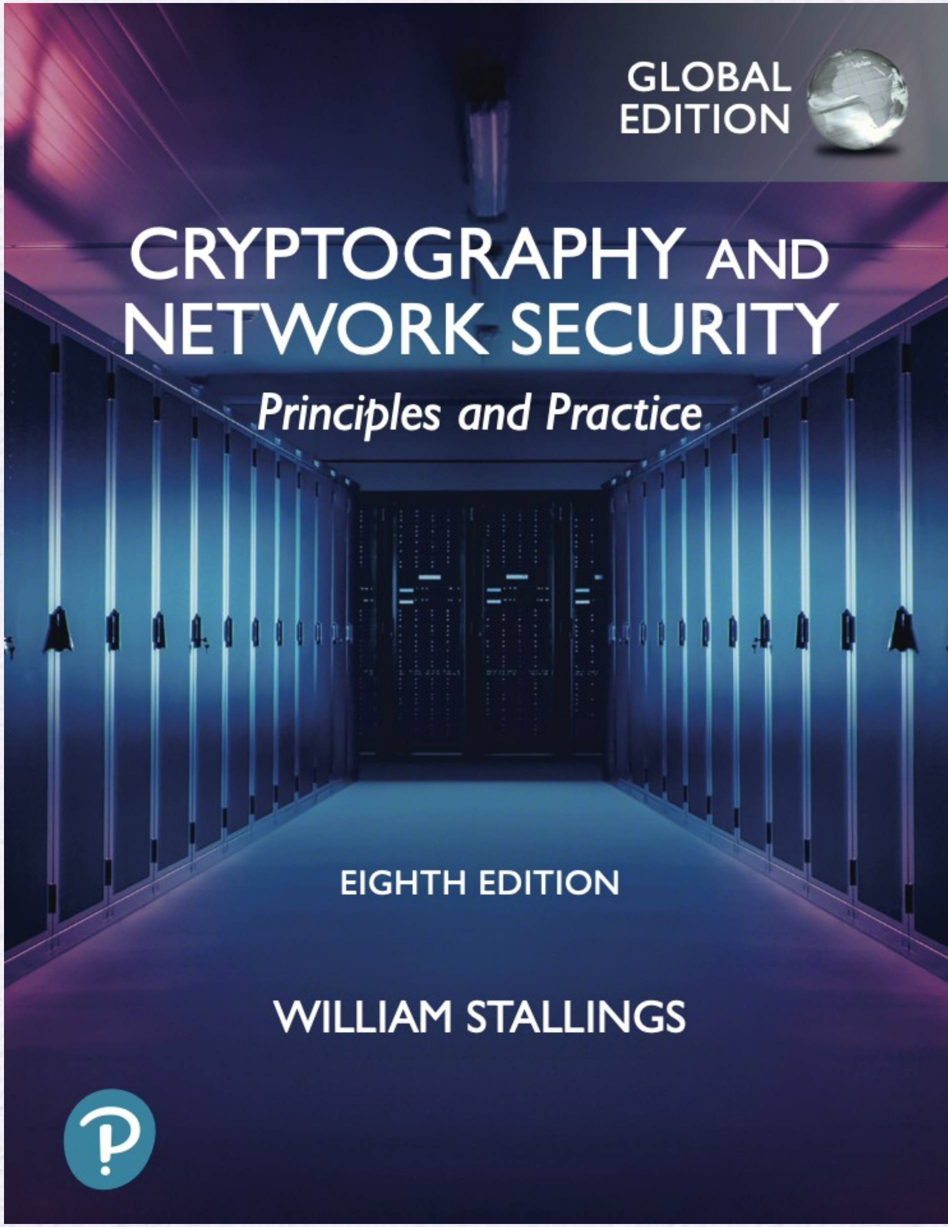
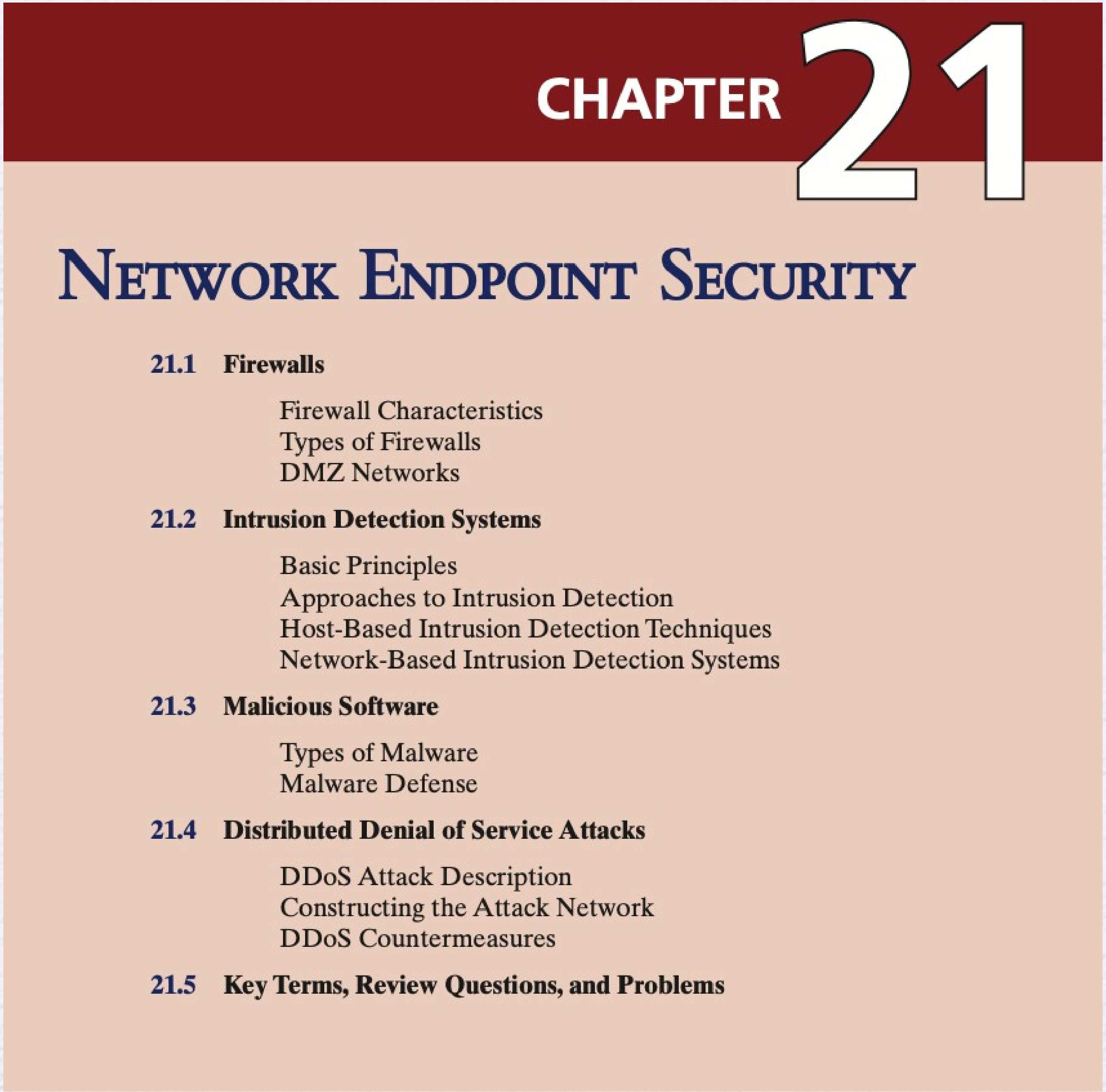
University of Nevada – Reno
Computer Science &
Engineering Department

CS454/654 Reliability and
Security of Computing
Systems - Fall 2024

Lecture 22

Dr. Batyr Charyyev
bcharyyev.com



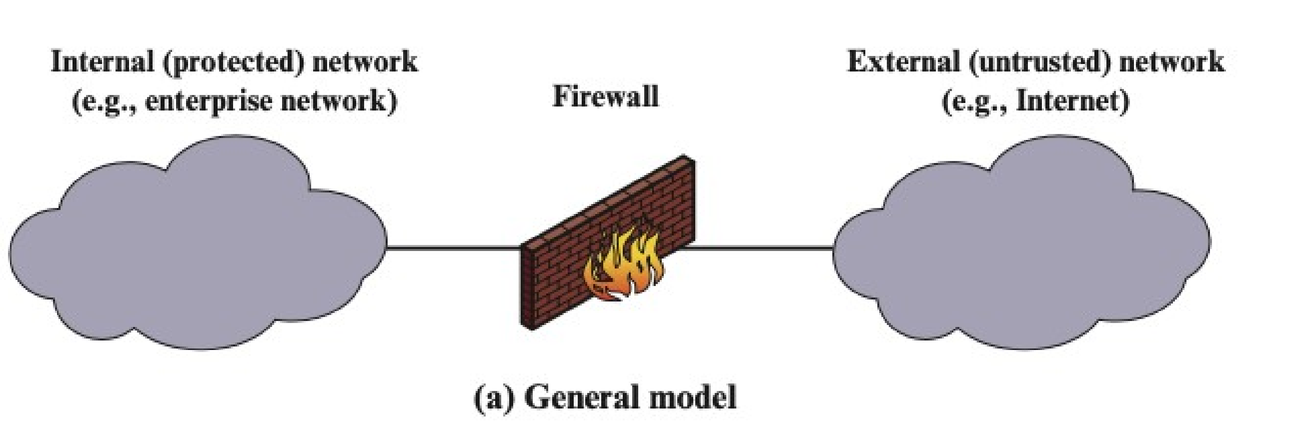


CHAPTER 21

Network Endpoint Security

Firewalls

- Deployed on outer perimeter of the network infrastructure
- Also deployed in inner network to segregate portions of the network.
- Enforces access policy.


Internal (protected) network
(e.g., enterprise network)
Firewall
External (untrusted) network
(e.g., Internet)

(a) General model

- **Four techniques** that firewalls use to control access
  - **Service control:** What type of services can be accessed
  - **Direction control:** What should be the direction of the traffic for service
  - **User control:** Tailoring the access depending on user.
  - **Behavioral control:** How particular service can be used.

Firewalls

Firewall enables

- Traffic monitoring.
- Network address translation (NAT) and logging internet usage.
- Facilitate Virtual Private Networks (VPN)

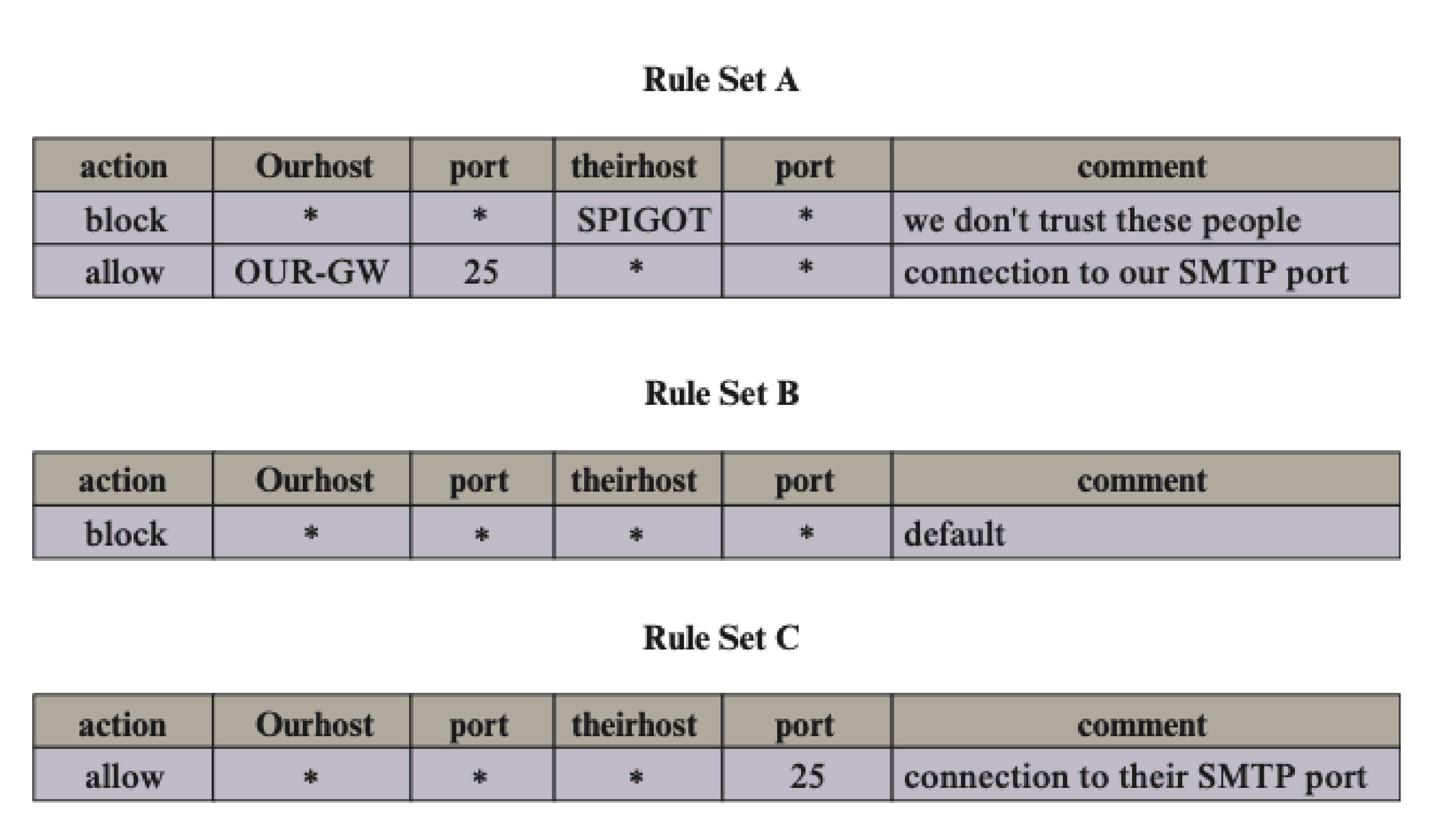
However, firewall can not protect internal threats.

Types of Firewalls

- Packet Filtering
- Stateful Inspection Firewalls
- Application Level Gateway
- Circuit-level gateway

Packet Filtering

- Apply filtering to traffic based on source/destination IP, protocol, and port number.
- Examine each individual packet and apply predefined rules.
- Cisco ASA 5500-X Series Firewalls - Supports simple packet filtering https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/series.html



Rule Set A

action	Ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

Rule Set B

action	Ourhost	port	theirhost	port	comment
block	*	*	*	*	default

Rule Set C

action	Ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

Stateful Inspection Firewalls

- Monitors the state of active connections and ensures that only legitimate packets that are part of an ongoing session are allowed through.

- The firewall compares incoming packets with a state table that contains information about current connections.

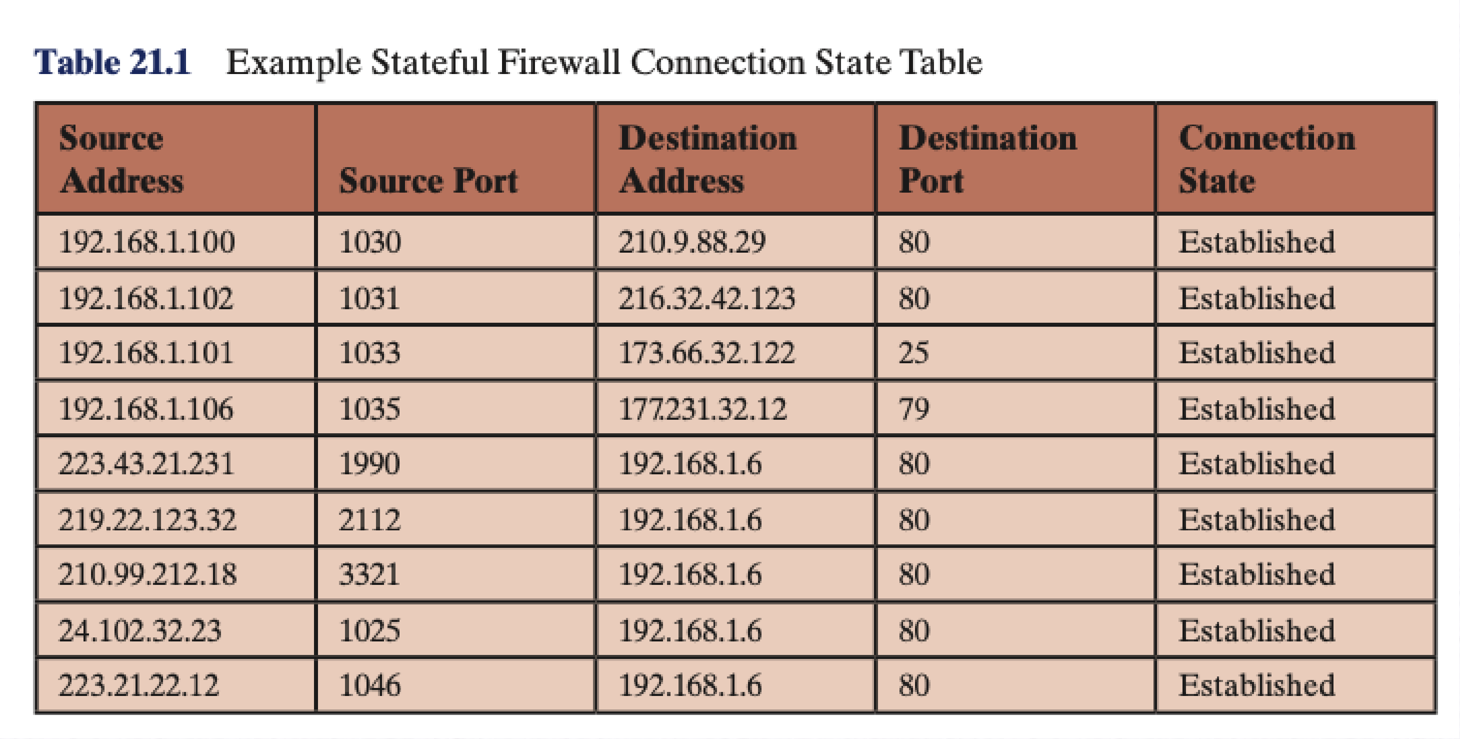


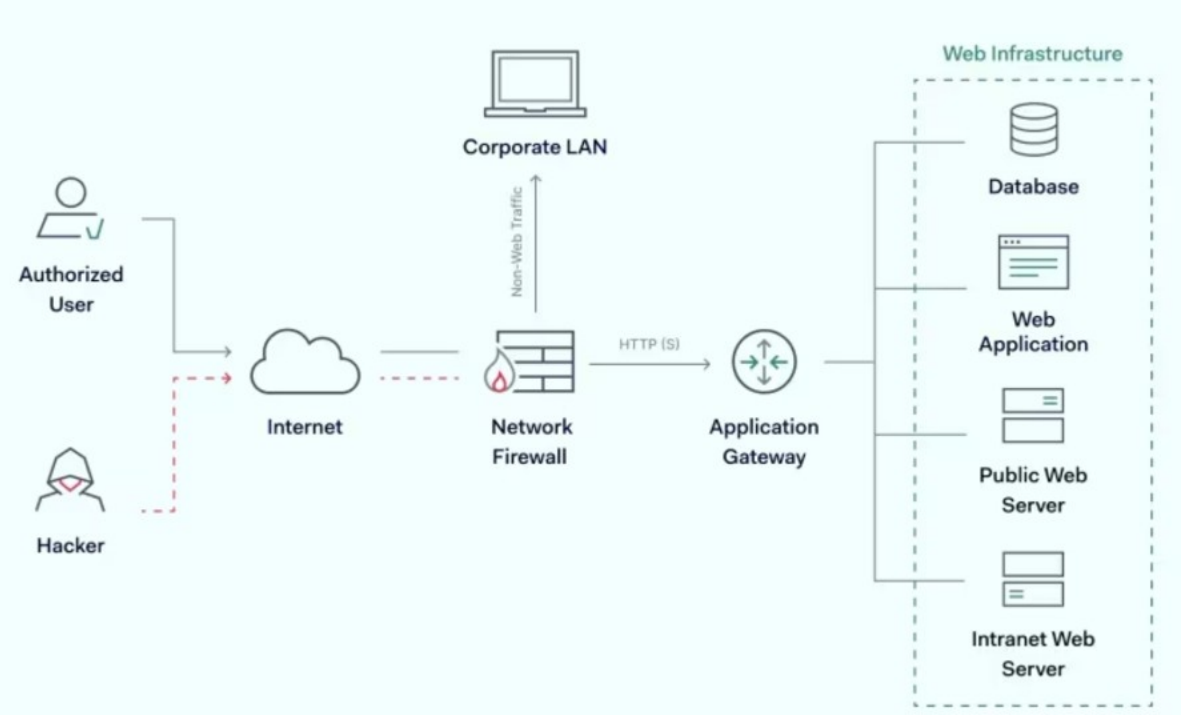
Table 21.1 Example Stateful Firewall Connection State Table

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Application-Level Gateway (Proxy Firewall)

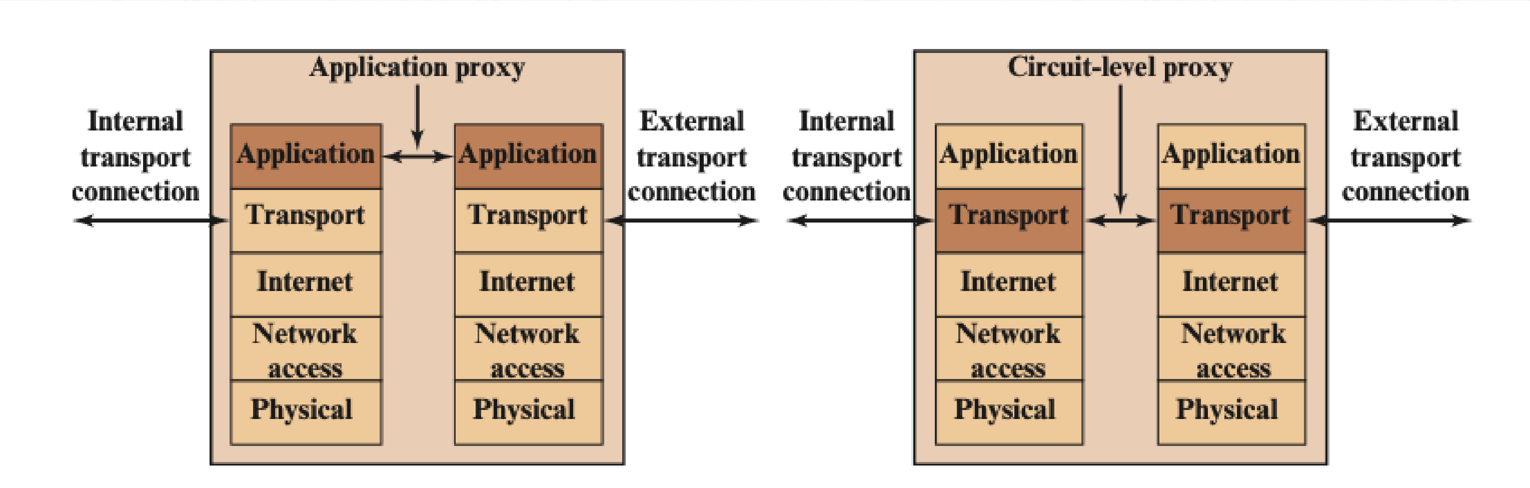
- An application-level gateway, also known as an application proxy, operates as a relay for application-level traffic, here how it works
  - **Client Interaction**: The user initiates a connection using a TCP/IP application (like Telnet or FTP) and contacts the firewall gateway.
  - **Authentication:** Upon connection, the gateway asks the user for information, such as the remote host's name, user ID, and authentication credentials.
  - **Relaying Traffic:** The gateway then contacts the application on the remote host, forwarding the application data between the client and the server.

- **Application-Specific Proxy:** The gateway only relays traffic for applications it has been specifically configured to handle.
- **Feature Control:** Administrators can configure the gateway to allow only certain features of an application.



Circuit-level gateway

- The circuit-level gateway establishes two separate TCP connections: from client (external) to firewall, and from firewall to server (internal). Then it acts as a relay.
- It simply forwards TCP segments (i.e., packets) from one connection to the other without inspecting the contents of the traffic.
- A typical use case for a circuit-level gateway is when a network administrator trusts the external users but wants to control the connections that are established from the internal network to the external network (and vice versa).



(d) Application proxy firewall

(e) Circuit-level proxy firewall

Demilitarized Zone (DMZ)

- Positioned between external and internal firewalls.
- The DMZ hosts publicly accessible systems like web servers, email servers, and DNS servers. These systems require external connectivity (e.g., to the internet) but also need protection from the internet.
- **External Firewall:** Provides basic protection and access control for the DMZ and the enterprise network from the external network.
- **Internal Firewalls:** Offer more detailed filtering and protect both the core network and the DMZ, ensuring that internal systems are protected from external attacks
- **Benefits**
  - Layered defense
  - Controlled exposure
  - Internal Segmentation

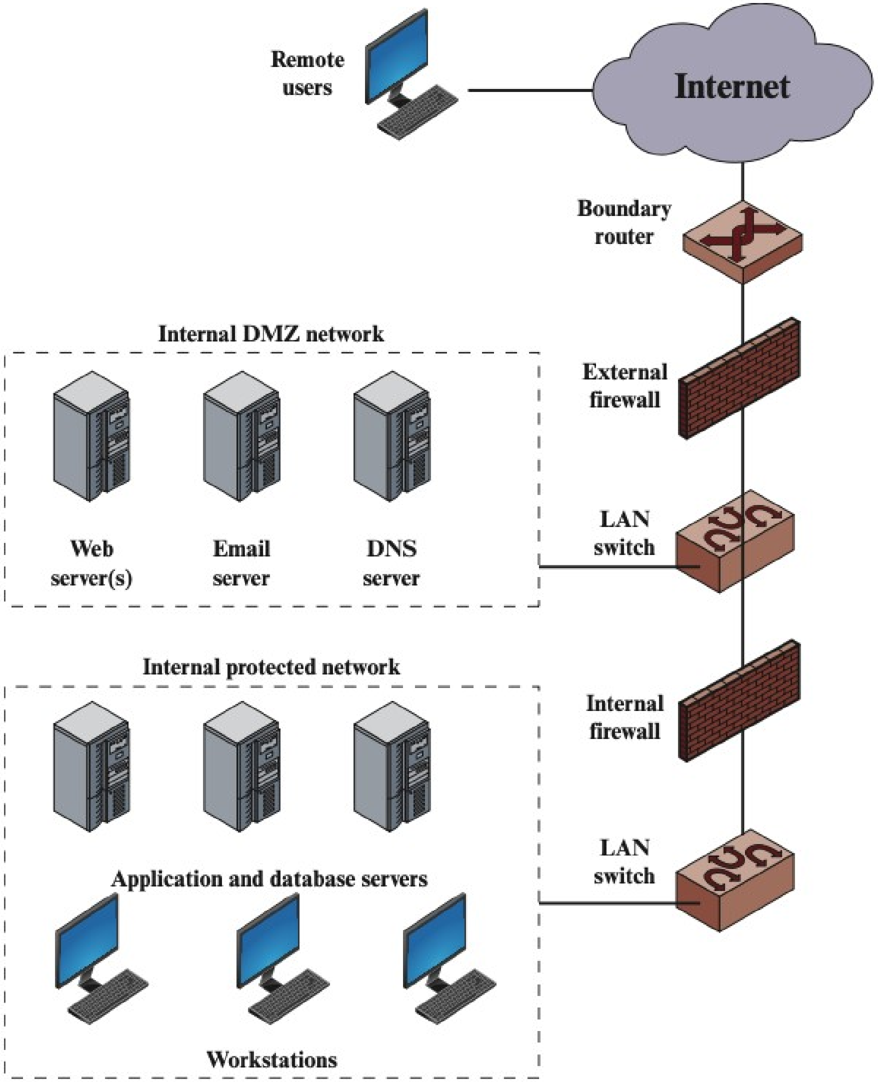


Figure 21.3 Example Firewall Configuration

Intrusion Detection Systems (IDS)

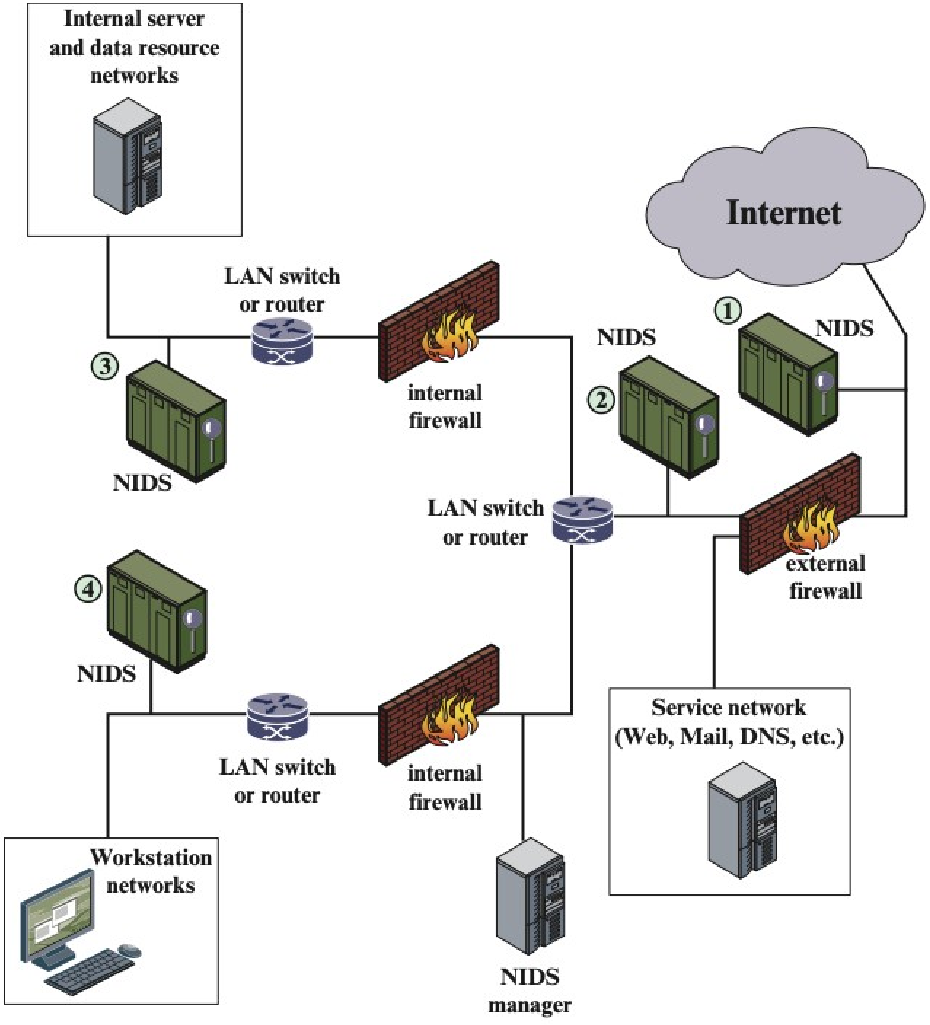
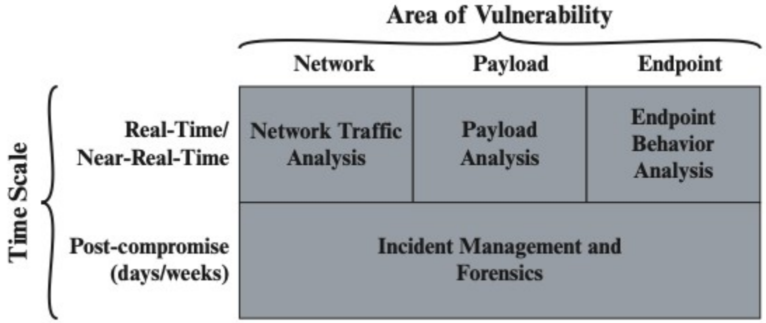


Figure 21.6 Example of NIDS Sensor Deployment

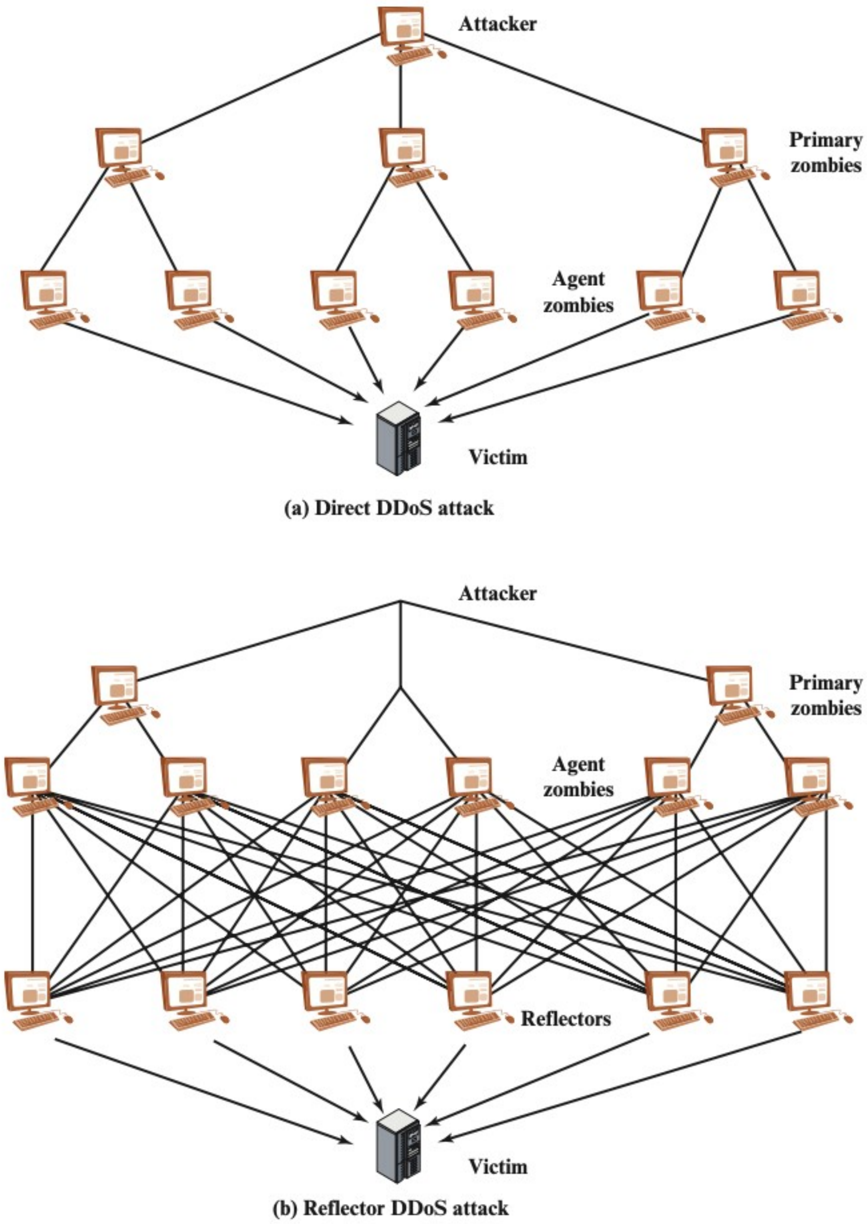
Host-Based Intrusion Detection Techniques
Network-Based Intrusion Detection Systems



		Area of Vulnerability		
		Network	Payload	Endpoint
Time Scale	Real-Time/ Near-Real-Time	Network Traffic Analysis	Payload Analysis	Endpoint Behavior Analysis
	Post-compromise (days/weeks)	Incident Management and Forensics		

Figure 21.7 Five Elements of Malware Defense

Denial of Service Attacks (DDoS)



(a) Direct DDoS attack

(b) Reflector DDoS attack

Figure 21.9 Types of Flooding-Based DDoS Attacks

Mirai - Denial of Service Attacks (DDoS)

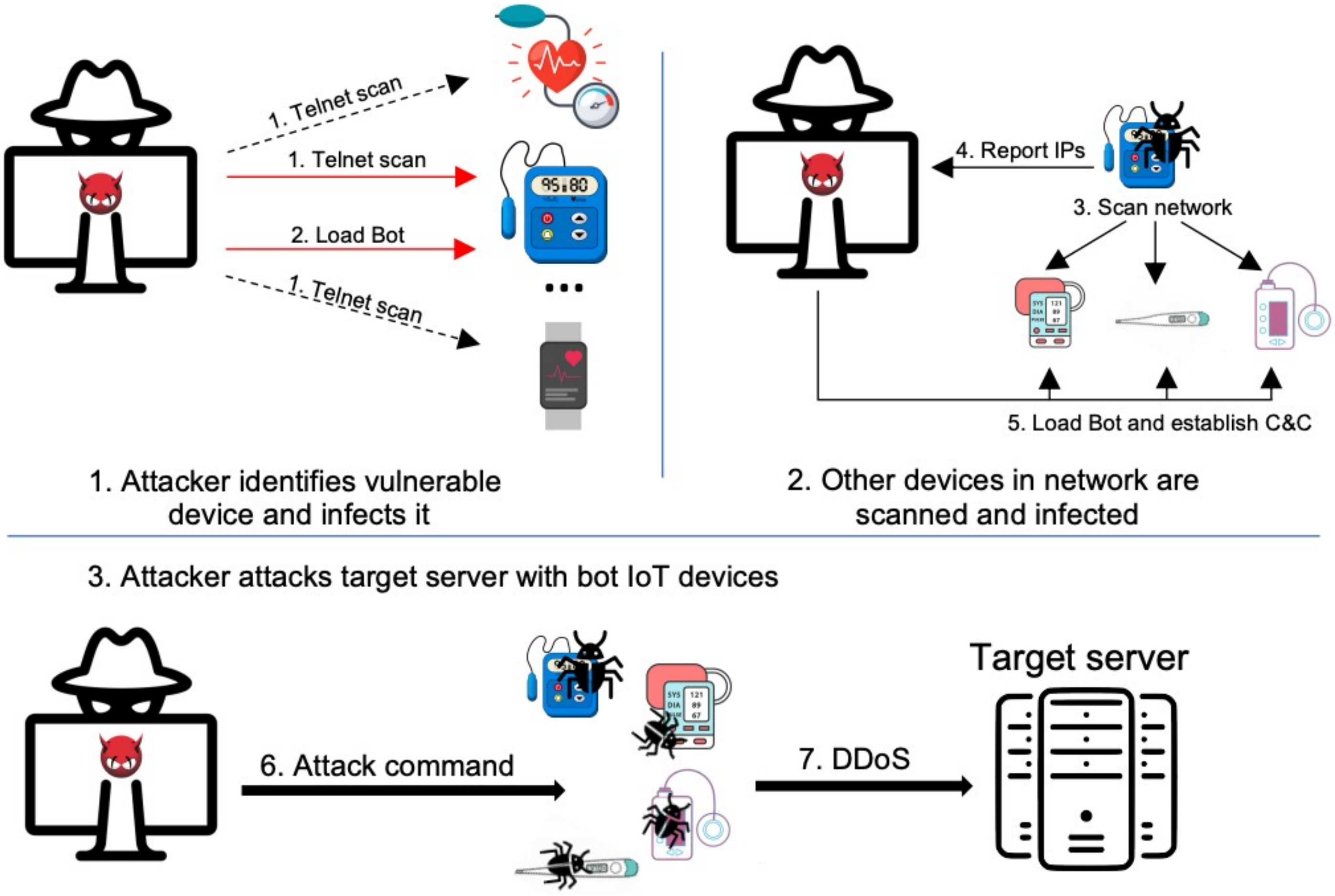
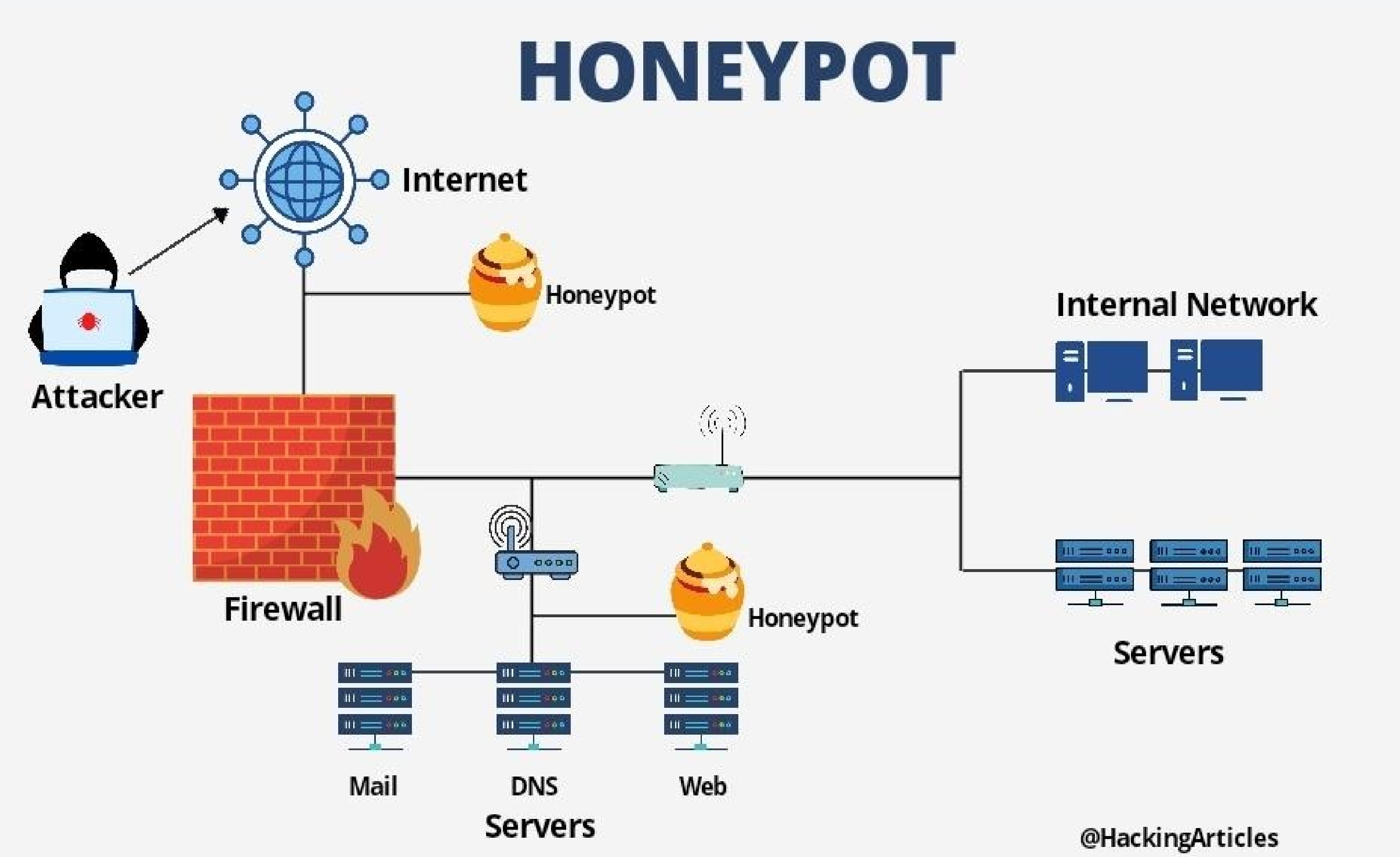
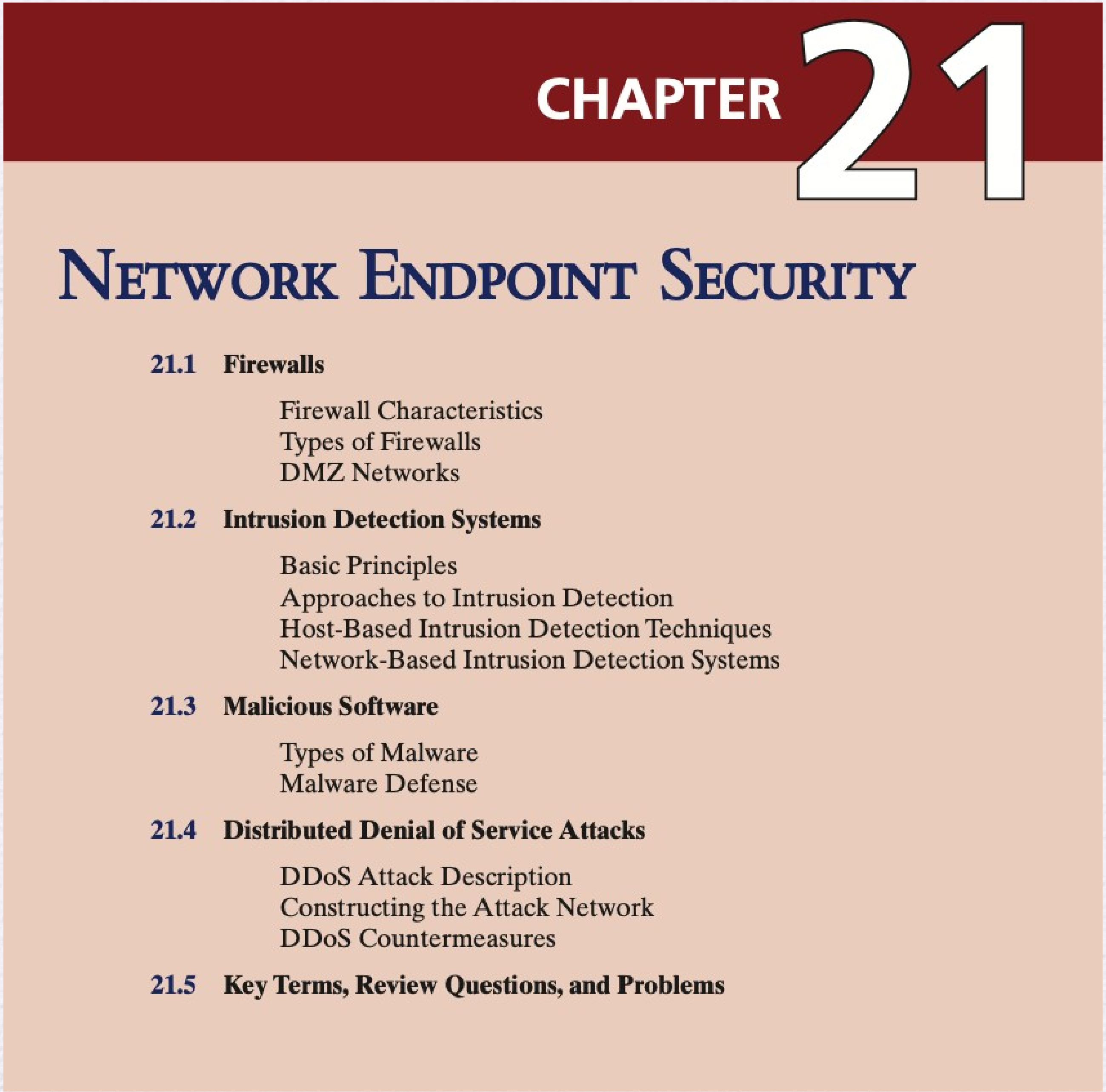

1. Telnet scan
1. Telnet scan
2. Load Bot
1. Telnet scan
95 80
1. Attacker identifies vulnerable device and infects it
4. Report IPs
3. Scan network
SYS DIA PULSE 121 89 67
5. Load Bot and establish C&C
2. Other devices in network are scanned and infected
3. Attacker attacks target server with bot IoT devices
6. Attack command
7. DDoS
Target server

Fig. 8. Attack scenario: DDoS attack with Mirai.



- **Honeyd**: https://github.com/DataSoft/Honeyd
- **Kippo**: https://github.com/desaster/kippo
- **Cowrie**: https://github.com/cowrie/cowrie
- **Dionaea**: https://www.honeynet.org/projects/active/dionaea/
- **IRASSH**: https://github.com/adpauna/irassh/



CHAPTER 21

Network Endpoint Security

21.1 Firewalls

Firewall Characteristics
Types of Firewalls
DMZ Networks

21.2 Intrusion Detection Systems

Basic Principles
Approaches to Intrusion Detection
Host-Based Intrusion Detection Techniques
Network-Based Intrusion Detection Systems

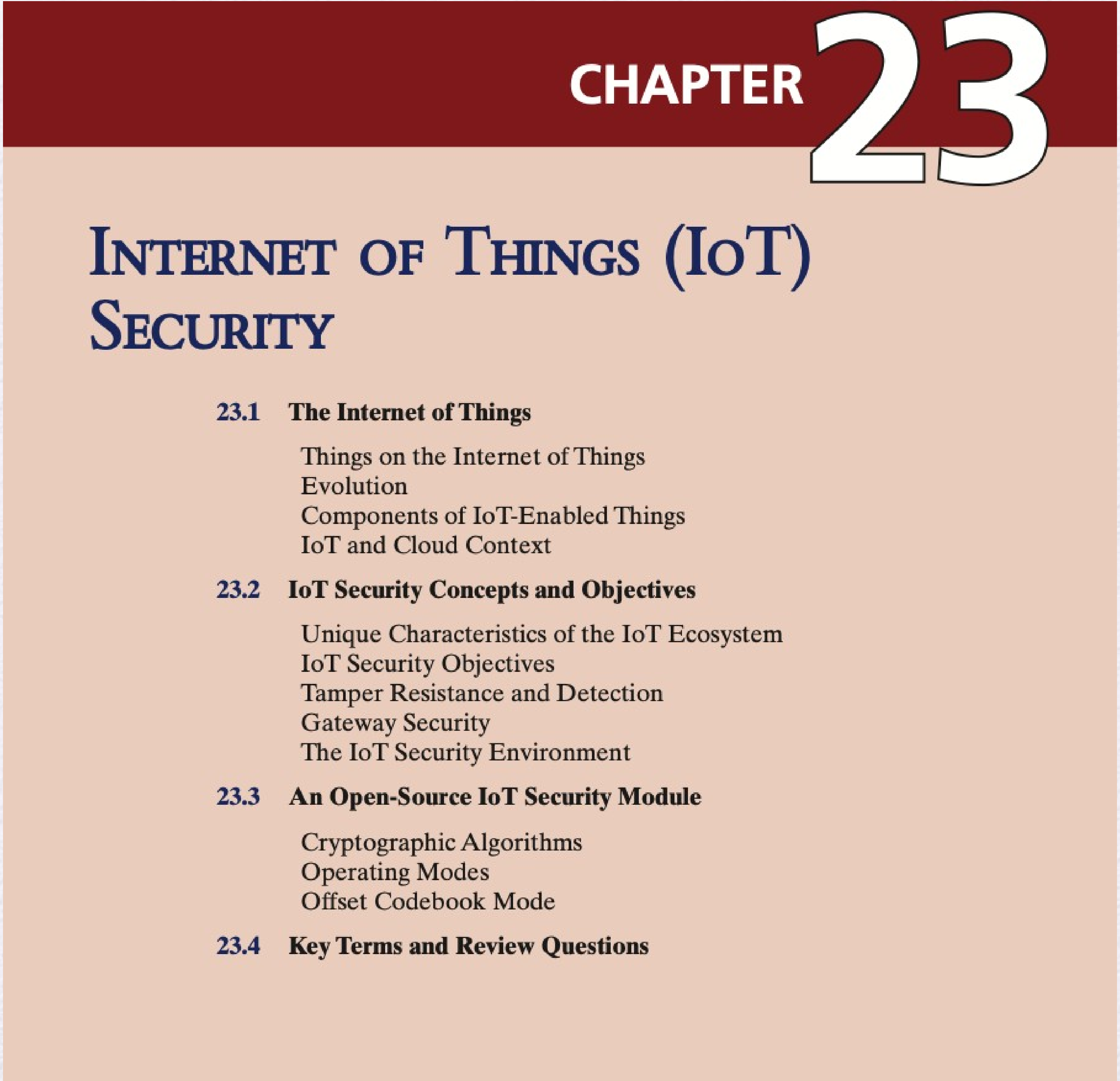
21.3 Malicious Software

Types of Malware
Malware Defense

21.4 Distributed Denial of Service Attacks

DDoS Attack Description
Constructing the Attack Network
DDoS Countermeasures

21.5 Key Terms, Review Questions, and Problems



CHAPTER 23

Internet of Things (IoT) Security

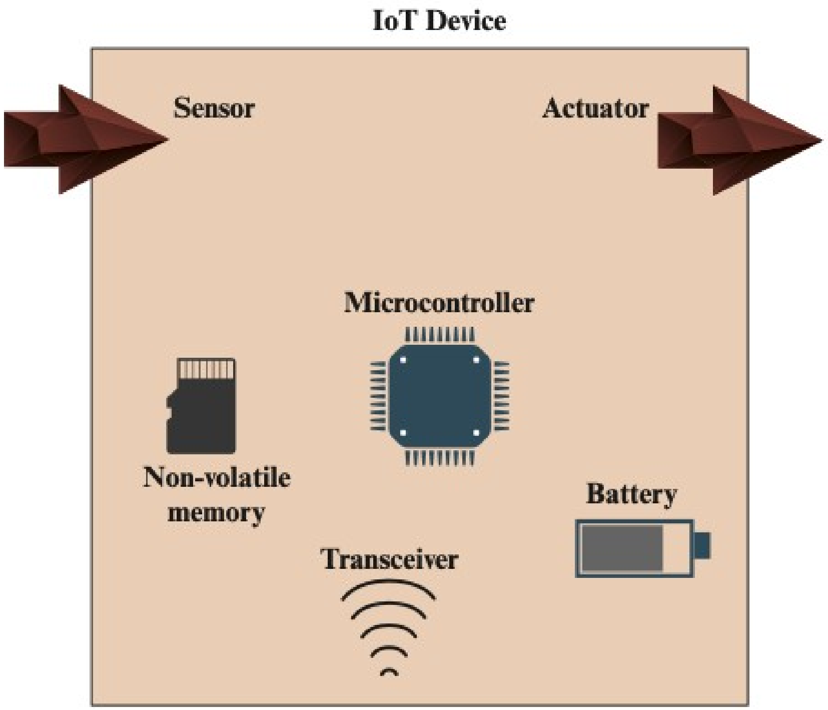


Figure 23.1 IoT Components

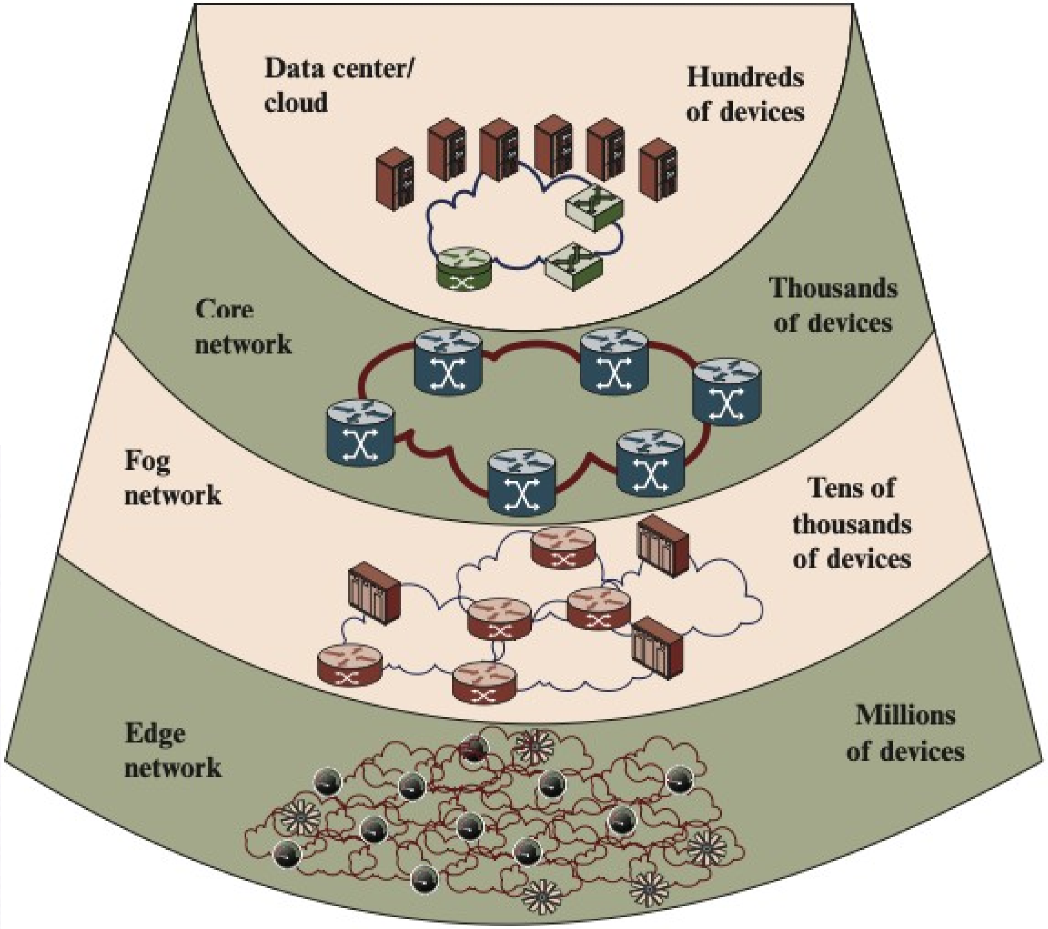


Figure 23.2 The IoT/Cloud Context

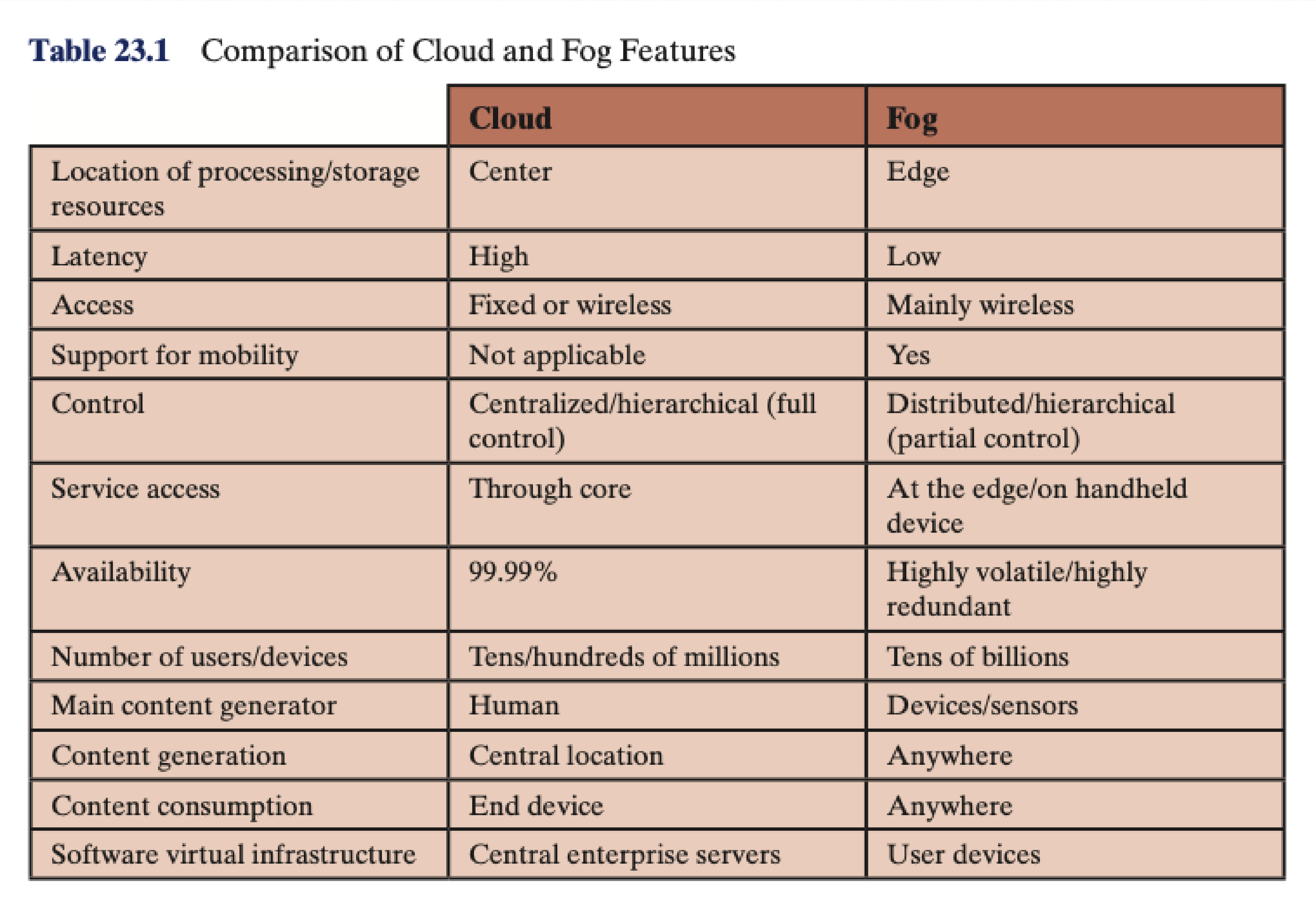


Table 23.1 Comparison of Cloud and Fog Features

	Cloud	Fog
Location of processing/storage resources	Center	Edge
Latency	High	Low
Access	Fixed or wireless	Mainly wireless
Support for mobility	Not applicable	Yes
Control	Centralized/hierarchical (full control)	Distributed/hierarchical (partial control)
Service access	Through core	At the edge/on handheld device
Availability	99.99%	Highly volatile/highly redundant
Number of users/devices	Tens/hundreds of millions	Tens of billions
Main content generator	Human	Devices/sensors
Content generation	Central location	Anywhere
Content consumption	End device	Anywhere
Software virtual infrastructure	Central enterprise servers	User devices

Unique Characteristics of the IoT Ecosystem

- **Very large attack surfaces**
- **Limited device resources**
- **Complex ecosystem**
- **Fragmentation of standards and regulations**
- **Widespread deployment**
- **Low cost**
- **Lack of expertise**: IoT is still a relatively new and rapidly evolving technology. There are a limited number of people with suitable cybersecurity training and experience.
- **Security updates**
- **Insecure programming**
- **Unclear liabilities**

IoT Device Identification for Network Management

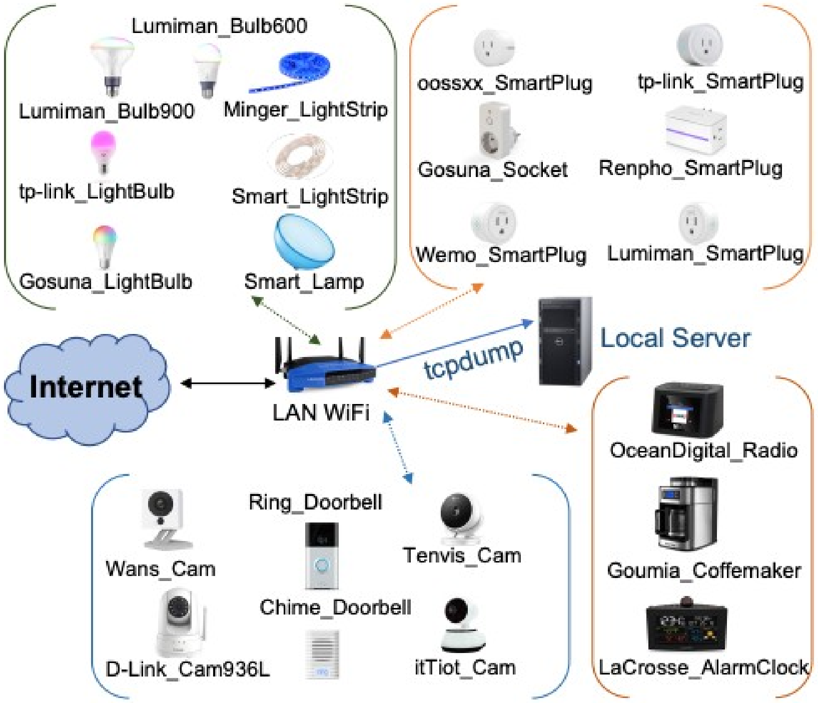
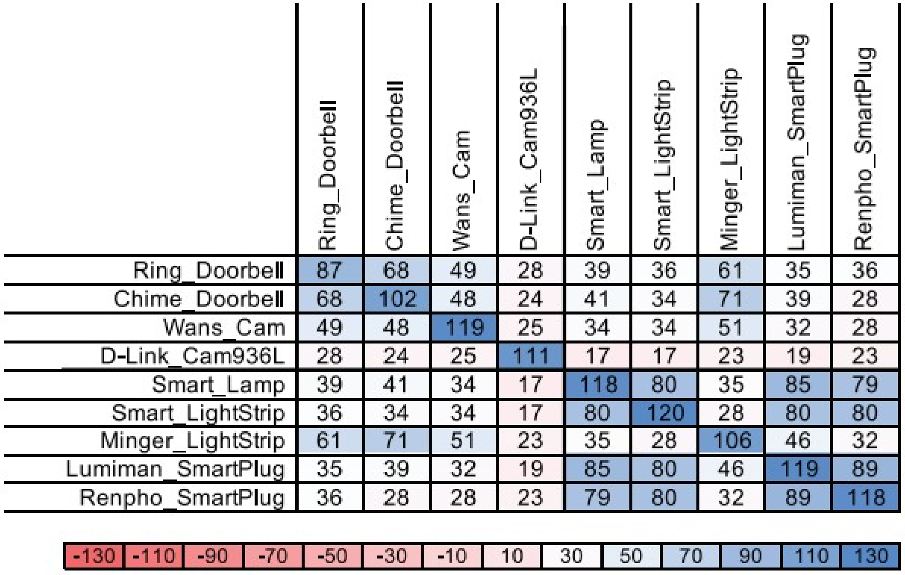


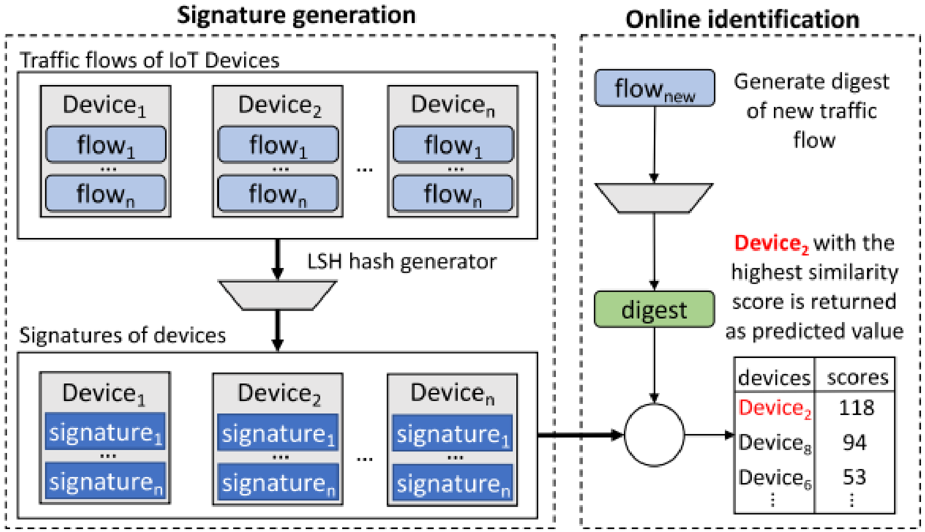
Fig. 1: Testbed for traffic collection from the 22 IoT devices



	Ring_Doorbell	Chime_Doorbell	Wans_Cam	D-Link_Cam936L	Smart_Lamp	Smart_LightStrip	Minger_LightStrip	Lumiman_SmartPlug	Renpho_SmartPlug
Ring_Doorbell	87	68	49	28	39	36	61	35	36
Chime_Doorbell	68	102	48	24	41	34	71	39	28
Wans_Cam	49	48	119	25	34	34	51	32	28
D-Link_Cam936L	28	24	25	111	17	17	23	19	23
Smart_Lamp	39	41	34	17	118	80	35	85	79
Smart_LightStrip	36	34	34	17	80	120	28	80	80
Minger_LightStrip	61	71	51	23	35	28	106	46	32
Lumiman_SmartPlug	35	39	32	19	85	80	46	119	89
Renpho_SmartPlug	36	28	28	23	79	80	32	89	118

-130	-110	-90	-70	-50	-30	-10	10	30	50	70	90	110	130

Fig. 2. Nilsimsa hash similarity score for sample devices.



devices	scores
Device$_2$	118
Device$_8$	94
Device$_6$	53
⋮	⋮

Fig. 3. Signature generation and online device identification.

IDS for IoT

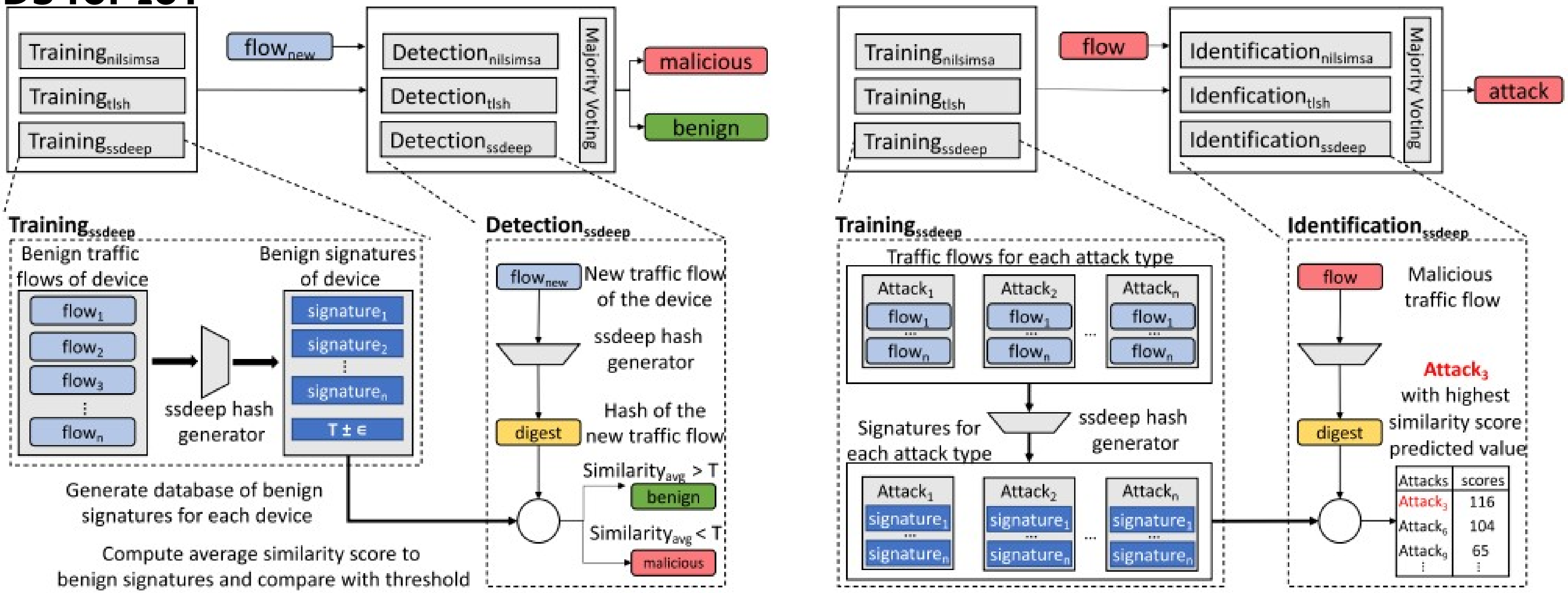


FIGURE 5. Locality sensitive anomaly detection and identification system.

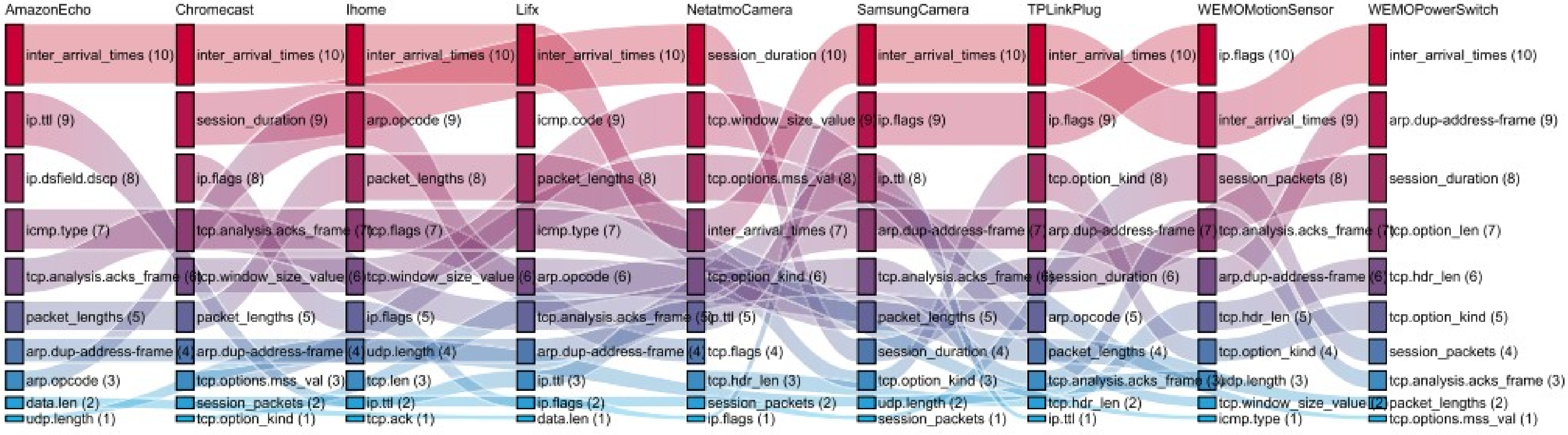
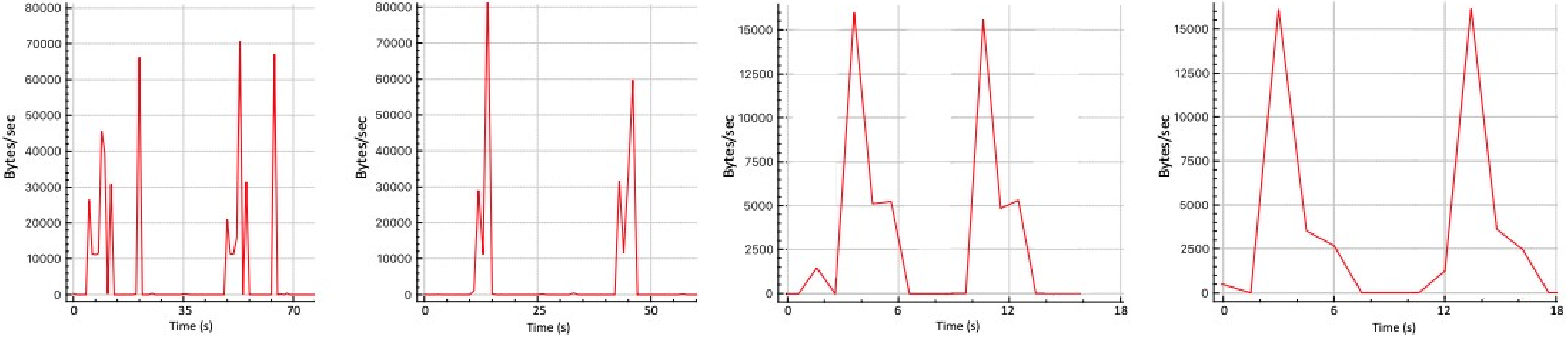


FIGURE 1. Ranking of network traffic features of sample IoT devices based on discriminative power.



a) Alexa: What is my sport update

b) Alexa: What is Roblox?

c) Microsoft's Cortana Activation: Cortana

d) Microsoft's Cortana Misactivation:
Narcos S3 E2-Cocaine, Jane The Virgin S5 E5- Correctly

Figure 2: Traffic rates of voice commands on smart speakers, each voice command repeated two times.

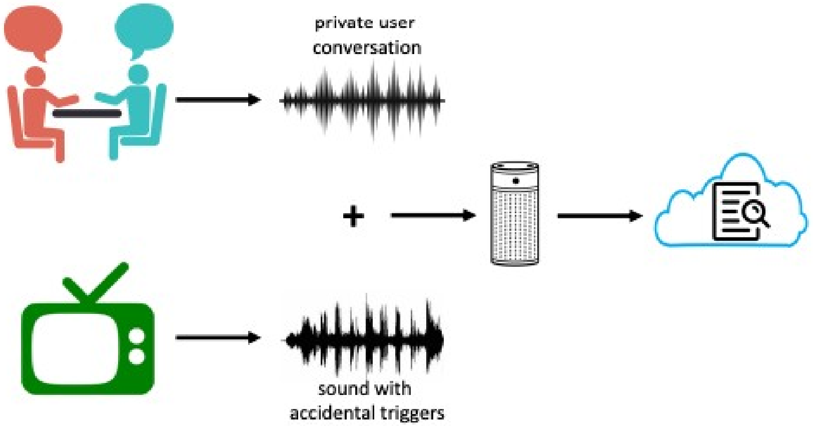


Figure 4: Unintentional activation of the smart speaker.

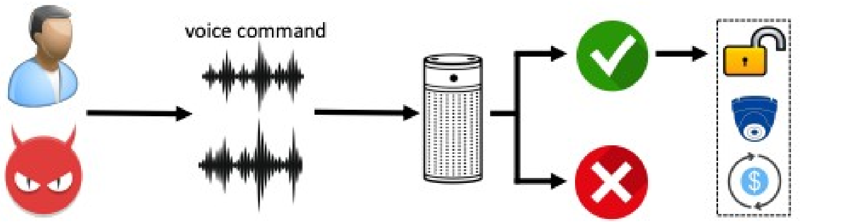


Figure 5: Adversary interacts with the smart speaker by issuing the wake word and other voice commands imitating device owner.