Practice Questions

1. Inferential Injection is also called: A. Union SQL Injection
B. Blind Injection
C. Error-based SQL Injection D. In-band SQL Injection

2. An attacker is using same communication channel to launch the injection attack and gather information from the response. Which type of SQL injection is being performed?
A. In-Band SQL Injection
B. Inferential SQL Injection
C. Out-of-Band SQL Injection
D. Union-Based SQL Injection

3. Which SQL statement is used to extract data from a database? A. OPEN
B. SELECT
C. EXTRACT
D. GET

4. Which SQL statement is used to update data in a database? A. MODIFY
B. SAVE AS
C. SAVE
D. UPDATE

5. Which SQL Query is correct to extract only "UserID" field from the "Employees" table in the database?
A. EXTRACT UserID FROM Employees
B. SELECT UserID FROM Employees
C. SELECT UserID
D. EXTRACT UserID

6. What does SQL stand for?
A. Structured Question Language B. Structured Query Language C. Strong Question Language D. Strong Query Language

Chapter 16: Hacking Wireless Networks

Technology Brief

Wireless networks are a very common and popular technology. Because of the ease and mobility of the wireless network, it has been replacing the installation of wired networks. Using wireless networks increases not only mobility but also flexibility for end users. Another advantage of wireless technology is that it helps connect remote areas where wired technology is difficult to implement. In the early days of wireless technology, the network was not secure enough to protect information. However, many encryption techniques are used nowadays to secure wireless communication channels. In this chapter, we will discuss the concept of wireless networks, threats and vulnerabilities, attacks on wireless technologies, and some defene techniques.

Wireless Concepts

Wireless Networks

The wireless network is a type of computer network capable of transmitting and receiving data through a wireless medium such as radio waves. The major advantage of this type of network is the reduced costs of wires and devices, etc. and the ease of installation compared to the complexity of wired networks. Usually, wireless communication relies on radio communication. Different frequency ranges are used for different types of wireless technology depending on requirements. The most common example of wireless networks are cell phone networks, satellite communications, microwave communications, etc. These wireless networks are popularly used for Personal, Local, Wide Area Networks.

Wireless Terminologies

GSM

Global System for Mobile Communication (GSM) is a standard set by the European Telecommunication Standards Institute. It is a second-generation (2G) protocol for digital cellular networks. 2G was developed to replace 1G (analog) technology. 2G has been replaced by the 3G UMTS standard, and the 4G LTE standard follows. GSM networks mostly operate on 900 MHz or 1800 MHz frequency bands.

Access Point

In wireless networks, an Access Point (AP) or Wireless Access Point (WAP) is a hardware device that allows wireless connectivity to the end devices. The access point can be integrated with a router or a separate device can be connected to the router.

SSID

Service Set Identifier (SSID) is a type of access point. A wireless network is identified by this name.

BSSID

This is the MAC address of an access point.

ISM Band

ISM band, also called the unlicensed band, is a radio frequency band dedicated to the industrial, scientific, and medical use. The 2.54GHz frequency band is dedicated to ISM. Microwave ovens, cordless phones, medical diathermy machines, military radars, and industrial heaters are some of the equipment that use this band.

Orthogonal Frequency Division Multiplexing (OFDM)

Orthogonal Frequency Division Multiplexing (OFDM) is a method of digital encoding on multiple carrier frequencies. It is used in digital televisions, audio broadcasting, DSL internet, and 4G communication.

Frequency Hopping Spread Spectrum (FHSS)

FHSS is a technique of transmitting radio signals by switching or hopping the carrier to different frequencies.

Types of Wireless Networks

The types of Wireless Networks deployed in a geographical area are categorized as: • Wireless Personal Area Network (Wireless PAN)

- Wireless Local Area Network (WLAN)
- Wireless Metropolitan Area Network (WMAN)
- Wireless Wide Area Network (WWAN)

However, a wireless network can be defined depending on the deployment scenario. The following are some of the wireless network types used in different scenarios.

Extension to a Wired Network


Cell Phone
Wireless Printer
Access Point
Router
Internet
Wireless User
Extention Point
Wireless User

Figure 16-01: Extension to a Wired Network

Multiple Access Points

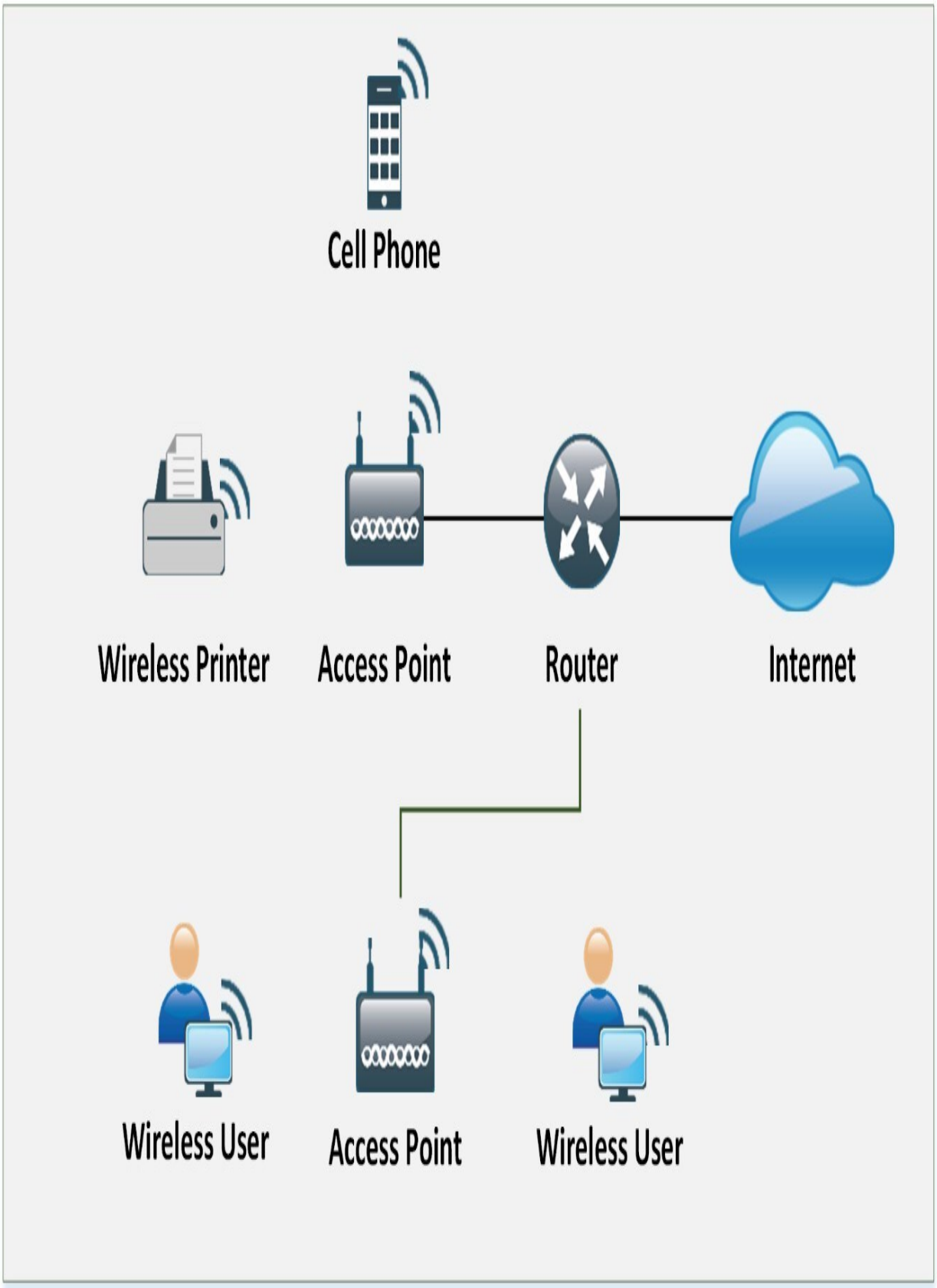

Cell Phone
Wireless Printer
Access Point
Router
Internet
Wireless User
Access Point
Wireless User

Figure 16-02: Multiple Access Points

3G/4G Hotspot

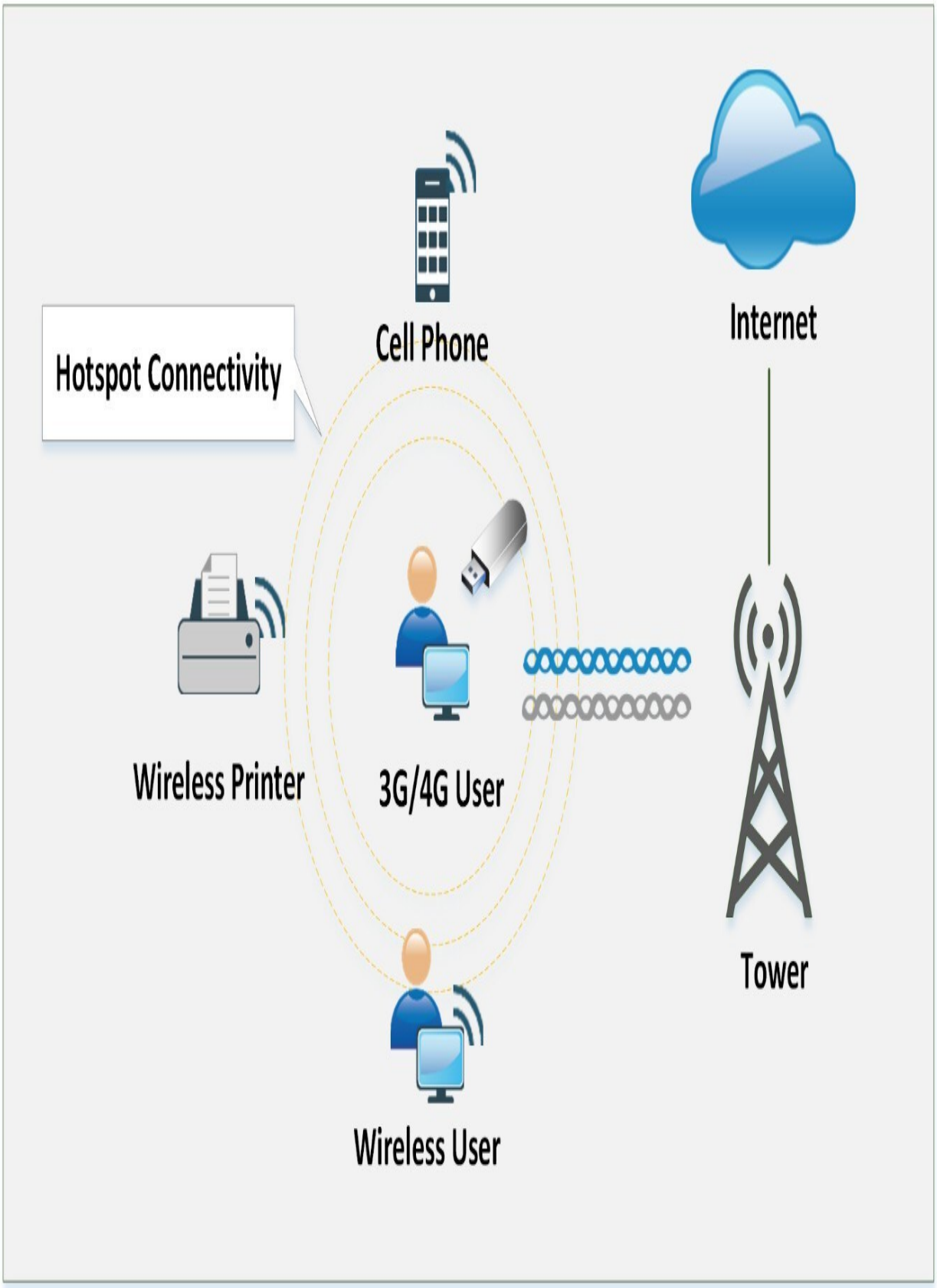

Hotspot Connectivity
Cell Phone
Internet
Wireless Printer
3G/4G User
Tower
Wireless User

Figure 16-03: Hotspot Network

Wireless Standards

Standard	Frequency
802. 1 1a	5 GHz
802. 1 1b	2.4 GHz
802. 1 1g	2.4 GHz
802. 1 1n	2.4 , 5 GHz
802. 16 (WiMAX)	10-66 GHz
Bluetooth	2.4 GHz

Modulation Speed OFDM 54 Mbps DSSS 1 1 Mbps OFDM, DSSS 54 Mbps OFDM 54 Mbps OFDM 70- 1000 Mbps GFSK 1-3 Mbps

Table 16-01: Wireless Standards

Service Set Identifier (SSID)

Service Set Identifier (SSID) is the name of an access point. Technically, SSID is a token that is used to identify 802. 1 1 networks (Wi-Fi) of 32 bytes. The Wi-Fi network continuously broadcasts SSID (if enabled). This broadcasting provides identification and access to the wireless network. If the SSID broadcast is disabled, wireless devices will not find the wireless network unless each device is manually configured with the SSID. Default parameters such as default SSID and password must be changed to avoid compromise.

Wi-Fi Technology

Wi-Fi is wireless local area networking technology which follows 802. 1 1 standards. Many devices such as personal computers, gaming consoles, mobile phones, tablets, modern printers, and many more are Wi-Fi compatible. These Wi-Fi Compatible devices are connected to the internet through a Wireless Access Point. Several subprotocols in 802. 1 1, such as 802. 1 1 a/b/g/n, are used in WLAN.

Wi-Fi Authentication Modes

There are two basic modes of authentication in Wi-Fi-based networks:
1. Open Authentication

2. Shared Key Authentication

Open Authentication

The Open System Authentication process requires six frame communications between the client and the responder to complete the process of authentication.

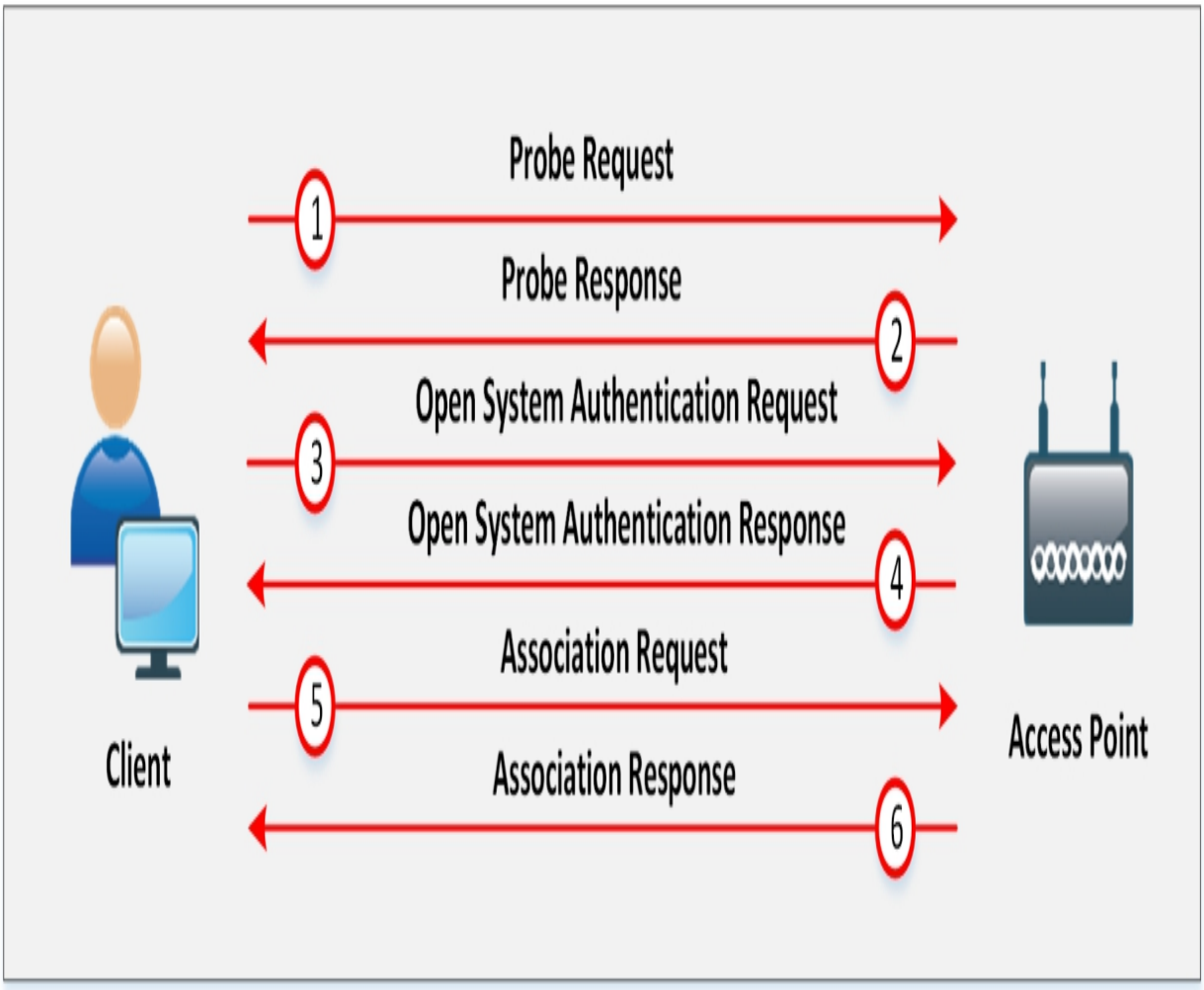


Figure 16-04: Open Authentication

• In a Wi-Fi-based LAN network, when a wireless client attempts to connect through Wi-Fi, it initiates the process of association by sending a probe request. This probe request is to discover the 802. 1 1 network. The probe request contains the client's supported data rate information. Association is simply a process of connecting to a wireless network

• If the access point found compatible parameters such as data rate and encryption technique with the client, its respond to the client's probe request contains parameters such as SSID, data rate, encryption, etc.

• The client sends an open authentication request (authentication frame) to the access point with the sequence 0x000 1 to set authentication to open
• The access point replies to the open authentication request with the sequence 0x0002
• After receiving the open system authentication response, the client sends association requests with security parameters such as chosen encryption to the access point
• The access point responds with a request to complete the process of association and the client can start sending data

Shared Key Authentication

The Shared Key Authentication mode requires four frames to complete the authentication process.

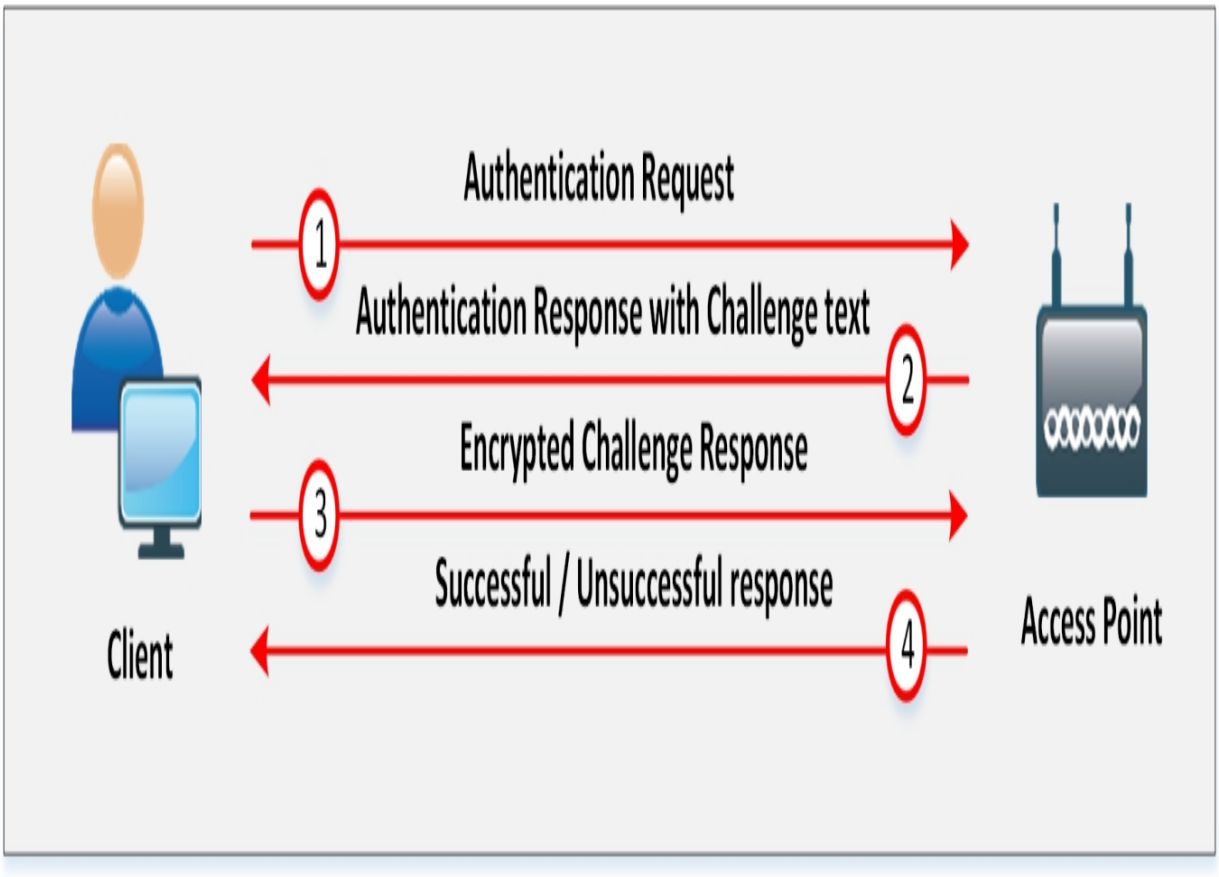


Figure 16-05: Shared Key Authentication

• The first frame is the initial authentication request frame sent by the client to the responder or access point
• The access point responds to the authentication request frame with the authentication response frame with a challenge text
• The client will encrypt the challenge with the shared secret key and send it back to the responder
• The responder decrypts the challenge with the shared secret key. If the decrypted challenge matches the challenge text, a successful authentication response frame is sent to the client

Wi-Fi Authentication with Centralized Authentication Server

Nowadays, the basic WLAN technology most commonly and widely deployed all over the world is IEEE 802. 1 1. The authentication option for the IEEE 802. 1 1 network is the Shared-Key-Authentication mechanism or WEP (Wired Equivalency Privacy). Another option is

Open Authenticatio n. These options are not capable of securing the wireless network, hence IEEE 802. 1 1 to date remains insecure.

These two authentication mechanisms, Open and Shared Authentication, cannot effectively secure the network because WEP only supports static, pre-shared keys; and in Shared-Key Authentication, a challenge is forwarded to the client from the access point, the client encrypts the challenge with a pre-share WEP key and sends it back to the access point. On a wireless medium, this process of authentication is vulnerable man-in-the-middle attacks. An eavesdropper can sniff the traffic and extract both the plain-text challenge and the cypher-text challenge and calculate the key.

IEEE 802. 1x comes with an alternative Wireless LAN security feature that offers an enhanced user authentication option with Dynamic key distribution. IEEE 802. 1x is a focused solution for a WLAN framework offering Central Authentication. IEEE 802. 1x is deployed with Extensible Authentication Protocol (EAP) as a WLAN security solution.

The major components on which this enhanced WLAN security solution IEEE 802. 1x with EAP depends are:
1. Authentication
2. Encryption
3. Central Policy

Authentication: A Mutual Authentication process between an endpoint user and the authentication server RADIUS, i.e. commonly ISE or ACS.
Encryption: Encryption keys are dynamically allocated after the authentication process.
Central Policy: Central Policy offers management and control of re-authentication, session timeout, regeneration and encryption keys, etc.

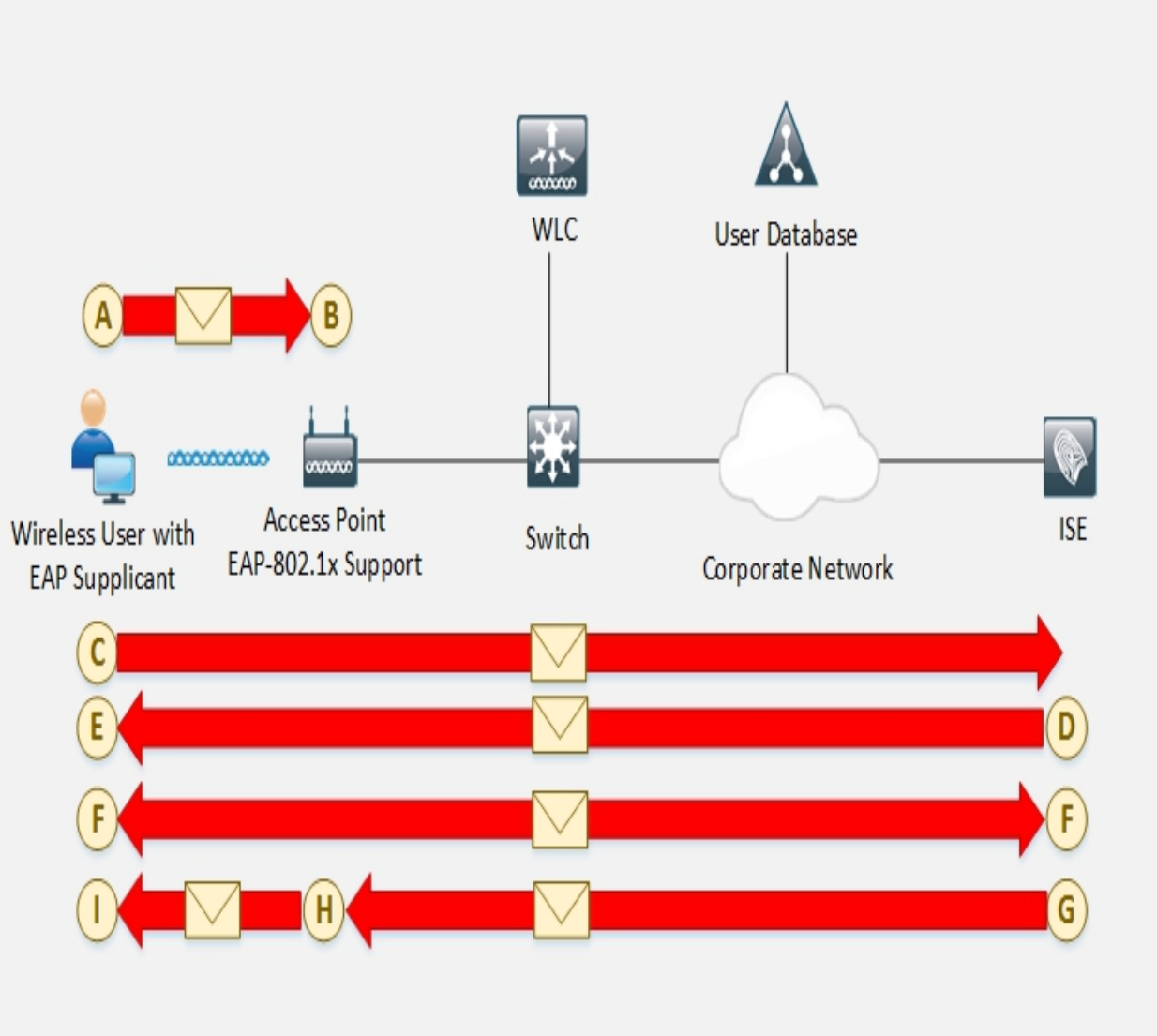


Figure 16-06: IEEE 802. 1x-EAP Authentication Flow

Wireless 802. 1x - EAP Authentication Flow

A. In the above figure, a wireless user with EAP Supplicant connects to the network to access resources through an access point.
B. As it connects and a link turns up, the access point blocks all traffic from the recently connected device until this user logs in to the network.

C. A user with EAP supplicant provides login credentials that commonly are username and password, but it can be user ID and a one-time password or a combination of user ID and a certificate. When the user provides login credentials, these credentials are authenticated by the authentication server, which is the RADIUS server.

D. Mutual authentication is performed at point D and E between the authentication server and the client. This is a two-phase authentication process. In the first phase, the server authenticates the user.

E. In the second phase, the user authenticates the server or vice versa. F. After the mutual authentication process, mutual determination of the WEP key between server and client is performed. The client must save this session key. G. The RADIUS authentication server sends this session key to the access point. H. Finally, the access point encrypts the broadcast key with the session key and sends the encrypted key to the client.

I. The client already has a session key, which is used to decrypt the encrypted broadcast key packets. Now the client can communicate with the access point using session and broadcast keys.

Note: Extensible Authentication Protocol (EAP) is used in smart cards to transfer a certificate in a secure manner. Both client and authentication server mutually authenticate over a EAP-TLS session with a digital certificate.

Wi-Fi Chalking

Wi-Fi Chalking includes several methods of detecting open wireless networks. These techniques include:

- War Walking: Walking around to detect open Wi-Fi networks
- War Chalking: Using symbols and signs to advertise open Wi-Fi networks • War Flying: Detection of open Wi-Fi networks using drones
- War Driving: Driving around to detect open Wi-Fi networks

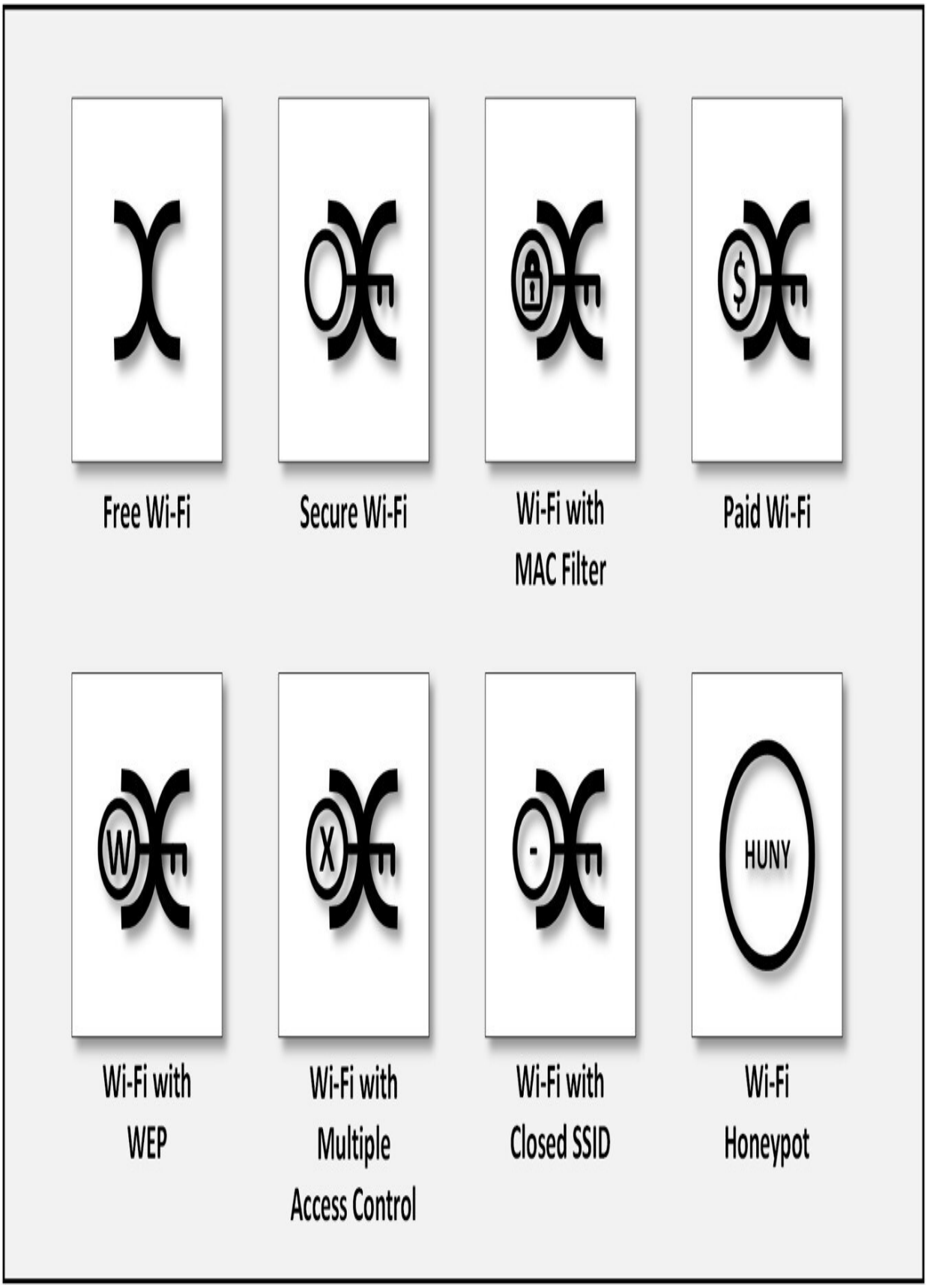


Figure 16: 03: Wi-Fi Symbols

Figure 16-07: Wi-Fi Symbols

Types of Wireless Antenna

Directional Antenna

Directional Antennas are designed to function in a specific direction to improve the efficiency of the antenna and communication by reducing interference. The most common type of directional antenna is a dish, as used with satellite TV and internet. Other types of directional antenna are Yagi Antenna, Quad Antenna, Horn Antenna, Billboard Antenna, and helical Antenna.

Omnidirectional Antenna

Aomnidirectional Antennas radiate uniformly in all directions. The radiation pattern is often described as Doughnut shaped. The most common use of omnidirectional antenna is radio broadcasting, cell phones, and GPS. Types of omnidirectional antenna include Dipole Antenna and Rubber Ducky Antenna.

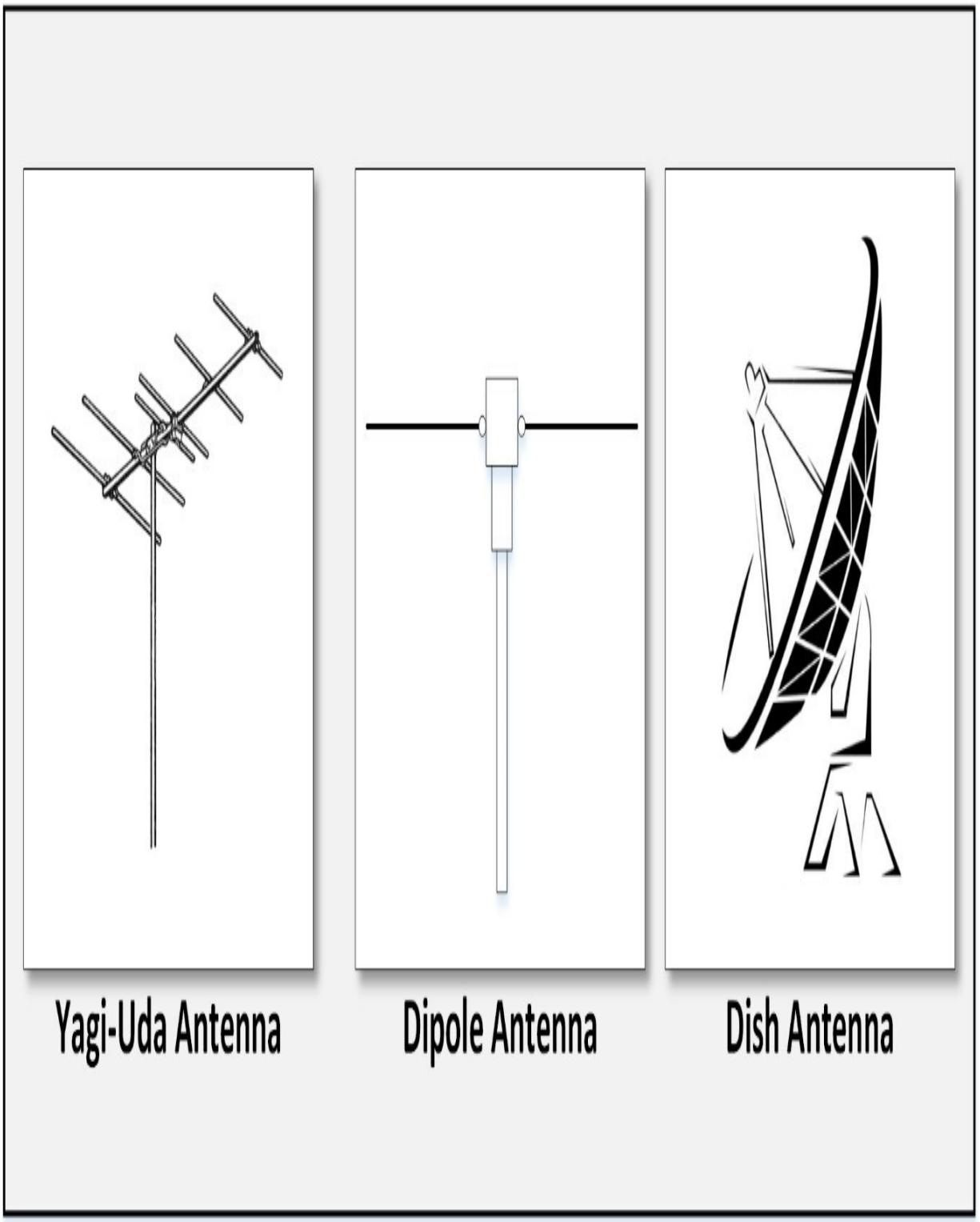


Figure 16-08: Types of Antenna

Parabolic Antenna

Parabolic Antenna, as the name suggests, depends on a parabolic reflector. The curved surface of parabola directs the radio waves. The most popular type of parabolic antenna is called Dish Antenna or Parabolic Dish. These are commonly used in radars, weather detection, satellite television, etc.

Yagi Antenna

Yagi-Uda Antenna, commonly known as Yagi antenna, is a directional antenna comprised of parasitic elements and driven elements. It is lightweight, inexpensive, and simple to construct. It is used in terrestrial television and point-to-point fixed radar communication, etc.

Dipole Antenna

The dipole antenna is the simplest antenna consisting of two identical dipoles. One side is connected to the feed line whereas another is connected to the ground. The most popular use of a dipole antenna is in FM reception and TV.

Wireless Encryption
WEP Encryption

Wired Equivalent Privacy (WEP) is the oldest and weakest encryption protocol. It was developed to ensure security of wireless protocols. However, it is highly vulnerable. It uses 24-bit Initialization Vector (IV) to create a stream cipher RC4 with Cyclic Redundant Check (CRC) to ensure confidentiality and integrity. A standard 64-bit WEP uses a 40-bit key, 128-bit WEP uses a 104-bit key, and 256-bit WEP a uses a 232-bit key. Authentications used with WEP are Open System Authentication and Shared Key Authentication.

Working of WEP Encryption

Initialization Vector (IV) and Key together are called WEP Seed. This WEP Seed is used to create RC4 Key. RC4 generates a pseudorandom stream of bits. This pseudorandom

stream is XORed with the plain text to encrypt the data. CRC32 Checksum is used to calculate the Integrity Check Value (ICV).

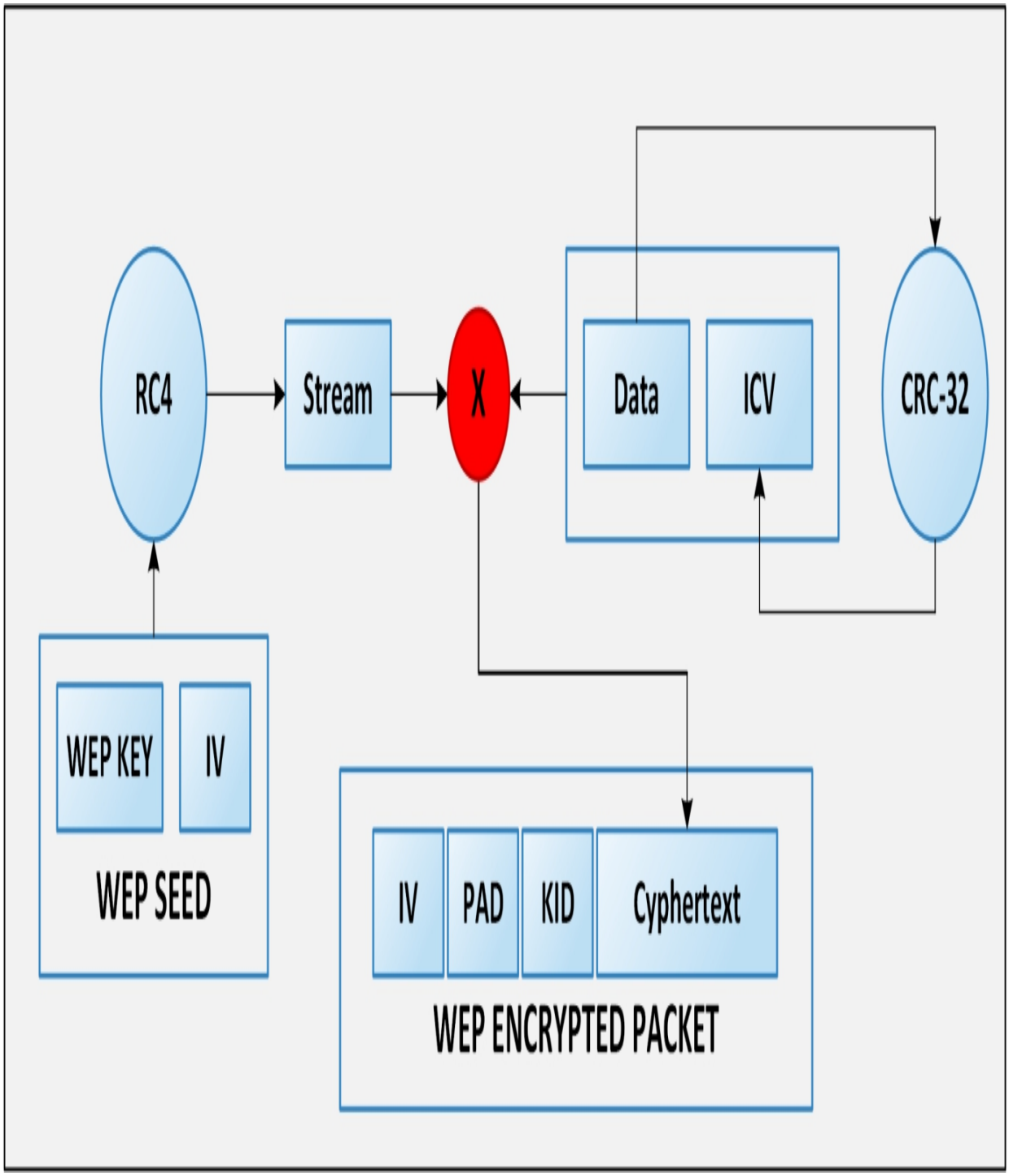


Figure 16-09: WEP Encryption Flow

Weak Initialization Vectors (IV)

The one of the major issues with WEP is with Initialization Vector (IV). The IV value is too small to protect from reuse and replay. The RC4 Algorithm uses IV and Key to create

a stream using a Key Scheduling algorithm. Weak IV reveals information. WEP has no built-in provision to update the key.

Breaking WEP Encryption

Breaking WEP Encryption can be performed by following the steps outlined below: 1. Monitor the access point channel.
2. Test the injection capability of the access point.

3. Use tools to exploit authentication.
4. Sniff the packets using Wi-Fi sniffing tools.
5. Use an encryption tool to inject encrypted packets.
6. Use the cracking tool to extract the encryption key from IV.

WPA Encryption

Wi-Fi Protected Access (WPA) is another data encryption technique that is popularly used for WLAN networks based on 802. 1 1i standards. This security protocol was developed by Wi-Fi Alliance to secure the WLAN networks against weaknesses and vulnerabilities found in Wired Equivalent Privacy (WEP). The deployment of WPA requires firmware upgrades for wireless network interface cards designed for WEP. Temporal Key Integrity Protocol (TKIP) dynamically generates a new key for each packet of 128-bits to prevent a threat that is vulnerable to WEP. WPA also contains Message Integrity Check as a solution to Cyclic Redundancy Check (CRC) that was introduced to WEP to overcome the flaw of strong integrity validation. ### *Temporal Key Integrity Protocol*

Temporal Key Integrity Protocol (TKIP) is a protocol used in IEEE 802. 1 1i Wireless networks. This protocol is used in Wi-Fi Protected Access (WPA). TKIP has introduced three security features:

1. Secret root key and Initialization Vector (IV) Mixing before RC4.
2. Sequence Counter to ensure receiving in order and prevent replay attacks.
3. 64-bit Message Integrity Check (MIC).

How WPA Encryption Works

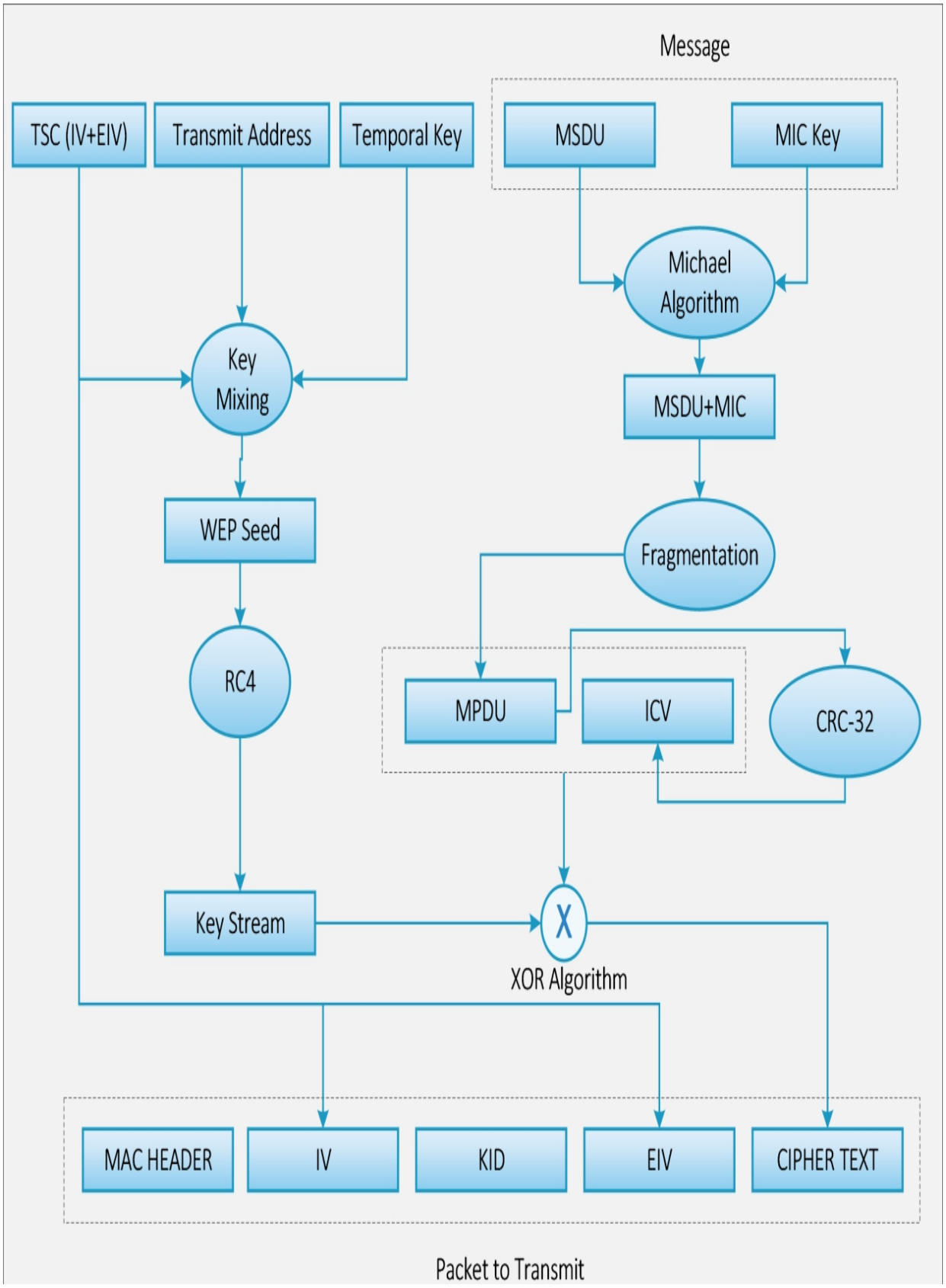


Figure 16-10: WPA Encryption Flow

1. Temporal Encryption Key, Transmit Address, and TKIP Sequence Number are initially mixed to create a WEP seed before input to the RC4 algorithm.
2. The WEP seed is input to the RC4 algorithm to create a Key Stream.
3. MAC Service Data Unit (MSDU) and Message Integrity Check (MIC) are combined using the Michael Algorithm.
4. The result of the Michael Algorithm is fragmented to generate a MAC Protocol Data Unit (MPDU).
5. A 32-bit Integrity Check Value (ICV) is calculated for MPDU.
6. The combination of MPDU and ICV that is XORed with the Key Stream is created in the second step to create Ciphertext.

WPA2 Encryption

WPA 2 is designed to overcome and replace WPA, providing better security using a 192- bit encryption and individual encryption for each user, making it more complicated to compromise. It uses Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), and Advanced Encryption Standard (AES) based encryption. Wi-Fi Allowance also introduced a more advanced security protocol WPA3 in 20 18 to overcome WPA2 with additional capabilities and security.

WPA 2-Personal requires a password (Pre-Shared Key) to protect the network from unauthorized access. In this mode, each wireless device encrypts traffic with a 128-bit derived key from a passphrase of 8 to 63 ASCII characters. WPA2-Enterprise includes EAP or RADIUS for a centralized authentication mechanism. Using this centralized authentication with additional authentication mechanisms, such as Kerberos and Certificates, makes wireless networks more secure.

Encryption
Encryption Algorithm

IV Size
Encryption Key

Integrity Check Mechanism WEP RC4
WPA RC4 , TKIP

WPA 2 AES , CCMP
24-bits 40/ 104-Bits CRC32

48-bits 128-Bits Michael Algorithm and CRC32
48-bits 128-Bits CBC-MAC
Table 16-02: Comparing 802. 1 1 Encryption Protocols

Breaking WPA Encryption

1. Brute-force the WPA PSK user-defined password using Dictionary Attack.
2. Capture the WPA/WPA2 Authentication Handshake packets to crack the WPA Key offline.
3. Force the connected client to disconnect and then reconnect to capture the authentication packets to brute force the Pairwise Master Key (PMK).

Wireless Threats

Access Control Attacks

Wireless Access Control Attacks are attacks in which an attacker penetrates the wireless network by evading access control parameters, for example, by spoofing the MAC address, rogue access point, and misconfigurations, etc.

Integrity and Confidentiality Attacks

Integrity attacks include WEP injection, data frame injection, replay attacks, and bit flipping, etc. masquerading, information.

Confidentiality attacks include cracking, MITM attacks, etc. traffic analysis, session hijacking, in order to intercept confidential

Availability Attacks

Availability Attacks include flooding and denial-of-service attacks that prevent legitimate users from connecting or accessing the wireless

network. Availability attacks can be carried out by authentication flooding, ARP poisoning, de-authentication attacks, disassociation attack, etc.

Authentication Attacks

An Authentication Attack attempts to steal identified information or legitimated wireless client in order to gain access to the network by impersonating a legitimate user. It may include password cracking techniques, identity theft, password guessing.

Rogue Access Point Attack

A Rogue Access Point Attack is a technique whereby a legitimate wireless network is replaced with a rogue access point, usually with the same SSID. The user assumes the rogue access point as the legitimate access point and connects to it. Once a user is connected to the rogue access point, all traffic will direct through it and the attacker can sniff the packet to monitor activity.

Client Misassociation

Client Misassociation includes a rogue access point outside the parameters of a corporate network. Once an employee is connected to this rogue access point mistakenly, all traffic will pass to the internet through the attacker.

Misconfigured Access Point Attack

A Misconfigured Access Point Attack gains access to a legitimate access point by taking advantage of its misconfigurations. Misconfigurations may be a weak password, default password configuration, or a wireless network without password protection, etc.

Unauthorized Association

Unauthorized Association is another technique in which infected users act as an access point, allowing an attacker to connect to the corporate network. These Trojans create a soft access point through

malicious scripting, which allows the devices such as laptops to turn their WLAN cards into transmitters, transmitting the WLAN network.

Ad Hoc Connection Attack

Ad Hoc Connection is an insecure network because it does not provide strong authentication and encryption. An attacker may attempt to compromise the client in ad hoc mode.

Signal Jamming Attack

A Signal Jamming Attack requires high gain frequency signals, which cause a denial-ofservice attack. The Carrier Sense Multiple Access/Collision Avoidance Algorithm requires waiting time to transmit after detecting a collision.

Wireless Hacking Methodology

Wi-Fi Discovery

The first step in hacking a wireless network in order to compromise it is to get information about it. Information can be collected by Active Footprinting and Passive Footprinting, as well as by using different tools. Passive footprinting includes sniffing packets using tools such as Airwaves, Net Surveyor and others to reveal information such as which live wireless networks are around. Active footprinting includes probing the access point to obtain information. In active footprinting, the attacker sends a probe request, and the access point sends a probe response.

GPS Mapping

GPS mapping is the process of creating a list of Wi-Fi networks that have been found using GPS. The GPS traces the location of the Wi-Fi networks and this information can then be sold to an attacker or hacking community.

Wireless Traffic Analysis

Traffic analysis of a wireless network includes capturing the packet to reveal any information such as broadcast SSID, authentication methods, encryption techniques, etc. There are several tools available to capture and analyze a wireless network, for example, Wireshark/Pilot tool, Omni peek, Commview, etc.

Launch Wireless Attacks

Attackers use tools, such as Aircrack-ng, and other attacks, such as ARP poisoning, MITM, Fragmentation, MAC Spoofing, De-authentication, Disassociation, and rogue access point, to initiate an attack on a wireless network.

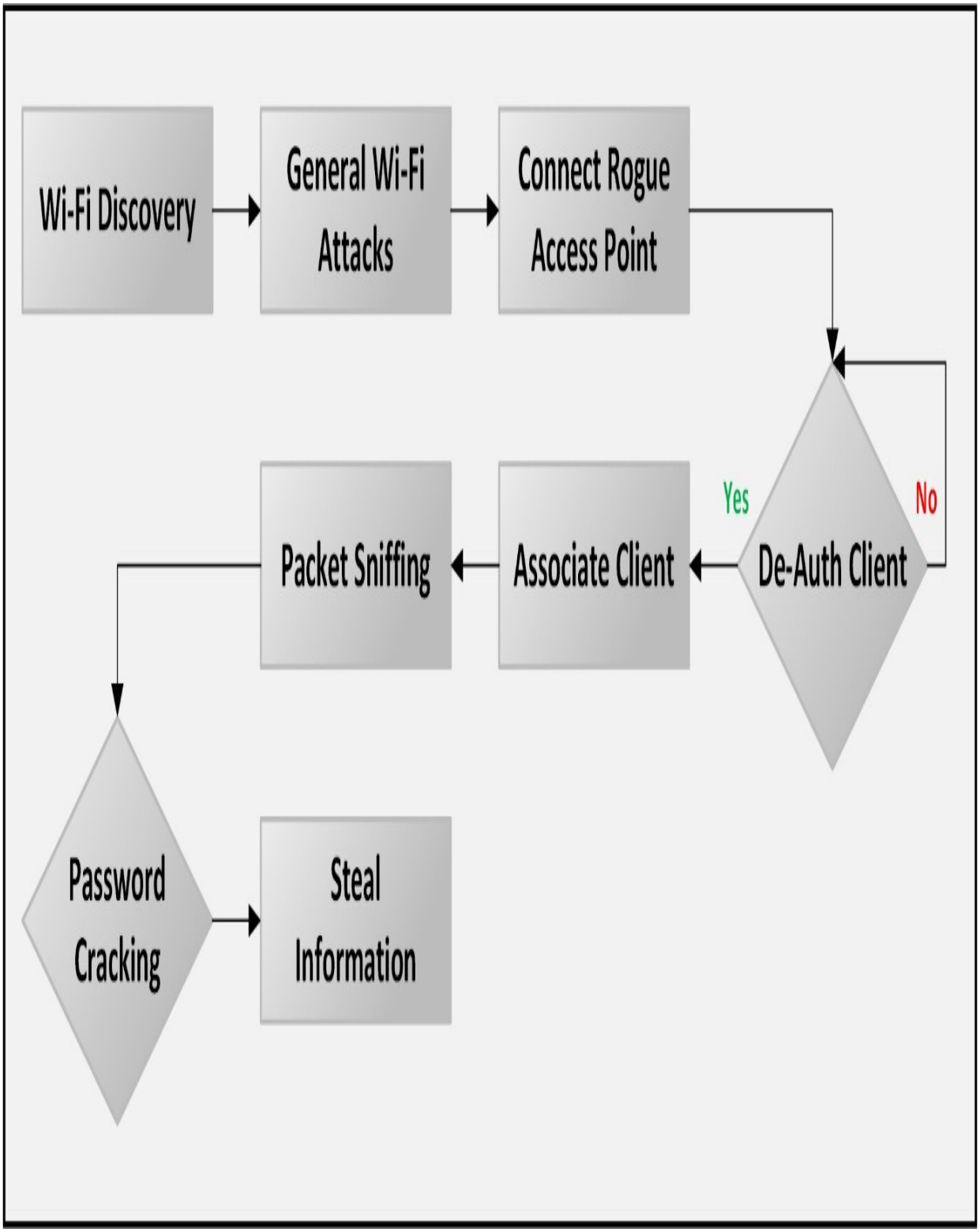


Figure 16-11: Wi-Fi Pentesting Framework

Bluetooth Hacking

Bluetooth Hacking refers to attacks on Bluetooth-based communication. Bluetooth is a popular wireless technology available in almost every mobile device. Bluetooth technology is used for short-range communication between the devices. It operates at 2.4 GHz frequency and can be effective up to 10 meters.

The Bluetooth discovery feature enables devices to be discovered by other Bluetooth enabled devices. The discovery feature can be enabled as continuous or set up for a short period.

Bluetooth Attacks

Blue Smacking

Blue Smacking is a type of Bluetooth DoS attack. In Blue Smacking, random packets overflow the target device. The ping of death is used to launch Bluetooth DoS attack by flooding a large number of echo packets.

Bluebugging

Bluebugging is another type of Bluetooth attack in which an attacker exploits Bluetooth devices to gain access and compromise security. Bluebugging is a technique accessing a Bluetooth-enabled device remotely. The attacker uses this to track the victim or access the contact list, messages, and other personal information.

Blue Jacking

Blue Jacking is the art of sending unsolicited messages to Bluetooth-enabled devices. A Blue Jacking hacker can send messages, images, and other files to other Bluetooth devices.

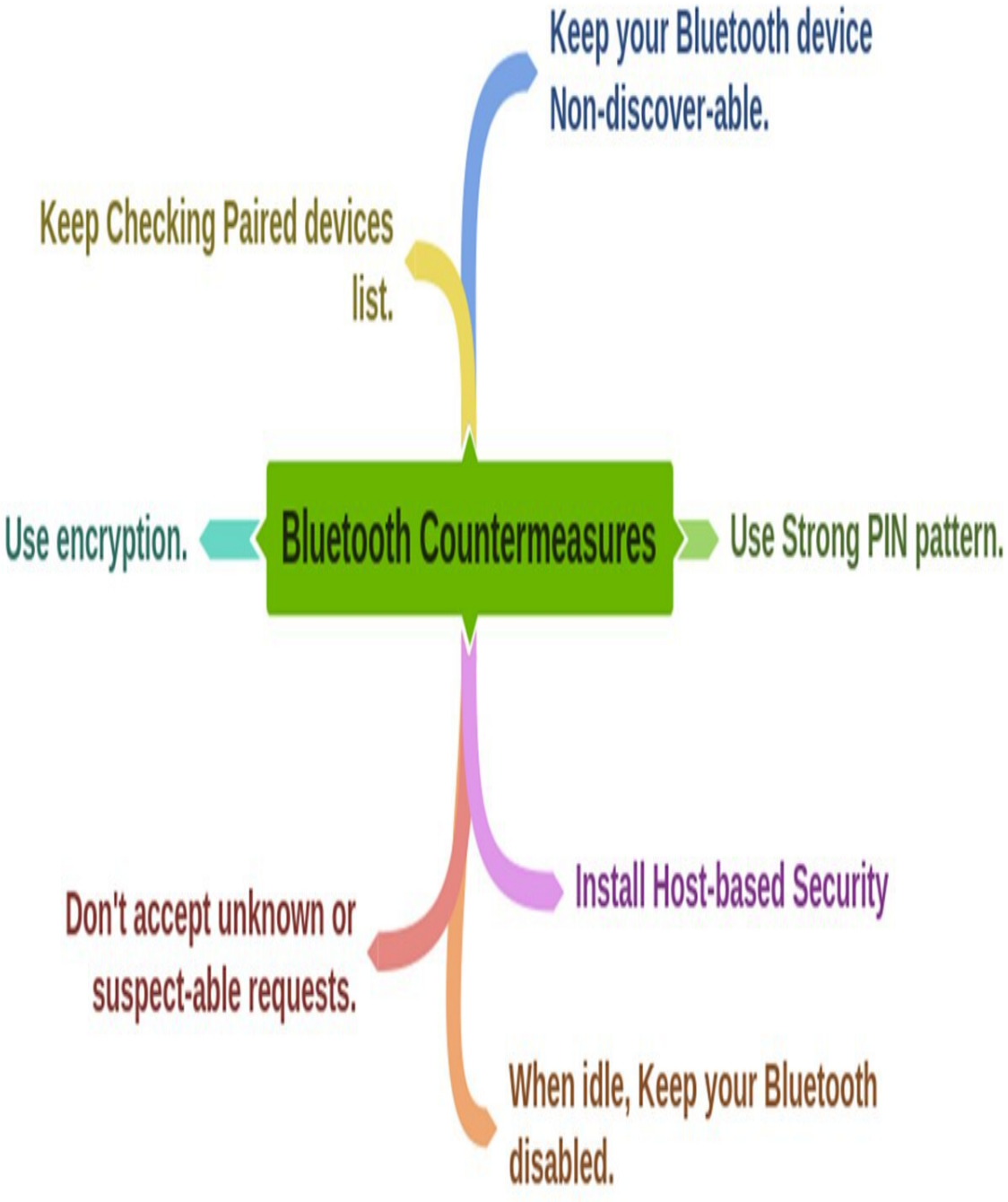
Blue Printing

Blue Printing is a technique or method for extracting information and details about a remote Bluetooth device. This information may be used for exploitation. Information such as firmware, the manufacturer and model of the device, etc. can be extracted.

Bluesnarfing

Bluesnarfing is another technique in which attackers steal information from Bluetoothenabled devices. In Bluesnarfing, attackers exploit the security vulnerabilities of Bluetooth software, access Bluetooth-enabled devices and steal information such as contact lists, text messages, email, etc.

Bluetooth Countermeasures



Wireless Intrusion Prevention Systems (WIPS)

Wireless Intrusion Prevention System (WIPS) is a network device for wireless networks. It monitors the wireless network, protects it against unauthorized access points, and performs automatic intrusion prevention. By monitoring the radio spectrum, it prevents rogue access points and generates alerts for the network administrator. The fingerprinting approach helps to avoid devices with spoofed MAC addresses. WIPS consists of three components, server, sensor, and console. Rogue access points, misconfigured APs, client misconfiguration, MITM, ad hoc networks, MAC spoofing, Honeypots, DoS attacks can all be mitigated using WIPS.

Wi-Fi Security Auditing Tool

Using Wireless Security tools is another approach to protecting wireless networks. This security software provides wireless network auditing, troubleshooting, detection, intrusion prevention, threat mitigation, rogue detection, day-zero threat protection, forensic investigation, and compliance reporting. Some of the popular Wi-Fi security tools are as follows:

- AirMagnet WiFi Analyzer
- Motorola's AirDefense Services Platform (ADSP)
- Cisco Adaptive Wireless IPS
- Aruba RFProtect

Lab 16- 1: Hacking a Wi-Fi Protected Access Network using Aircrackng

Case Study: Consider a Wi-Fi network secured with WPA. In this case, we will capture some 802. 1 1 (Wireless Network) packets and save them into a file. Using Cupp and Aircrack-ng utilities, we will create a password file and crack the password.

1. Capture some WLAN packets using the filter "eth.add==aa:bb:cc:dd:ee" and save the file.
2. Go to a Kali Linux terminal.

3. Change the directory to the desktop.
root@kali:~# cd Desktop
4. Download the "Cupp" utility to create wordlist.
root@kali:~# git clone https://github.com/chetan3 1295/cupp.git

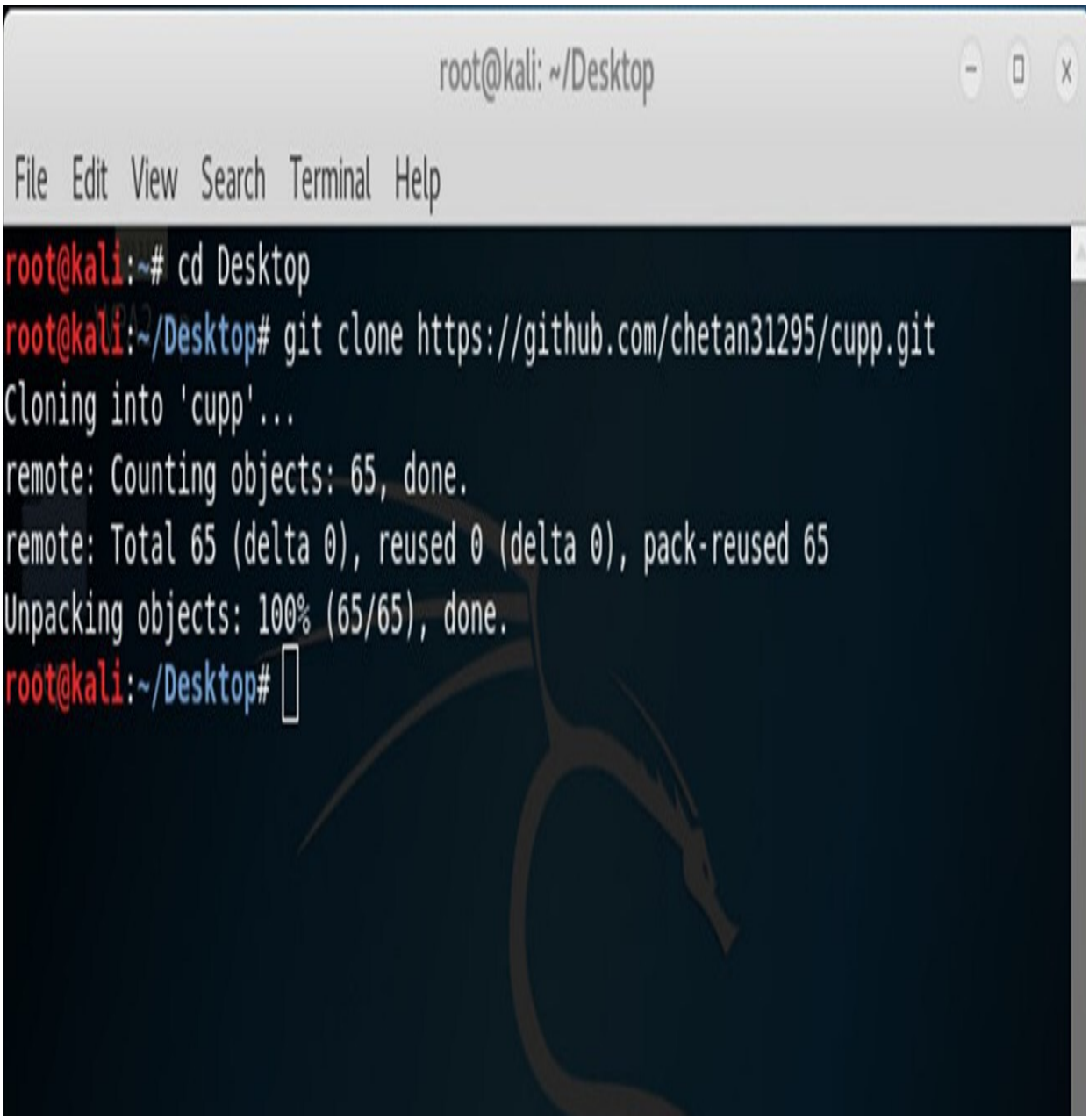


Figure 16-12: Downloading Cupp

5. Change the directory to /Desktop/Cupp. root@kali:~/Desktop# cd cupp
6. List the folders in the current directory. root@kali:~/Desktop/cupp#

ls

7. Run the utility cupp.py

root@kali:~/Desktop/cupp# ./cuppy.py

Figure 16_13: Running Cupp Utility

Figure 16-13. Running Cupp Utility

8. Use an interactive question for user password profiling.

```
root@kali:~/Desktop/cupp# ./cupp.py -i
```

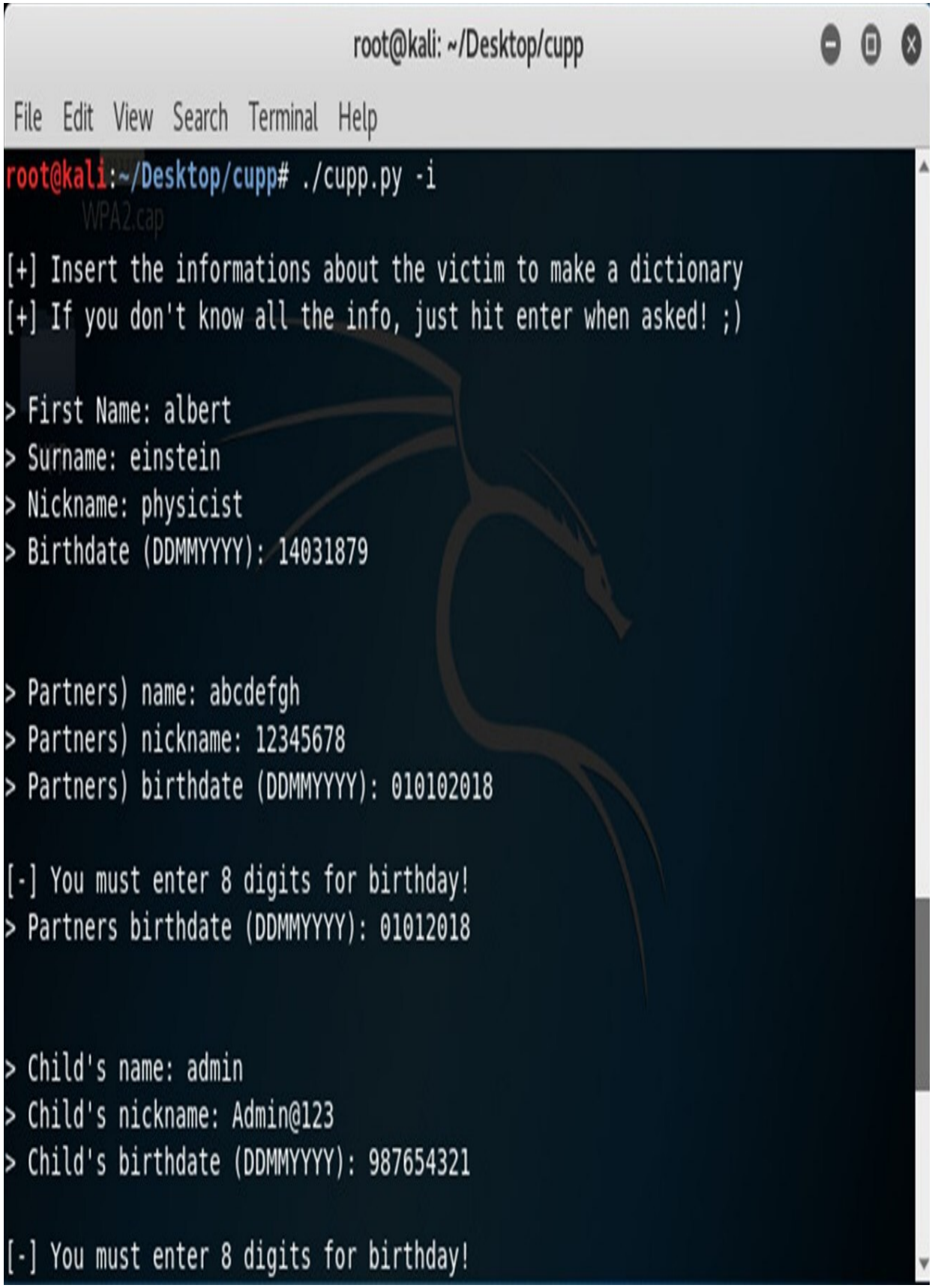

root@kali: ~/Desktop/cupp
File Edit View Search Terminal Help
root@kali:~/Desktop/cupp# ./cupp.py -i
[+] Insert the informations about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)
> First Name: albert
> Surname: einstein
> Nickname: physicist
> Birthdate (DDMMYYYY): 14031879
> Partners) name: abcdefgh
> Partners) nickname: 12345678
> Partners) birthdate (DDMMYYYY): 010102018
[-] You must enter 8 digits for birthday!
> Partners birthdate (DDMMYYYY): 01012018
> Child's name: admin
> Child's nickname: Admin@123
> Child's birthdate (DDMMYYYY): 987654321
[-] You must enter 8 digits for birthday!

Figure 16-14: Interactive Questions

9. Provide the closest information about the target. It will increase the chances of successful cracking.
10. You can add keywords.
11. You can add special characters.
12. You can add random numbers.
13. You can enable the Leet mode.

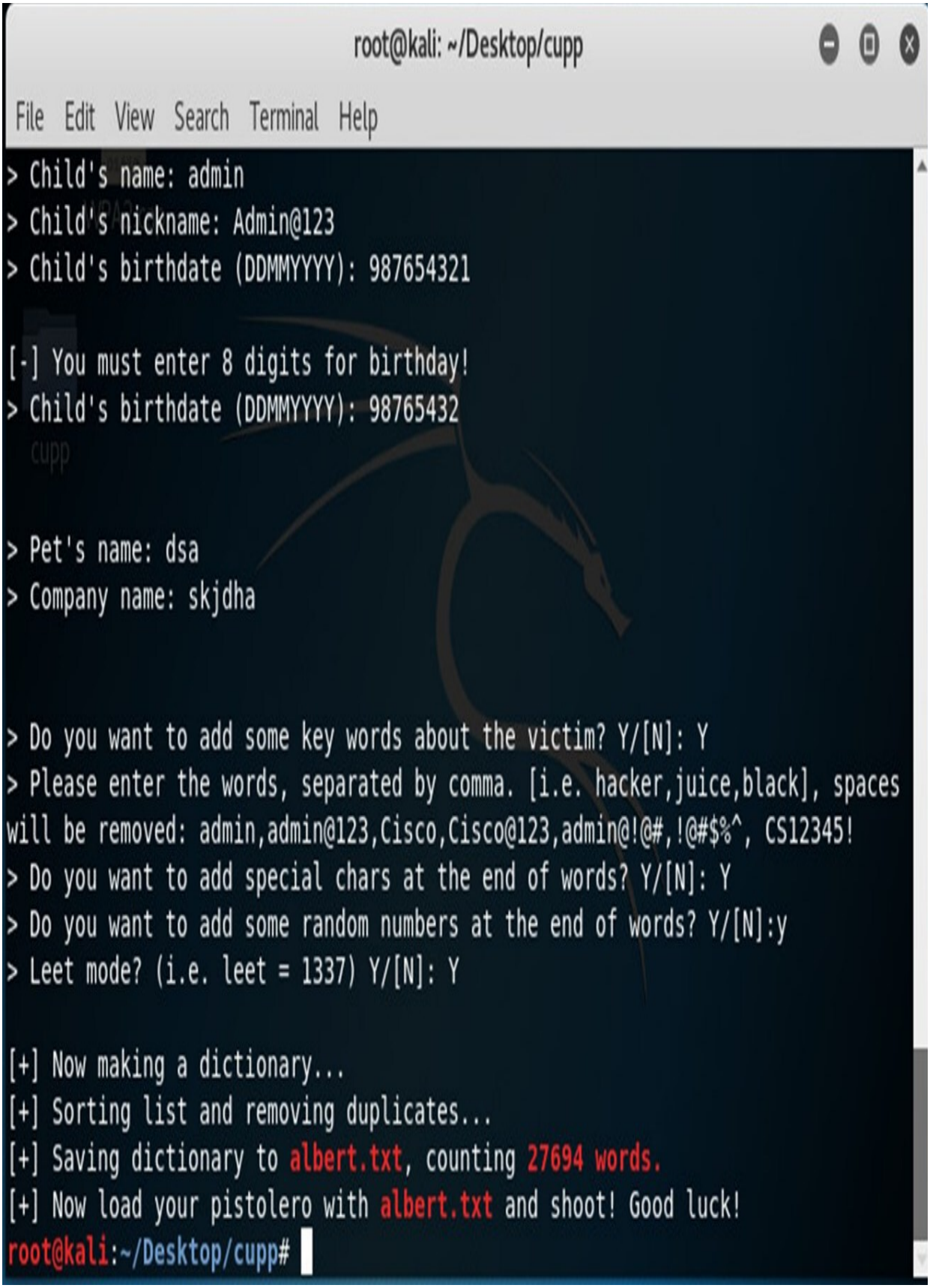


Figure 16 - 15 Wordlist Created

Figure 16-15 Wordlist Created

14. After successful completion, you will find a new text file named as the first name you typed in the interactive option. This file will contain many possible combinations. As shown in the figure below, albert.txt file has been created in the current directory.

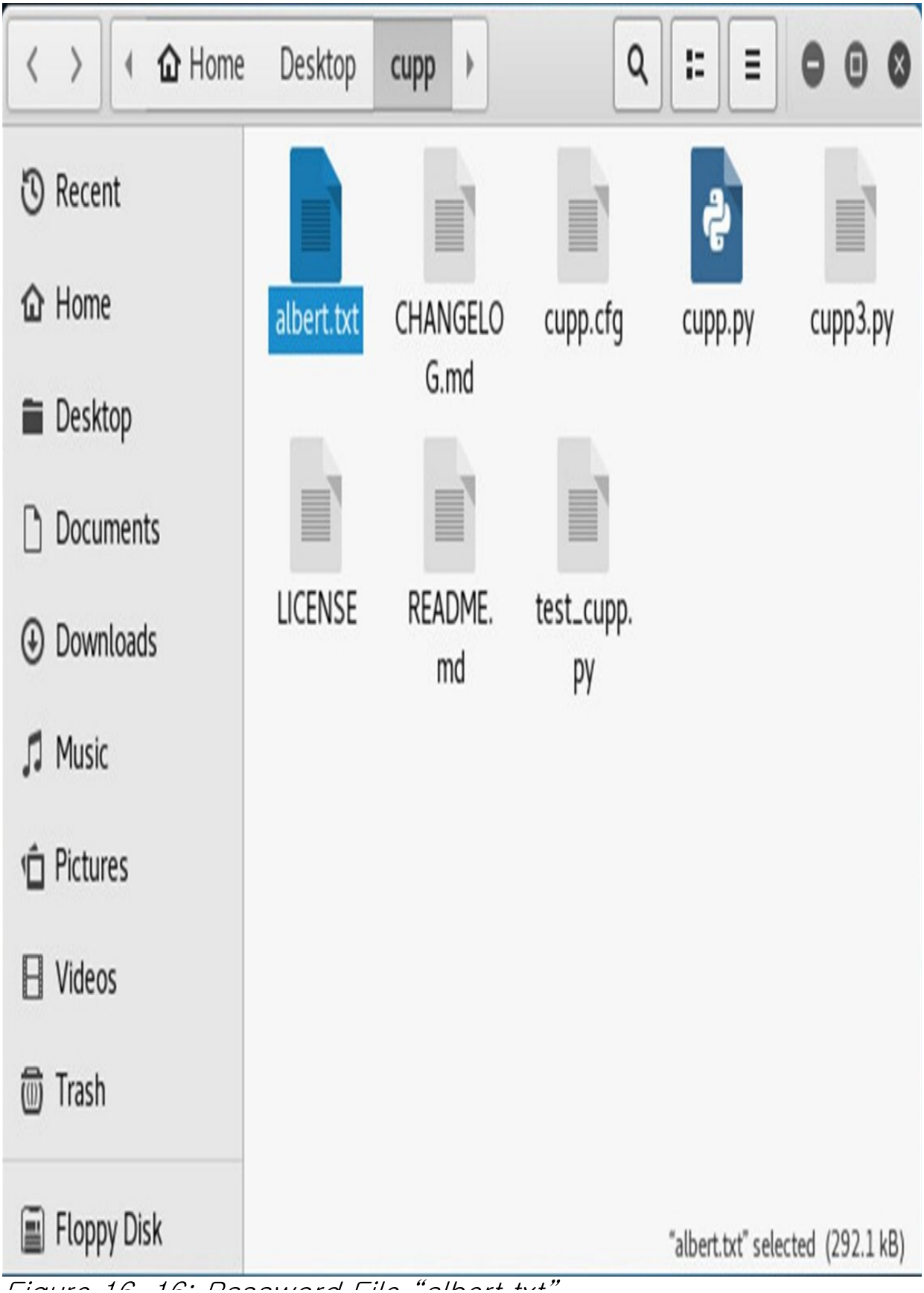


Figure 16–16: Password File "albert.txt"

Figure 16-16: Password File "albert.txt"

15. You can check the file by opening it.

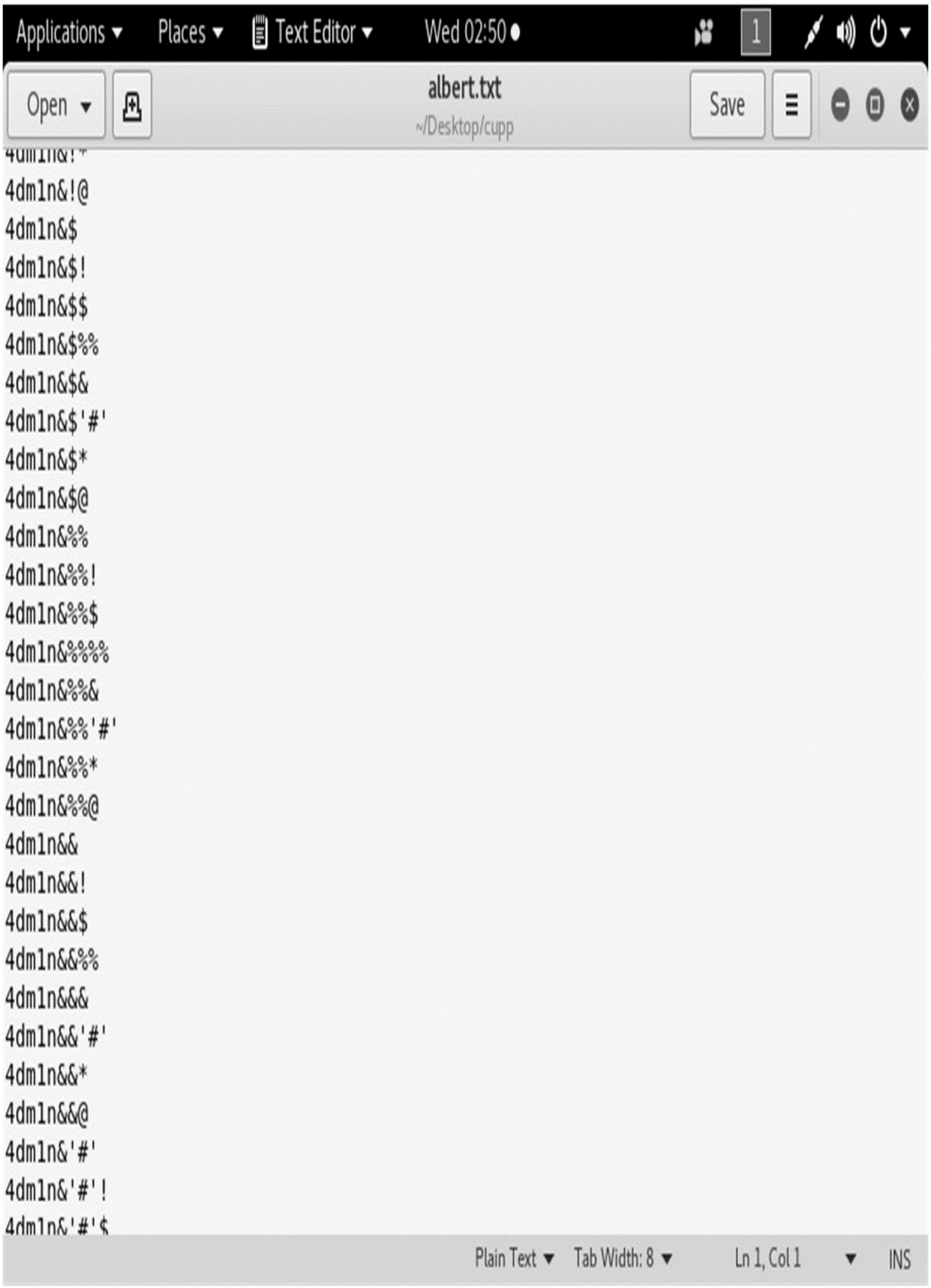

Applications
Places
Text Editor
Wed 02:50
1
Open
albert.txt
~/Desktop/cupp
Save
4dm1n&!*
4dm1n&!@
4dm1n&$
4dm1n&$!
4dm1n&$$
4dm1n&$%%
4dm1n&$&
4dm1n&$'#'
4dm1n&$*
4dm1n&$@
4dm1n&%%
4dm1n&%%!
4dm1n&%%$
4dm1n&%%%%
4dm1n&%%&
4dm1n&%%'#'
4dm1n&%%*
4dm1n&%%@
4dm1n&&
4dm1n&&!
4dm1n&&$
4dm1n&&%%
4dm1n&&&
4dm1n&&'#'
4dm1n&&*
4dm1n&&@
4dm1n&'#'
4dm1n&'#'!
4dm1n&'#'$
Plain Text
Tab Width: 8
Ln 1, Col 1
INS

Figure 16-17: Possible Combinations

16. Now crack the password using Aircrack-ng with the help of the password file created.

root@kali:~ # cd
root@kali:~ # aircrack-ng -a2 -b < *BSSID of WLAN Router* > -w /root/Desktop/cupp/Albert.txt '/root/Desktop/WPA.cap'

WPA.cap is a captured packet file.

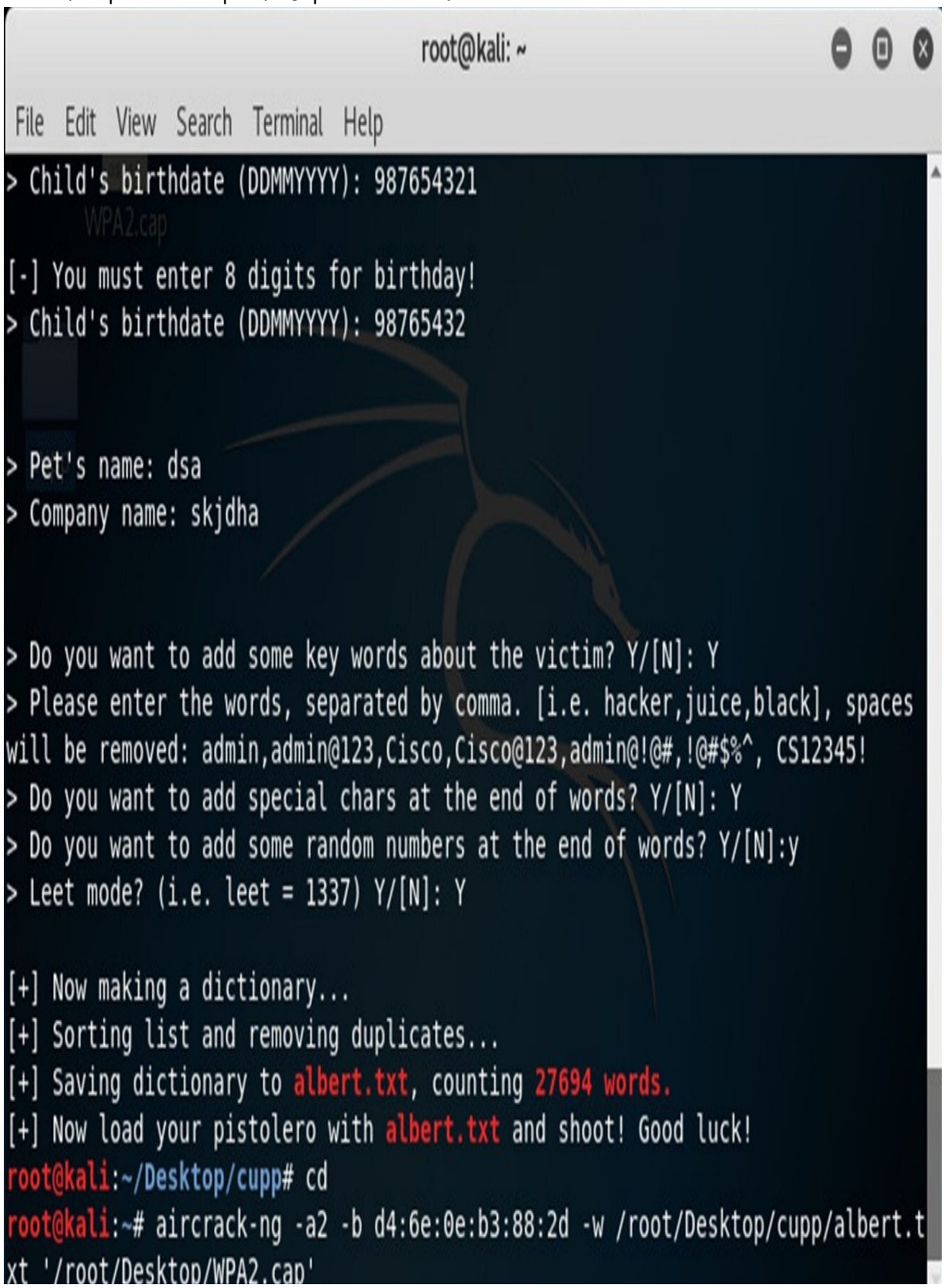


Figure 16-18: Cracking the Password

17. This will start the process and all keys will be checked.

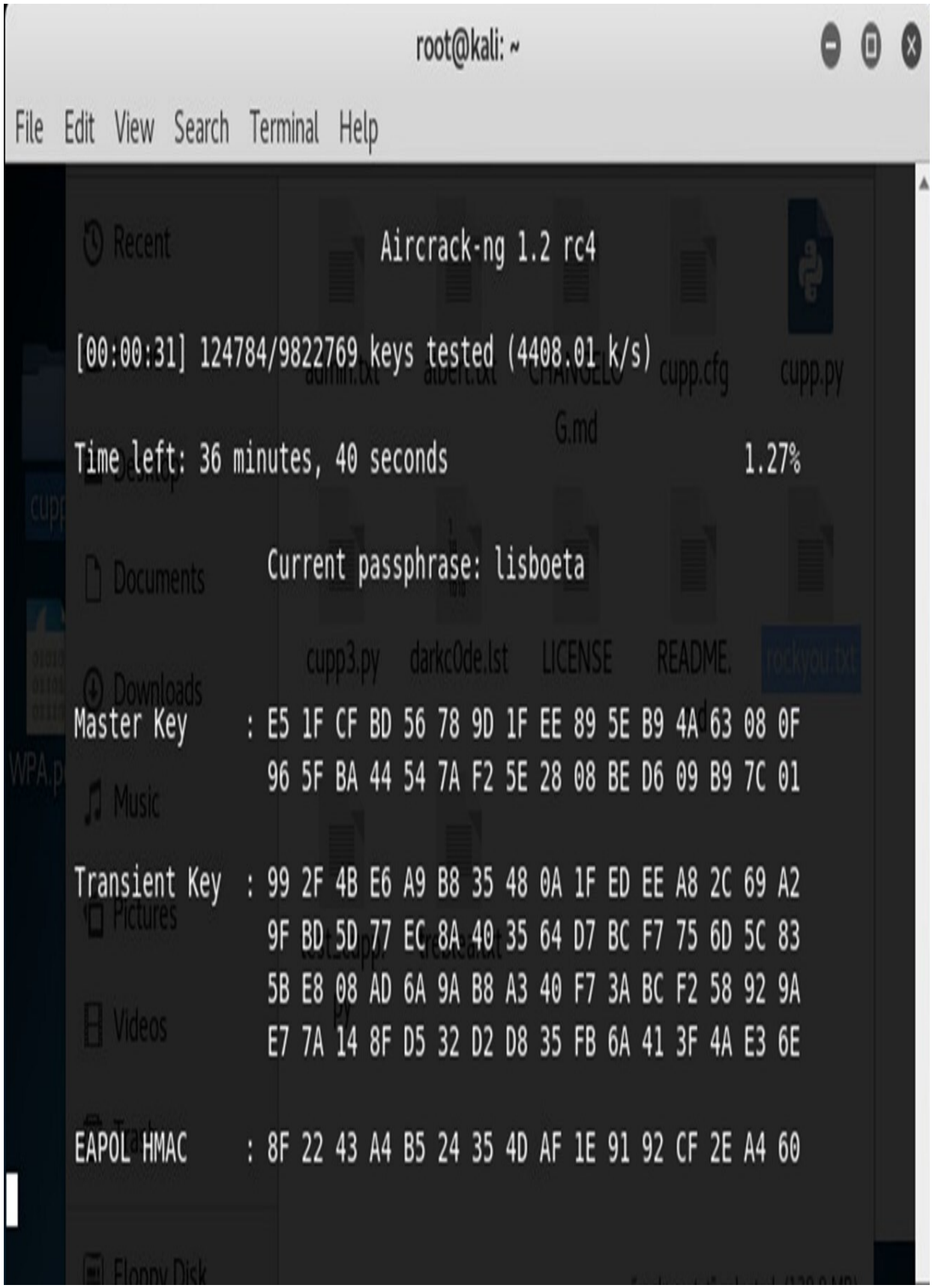

root@kali: ~
File Edit View Search Terminal Help
Aircrack-ng 1.2 rc4
[00:00:31] 124784/9822769 keys tested (4408.01 k/s)
Time left: 36 minutes, 40 seconds 1.27%
Current passphrase: lisboeta
Master Key : E5 1F CF BD 56 78 9D 1F EE 89 5E B9 4A 63 08 0F
96 5F BA 44 54 7A F2 5E 28 08 BE D6 09 B9 7C 01
Transient Key : 99 2F 4B E6 A9 B8 35 48 0A 1F ED EE A8 2C 69 A2
9F BD 5D 77 EC 8A 40 35 64 D7 BC F7 75 6D 5C 83
5B E8 08 AD 6A 9A B8 A3 40 F7 3A BC F2 58 92 9A
E7 7A 14 8F D5 32 D2 D8 35 FB 6A 41 3F 4A E3 6E
EAPOL HMAC : 8F 22 43 A4 B5 24 35 4D AF 1E 91 92 CF 2E A4 60

Figure 16-19: Cracking the Password

18. The result will either show you the key or will refuse to crack from the dictionary.

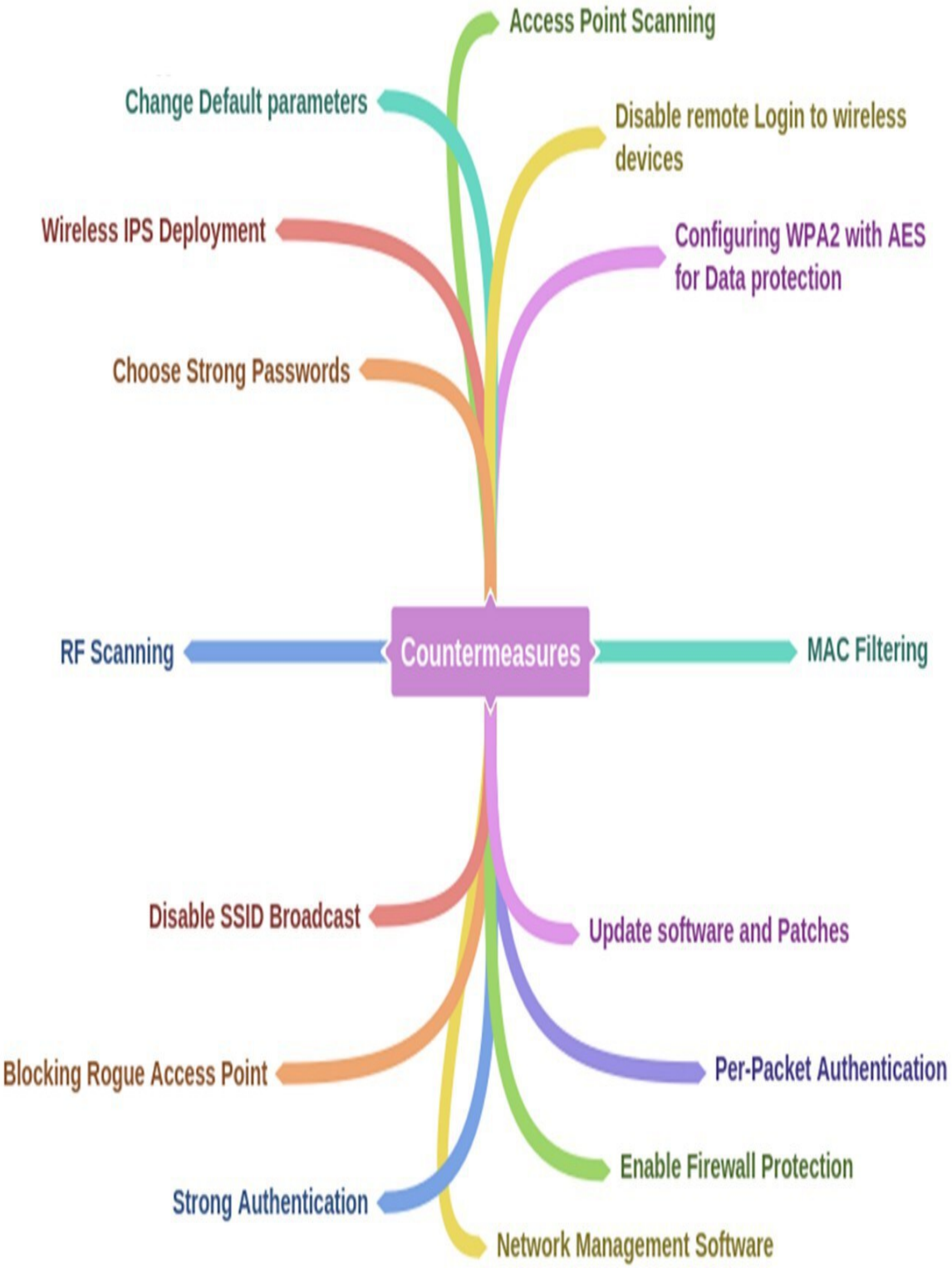

root@kali: ~
File Edit View Search Terminal Help
Aircrack-ng 1.2 rc4
[00:00:00] 20/113 keys tested (518.44 k/s)
Time left: 0 seconds 17.70%
KEY FOUND! [CS12345!]
Master Key : F5 EF 7C 79 10 DF DE 73 76 40 F9 4F 12 A4 BC E5
A7 8D CD E4 3E A2 F0 E5 23 37 AD 74 00 F0 3F 57
Transient Key : 94 49 E3 EC C8 BC B7 49 21 6F 9F 0B BF 88 4F 5F
9E C2 09 F9 E1 7D ED B9 F6 6F F2 DE 33 52 19 0E
3D F2 3E 86 44 E1 9F B0 88 63 F2 17 E4 56 54 6B
92 0D 1D 3A 13 62 12 30 C7 FB 91 1A 40 58 89 BC
EAPOL HMAC : 39 18 C7 3A C6 4B 98 AF 7A B7 0B F2 79 38 C4 A8
root@kali:~#

Figure 16-20: The Cracked Password

Countermeasures

Wireless Technologies such as Wi-Fi and Bluetooth are the most popular and widelyused technologies. These technologies can be secured using different network monitoring and auditing tools and by configuring strict access control policies and best practices. As discussed earlier in this Chapter, Wi-Fi encryptions and their issues, moving from WEP to WPA2, strong authentication, and encryptions, best practices will make it harder to compromise your wireless network. The following mind map shows the basic techniques and a countermeasure discussed in this Chapter.

Mind Map


Access Point Scanning
Change Default parameters
Disable remote Login to wireless devices
Wireless IPS Deployment
Configuring WPA2 with AES for Data protection
Choose Strong Passwords
RF Scanning
Countermeasures
MAC Filtering
Disable SSID Broadcast
Update software and Patches
Blocking Rogue Access Point
Per-Packet Authentication
Enable Firewall Protection
Strong Authentication
Network Management Software

Note: Kismet is a wireless network and device detector, sniffer, wardriving tool, and WIDS (Wireless Intrusion Detections) System for 802. 1 1 wireless LANS. It works on Linux and Windows 10 under the WSL system. On Linux, Kismet works with most WiFi cards, Bluetooth interfaces, and other hardware devices.

Netstumbler is a tool for Windows that facilitates detection of Wireless LANs using 802. 1 1b, 802. 1 1a, and 802. 1 1g WLAN standards. It runs on Microsoft Windows operating systems from Windows 2000 to Windows XP.

Practice Questions

1. Name of Access Point that is usually broadcasted for the identification of a wireless network is called:
A. SSID
B. BSSID
C. MAC
D. WLAN

2. In a Wi-Fi network with Open Authentication, how many frames are communicated between client and AP to complete the authentication process? A. 4
B. 5
C. 6
D. 7

3. In a Wi-Fi Network with Shared Key Authentication, how many frames are communicated between client and AP to complete the authentication process? A. 4
B. 5
C. 6
D. 7

4. Wi-Fi authentication with centralized authentication server is deployed by using:
A. WEP

B. WPA
C. WPA2
D. EAP

5. Doughnut Shaped Radiation pattern is obtained from: A. Omnidirectional Antennas
B. Directional Antennas
C. Dish Antenna
D. Yagi-Uda Antenna

6. Which Wireless encryption uses 24-bit Initialization Vector to create RC4 with CRC?
A. WEP
B. WPA
C. WPA2
D. EAP

7. Which of the following protocols ensures per packet key by dynamically generating a 128-bit key?
A. WEP
B. TKIP
C. MIC
D. CCMP

8. In a Bluetooth network, target devices are overflowed by random packets. Which type of Bluetooth attack is this?
A. BlueBugging
B. BlueJacking
C. BlueSnarfing
D. BlueSmacking

9. An attacker is attempting to gain remote access to a Bluetooth device to compromise its security, which type of attack is this?
A. BlueBugging
B. BlueJacking
C. BlueSnarfing
D. BlueSmacking

10. Which of the following tool is appropriate for packet sniffing in a wireless network?
A. Airsnort with Airpcap
B. Wireshark with Winpcap
C. Wireshark with Airpcap
D. Ethereal with Winpcap

11. Which device can detect rogue wireless access point? A. NGFW
B. HIDS
C. NIDS
D. WIPS

Chapter 17: Hacking Mobile Applications

Technology Brief

We have all seen how the rapid increase in mobile phone users, flexibility of functions, and advancement in performing tasks has brought a dramatic shift in technology. The smartphones currently available run on different popular Operating Systems such as iOS, Blackberry OS, Android, Symbian, and Windows, etc. They also offer application stores, for example, Apple's App Store and Android's Play Store, where users can download compatible and trusted applications to run on their respective Operating Systems. While mobile phones are a source of entertainment and have become a tool for carrying out personal and business tasks, they are also vulnerable. A smartphone infected with a malicious application can cause trouble for a secure network. As mobile phones are now regularly used for online financial transactions, through banking applications, for example, the devices must have strong security, ensuring transactions remain secure and confidential. Similarly, mobiles contain important data such as contacts, messages, emails, login credentials, and files that can be stolen easily once a phone is compromised.

Mobile Platform Attack Vectors
OWASP Top 10 Mobile Threats

OWASP stands for Open Web Application Security Project. OWASP provides unbiased and practical information about computer and internet applications. According to OWASP, the top 10 mobile threats are:

OWASP Top 10 Mobile Risks (20 16)	OWASP Top 10 Mobile Risks (20 14)
Improper Platform Usage	Weak Server Side Controls
Insecure Data Storage	Insecure Data Storage
Insecure Communication	Insufficient Transport Layer Protection
Insecure Authentication	Unintended Data Leakage
Insufficient Cryptography	Poor Authorization and Authentication
Insecure Authorization	Broken Cryptography
Client Code Quality	Client Side Injection
Code Tampering	Security Decisions Via Untrusted Inputs
Reverse Engineering	Improper Session Handling
Extraneous Functionality	Lack of Binary Protections

Table 17-01: OWASP Top 10 Mobile Risks

Mobile Attack Vector

There are several types of threats and attacks used on mobile devices. Some of the most basic threats are malware, data loss, and attacks on integrity. An attacker may attempt to launch attacks through a victim's browser using a malicious website or a compromised legitimate website. Social engineering attacks, data loss, data theft, data exfiltration are the most common attacks on mobile technology. The mobile attack vector includes:

- Malware
- Data Loss
- Data Tampering
- Data Exfiltration

Vulnerabilities and Risks on Mobiles

Apart from attacks, there are several other vulnerabilities and risks to a mobile platform. The most common risks are:

- Malicious third-party applications
- Malicious applications on Store
- Malware and rootkits
- Application vulnerability
- Data security

- Excessive permissions
- Weak encryptions
- Operating System update issues
- Application update issues
- Jailbreaking and Rooting
- Physical attack

Application Sandboxing Issue

Sandboxing is one of the most important components of security. It supports security as an integrated component in a security solution. The sandboxing feature is very different from other traditional anti-virus and anti-malware mechanisms. Sandboxing technology offers enhanced protection by analysing of emerging threats, malware, malicious applications, etc. in a sophisticated environment with in-depth visibility and control that is more granular. However, advanced malicious applications may be designed to bypass the sandboxing technology. Fragmented code and scripts with sleep timers are common techniques adopted by attackers to bypass the inspection process.

Mobile Spam and Phishing

Mobile Spamming is a spamming technique for the mobile platform in which unsolicited messages or emails are sent to targets. These spam contain malicious links designed to reveal sensitive information. Similarly, phishing attacks are often employed because they are easy to set up and difficult to stop. Messages and emails with notifications or stories about winning prizes or cash are the most commonly known spams. An attacker may ask for credentials on a direct phone call or message, or send spam messages or emails to redirect a user to a malicious or compromised legitimate website.

Open Wi-Fi and Bluetooth Networks

Public Wi-Fi, unencrypted Wi-Fi, and Bluetooth networks are other easy methods an attacker can use to intercept communication and reveal information. Users connected to public Wi-Fi may be a victim.

Bluebugging, Bluesnarfing and Packet Sniffing are common attacks on open wireless connections.

Hacking Android OS

Android is an Operating System for smartphones developed by Google also used is gaming consoles, PCs, and other IoT devices. As an open source platform, Android OS has flexible features. The major features of this Operating System are the wide range of support applications and its integration with different hardware and services. The Android Operating System has since gone through multiple major releases and the current ninth version, released in August 20 18, is Android Pie. Android 10Q is soon to be announced.

A popular feature of Android is its flexibility of third-party applications. Users can download, install, and remove these application (APK) files from application stores or from the internet. However, because of the open source nature of the platform, these can be a security risk; any third-party application can violate the policy of a trusted application. Many Android hacking tools outlined in this workbook are also not available in the Play store.

Device Administration API

Device Administration API was introduced in Android 2.2. Device Administration API ensures device administration at the system level, offering control over Android devices within a corporate network. Using these security-aware applications, an administrator can perform several actions, including remotely wiping the device. Here are examples of the types of applications that might use the Device Administration API:

- Email clients
- Security applications that can do a remote wipe • Device management services and applications

Root Access/Android Rooting

Rooting is the process of gaining privileged control over a device, commonly known as Root Access. In the Android Operating System,

rooting is the process of gaining privileged access to an Android device, such as a smartphone, tablet, etc., over a subsystem. As previously discussed, Android is the modified version of Linux kernel; root access gives "superuser" permissions. Root access is required to modify the settings and configurations that need administrator privileges; however, it can be used to alter system applications and settings to overcome limitations and restrictions. Once you have root access, you have full control of the kernel and applications. This rooting can be used for malicious intentions such as the installation of malicious applications, assigning excessive permissions, and installation of custom firmware.

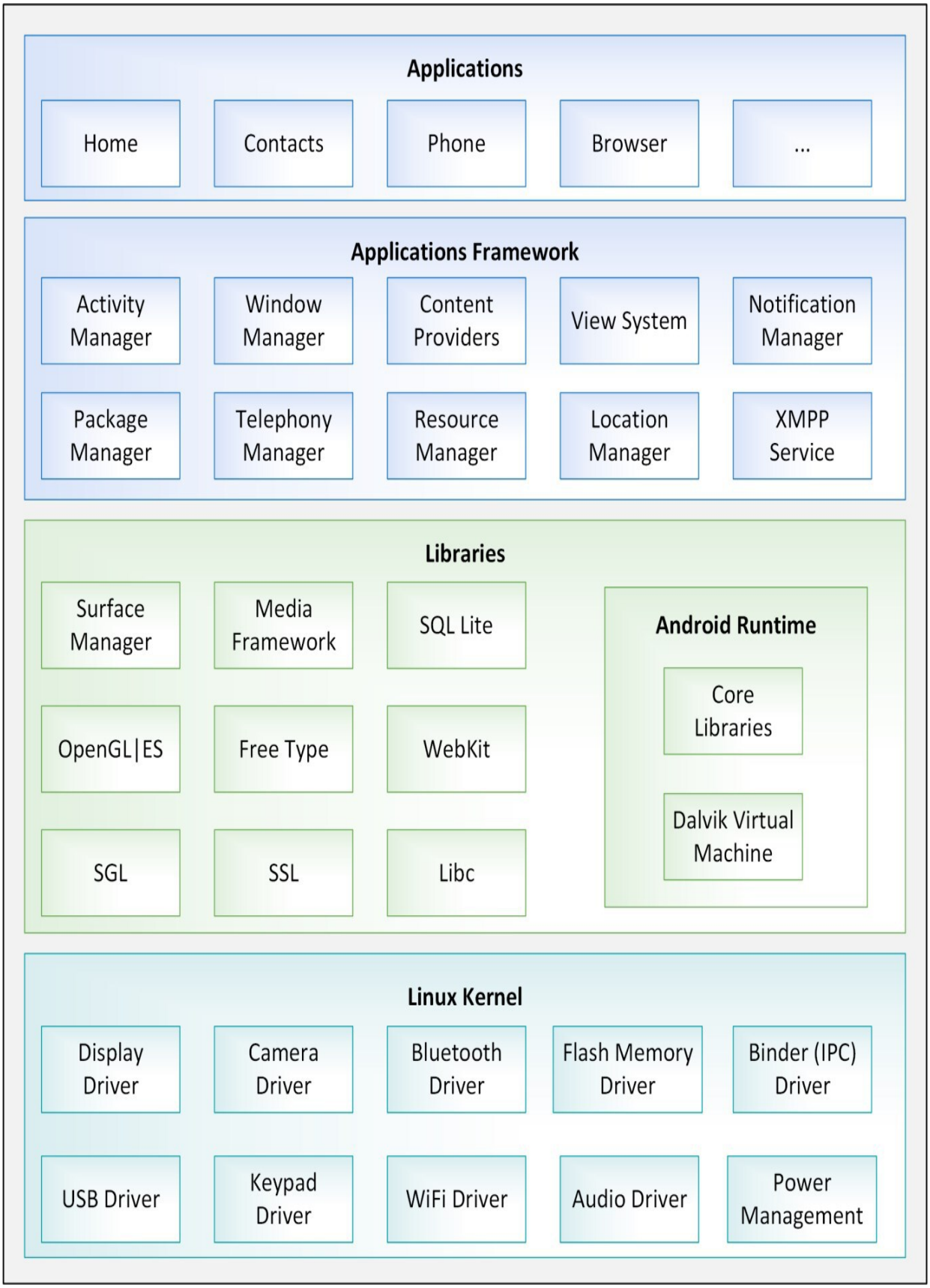


Figure 13.01: Android Framework

Figure 17-01: Android Framework

Android Phone Security Tools

There are several anti-virus applications, protection tools, vulnerability scanning tools, anti-theft, anf “find my phone” applications available on the Play store. These tools include:

- DroidSheep Guard
- TrustGo Mobile Security
- Sophos Mobile Security
- 360 Security
- Avira Antivirus Security
- AVL
- X-ray

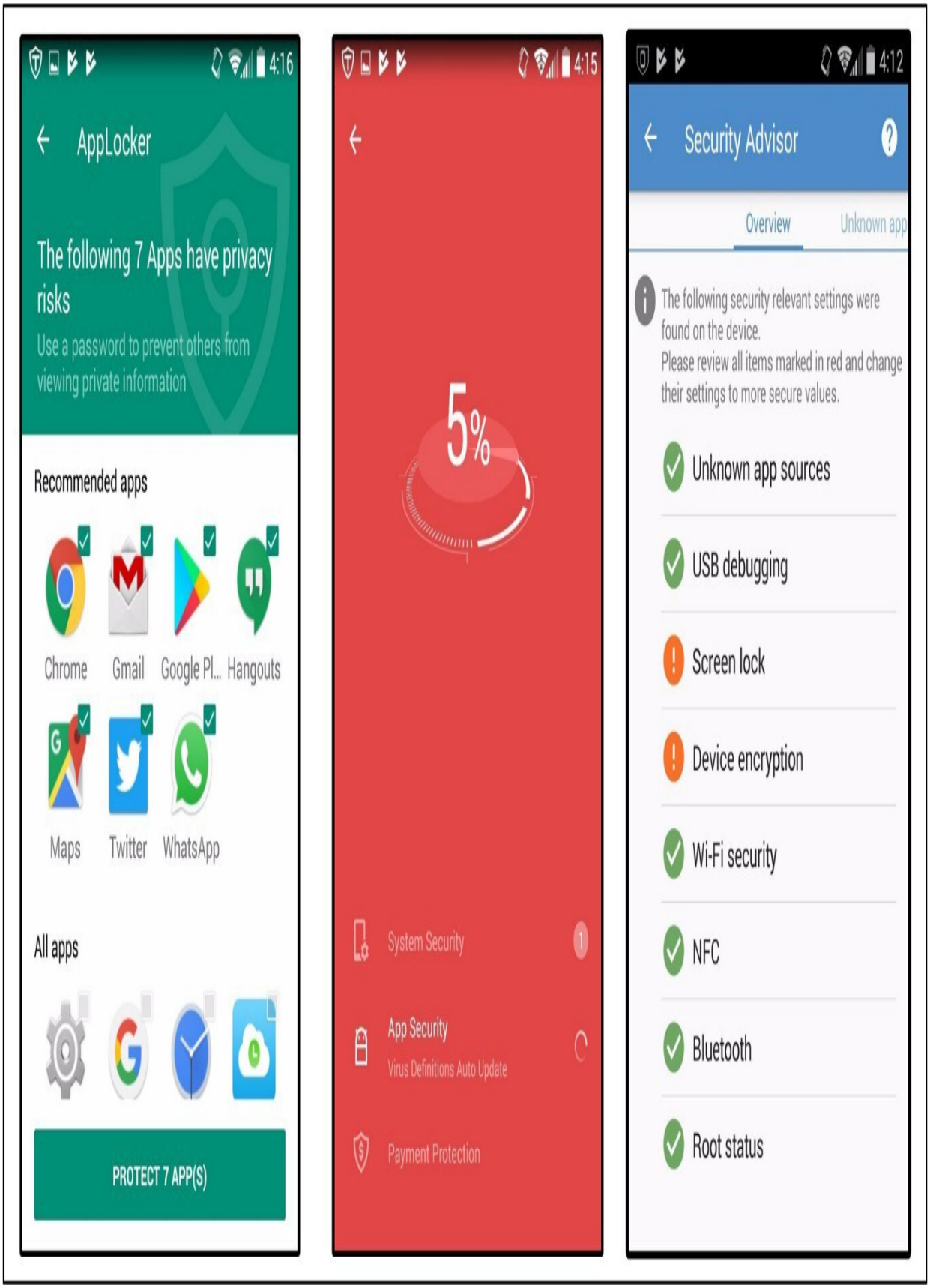


Figure 13_02: TrustGo and Sophos Application

Figure 17-02: TrustGo and Sophos Application

Hacking iOS

The Operating System Apple.Inc developed for iPhones is known as iOS. It is one of the most popular Operating Systems for mobile devices including iPhones, iPads, and iPods. The user interface in an iOS is based on direct manipulation using multi-touch gestures. Major iOS versions are released annually. The current version, iOS 12, was released on September 17, 20 18. iOS uses hardware-accelerated AES256 encryption and other additional encryption to encrypt data. iOS also isolates the application from other applications. Applications are not allowed to access another app's data.

Jailbreaking iOS

Jailbreaking is the concept of breaking the restriction "Jail". Jailbreaking is a form of rooting resulting in privilege escalation. iOS jailbreaking is the process of escalating privileges on iOS devices to either remove or bypass the factory default restrictions on software by using kernel patches or device customization. Jailbreaking allows root access to an iOS device, allowing unofficial applications to be downloaded. Jailbreaking is popular for removing restrictions, installation of additional injection, and software piracy.

Types of Jailbreaking

BIOS Jailbreaking is categorized into three types depending exploiting system vulnerability, vulnerabilities in first and third bootloader, etc. Apple can patch with iBoot exploit and Userland exploit.

1. Userland Exploit

A Userland Exploit is a type of iOS jailbreaking that allows user-level access without escalating to boot-level access. It can only be reserved by a user, not by an administrator. It allows user-level access without iBoot-level access.

2. iBoot Exploit

An iBoot Exploit is a type of iOS jailbreaking that allows user-level access and boot-level access. iBoot exploit is a jailbreak that can be

reversed by an administrator, not by a user. A jailbreak breaks all low-level authentication, including NOR access. It allows file system and iBoot access.

3. Bootrom Exploit

A Bootrom Exploit is a jailbreak that allows user-level access and iBoot-level access. The bootrom jailbreak differs from the iBoot exploit. It provides greater system-level access to the attacker and the immediate follow-on exploit capability is more dangerous for the target. software, malware

on privilege levels,

Jailbreaking Techniques

1. Tethered Jailbreaking

In Tethered Jailbreaking, when the iOS device is rebooted, it will no longer have a patched kernel. It may be stuck in a partially started state. With Tethered Jailbreaking, a computer is required to boot the device each time; i.e. the device is re-jailbroken each time. Using the jailbreaking tool, the device is started with the patched kernel.

2. Semi-tethered Jailbreaking

The Semi-tethered Jailbreaking technique is another solution standing in between Tethered and Untethered Jailbreaking. Using this technique, when the device is booting, it does not have a patched kernel but is able to complete the start-up process and entertain normal functions. Any modification will require start up with a patched kernel with jailbreaking tools.

3. Untethered Jailbreaking

In Untethered Jailbreaking, a device is completely booted. While booting, a kernel will be patched without any requirement from the computer and thus enabling the user to boot without a computer. This technique is harder to attempt.

Jailbreaking Tools

The following are some iOS jailbreaking tools:

- Pangu
- Redsn0w
- Absinthe
- evasin0n7
- GeekSn0w
- Sn0wbreeze
- PwnageTool
- LimeRaln
- Blackraln

Hacking Windows Phone OS

Windows Phone (WP) is another Operating System in the OS family, developed by Microsoft. The first launch was Windows Phone 7. Windows 7.5 Mango, released later, has a very low hardware requirement of 800 MHz CPU and 256 MB Ram. Windows 7 devices are not capable of upgrading to Windows 8 due to hardware limitations. Windows 8, 8. 1, released in 20 14, is replaced by Windows 10, released in 20 17.

Windows Phone

Windows Phone 8 is the second-generation Windows Phone from Microsoft. It replaces the Windows CE-based architecture that was used in Windows 7. Windows Phone 8 devices are manufactured not only by Microsoft but also Nokia, HTC, Samsung, and Huawei. Windows Phone 8 is the first mobile OS launched by Microsoft using the Windows NT kernel. Improvement of the file system, drivers, security, media, and graphics are features of Windows Phone 8. Windows Phone 8 is capable of supporting multi-core CPUs up to 64 cores. It is also capable of supporting 1280×720 and 1280×768 resolutions. Windows Phone 8 supports native 128-bit Bit locker encryption and Secure Boot as well as NTFS due to this switch. Internet Explorer 10 is the default browser in Windows 8 phones. Windows Phone 8 uses true multitasking, allowing developers to create apps that can run in the background and resume instantly.
Some other features of Windows Phone 8 include:

- Native code support (C++)
- NFC
- Remote Device Management
- VoIP and Video Chat Integration
- UEFI and Firmware Over the Air for Windows Phone Updates • App Sandboxing

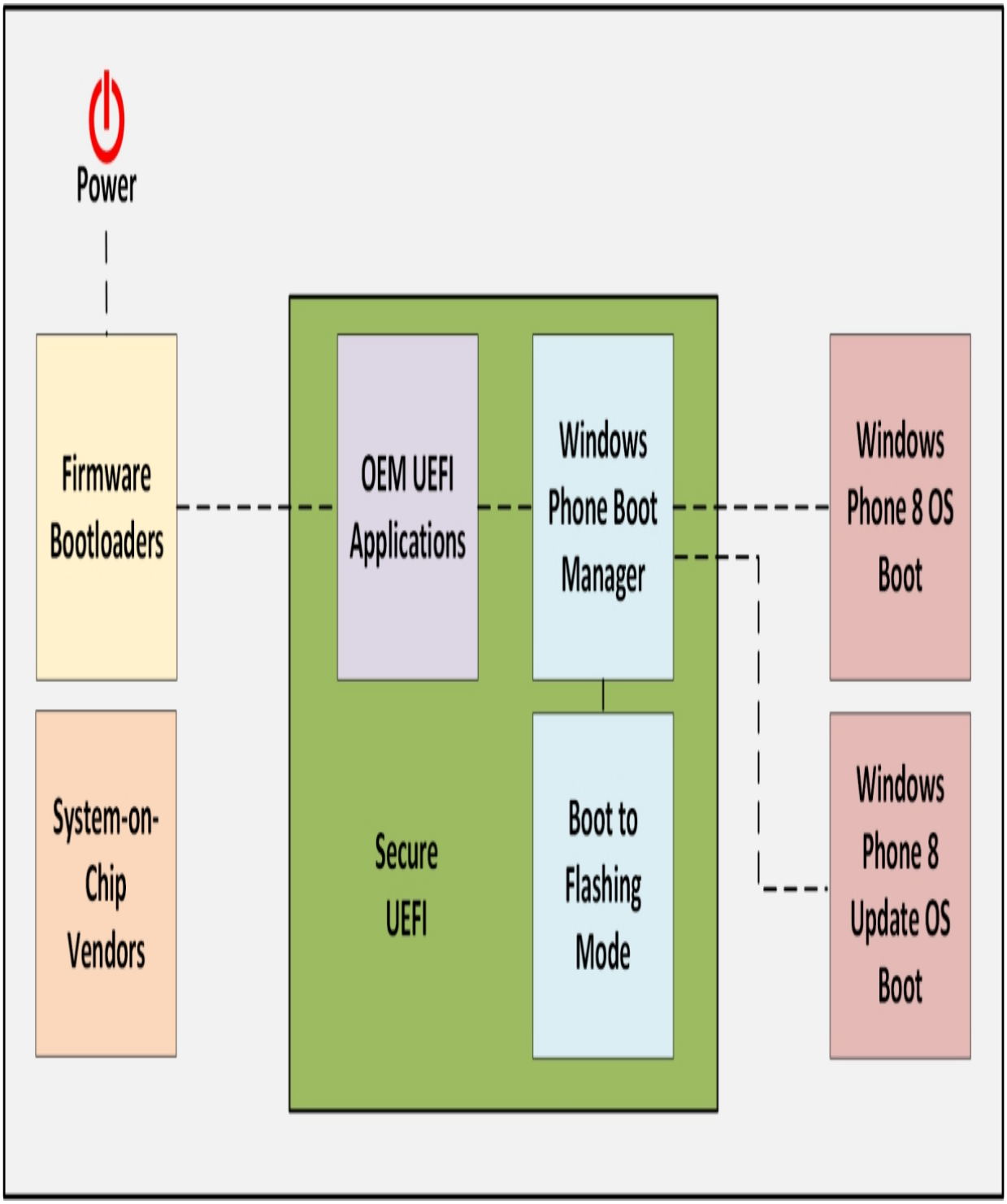


Figure 17-03: Windows 8 Secure Boot Process

Hacking BlackBerry

BlackBerry is another smartphone company that is formerly known as Research in Motion (RIM) Ltd. BlackBerry was considered the most

prominent and secure mobile phone. Its Operating System is known as BlackBerry OS.

BlackBerry Operating System

BlackBerry OS is the Operating System of BlackBerry phones. It provides multitasking with special input support such as trackwheel, trackball, and, most recently, the trackpad and touchscreen. BlackBerry OS is best known for its native support for corporate emails and its Java-based application framework, i.e., Java Micro Edition MIDP 1.0 and MIDP 2.0. Updates to the Operating System may be automatically available from wireless carriers that support the BlackBerry Over the Air Software Loading (OTASL) service.

BlackBerry Attack Vectors

Malicious Code Signing

Malicious Code Signing is the process of obtaining a code-signing key from the code signing service. An attacker may create a malicious application with the help of code signing keys obtained by manipulating information, for example, by anonymously using prepaid credit cards and fake details and publishing the malicious application on BlackBerry App world. BlackBerry App world is the official application distribution service. A user downloads this malicious application, which directs traffic to the attacker.

JAD File Exploit

Java Application Description (.jad) files contain the attributes if Java applications. These attributes include information and details about the application including the URL downloading the application. An attacker can install a malicious .jad file on the victim device. This crafted .jad file with spoofed information can be installed by the user. A malicious application can also be crafted for a denial-of-service attack.

Mobile Device Management (MDM)

The basic purpose of implementing Mobile Device Management (MDM) is deployment, maintenance, and monitoring of mobile devices that

make up the BYOD solution. Devices may include laptops, smartphones, tablets, notebooks, or any other electronic device that can be taken outside the corporate office, either home or to a public space, and then get connected to the corporate office. The following are some of the functions provided by MDM:

● Forcing a device to lock after certain login failures
● Enforcing a strong password policy on all BYOD devices
● Detecting any attempt to hack BYOD devices and then these devices' limiting

network access
● Enforcing confidentiality by using encryption as per an organization's policy ● Administering and implementing Data Loss Prevention (DLP) for BYOD devices.

This helps to prevent any kind of data loss due to an end user's carelessness

MDM Deployment Methods

Generally, there are two types of MDM deployment.

On-site MDM deployment: On-site/premises MDM deployment involves installing an MDM application on local servers inside a corporate data center or offices, which is then managed by local staff available on the site.
The major advantage of On-site MDM is granular control over the management of BYOD devices, which increases security to some extent.

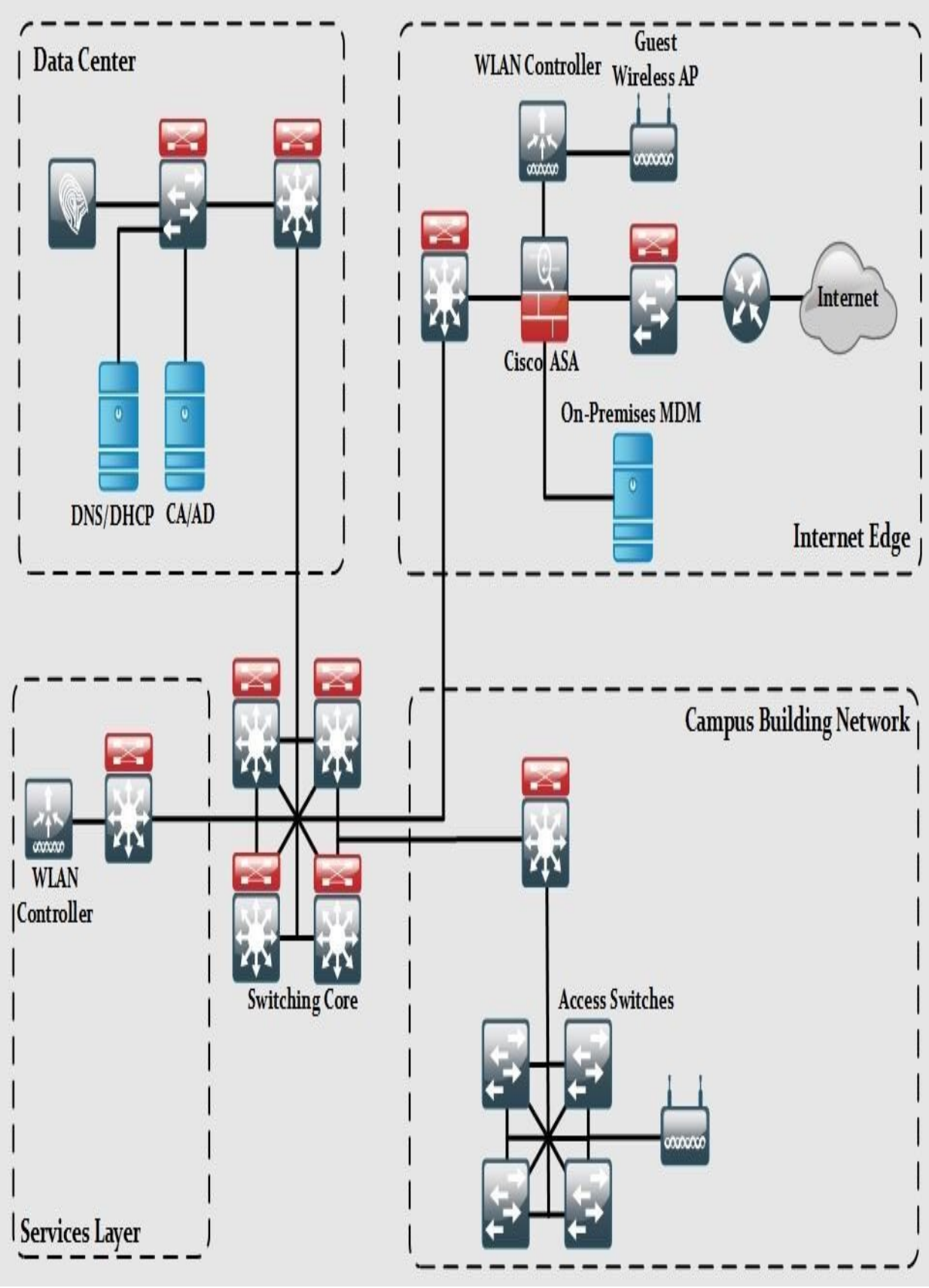


Figure 13.04: On-premises MDM High-level Deployment

Figure 17-04: On-premises MDM High-level Deployment Architecture

The on-site/premises MDM solution consists of the following architecture:

➢ Data Center: This may include ISE, DHCP, and DNS servers to support certain services apart from distribution and core switches. ISE is used to enforce the organization's security policies. DNS/DHCP servers are used to provide network connectivity. Similarly, CA and AD servers can also be used to provide access only to users with valid authentication credentials.

➢ Internet Edge: The basic purpose of this architecture is to provide connectivity to the public internet. This layer includes Cisco ASA firewall, to filter and monitor all traffic ingress and egress toward the public internet. Wireless LAN Controller (WLC) along with Access Points (APs) also feature in internet edge to support guest users. One of the key components at internet edge is the On-premises MDM solution, which maintains policies and configuration settings of all BYOD devices connected to the corporate network.

➢ Services Layer: This layer contains WLC for all the APs used by users within a corporate environment. Any other service required by corporate users, such as NTP and its supporting servers, can be found in this section.

➢ Core Layer: Like every other design, the core is the focal point of the whole network for routing traffic in a corporate network environment.

➢ Campus Building: A distribution layer switch acts as ingress/egress point for all traffic in a campus building. Users can connect to the campus building by connecting to access switches or wireless Access Points (APs).

Cloud-based MDM Deployment: In this type of deployment, MDM application software is installed and maintained by an outsourced management services provider. One of the main advantages of this kind of setup is low administrative load on the customer's end as

deployment and maintenance is the full responsibility of the service provider.
The cloud-based MDM deployment consists of the following components, as depicted in the figure 17-05:

➢ Data Centre: This may include ISE, DHCP, and DNS servers to support certain services apart from distribution and core switches. ISE is used to provide the enforcement of an organization's security policies. DNS/DHCP servers are used to provide network connectivity. Similarly, CA and AD servers can also be used to provide access only to users with valid authentication credentials.

➢ Internet Edge: The basic purpose of this section is to provide connectivity to the public internet. This layer includes Cisco ASA firewall to filter and monitor all the traffic ingress and egress toward the public internet. Wireless LAN Controller (WLC) along with Access Points (APs) are also included in internet edge to support guest users.

➢ WAN: The WAN module in cloud-based MDM deployment provides MPLS VPN connectivity from branch office to corporate office, internet access from branch offices and connectivity to cloud-based MDM application software. Cloud-based MDM solution maintains the policies and configuration settings of all BYOD devices connected to the corporate network.

➢ WAN Edge: This component acts as a focal point of all ingress/egress MPLS WAN traffic entering from and going to branch offices.

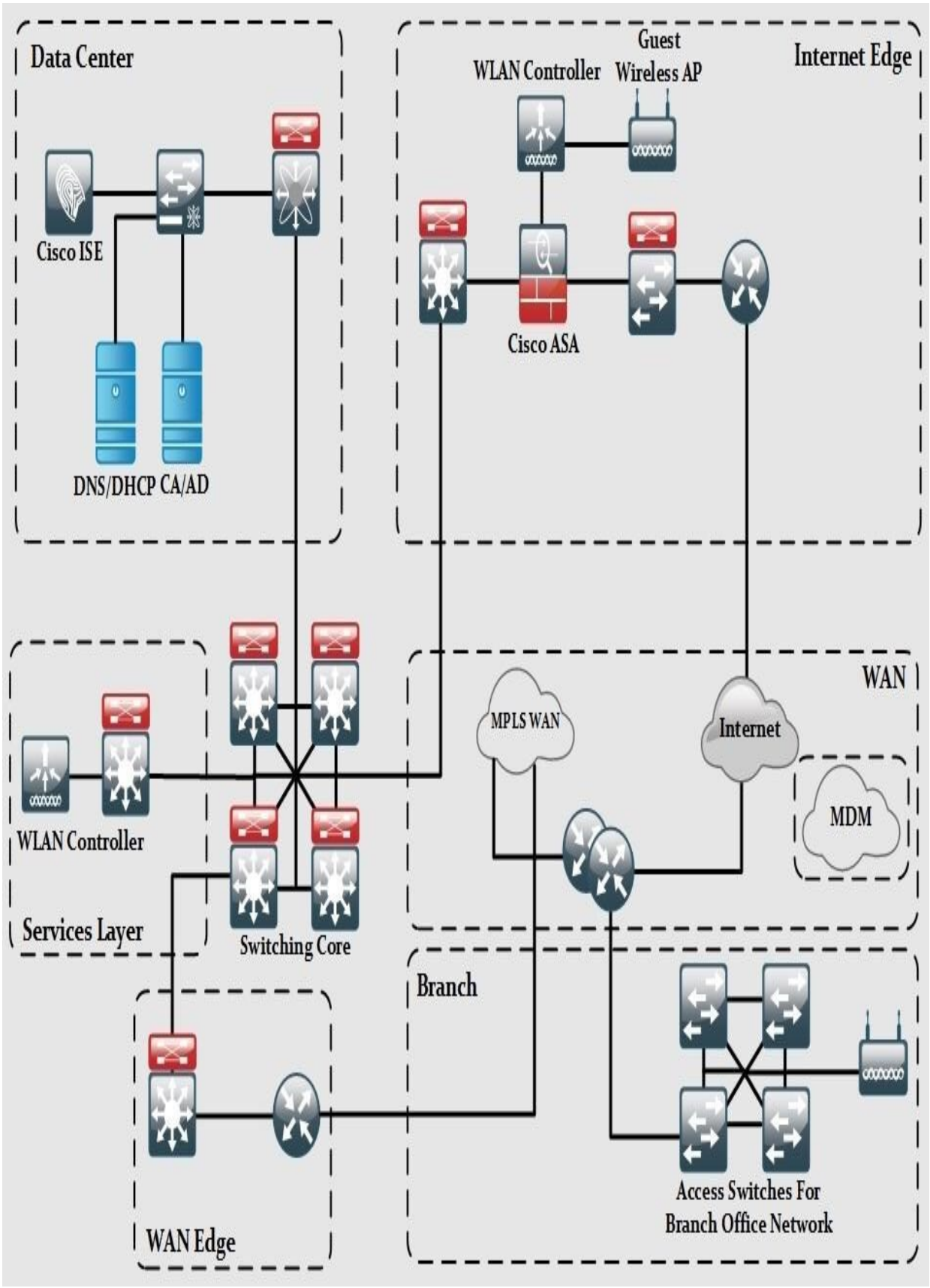

Data Center
Cisco ISE
DNS/DHCP CA/AD
Guest
WLAN Controller
Wireless AP
Internet Edge
Cisco ASA
WAN
MPLS WAN
Internet
MDM
WLAN Controller
Services Layer
Switching Core
Branch
Access Switches For
Branch Office Network
WAN Edge

Figure 17-05: Cloud-based MDM Deployment High-level Architecture

➢ Services: This layer contains WLC for all the APs used by users within a corporate environment. Any other service required by corporate users, such as NTP and its supporting servers, can also be found in this section.

➢ Core Layer: Like every other design, the core is the focal point of the whole network for routing traffic in a corporate network environment.

➢ Branch Offices: This component is comprised of a few routers acting as the focal point of ingress and egress traffic out of branch offices. Users can connect to the branch office network by connecting to access switches or wireless Access Points (APs).

Bring Your Own Device (BYOD)

This section discusses the importance of Bring Your Own Device (BYOD) and its highlevel architecture. As well as BYOD, one of its management approaches, Mobile Device Management (MDM), will also be discussed.

Although the concept of BYOD facilitates end users in some ways, it also brings new challenges for network engineers and designers. A constant challenge faced by today's network designers is to provide seamless connectivity while maintaining the organization's good security posture. An organization's security policies must be constantly reviewed to make sure that bringing any outside device onto the corporate network will not result in theft or compromise the organization's digital assets.

Some of the reasons for implementing BYOD solutions in an organization are:

➢ A Wide Variety of Consumer Devices: In the past, we had only PCs and wired connection was the only way to communicate. In the 2 1st century, not only have higher data rates resulted in countless

opportunities for the consumers, but the variety of devices on the internet has also increased. Looking around, we can see mobile devices such as smartphones, tablets, and even laptops constantly communicating with each other over some wired or wireless network. Employees often connect their smartphones to corporate networks during working hours and to the internet when they move home or to a café. Such situations demand the implementation of BYOD solutions in the corporate environment to stay safe from any kind of theft.

➢ No, Fix a Time for Work: In the past, we used to following a strict 8-hour working day. Today, we work during lunch and our working rosters can even be updated on weekly bases. Sometimes, we even work during the night to meet deadlines.

➢ Connecting to Corporate from Anywhere: Employees also demand connection to the corporate network anytime, when at home or in a café. The emergence of wireless networks and mobile networks like 3G/4G also enables them to connect, even from the most remote locations on earth.

BYOD Architecture Framework

There are rules to implementing BYOD in an organization. How flexible they should in accepting and enabling their employees to connect different types of device depends on a company's policy. Introducing BYOD may also require implementing or deploying new software and hardware features to cater for BOYD security aspects.

The Cisco BYOD framework is based on Cisco Borderless Network Architecture, and it tries to implement Best Common Practices (BCP) in designing branch office, home office, and campus area networks.

Figure 17-06 shows the Cisco BYOD architecture, and the following section gives a short explanation of each component.

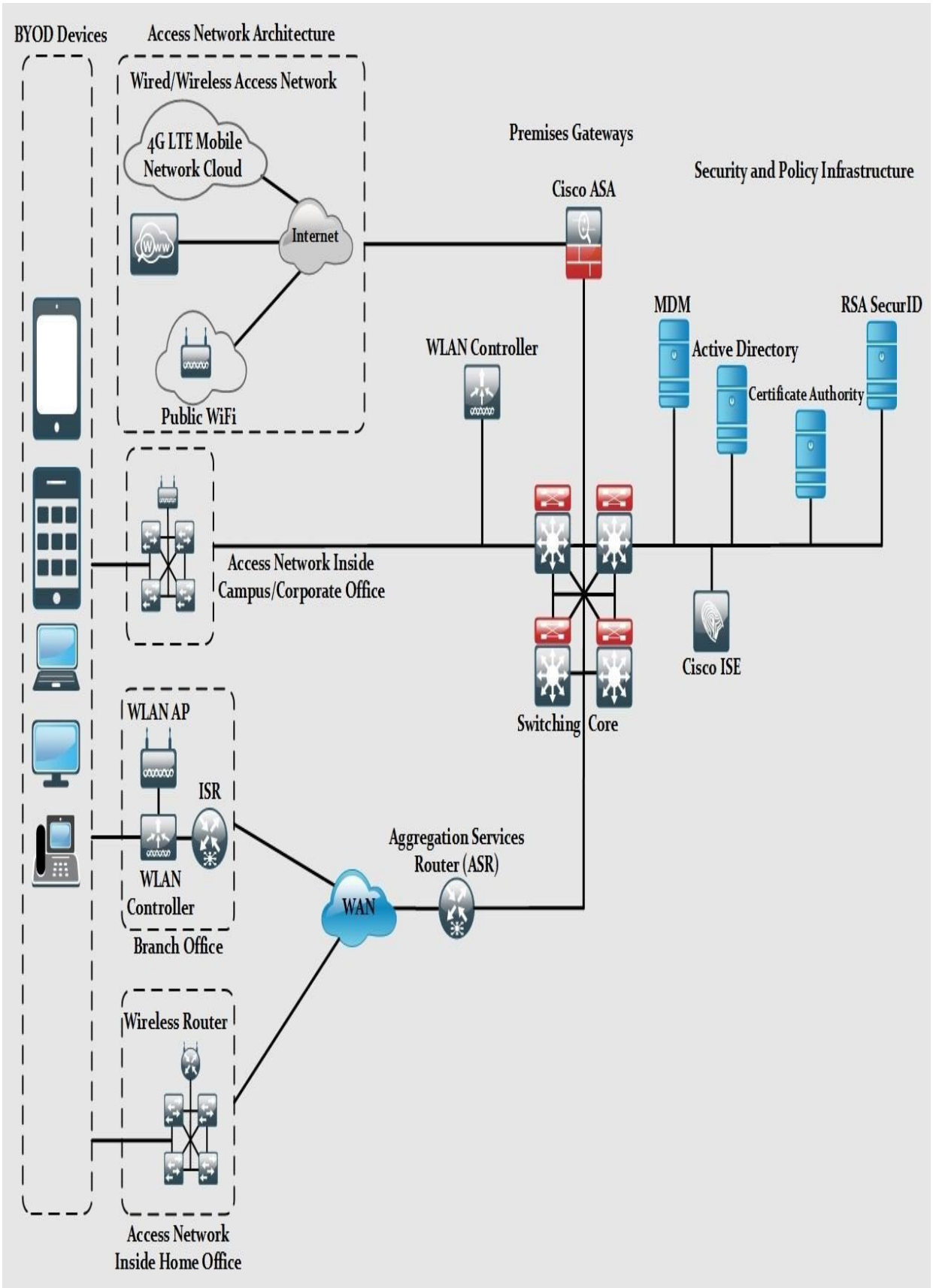

BYOD Devices
Access Network Architecture
Wired/Wireless Access Network
4G LTE Mobile Network Cloud
Internet
Public WiFi
Premises Gateways
Security and Policy Infrastructure
Cisco ASA
MDM
RSA SecurID
WLAN Controller
Active Directory
Certificate Authority
Access Network Inside Campus/Corporate Office
Cisco ISE
Switching Core
WLAN AP
ISR
Aggregation Services Router (ASR)
WLAN Controller
WAN
Branch Office
Wireless Router
Access Network Inside Home Office

Figure 17-06: BYOD High-level Architecture

BYOD Devices: These endpoint devices are required to access the corporate network for daily business needs. BYOD Devices may include both corporate and personally owned devices, regardless of their physical location. During the day, they may be at the corporate office and at night, they may be in a café or restaurant. Common BYOD devices include smartphones, laptops, etc.

Wireless Access Points (AP): Cisco Wireless Access Points (APs) provide wireless connectivity to the corporate network for the above-defined BYOD devices. Access points are installed physically at the campus, branch, or even home office to facilitate employees.

Wireless LAN Controllers: WLAN Controllers provide centralized management and monitoring of the Cisco WLAN solution. WLAN is integrated with Cisco Identity Service Engine to enforce authorization and authentication of BYOD end-point devices.

Identity Service Engine (ISE): ISE is one of the most critical elements in Cisco BYOD architecture as it implements authentication, authorization, and accounting on BYOD end-point devices.

Cisco AnyConnect Secure Mobility Client: Cisco AnyConnect Client software provides end users with connectivity to the corporate network. Its uses 802. 1x features to provide access to campus, office, or home office network. When end users need to connect to the public internet, AnyConnect uses a VPN connection to ensure the confidentiality of corporate data.

Integrated Services Router (ISR): Cisco ISR routers are preferred in BYOD architecture for proving WAN and internet access for branch and home office networks. They are also used to provide VPN connectivity for mobile BYOD devices within an organization.

Aggregation Services Router (ASR): Cisco ASR routers provide WAN and internet access for corporate and campus networks. They

also act as aggregation points for connections coming from the branch and home office to corporate networks with the Cisco BYOD solution.

Cloud Web Security (CWS): Cisco Cloud Web Security provides enhanced security for all BYOD devices that access the internet using public hotspots and 3G/4G networks.

Adaptive Security Appliance (ASA): Cisco ASA provides the standard security solutions at the internet edge of campus, branch, and home office networks within BYOD architecture. Apart from integrating the IPS/IDS module within itself, ASA also acts as the termination point of VPN connections made by Cisco AnyConnect Client software over the public internet to facilitate BYOD devices.

RSA SecurID: RSA SecurID generates a one-time password (OTP) for BYOD devices that need to access network applications requiring OTP.

Active Directory: Active Directory provides centralized command and control of domain users, computers, and network printers. It restricts access to network resources only to defined users and computers.

Certificate Authority: Certificate authority can be used to allow access to corporate networks to only those BYOD devices with a valid corporate certificate installed. Those devices without a certificate may have no access to the corporate network, but limited internet connectivity as defined in the corporate policy.

Mind Map


Bring Your Own Device (BYOD)
BYOD Architecture
Organization's Policy & requirements based Implementation
Cisco Border-less Network Architecture
BYOD Benifits
Anywhere-Anytime
Increased Productivity
Flexibility
Different Devices support
BYOD Deployment
On-Premises Deployment
Cloud-Based Deployment
BYOD Risks
Data Confidentiality issue
Disgruntled Employees
Data Leakage
Lack of Awareness
Different Device support
Bypassing Policy
Mobile Device Management (MDM)
Detection of BYOD Devices Hacks
Login Attempt Failure Policy
Strong Password Policy Enforcement
Implementation of Data Loss Prevention (DLP) policy

Mobile Security Guidelines

There are a number of techniques and methods that can be followed in order to avoid trouble while using mobile phones. Apart from built-in features and precautions, several tools are available on every official application store to provide a user with better security for their devices. Some of the recommended practices for securing your mobile phone are as follows:

- Avoid auto-upload of files and photos
- Perform a security assessment on applications
- Turn Bluetooth off
- Allow only necessary GPS-enabled applications
- Do not connect to open networks or public networks unless necessary • Install applications from trusted or official stores
- Configure string passwords
- Use Mobile Device Management (MDM) software
- Use Remote Wipe Services
- Update Operating Systems
- Do not allow rooting/jailbreaking
- Encrypt your phone
- Perform periodic backups
- Filter emails
- Configure application certification rules
- Configure mobile device policies
- Configure Auto-Lock

Practice Questions

1. Jailbreaking refers to: A. Root access to a device B. Safe mode of a device C. Compromising a device D. Exploiting a device

2. When an iOS device is rebooted, it will no longer have a patched kernel and may stick in a partially started state. Which type of Jailbreaking is performed on it?
A. Tethered Jailbreaking
B. Semi-Tethered Jailbreaking

C. Untethered Jailbreaking
D. Userland Exploit

3. Official Application store for Blackberry platform is: A. App Store
B. App World
C. Play Store
D. Play World

4. Which of the following is the most appropriate solution if an administrator is required to monitor and control over mobile devices running on a corporate network?
A. MDM
B. BYOD
C. WLAN Controller
D. WAP

Chapter 18: IoT Hacking

Technology Brief

This module is added in CEHv 10 with the objective of understanding IoT concepts and providing an overview of IoT threats and attacks, IoT hacking methodology, tools and techniques of IoT hacking, security tools, and penetration testing. Internet of Things (IoT) is an environment of physical devices, such as home appliances, electronic devices, sensors, etc., that are embedded in software programs and network interface cards to make them capable of connecting and communicating with the network.

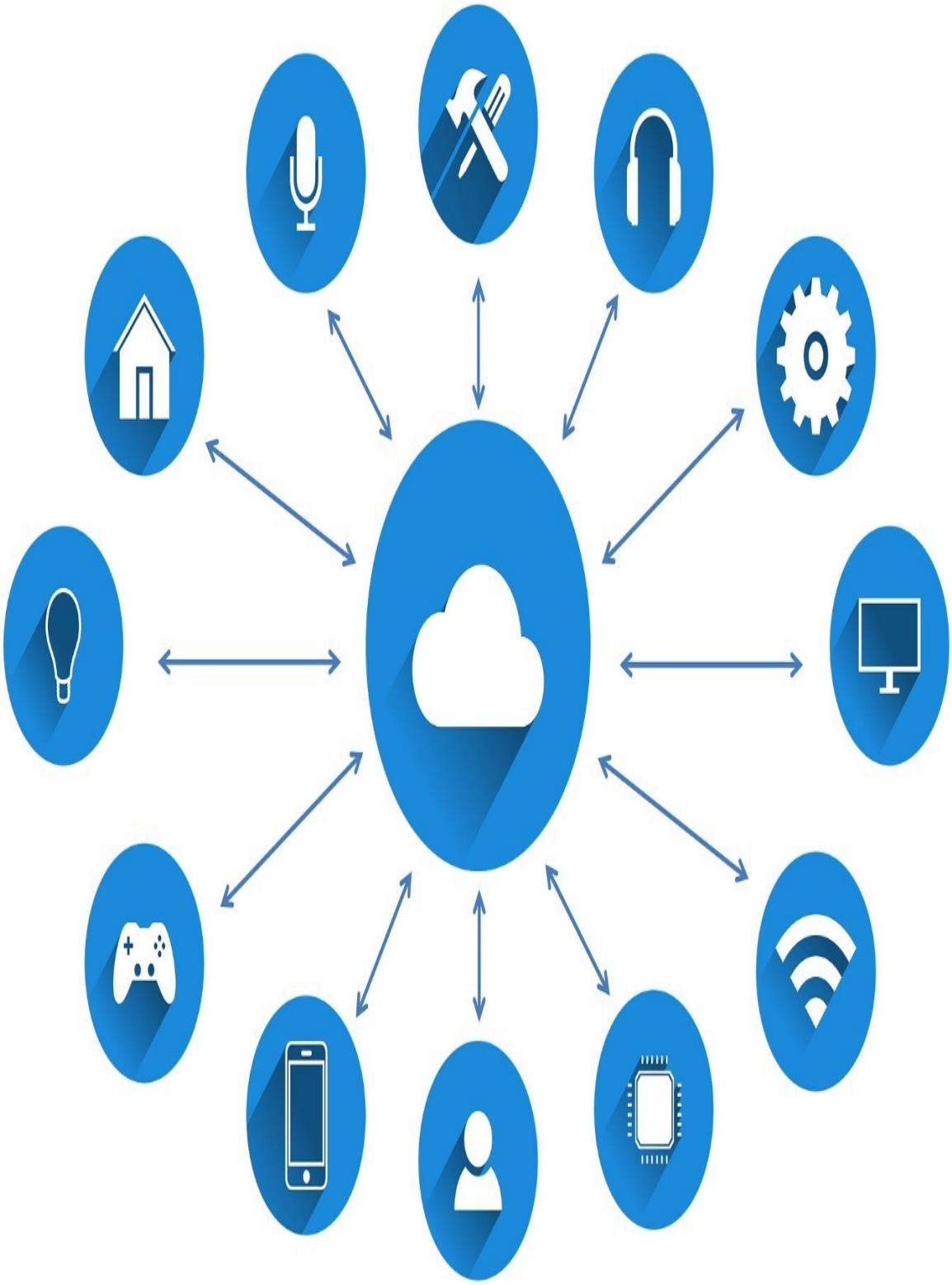


Figure 18. 01: Internet of Things (IoT)

Figure 18-01: Internet of Things (IoT)

The Concept of Internet of Things (IoT)

The world is rapidly moving towards automation. The need for automated devices where we have control of daily tasks at our fingertips is increasing day by day. As we all know, there is a performance and productivity difference between manual and automated processes, and moving toward the interconnection of things will processes even faster. The term "things" refers to machines, appliances, vehicles, sensors, and many other devices. An example of automation through the Internet of Things is a CCTV camera in a building capturing an intrusion and immediately generating an alert on client devices at their remote location. Similarly, we can connect devices over the internet to communicate with other devices.

IoT technology requires a unique identity. IP addresses, especially IPv6 addresses, provide each device with a unique identity. IPv4 and IPv6 planning and deployment over an advanced network structure requires thorough consideration of advanced strategies and techniques. In IP version 4, a 32-bit address is assigned to each network node for identification while in IP version 6, 128 bits are assigned to each node for unique identification. IPv6 is an advanced version of IPv4 that can accommodate the emerging popularity of the internet, the increasing number of users and devices, and advancements in networking. Advanced IP addresses need to take into account IP addresses that efficiency, reliability, and scalability in the overall network model.

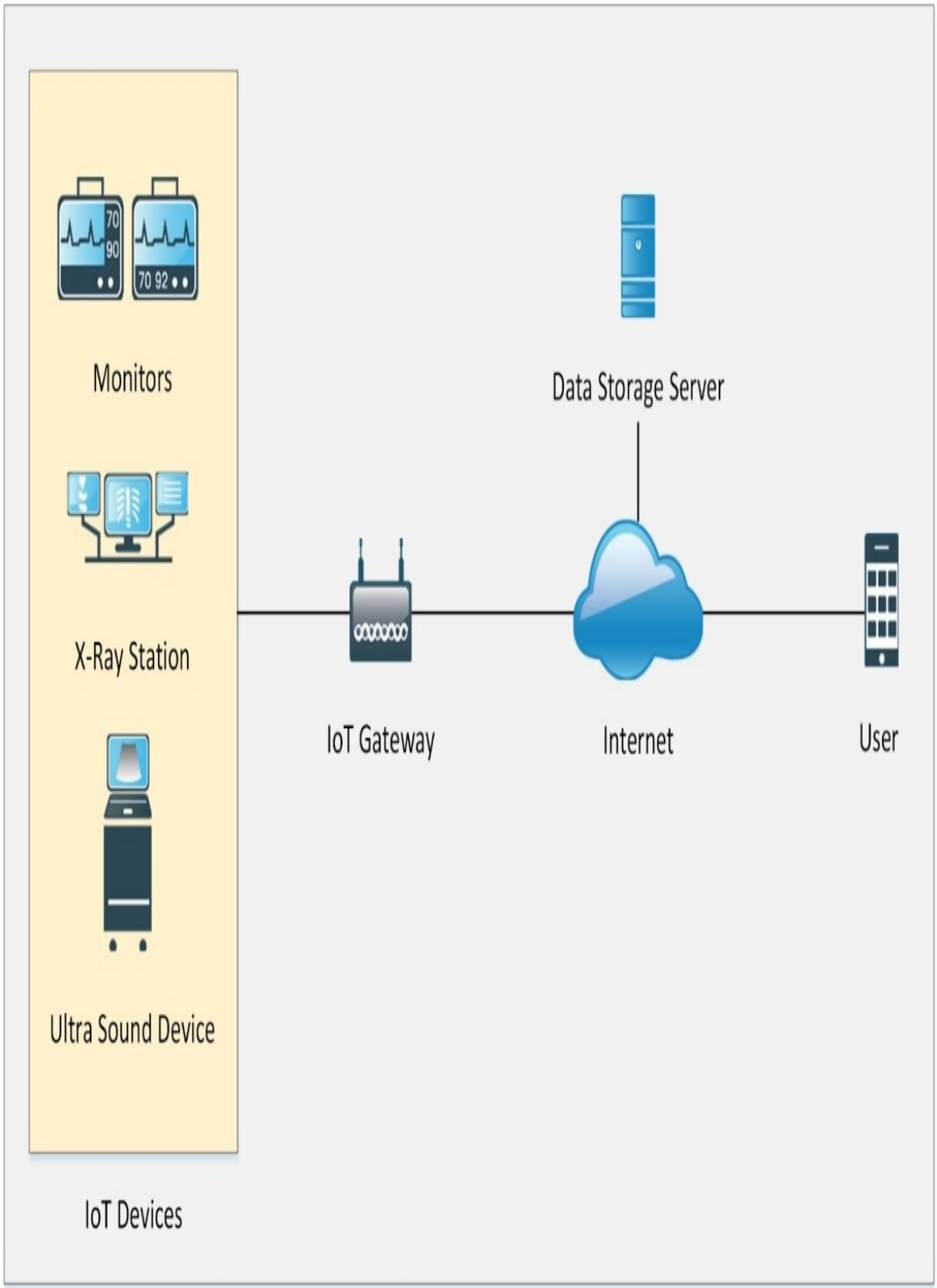


Figure 18.02: Internet of Things (IoT) Workflow

Figure 18-02: Internet of Things (IoT) Workflow

How Does the Internet of Things Work?

IoT devices can either use IoT gateways to communicate with the internet or they can communicate with the internet directly. The integration of controlled equipment, a logic controller, and advanced programmable electronic circuits makes them capable of communicating and being controlled remotely.

The architecture of IoT depends on five layers, as follows:

1. Application Layer
2. Middleware Layer
3. Internet Layer
4. Access Gateway Layer
5. Edge Technology Layer

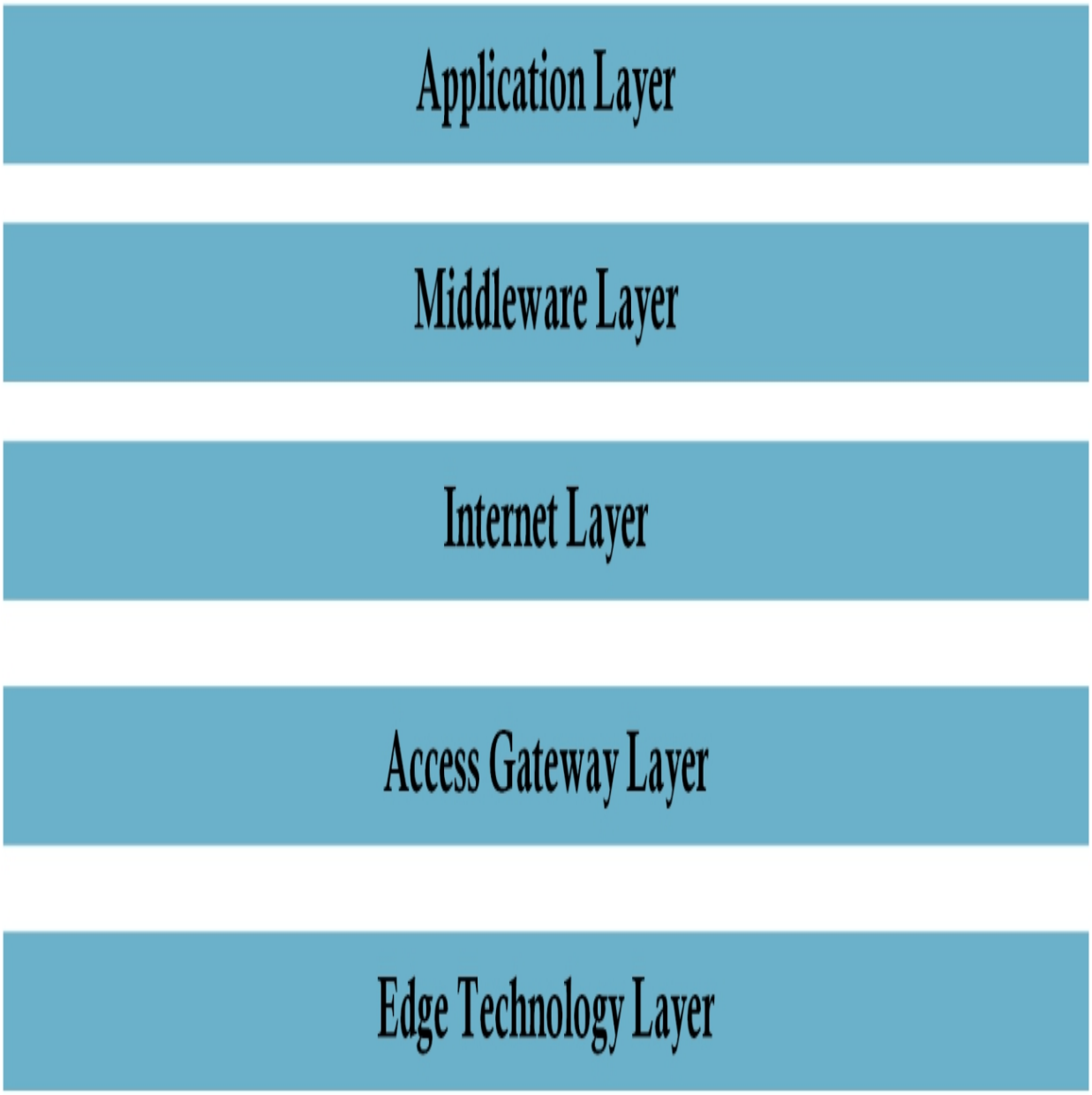


Figure 18-03: Internet of Things (IoT) Architecture

- The Application Layer is responsible for delivering data to users. This is a user interface for controlling, managing and commanding these IoT devices
- The Middleware Layer is for device and information management
- The Internet Layer is responsible for endpoint connectivity
- The Access Gateway Layer is responsible for protocol translation and messaging
- The Edge Technology Layer covers IoT capable devices

IoT Technologies and Protocols Wireless Communication Short Range Medium Range

Long Range Wired
Communication

Operating System
Bluetooth Low Energy (BLE) Ha-Low
Light-Fidelity (Li-Fi)

LTE-Advanced Low-Power Wide Area

Networking (LPWAN)

Very Small Aperture Terminal

(VSAT)
Ethernet RIOT OS

Multimedia over Coax Alliance (MoCA)
ARM mbed OS

Near Field Communication (NFC)
Cellular Power-Line Communication (PLC)
Real Sense OS X
Radio Frequency

Identification Ubuntu Core (RFID)
Wi-Fi Integrity RTOS *Table 18-01: Internet of Things (IoT) Technologies and Protocols*

IoT Communication Models

IoT devices can communicate with other devices in several ways. The following are some of the IoT communication models.

Device-to-Device Model

The Device-to-Device Model is a basic IoT communication model in which two devices communicate with each other without interfering with any other device. Communication between these two devices is established using communication mediums such as a wireless network. An example of a device-to-device communication model can be a

mobile phone user and a Wi-Fi printer. The user can connect a Wi-Fi printer using a Wi-Fi connection and send commands to the printer. These devices are independent of the vendor. A vendor's mobile phone can communicate with the wireless printer of a different manufacturer due to interoperability. Similarly, any home appliance connected with wireless remote control through a medium, such as Wi-Fi, Bluetooth, NFC, or RFID, is an example of the device-to-device communication model.

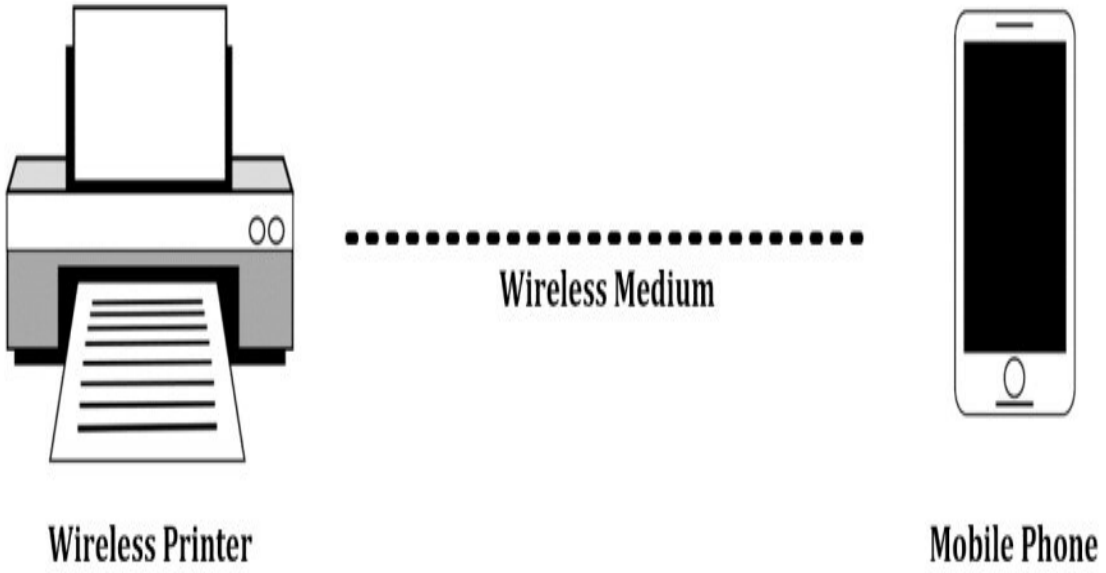


Figure 18-04: Device-to-Device Communication Model

Device-to-Cloud Model

The Device-to-Cloud Model is another model IoT device communication model in which IoT devices directly communicate with the application server. For example, consider a real-life scenario of a home where multiple sensors are installed for security purposes, for example, motion detectors, cameras, temperature sensors, etc. These sensors are directly connected to the application server, which can be hosted locally or on the cloud. The application server provides information exchange between these devices.
Similarly, Device-to-Cloud communication scenarios are found in a

manufacturing environment where different sensors communicate with the application server. Application severs process data, perform predictive maintenance, execute required and remediation actions to automate processes, and accelerate production.

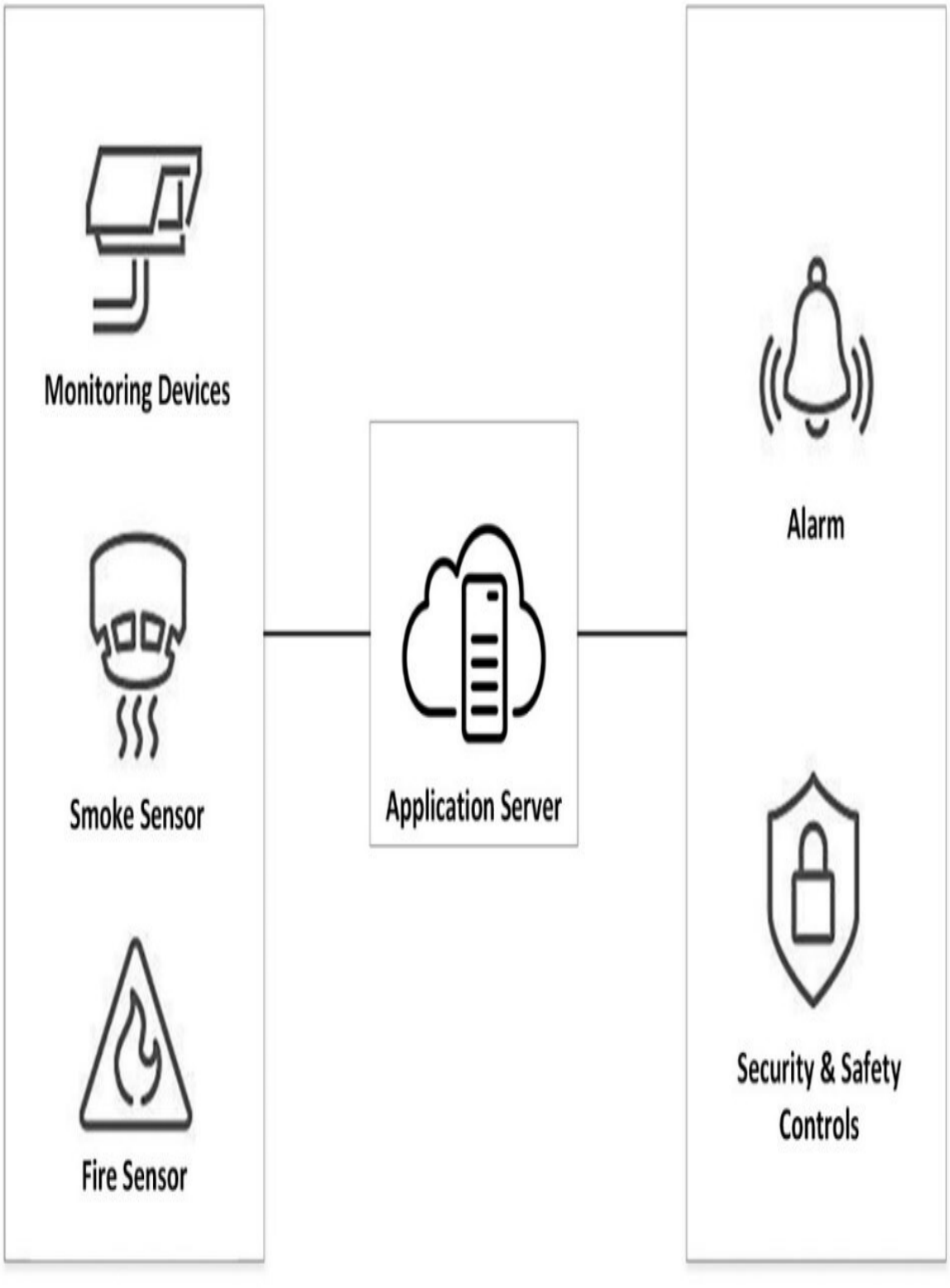


Figure 18_05: Device_to_Cloud Communication Model

Figure 18-05: Device-to-Cloud Communication Model

Device-to-Gateway Model

The Device-to-Gateway model is similar to the device-to-cloud model. IoT gateway devices collect data from sensors and send it to the remote application server. In addition, there is a consolidation point where the data being transmitted can be controlled. This gateway can provide security and other functionality, such as data or protocol translation.

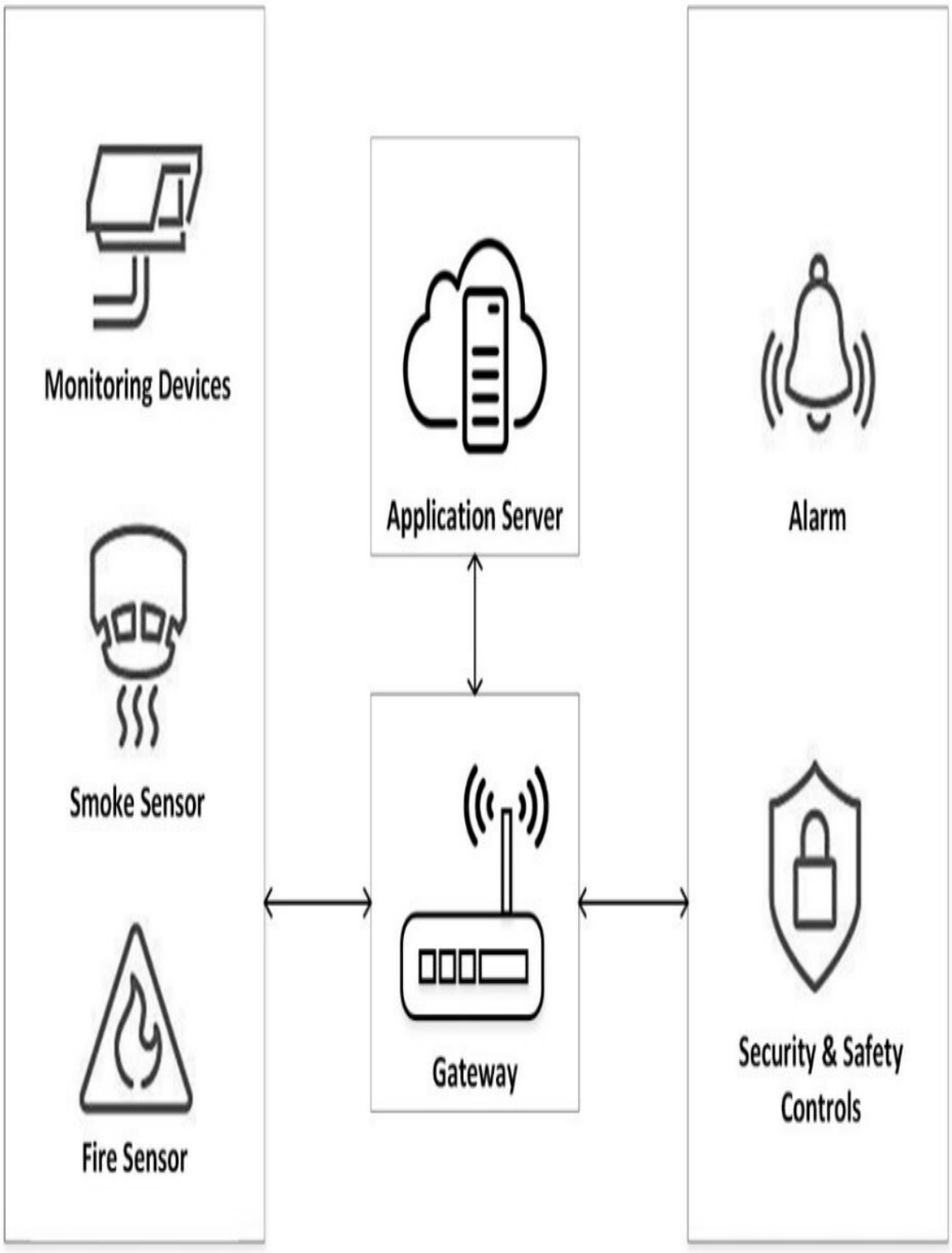


Figure 18-06: Device-to-Gateway Communication Model

Back-end Data-sharing Model

The Back-end Data-sharing Model is an advanced model in which devices communicate with the application servers. This scenario is used in a collective partnership between different application providers. The Back-end Data sharing model extends the deviceto-cloud model to a scalable scenario where sensors are accessed and controlled by multiple authorized third parties.

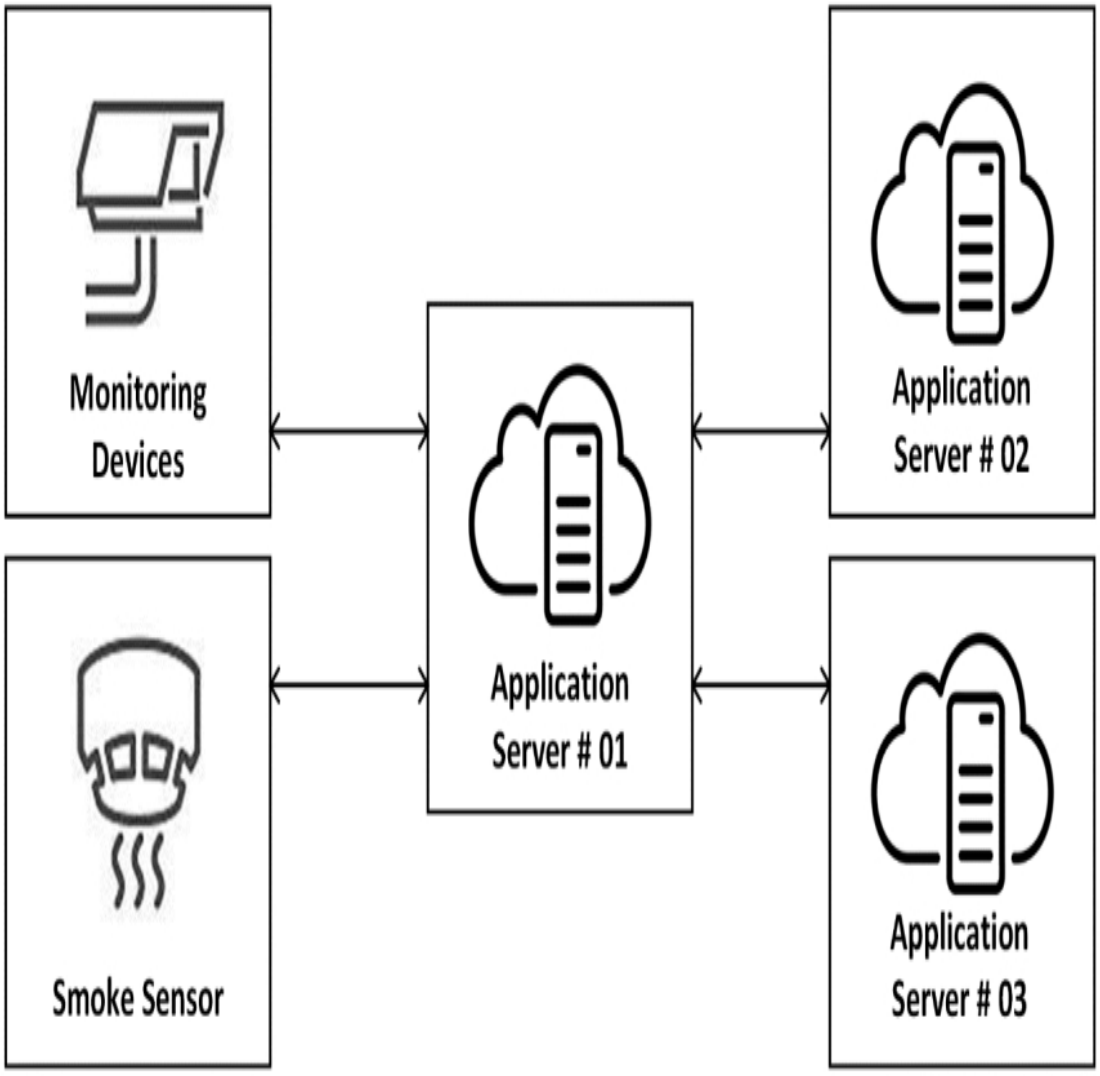


Figure 18-07: Back-End Data Sharing Model

There are many challenges to Internet of Things (IoT) deployment. While it creates ease, mobility, and more control over processes, it also brings threats, vulnerabilities, and challenges to the IoT technology. Some major challenges to IoT technology are as follows:

1. Lack of Security
2. Vulnerable Interfaces
3. Physical Security Risk
4. Lack of Vendor Support
5. Difficulties Updating Firmware and OS
6. Interoperability Issues

OWASP Top 10 IoT Vulnerabilities

The OWASP Top 10 IoT Vulnerabilities from 20 14 are as follows:

Rank Vulnerabilities I 1 Insecure Web Interface
I2 Insufficient Authentication/Authorization I3 Insecure Network Services
I4 Lack of Transport Encryption/Integrity Verification I5 Privacy Concerns
I6 Insecure Cloud Interface
I7 Insecure Mobile Interface
I8 Insufficient Security Configurability
I9 Insecure Software/Firmware

I 10 Poor Physical Security

Table 18-02: OWASP Top 10 IoT Vulnerabilities

IoT Attack Areas

The following are the most common attack areas in an IoT network: ■ Device Memory Containing Credentials
■ Access Control
■ Firmware Extraction
■ Privileges Escalation
■ Reset to an Insecure State
■ Removal of Storage Media
■ Web Attacks
■ Firmware Attacks
■ Network Services Attacks

- Unencrypted Local Data Storage
- Confidentiality and Integrity Issues
- Cloud Computing Attacks
- Malicious Updates.
- Insecure APIs
- Mobile Application Threats

IoT Attacks

DDoS Attack

A Distributed-Denial-of-Service Attack, as defined earlier, is intended to make the target's services unavailable. Using a Distributed-DOS attack, all IoT devices, IoT gateways and application servers can be targeted, and flooding requests toward them can result in a denial of service.

Rolling Code Attack

Rolling Code or Code Hopping is another technique that can be exploited. In this technique, an attacker captures the code, sequence, or signal coming from transmitter devices while simultaneously blocking the receiver from receiving the signal. The captured code will later be used to gain unauthorized access.

For example, a victim sends a signal to unlock his garage or his car. Car central locking works through radio signals. An attacker, using a signal jammer, can prevent the car's receiver from receiving the signal and simultaneously capture the signal sent by the owner of the car. Later, the attacker can unlock the car using the captured signal.

BlueBorne Attack

The BlueBorne Attack is performed using different techniques for exploiting Bluetooth vulnerabilities. These techniques, used to gain unauthorized access to Bluetooth enabled devices, are called BlueBorne Attacks.

Jamming Attack

A Jamming Attack uses signals to prevent devices communicating with each other as well as with the server.

Backdoor

This involves deploying a Backdoor on an organization's computer to gain unauthorized access to the private network.

Some other types of IoT attacks include:

- Eavesdropping
- Sybil Attack
- Exploit Kits
- Man-in-the-Middle Attack
- Replay Attack
- Forged Malicious Devices
- Side Channel Attack
- Ransomware Attack

IoT Hacking Methodology

Hacking methodology for the IoT platform is same as the methodology for other platforms, and is defined below:

Information Gathering

The first step in hacking the IoT environment requires information gathering. This includes extraction of information, such as IP address, running protocols, open ports, type of device, vendor information, etc. Shodan, Censys, and Thingful are search engines commonly used to find information about IoT devices. Shodan is a helpful platform for discovering and gathering information about IoT devices. As shown in the figure 18-08, information can gathered for CSR 1000v deployed across the world.

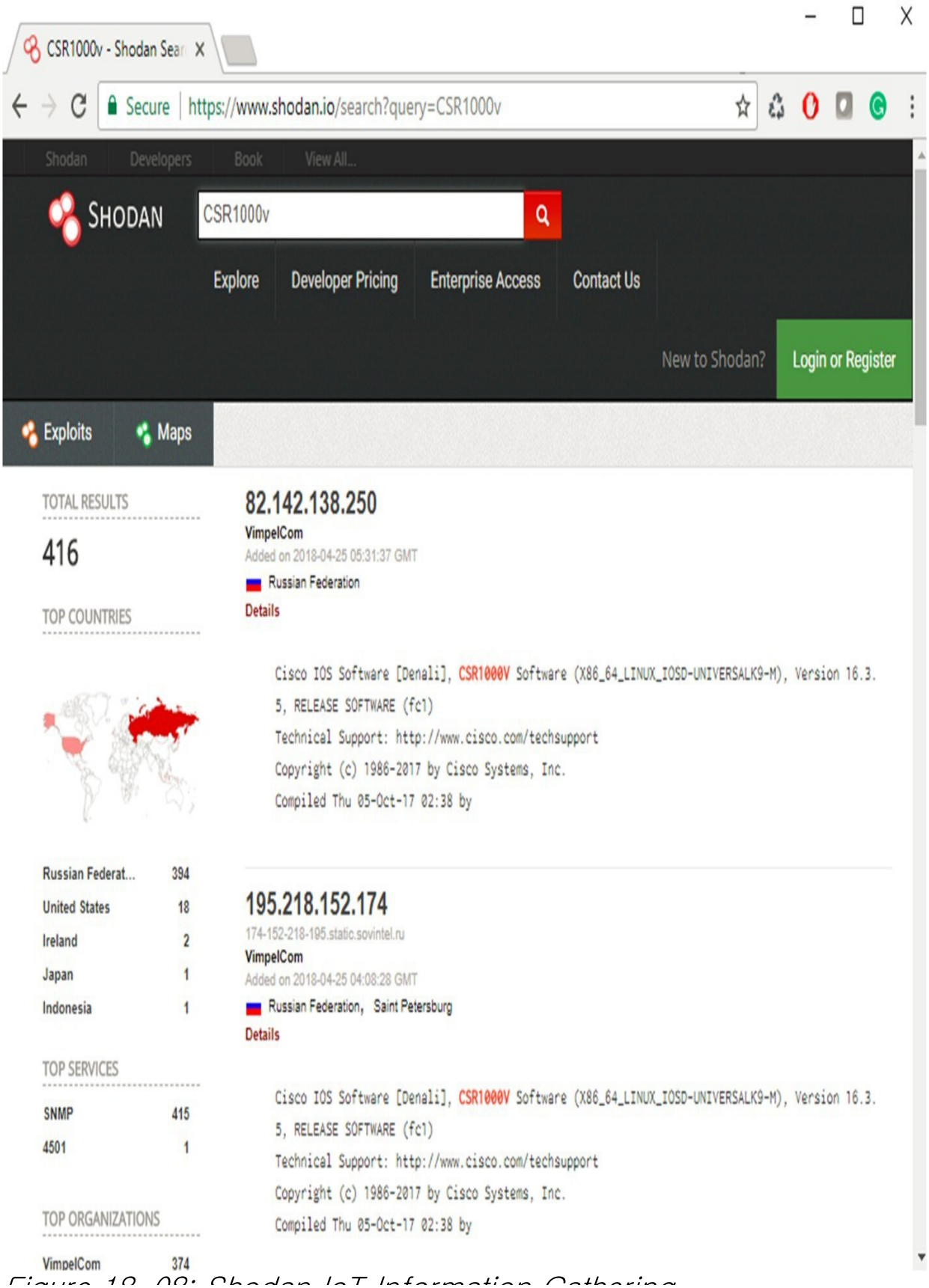


Figure 18_08: Shodan IoT Information Gathering

Figure 18-08: Shodan IoT Information Gathering

Vulnerability Scanning

Vulnerability Scanning vulnerabilities such as includes scanning weak passwords, a network and devices to

software and firmware bugs, identify default configuration, etc. Multi-ping, Nmap, RIoT Vulnerability scanner, and Foren6 are used for scanning against vulnerabilities.

Launch Attack

The attack launch phase includes exploiting these vulnerabilities using different attacks, for example, DDoS, Rolling Code, jamming, etc. RFCrack, Attify Zigbee Framework, and HackRF 1 are popular tools for launching attacks.

Gain Access

Gaining Access includes taking control of the IoT environment. Gaining access, escalating privileges to the administrator, or installation a backdoor can also be included in this phase.

Maintain Attack

Maintaining an Attack includes logging out without being detected, clearing logs and covering tracks.

Countermeasures:

Countermeasures for IoT devices include the following and are recommended by manufacturing companies:

■Firmware updates
■Block unnecessary ports
■Disable Telnet
■Use encrypted communication such as SSL/TLS
■Use strong passwords
■Use encryption of drives
■User account lockout
■Periodic assessment of devices
■Secure password recovery

■Two-Factor Authentication
■Disable UPnP

Practice Questions

1. How many layers are there in an architecture of IoT? A. 4
B. 5
C. 6
D. 7

2. Which layer in IoT architecture is responsible for device and information management?
A. Middleware Layer
B. Application Layer
C. Access Gateway Layer
D. Edge Technology Layer

3. Which layer is responsible for protocol translation and messaging? A. Middleware Layer
B. Application Layer
C. Access Gateway Layer
D. Edge Technology Layer

4. IoT device directly communicating with the application server is: A. Device-to-Device Model
B. Device-to-Cloud Model
C. Device-to-Gateway Model
D. Back-End Data Sharing Model

5. An eavesdropper records the transmission and replays it at a later time to cause the receiver to 'unlock', this attack is known as:
A. Rolling Code Attack
B. RF Attack
C. BlueBorne Attack
D. Sybil Attack

Chapter 19: Cloud Computing

Technology Brief

Cloud Computing technology has gained popularity nowadays because of its flexibility and mobility support. Cloud computing allows access to personal and shared resources with minimal management. It often relies on the internet. There is also a third-party cloud solution available, which saves on expanding resources and maintenance. One popular example of cloud computing is Amazon Elastic Cloud Compute (EC2), which is highly capable, low cost, and flexible. The main features of cloud computing include:

- On-Demand Self-Service
- Distributed Storage
- Rapid Elasticity
- Measured Services
- Automated Management
- Virtualization

Types of Cloud Computing Services

There are three types of Cloud Computing Services:
- Infrastructure-as-a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)

Infrastructure-as-a-Service (IaaS)

Infrastructure-as-a-Services (IaaS), also known as cloud infrastructure service, is a selfservice model. IaaS is used for accessing, monitoring, and managing purposes. For example, rather than purchasing additional hardware such as firewalls, networking devices, servers, etc. and spending money on deployment, management, and maintenance, the IaaS model offers cloud-based infrastructure for deploying remote data centers. The most popular examples of IaaS are Amazon EC2, Cisco Metapod, Microsoft Azure, and Google Compute Engine (GCE).

Platform-as-a-Service (PaaS)

Platform-as-a-Service is another cloud computing service. It allows users to develop, run, and manage applications. PaaS offers development tools, configuration management, and deployment platforms, and migrating an app to a hybrid model. It helps to develop and customize applications, manage OSes, visualization, storage, and networking, etc. Examples of PaaS are Google App Engine, Microsoft Azure, and Intel Mash Maker.

Software-as-a-Service (SaaS)

Software-as-a-Service (SaaS) is one of the most widely used cloud computing service. SaaS is mostly the first example of cloud computing that many users experience. Often without even realizing that they are interacting with a cloud service. Hosted software applications are readily available via a web browser, or a thin client is sometimes indistinguishable to the user because they want to run the software application and without knowing about details operating behind the applications software. An example of SaaS is office software such as Office 365, Cisco WebEx, Citrix GoToMeeting, Google Apps, messaging software, DBMS, CAD, ERP, HRM, etc.

Cloud Deployment Models

The following are the Deployment Models for cloud services:

Deployment Model Description Public Cloud
Private Cloud
Hybrid Cloud

Community Cloud Public Clouds are hosted by a third party offering different types of cloud computing services

Private Clouds are hosted by individuals. Corporate companies usually deploy their own private clouds because of their security policies

Hybrid Clouds comprise of both private and public clouds. The private cloud is for their sensitive data and the public cloud is to scale up capabilities and services

Community Clouds are accessed by multiple parties having common goals and shared resources

Table 19-01: Cloud Deployment Models

NIST Cloud Computing Reference Architecture

This Architecture is a generic high-level conceptual reference architecture presented by NIST (National Institute of Standards and Technology). NIST cloud computing refers the architecture which identifies the major components of cloud and their functions in cloud computing. NIST Architecture is intended to facilitate the understanding of the requirements, uses, characteristics, and standards of cloud computing.

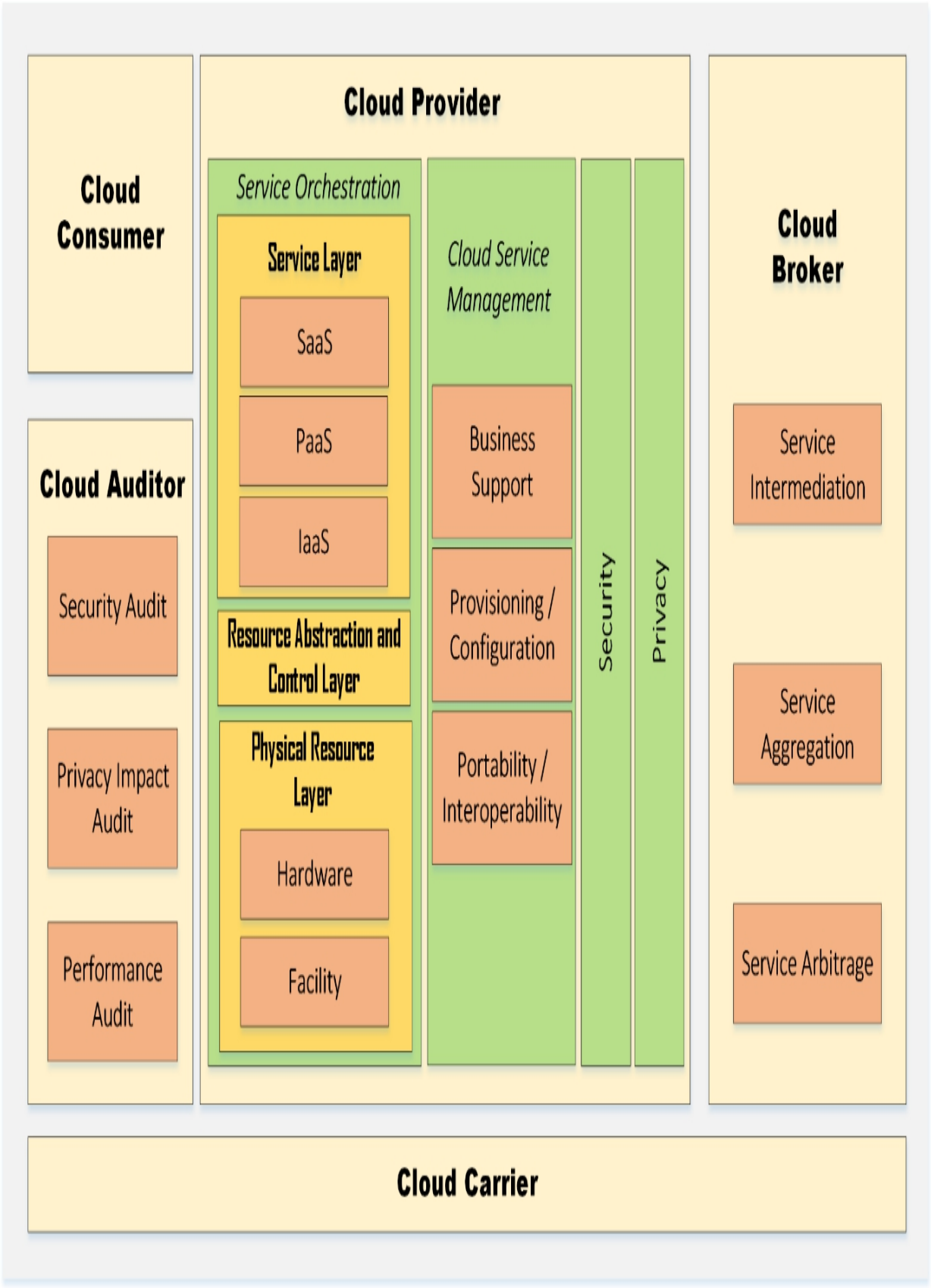


Figure 10- 01: NIST Cloud Computing Reference Architecture

Figure 19-01: NIST Cloud Computing Reference Architecture
NIST Cloud Computing Architecture defines five major actors, Cloud Consumer, Cloud Provider, Cloud Auditor, Cloud Broker, and Cloud Carrier.

Actor	Definition
Cloud Consumer	A person or organization that maintains a business relationship with, and uses service from Cloud Providers.
Cloud Provider	A person, organization, or entity that is responsible for making a service available to interested parties
Cloud Auditor	A party that can conduct an independent assessment of cloud services, information system operations, performance, and the security of cloud implementation
Cloud Broker	An entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers

Table 19-02: Actors

Cloud Computing Benefits

There are abundant advantages of cloud computing, of which some of the most important are discussed here.

Increased Capacity:

By using cloud computing, users do not have to worry about the capacity of their infrastructure, as the cloud platform provides unlimited capacity; a customer can use as much or as little capacity as he/she needs.

Increased Speed:

The cloud computing environment has dramatically reduced the time and cost of new IT services, thus increasing the speed at which

organizations can access IT resources. *Low Latency:*
By using cloud computing, customers can implement their applications with just a few clicks, doing all their tasks easily in a short time and with minimum latency. *Less Economic Expense:*

The major advantage of cloud computing is the low financial cost. There is no need to purchase dedicated hardware for a particular function. Networking, datacenters, firewalls, applications, and other services can be easily virtualized over the cloud, saving on the cost of purchasing hardware, configuration and management complexity, and maintenance.

Security:

Cloud computing is also efficient in terms of security, with effective patch management and security updates. Disaster recovery, dynamically scaling defensive resources, and other security services offer protection against cloud computing threats.

Understanding Virtualization

Virtualization in computer networking is a process of deploying a machine or multiple machines virtually on a host. These virtually deployed machines use the host machine's system resources by applying a logical division. The major difference between a physically deployed machine and a virtual machine is the system resources and hardware. Physical deployment requires separate dedicated hardware for a single Operating System whereas a virtual machine host can support multiple Operating Systems over a single system, sharing resources such as storage.

The Benefits of Virtualization in the Cloud

The major advantage of Virtualization is cost reduction. Purchasing dedicated hardware is costly and requires maintenance, management, and security. Additional hardware consumes space and power whereas virtualization supports multiple machines on a single hardware. Furthermore, virtualization reduces administration, management,

networking tasks, and ensures efficiency. Virtualization over the cloud is even more effective where there is no need to install any hardware. You can easily access them from anywhere, any time.

Cloud Computing Threats

Although cloud computing offers many services with efficiency and flexibility, there are also some threats from which cloud computing is vulnerable. These threats include data loss/breach, insecure interfaces and APIs, malicious insiders, privilege escalations, natural disasters, hardware failure, authentication problems, VM level attacks, and much more.

Data Loss/Breach

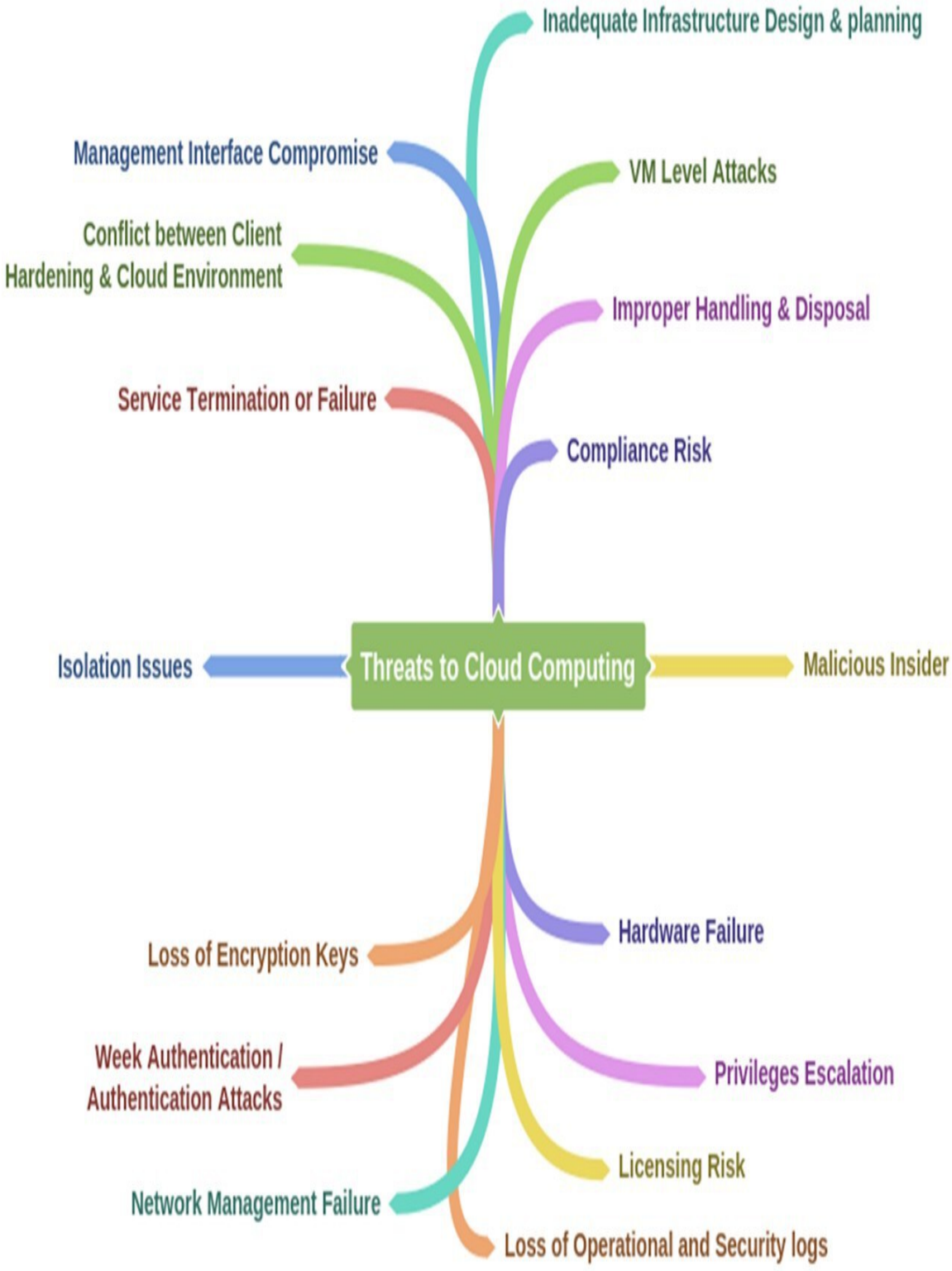
Data Loss and Data Breach are the most common threats to every platform. Improper encryption or loss of encryption keys may result in data modification, erasing, theft, or misuse.

Abusing Cloud Services

Abusing Cloud Services includes using the service for malicious intent as well as using these services abusively. For example, an attacker can abuse the Dropbox service by spreading a massive phishing campaign. Similarly, a cloud service can be used to host malicious data and botnet commands and controls, etc.

Insecure Interface and APIs

Software User Interface (UI) and Application Programming Interfaces (APIs) are the interfaces used by customers to interact with the service. They need to be secure from malicious attempts. Such interfaces can be made secure with a good program of monitoring, orchestration, management, and provisioning.



Cloud Computing Attacks

Cloud Computing Attacks

In cloud computing, the following are the most common attacks used by attackers to extract sensitive information, for example, personal credentials or gaining unauthorized access. Cloud Computing Attacks include:

- Service Hijacking with Social Engineering Attacks
- Session Hijacking with XSS Attacks
- Domain Name System (DNS) Attacks
- SQL Injection Attacks
- Wrapping Attacks
- Service Hijacking with Network Sniffing
- Session Hijacking with Session Riding
- Side Channel Attack or Cross-Guest VM Breaches
- Cryptanalysis
- DoS/DDoS Attacks

Service Hijacking with Social Engineering Attacks

We have already discussed social engineering attacks. Using social engineering techniques, an attacker may attempt to guess a password. Social engineering attacks result in unauthorized access exposing sensitive information according to the privilege level of the compromised user.

Service Hijacking with Network Sniffing

Using Packet Sniffing tools by placing him/herself in the network, an attacker can capture sensitive information such as passwords, session IDs, cookies, and another web service-related information such as UDDI, SOAP, and WSDL.

Session Hijacking with XSS Attacks

By launching Cross-site Scripting (XSS), an attacker can steal cookies by injecting malicious code into the website.

Note: A cross-site request forgery is an attack that forces an end user to execute unwanted actions on a web application on which they are

authenticated.

Session Hijacking with Session Riding

Session Riding is intended for session hijacking. An attacker may exploit it by attempting a cross-site request forgery. The attacker uses a currently active session and rides on it by executing the requests such as modification of data, erasing data, online transactions, and password changes by tricking the user to click on a malicious link.

Domain Name System (DNS) Attacks

Domain Name System (DNS) attacks include DNS Poisoning, Cybersquatting, Domain Hijacking, and Domain Snipping. An attacker may attempt to spoof by poisoning the DNS server or cache to obtain credentials of internal users. Domain hijacking involves stealing a cloud service domain name. Similarly, through phishing frauds, users can be redirected to a fake website.

Side Channel Attacks or Cross-guest VM Breaches

A Side Channel Attacks or Cross-guest VM Breach is an attack that requires the deployment of a malicious virtual machine on the same host. For example, suppose an attacker targets a physical host hosting a virtual machine that offers cloud services. The attacker can install a malicious virtual machine on the host to take advantage of resource sharing, for example, the processor cache or cryptographic keys. A malicious insider or an attacker can perform installation by impersonating a legitimate user.

Similarly, there are other attackers, discussed earlier, which are also vulnerable to cloud computing such as SQL Injection Attack (injecting malicious SQL statements to extract information), Cryptanalysis Attacks (of weak or obsolete encryption) Wrapping Attack (duplicating the body of message), Denial-of-Service (DoS) and Distributed Denial-ofService (DDoS) Attacks.

Cloud Security

Cloud Computing Security refers to the security implementation and deployment of a system to prevent security threats. Cloud security includes control policies, deployment of security devices such as application firewalls and Next Generation IPS devices, and strengthening the cloud computing infrastructure. It also includes actions at the service provider end as well as the user end.

Cloud Security Control Layers

Application Layer

Several security mechanisms, devices, and policies provide support at different cloud security control layers. At the application layer, web application firewalls are deployed to filter traffic and observe its behavior. Similarly, Systems Development Life Cycle (SDLC), Binary Code Analysis and Transactional Security provide security for online transactions, and script analysis, etc.

Information

To provide confidentiality and integrity of information communicated between client and server, different policies are configured to monitor any data loss. These policies include Data Loss Prevention (DLP) and Content Management Framework (CMF). Data Loss Prevention (DLP) is a feature that prevents information leaking from the network. Traditionally information may include a company or organization's confidential details, proprietary, financial, and other sensitive information. The Data Loss Prevention feature also ensures compliance with rules and regulations using Data Loss Prevention policies to prevent users from intentionally or unintentionally sending out confidential information.

Management

Security regarding the management of cloud computing is performed through different approaches such as Governance, Risk Management, and Compliance (GRC), Identity and Access Management (IAM), and Patch and Configuration management. These approaches help to control and manage secure access to resources.

Network Layer

There are solutions available to secure the network layer in cloud computing such as the deployment of Next Generation IDS/IPS

devices, Next Generation Firewalls, DNSSec, Anti-DDoS, OAuth, and Deep Packet Inspection (DPI). The Next Generation Intrusion Prevention System, known as NGIPS, is one of the most efficient and proactive components in the Integrated Threat Security Solution. To secure a network's complex infrastructure, NGIPS provides a strong security layer with deep visibility, enhanced security intelligence, and advanced protection against emerging threats. Cisco's NGIPS provides deep network visibility, automation, security intelligence, and next level protection. It uses the most advanced and effective intrusion prevention

capabilities to catch emerging sophisticated network attacks. It continuously collects information regarding the network, including Operating System information, file and application information, device and user information, etc. This information helps NGIPS to map the network maps and host profiles, providing contextual information to make better decisions about intrusive events.

Trusted Computing

The Root of Trust (RoT) is established by validating each component of hardware and

software from the end entity up to the root certificate. It is intended to ensure that only trusted software and hardware can be used, while at the same time retaining flexibility.

Computer and Storage

Computing and Storage in the cloud can be secured by implementing Host-based Intrusion Detection or Prevention Systems HIDS/HIPS. Examples of these are Configuring Integrity Check, File System Monitoring and Log File Analysis, Connection Analysis, Kernel Level Detection, Encrypting the Storage, etc. Host-based IPS/IDS is

normally deployed for the protection of a specific host machine and it works strictly with the machine's Operating System Kernel. It creates a filtering layer to filter out any malicious application call to the OS.

Physical Security

Physical Security is always a priority for securing anything. As it is also

the first layer

OSI model, if a device is not physically secure, any sort of security configuration will not be effective. Physical security includes protection against man-made attacks such as theft, damage, and unauthorized physical access, as well as environmental impact such as rain, dust, power failure, fire, etc.

Responsibilities in Cloud Security

Cloud Service Provider

The responsibilities of a cloud service provider include providing the following security controls:

- Web Application Firewall (WAF)
- Real Traffic Grabber (RTG)
- Firewall
- Data Loss Prevention (DLP)
- Intrusion Prevention Systems
- Secure Web Gateway (SWG)
- Application Security (App Sec)
- Virtual Private Network (VPN)
- Load Balancer
- CoS/QoS
- Trusted Platform Module
- Netflow and others

Cloud Service Consumer

The responsibilities of a cloud service consumer include managing the following security controls:

- Public Key Infrastructure (PKI)
- Security Development Life Cycle (SDLC)
- Web Application Firewall (WAF)
- Firewall
- Encryption
- Intrusion Prevention Systems
- Secure Web Gateway

- Application Security
- Virtual Private Network (VPN) and others

Resiliency and Automation Strategies
Automation/Scripting

For administrators and clients, automation and scripting is a powerful tool that provides protection along with efficiency in executing tasks. Automation provides accuracy and reduces risks. Otherwise these tasks are manually performed by humans using command line execution or GUI operations. However, scripts can be connected to reduce the complexity of actions that require a sequence of commands to be performed.

Automated Courses of Action

A scripting system can be seen as a best friend for all professionals who believe in effective technical work as it provides Automated Courses of Action, thereby saving time. The importance of scripts and automation can be seen by the fact that it is specified in the National Institute of Standards and Technology Special publication in 800-53 series.

Continuous Monitoring

Continuous Monitoring is the procedure followed to keep a check on the functioning of the process functioning and to reduce risks associated with it. It is a risk assessment procedure that follows NIST Risk Management Framework (RMF) methodology that is used for security controls.

Configuration Validation

Over time systems become outdated. Systems are designed and configured to perform a specific function and configuration is validated against security standards. In order to upgrade a system's configuration when necessary, a method called automated testing can be used to resolve issues that may include multiple configuration management.

Templates

Templates are a key element for making servers, programs, or for the entire system too. Templates enable an infrastructure to become a real service. Using templates can help to set business standards and technology stacks used by clients.

Master Image

An organization can be fully patched into a Master Image that backups all applications, Operating Systems, and, most importantly, data. By using a master image, many administrative tasks can be made easier and error free. The master image can also be used for enterprises with multiple desktops because if any error is found, it can be removed by fixing and deploying it on any single PC.

Non-Persistence

A system is said to be non-persistent when the changes made in it are not permanent. The files, applications, and programs installed on the system are not permanent because any changes made in the configuration are not saved. Making the system non-persistent secures it from certain malware.

Snapshots

A snapshot is a prompt point on a machine that allows the virtual machine to restore the previous points. Snapshots are very important because they act as a memory point for the entire system.

A snapshot allows you to return to the previous point. If you want to make changes in your system, first take a snapshot of it, then make the changes and if you do not like the result, you can return to the previous point with the help of the snapshot.

Revert to Known State

The capability of an Operating System to snapshot any virtual machine is known as Reverting to a Known State. Most Operating Systems have

this capability as a built-in program. This option is mainly found in Microsoft Office where the system creates a restore point by default before the update process.

Rollback to Known Configuration

Rolling back to a Known Configuration can be also defined as getting back to a known state. You can use this option, for example, if you have made any incorrect configuration to your system and you want to get back to the previous state.

Live Boot Media

A bootable system known as Live Boot Media is loaded on an optical disc or USB, which it is specially designed to be bootable from. This is used to boot the system from an external Operating System.

Elasticity

Increasing the capacity of a system to handle workload by using additional hardware to scale up space is called Elasticity. This can also be set to automatic mode in some environments such as a cloud environment.

Scalability

A system's ability to accommodate more load by using additional hardware or sources is known as Scalability. The term is commonly used in server farms and database clusters because they face scaling issues due to workload.

Distributive Allocation

When a request is made to a range of resources for transparent allocation, it is called Distributive Allocation. When a number of resources are allocated dynamically to respond a load, it is the point where distributive allocation handles the task.

Redundancy

Redundancy in computer networks means having additional or alternate resources available for use, usually as a back-up or fail-over plan. Typically in an architecture, network devices, network links, and other equipment are set up redundantly. Data centers and ISPs, for example, have redundant links to ensure high availability.

Fault Tolerance

Fault Tolerance is defined as the uninterrupted functioning of a system despite the occurrence of fault. Data and services can be mirrored to ensure there is no disruption. This can be a useful tool in servers because they are more critical to operations.

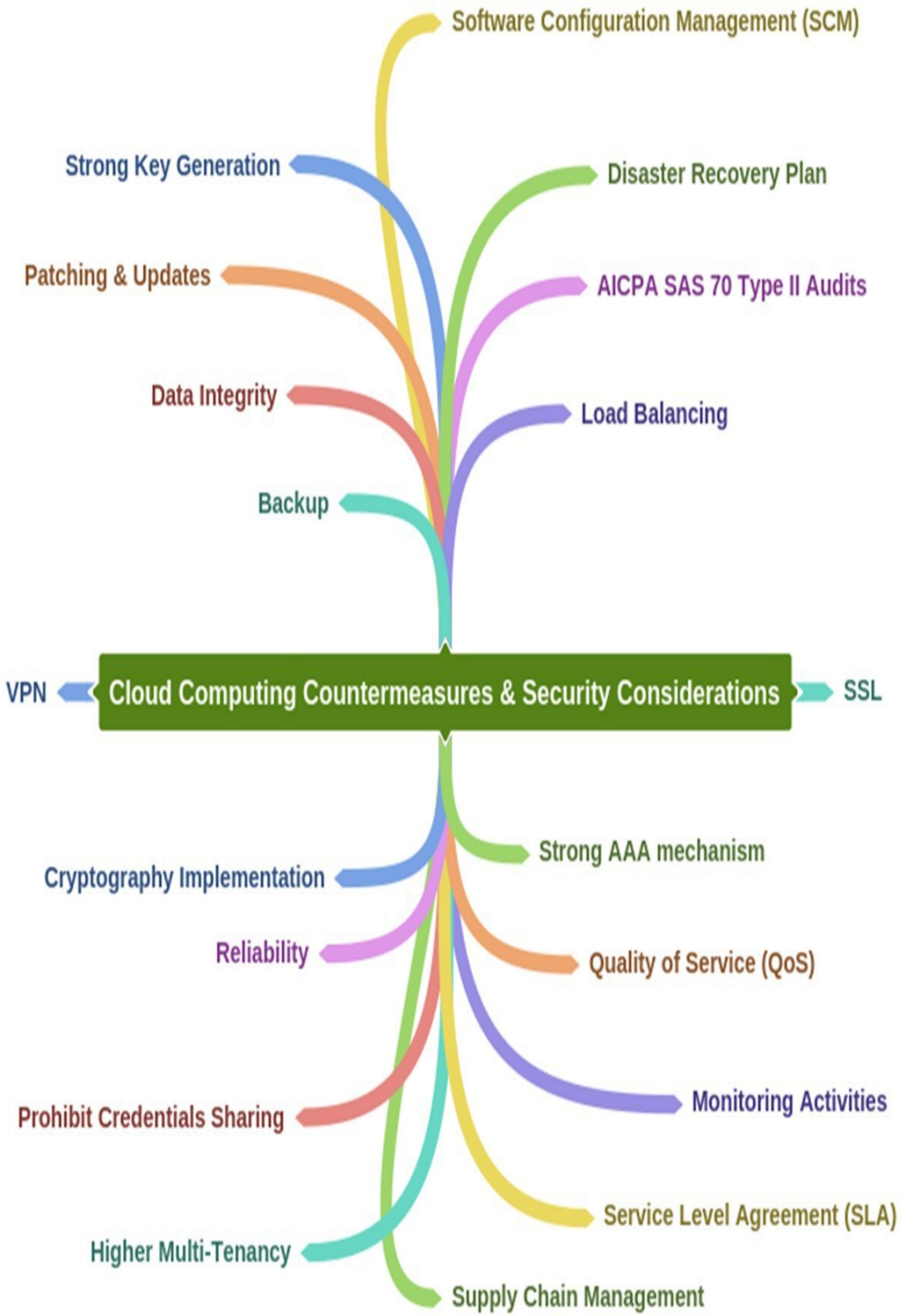
High Availability

High Availability is the ability of a system to maintain space for data and operational services regardless of any disrupting events, or faults. High availability achieves the same goal as fault tolerance in ensuring the availability of data and services.

RAID

RAID stands for Redundant Array Independent Disks. It is used to increase the reliability of storage disks. It takes data that is commonly stored on a disk and sends it to many others, keeping the data stored in various places. RAID also increases the speed of data recovery because multiple disks are busy recovering data rather than a single disk.

Mind Map


Cloud Computing Countermeasures & Security Considerations
Software Configuration Management (SCM)
Strong Key Generation
Disaster Recovery Plan
Patching & Updates
AICPA SAS 70 Type II Audits
Data Integrity
Load Balancing
Backup
VPN
SSL
Strong AAA mechanism
Cryptography Implementation
Reliability
Quality of Service (QoS)
Monitoring Activities
Prohibit Credentials Sharing
Service Level Agreement (SLA)
Higher Multi-Tenancy
Supply Chain Management

Cloud Security Tools
Core CloudInspect

Core Security Technologies offer Core CloudInspect, a cloud security testing solution for Amazon Web Services (AWS). This tool benefits from Core Impact and Core Insight technologies to offer penetration testing as a service from Amazon Web Services for EC2 users.

CloudPassage Halo

CloudPassage Halo provides a broad range of security controls. It is a Focused Cloud Security Solution that prevents attacks and detects compromises. CloudPassage Halo operates under the ISO27002 security standard and is audited annually against PCI Level 1 and SOC 2. Halo is the only workload security automation platform that offers on-demand delivery, at speed and scale, of security controls across data centers, Private/Public clouds, virtual machines, and containers. Unlike traditional security systems, Halo and its robust APIs integrate with popular CI/CD tool chains and processes, providing just-in-time feedback to fix vulnerabilities early in the development cycle. Halo easily integrates with popular infrastructure automation and orchestration platforms, allowing Halo to be easily deployed to monitor the security and compliance posture of workloads continuously.

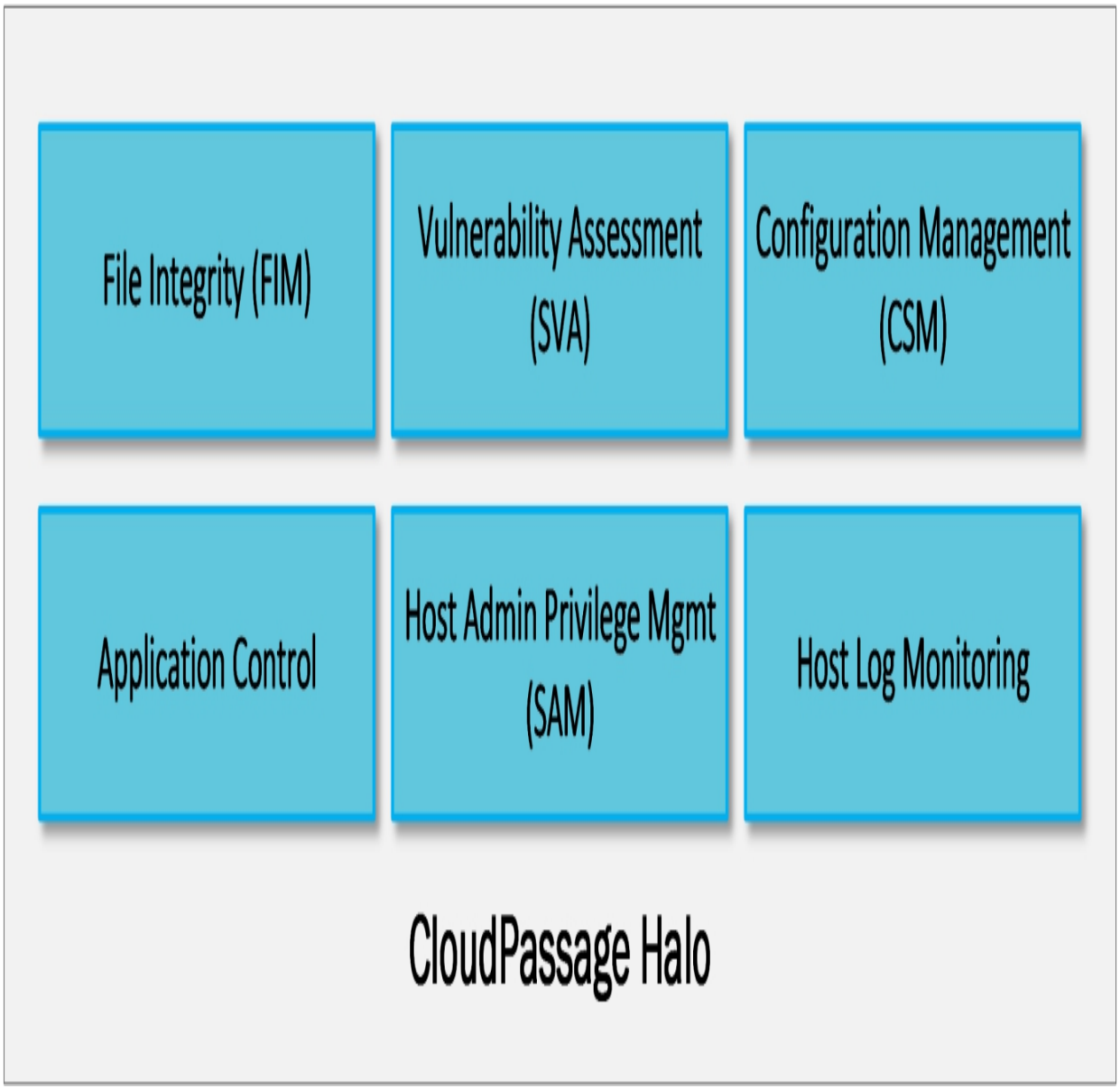


Figure 19-02: CloudPassage Halo Components

Mind Map


Cloud Computing
Types of Cloud Computing Services
Platform-as-a-Service (PaaS)
Infrastructure-as-a-Service (IaaS)
Software-as-a-Service (SaaS)
NIST Architecture
Cloud Carrier
Cloud Service Provider
Cloud Consumer
Cloud Auditor
Cloud Broker
Security Considerations
Disaster Recovery Plan
SLA
AAA
Strong Cryptography
Multi-Tenancy
QoS
Load balancing
Attacks
Side Channel Attack
Service Hijacking
Domain Name System (DNS) Attack
SQL Injection Attack
Wrapping Attack
Network Sniffing
Session Riding
DoS / DDoS Attack
Threats
Isolation Issues
VM Level Attacks
Abusing Cloud Services
Data Loss / Breach
Insecure interfaces
Insecure APIs
Malicious Insider
Countermeasures
Root of Trust (RoT)
Identity & Access Management (IAM)
Content Management Framework (CMF)
NGIPS / NGIDS
SDLC
Binary Code Analysis
Data Loss Prevention (DLP)
Governance, Risk management & Compliance (GRC)
HIDS / HIPS
Cloud Deployment Models
Private Cloud
Public Cloud
Hybrid Cloud
Community Cloud