	8479.26
129.82.3.213	129.82.3.255	3	276	3	276	0	0	0.124854000	1.5011	1470.89	N/A
129.82.3.213	224.0.0.252	2	128	2	128	0	0	0.125359000	0.4172	2454.57	N/A
129.82.3.2	224.0.0.102	11	1 034	11	1 034	0	0	0.253477000	28.4035	291.23	N/A
129.82.3.52	129.82.3.63	5	1 170	5	1 170	0	0	0.875120000	8.7573	1068.82	N/A
129.82.3.3	224.0.0.102	10	940	10	940	0	0	2.283909000	25.0739	299.91	N/A
129.82.3.213	239.255.255.250	4	860	4	860	0	0	3.466888000	3.0013	2292.37	N/A
129.82.3.3	224.0.0.13	1	70	1	70	0	0	7.073001000	0.0000	N/A	N/A
129.82.3.2	224.0.0.1	1	60	1	60	0	0	13.060191000	0.0000	N/A	N/A
129.82.3.233	239.255.255.250	4	832	4	832	0	0	13.639861000	3.0020	2217.20	N/A
65.52.108.199	129.82.3.53	3	353	1	192	2	161	14.787870000	0.0751	N/A	17156.41
74.125.69.188	129.82.3.53	2	121	1	66	1	55	14.974728000	0.0124	N/A	N/A
0.0.0.0	255.255.255.255	1	342	1	342	0	0	15.313319000	0.0000	N/A	N/A
129.82.3.53	172.217.1.206	2	121	1	55	1	66	15.600655000	0.0026	N/A	N/A
40.97.166.34	129.82.3.53	2	151	1	97	1	54	15.968785000	0.0503	N/A	N/A
40.97.138.82	129.82.3.53	6	1 510	4	1 402	2	108	16.018826000	0.0003	38149659.86	2938775.51
129.82.3.52	224.0.0.251	1	60	1	60	0	0	17.218378000	0.0000	N/A	N/A
129.82.3.53	255.255.255.255	1	193	1	193	0	0	17.478668000	0.0000	N/A	N/A
129.82.3.53	129.82.3.63	1	193	1	193	0	0	17.479598000	0.0000	N/A	N/A
129.82.3.53	239.255.255.250	1	46	1	46	0	0	18.126964000	0.0000	N/A	N/A
129.82.3.2	224.0.0.13	1	70	1	70	0	0	19.105339000	0.0000	N/A	N/A

Trusted Flows - Device Behavior

- One-class SVM is an unsupervised algorithm that learns a decision function for novelty detection:
  - RBF (Gaussian Kernel)
  - Classifies new data as similar or different to the training set.
  - Classifies new data as similar or different to the training set.
  - Training set will be previous *t-n* windows of recent history (data) plus the exponential decay history
  - Testing set will be *t-1* windows of data.



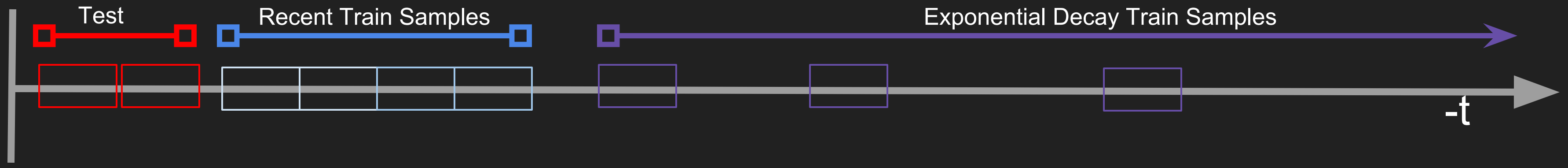
Trusted Flows - One-Class SVM

Online learning with exponential decay sampling.

$$S_{test} = \sum_{i=0}^{i=-t} i$$

$$S_{train} = \sum_{i=-t}^{i=-t-w} i + \sum_{i=-t-w-1}^{\infty} 2^i$$

□ =*w* = flow stats for given time *t*



Trusted Flows - Trust

- Trust score based on:
  - What we know about the device (K)
    - Binary Values
      - Certificate (valid) or (none/invalid) = [1,0] or [0,1]
      - Common Vulnerability Scoring System[5] (CVSS)
        - (CVSS = 0) = [1,0] or (CVSS > 0) = [0,1]
      - Shodan[6] presence (present) or (none) = [0,1] or [1,0]
      - Use of encryption
  - Past behavior of device (B)
    - How many outliers outside of boundary over time?
    - *m* is a factor to adjust the influence of outliers on the trust model.

$$T = \begin{cases} \frac{\sum k_T}{mB}, & if B \geq 1 \\ \sum k_T, & otherwise \end{cases}$$

$$U = \begin{cases} mB \sum k_U, & if B \geq 1 \\ \sum k_U, & otherwise \end{cases}$$

$$F_T = [T, U]$$

$F_T \geq F_U$ netflow is allowed
otherwise netflow is denied

Questions