UNB EST. 1785 UNIVERSITY OF NEW BRUNSWICK | Canadian Institute for Cybersecurity

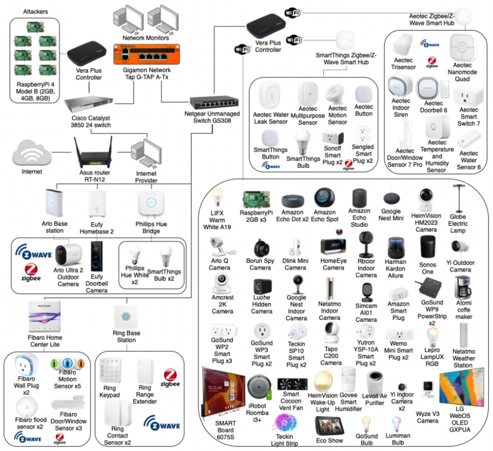
CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment

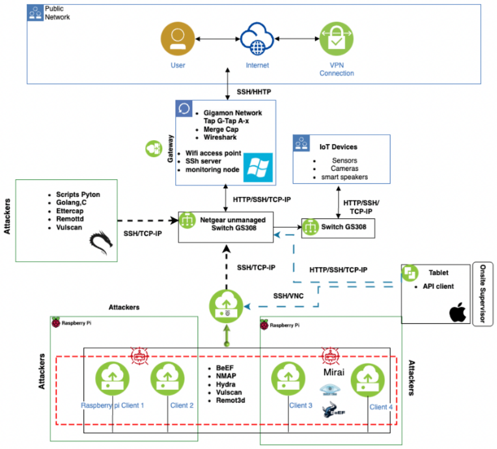
Euclides Carlos Pinto Neto, Sajjad Dadkhah, Raphael Ferreira, Alireza Zohourian, Rongxing Lu, Ali A. Ghorbani

The main goal of this research is to propose a novel and extensive IoT attack dataset to foster the development of security analytics applications in real IoT operations. To accomplish this, 33 attacks are executed in an IoT topology composed of 105 devices. These attacks are classified into seven categories, namely DDoS, DoS, Recon, Web-based, Brute Force, Spoofing, and Mirai. Finally, all attacks are executed by malicious IoT devices targeting other IoT devices.

Extracted Features:

#	Feature	Description
1	Header Length	Mean of the Header Lengths of the Transport Layer
2	Time-To-Live	Time-To-Live
3	Rate	Speed of packet transmission within a window in packets/sec
4	fin flag number	Proportion of packets with FIN flags in the window
5	syn flag number	Proportion of packets with SYN flags in the window
6	rst flag number	Proportion of packets with RST flags in the window
7	psh flag number	Proportion of packets with PSH flags in the window
8	ack flag number	Proportion of packets with ACK flags in the window
9	ece flag number	Proportion of packets with ECE flags in the window
10	cwr flag number	Proportion of packets with CWR flags in the window
11	syn count	Count of Syn flag occurrences in packets
12	ack count	Count of Ack flag occurrences in packets
13	fin count	Count of Fin flag occurrences in packets
14	rst count	Count of Rst flag occurrences in packets
15	IGMP	Average no. of IGMP packets in the window
16	HTTPS	Average no. of HTTPS packets in the window
17	HTTP	Average no. of HTTP packets in the window
18	Telnet	Average no. of Telnet packets in the window
19	DNS	Average no. of DNS packets in the window
20	SMTP	Average no. of SMTP packets in the window
21	SSH	Average no. of SSH packets in the window
22	IRC	Average no. of IRC packets in the window
23	TCP	Average no. of TCP packets in the window
24	UDP	Average no. of UDP packets in the window
25	DHCP	Average no. of DHCP packets in the window
26	ARP	Average no. of ARP packets in the window
27	ICMP	Average no. of ICMP packets in the window
28	IPv	Average no. of IPv packets in the window
29	LLC	Average no. of LLC packets in the window
30	Tot Sum	Total packet length within the aggregated packets (window)
31	Min	Shortest packet length within the aggregated packets (window)
32	Max	Longest packet length within the aggregated packets (window)
33	AVG	Mean of the packet length within the aggregated packets (window)
34	Std	Standard deviation of the packet length within the aggregated packets (window)
35	Tot Size	(Avg.) Length of the Packet
36	IAT	Interval mean between the current and previous packet in the window
37	Number	Total number of packets in the window
38	Variance	Variance of the packet lengths in the window
39	Protocol Type	Mode of protocols found in the window





Public Network

User

Internet

VPN Connection

SSH/HHTP

Gateway

- Gigamon Network Tap G-Tap A-x
- Merge Cap
- Wireshark

- Wifi access point
- SSh server
- monitoring node

IoT Devices

- Sensors
- Cameras
- smart speakers

HTTP/SSH/TCP-IP

HTTP/SSH/ TCP-IP

Attackers

- Scripts Pyton
- Golang,C
- Ettercap
- Remottd
- Vulscan

SSH/TCP-IP

Netgear unmanaged Switch GS308

Switch GS308

SSH/TCP-IP

HTTP/SSH/TCP-IP

Tablet

- API client

Onsite Supervisor

SSH/VNC

Attackers

Raspberry Pi

Raspberry Pi

Attackers

- BeEF
- NMAP
- Hydra
- Vulscan
- Remot3d

Mirai

Raspberry pi Client 1

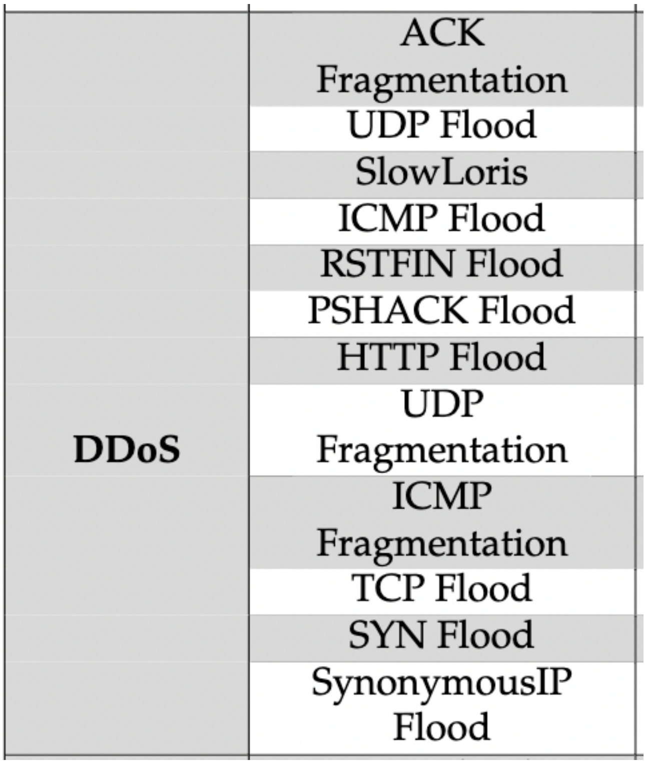
Client 2

Client 3

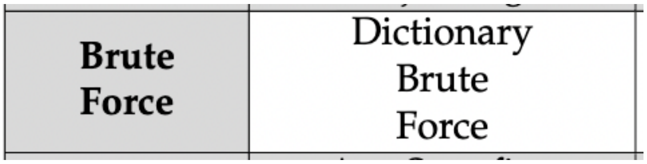
Client 4

Attackers

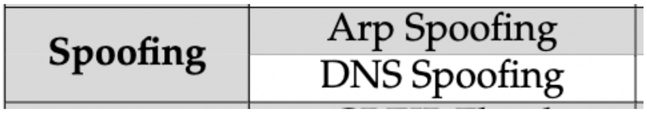
Attacks Executed:



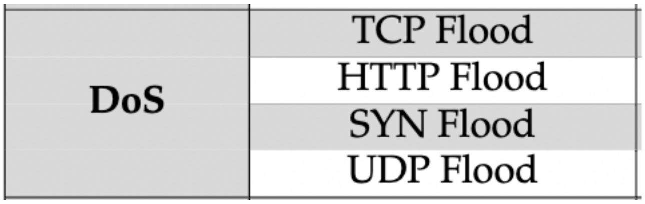
DDoS	ACK Fragmentation
	UDP Flood
	SlowLoris
	ICMP Flood
	RSTFIN Flood
	PSHACK Flood
	HTTP Flood
	UDP Fragmentation
	ICMP Fragmentation
	TCP Flood
	SYN Flood
	SynonymousIP Flood



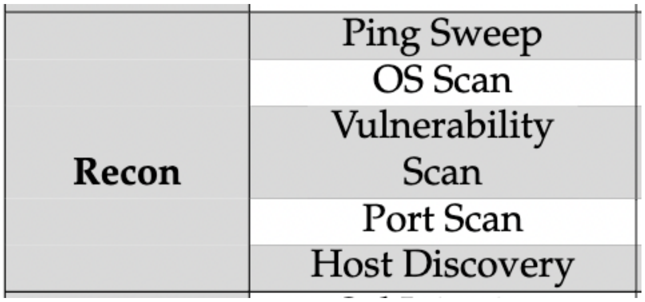
Brute Force	Dictionary Brute Force



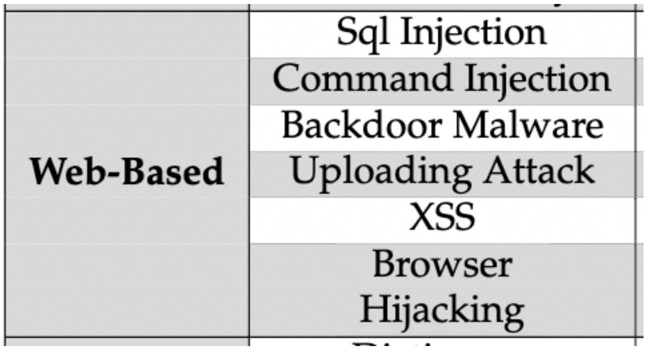
Spoofing	Arp Spoofing
	DNS Spoofing



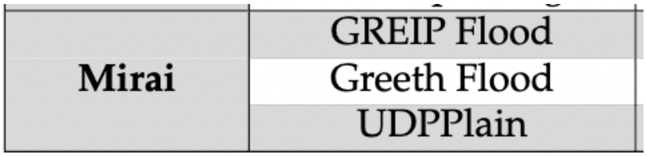
DoS	TCP Flood
	HTTP Flood
	SYN Flood
	UDP Flood



Recon	Ping Sweep
	OS Scan
	Vulnerability Scan
	Port Scan
	Host Discovery



Web-Based	Sql Injection
	Command Injection
	Backdoor Malware
	Uploading Attack
	XSS
	Browser Hijacking



Mirai	GREIP Flood
	Greeth Flood
	UDPPlain