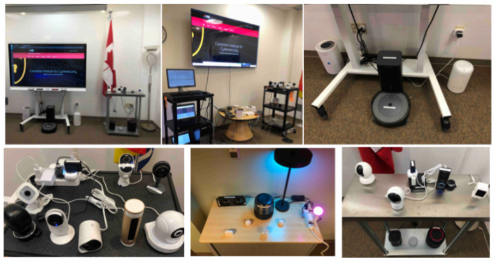
EST. 1785 UNB UNIVERSITY OF NEW BRUNSWICK | Canadian Institute for Cybersecurity

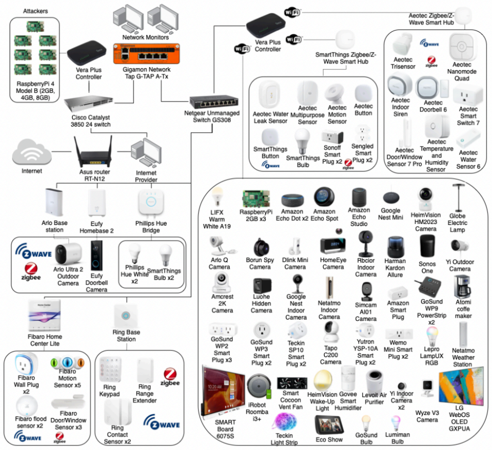
CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment

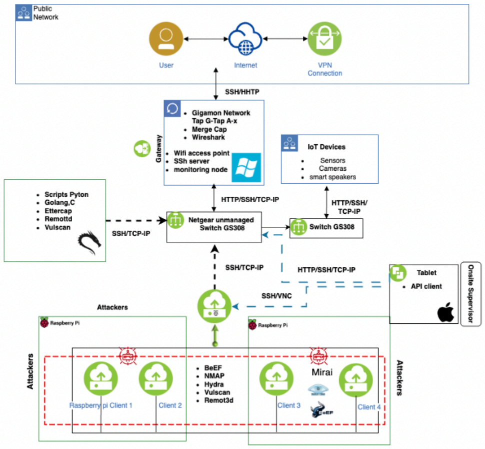
Euclides Carlos Pinto Neto, Sajjad Dadkhah, Raphael Ferreira, Alireza Zohourian, Rongxing Lu, Ali A. Ghorbani

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:

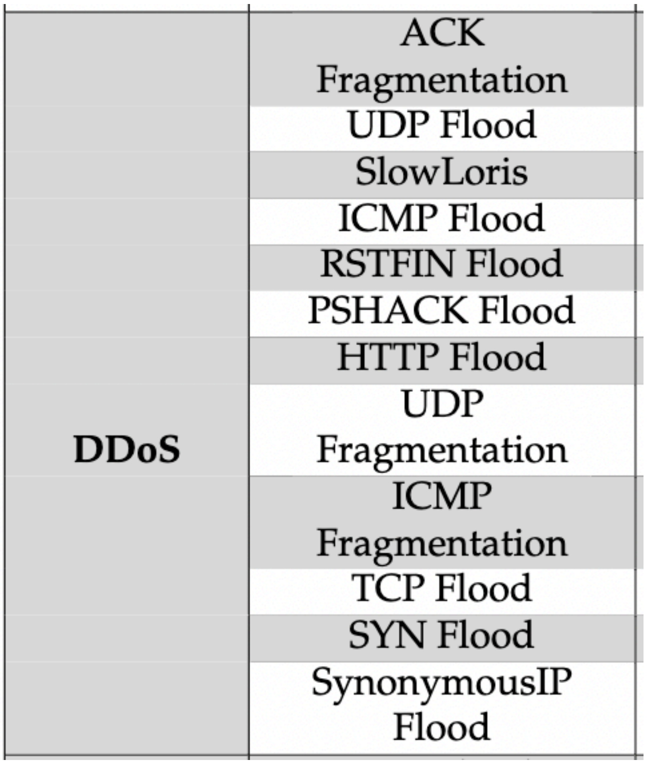




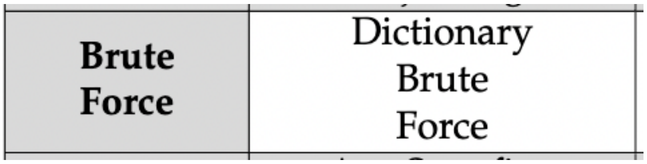


#	Feature	Description
1	ts	Timestamp
2	flow duration	Duration of the packet's flow
3	Header Length	Header Length
4	Protocol Type	IP, UDP, TCP, IGMP, ICMP, Unknown (Integers)
5	Duration	Time-to-Live (ttl)
6	Rate	Rate of packet transmission in a flow
7	Srate	Rate of outbound packets transmission in a flow
8	Drate,	Rate of inbound packets transmission in a flow
9	fin flag number	Fin flag value
10	syn flag number	Syn flag value
11	rst flag number	Rst flag value
12	psh flag numbe	Psh flag value
13	ack flag number	Ack flag value
14	ece flag numbe	Ece flag value
15	cwr flag number	Cwr flag value
16	ack count	Number of packets with ack flag set in the same flow
17	syn count	Number of packets with syn flag set in the same flow
18	fin count	Number of packets with fin flag set in the same flow
19	urg coun	Number of packets with urg flag set in the same flow
20	rst count	Number of packets with rst flag set in the same flow
21	HTTP	Indicates if the application layer protocol is HTTP
22	HTTPS	Indicates if the application layer protocol is HTTPS
23	DNS	Indicates if the application layer protocol is DNS
24	Telnet	Indicates if the application layer protocol is Telnet
25	SMTP	Indicates if the application layer protocol is SMTP
26	SSH	Indicates if the application layer protocol is SSH
27	IRC	Indicates if the application layer protocol is IRC
28	TCP	Indicates if the transport layer protocol is TCP
29	UDP	Indicates if the transport layer protocol is UDP
30	DHCP	Indicates if the application layer protocol is DHCP
31	ARP	Indicates if the link layer protocol is ARP
32	ICMP	Indicates if the network layer protocol is ICMP
33	IPv	Indicates if the network layer protocol is IP
34	LLC	Indicates if the link layer protocol is LLC
35	Tot sum	Summation of packets lengths in flow
36	Min	Minimum packet length in the flow
37	Max	Maximumpacket length in the flow
38	AVG	Average packet length in the flow
39	Std	Standard deviation of packet length in the flow
40	Tot size	Packet's length
41	IAT	The time difference with the previous packet
42	Number	The number of packets in the flow
43	Magnitue	(Average of the lengths of incoming packets in the flow + Average of the lengths of outgoing packets in the flow) ** 0.5
44	Radius	(Variance of the lengths of incoming packets in the flow + Variance of the lengths of outgoing packets in the flow) ** 0.5
45	Covariance	Covariance of the lengths of incoming and outgoing packets
46	Variance	Variance of the lengths of incoming packets in the flow / The variance of the lengths of outgoing packets in the flow
47	Weight	Number of incoming packets * Number of outgoing packets

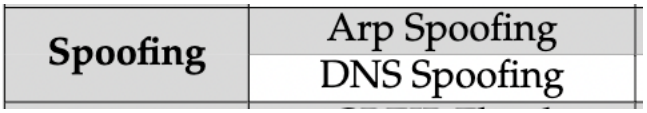
Attacks Executed:



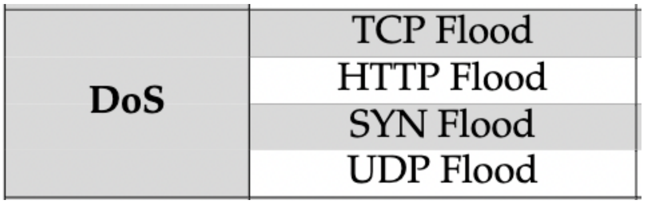
DDoS	ACK Fragmentation
	UDP Flood
	SlowLoris
	ICMP Flood
	RSTFIN Flood
	PSHACK Flood
	HTTP Flood
	UDP Fragmentation
	ICMP Fragmentation
	TCP Flood
	SYN Flood
	SynonymousIP Flood



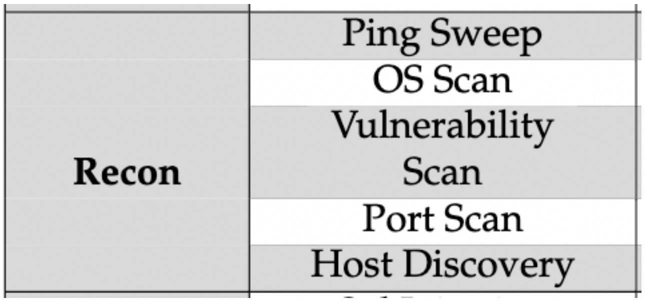
Brute Force	Dictionary Brute Force



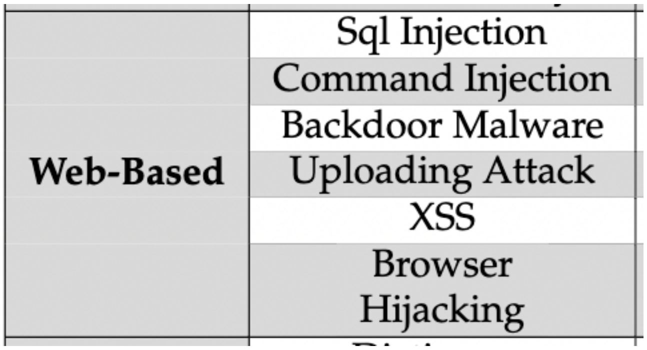
Spoofing	Arp Spoofing
	DNS Spoofing



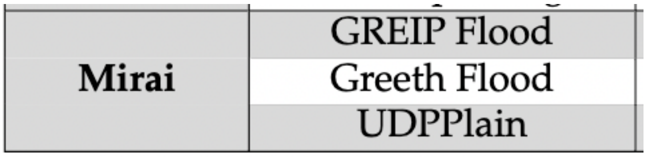
DoS	TCP Flood
	HTTP Flood
	SYN Flood
	UDP Flood



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