UNIT - 4

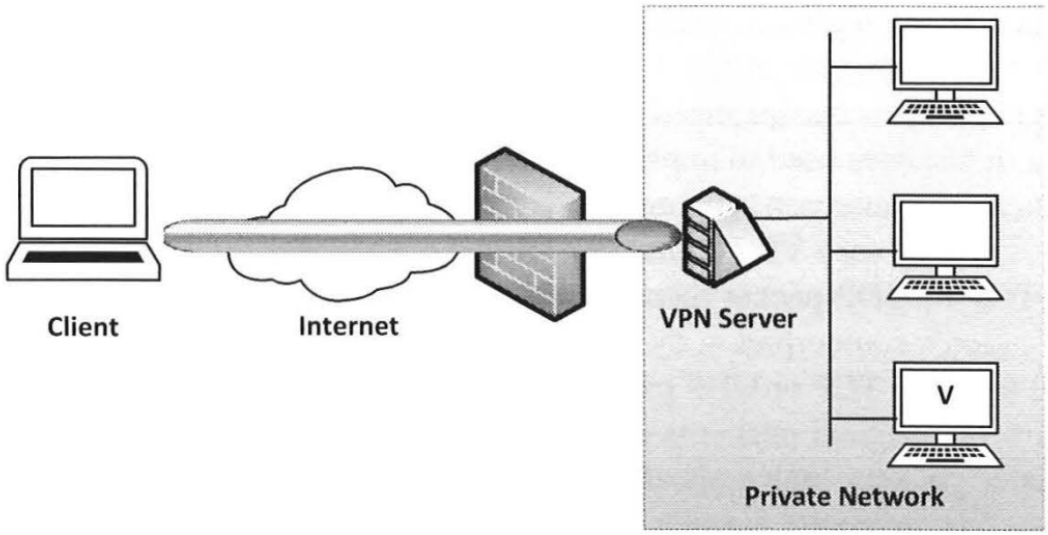
Virtual Private Network

Requirements

- User authenticated: Due to the locks or security guards employed by organi zati ons and
  homes, users who can use a private network have already been authorized, and their
  identities verified.
- Content protected: The content of the communication within the private network cannot
  be seen from outside. This is achieved as long as cables are physically secured and Wi-Fi
  are encrypted.
- Integrity preserved: Nobody from outside can insert fake data into the private network or
  make changes to the existing data inside the private network.

Virtual Private Network Creation

- Having a designated host (VPN server) on the network
- Outside computers have to go through the VPN server to reach the hosts inside a private network via authentication.
- VPN server is exposed to the outside and the internal computers are still protected, via firewalls or reserved IP addresses.

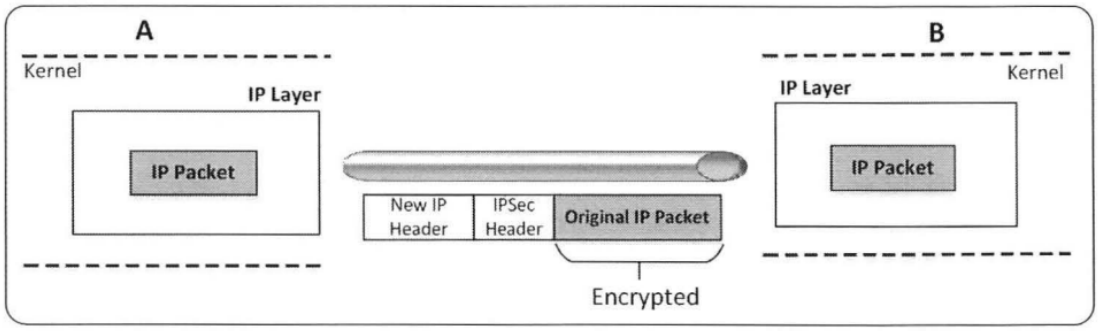


IP Tunneling

Encapsulating encrypted IP packet inside another IP packet for reaching the final destination.:

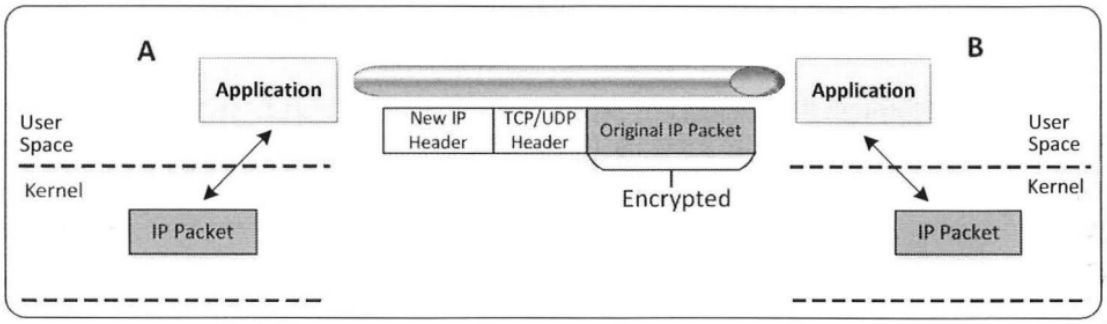
1. **IPSec Tunneling:** - Illustration of encapsulating the original packet inside a new IP packet.
    - **Protocol Used:** Internet Protocol Security (IPSec).
    - **Operating Layer:** Operates at the IP layer.
    - **Mode:** Utilizes Tunneling Mode, where the entire original IP packet is encapsulated into a new IP packet with an added header.
    - **Implementation:** Takes place inside the IP layer in the kernel.

- **Purpose:** Often used to implement Virtual Private Networks (VPNs).



(a) IPSec Tunneling

2. **TLS/SSL Tunneling:** - Illustration of encapsulating the original packet inside a TCP or UDP packet using TLS/SSL tunneling.
    - **Protocol Used:** Transport Layer Security (TLS) or Secure Sockets Layer (SSL).
    - **Operating Layer:** Operates on top of the transport layer protocols TCP or UDP.
    - **Implementation:** Takes place outside of the kernel, in an application.
    - **Process:** Each VPN-bound IP packet is handed to a dedicated application, which encapsulates it inside a TCP or UDP packet. The new IP packet is then sent to the application's counterpart at the other end of the tunnel, where the original packet is extracted from the TCP or UDP payload.
    - **Security:** Both ends of the tunnel use TLS/SSL on top of TCP/UDP to secure the encapsulated packets.
    - **Popularity:** Increasingly popular due to being implemented inside an application, simplifying the complexity compared to kernel-level solutions.



(b) TLS/SSL Tunneling

Virtual Network Interface

TUN / TAP interfaces connect a computer to a user-space program. They can be seen as a simple point-to-point network device, which connects two computers, except that one of the computers is only a user-space program that pretends to be a computer.

Aspect	TUN Interface	TAP Interface
Layer of Operation	Works at the IP level (OSI Layer 3)	Works at the Ethernet level (OSI Layer 2)
Network Stack Layer	Layer 3	Layer 2
Supported Communication	Primarily point-to-point (P2P) communication	Supports any layer 3 protocol; not limited to P2P
Broadcast/Multicast Support	Configurable to support broadcast/multicast using flags	Supports broadcast/multicast inherently
Packet Delivery	Delivers packets to user-space program, including IP headers	Functions like a network adapter, handling Ethernet frames
Use in VPNs	Commonly used to build VPNs	Not typically used for VPNs, more for virtual network adapters
Bridge Networks	Not typically used for creating bridge networks	Extensively used for creating bridge networks

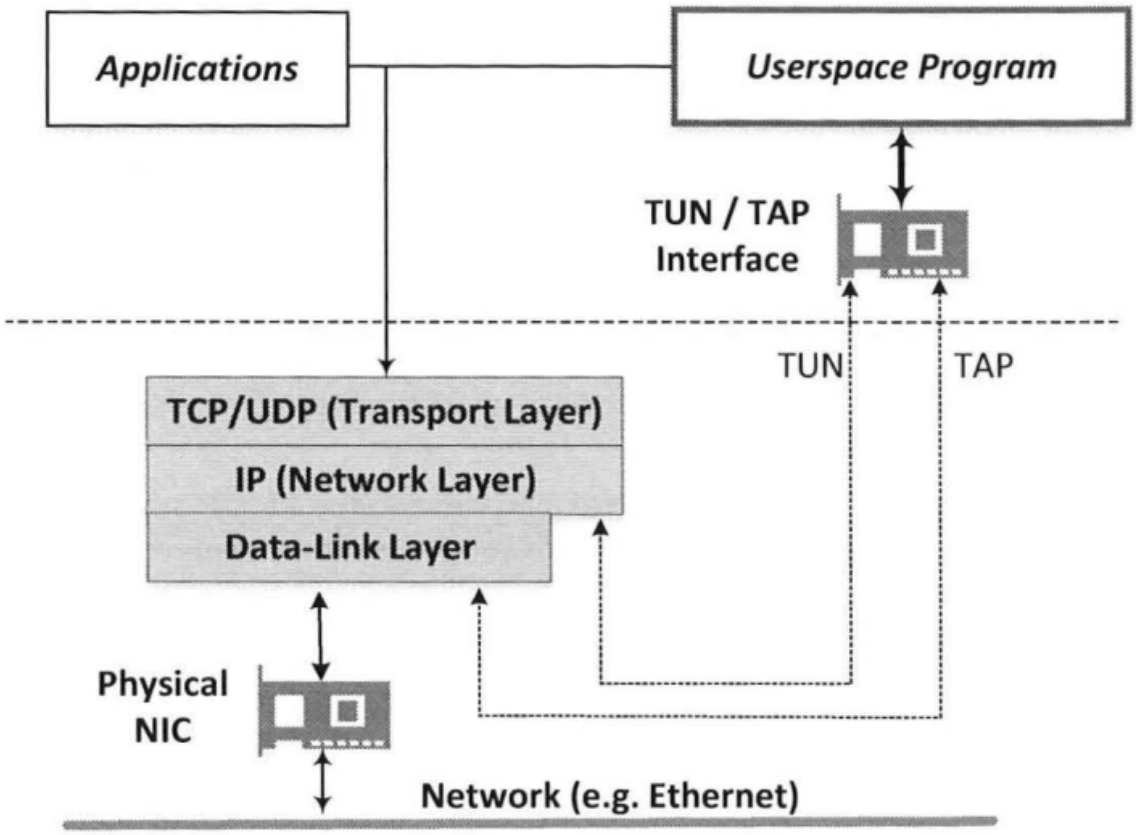
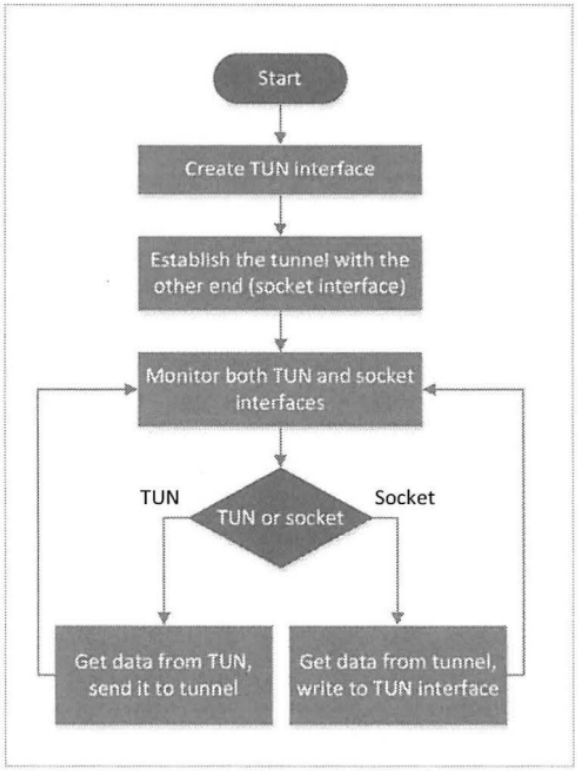
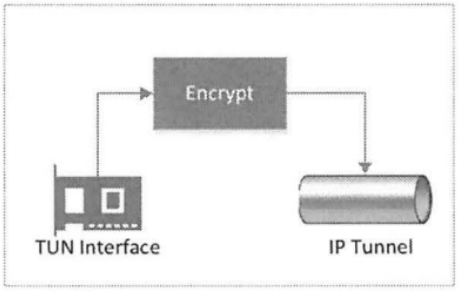


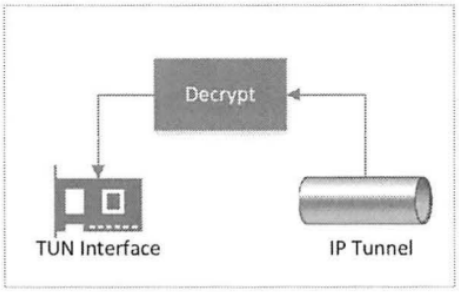
Figure 19.4: Virtual Network Interfaces



(a) The Flow of the Program



(b) From TUN Interface to Tunnel



(c) From Tunnel to TUN Interface

Bypassing Filters using VPN

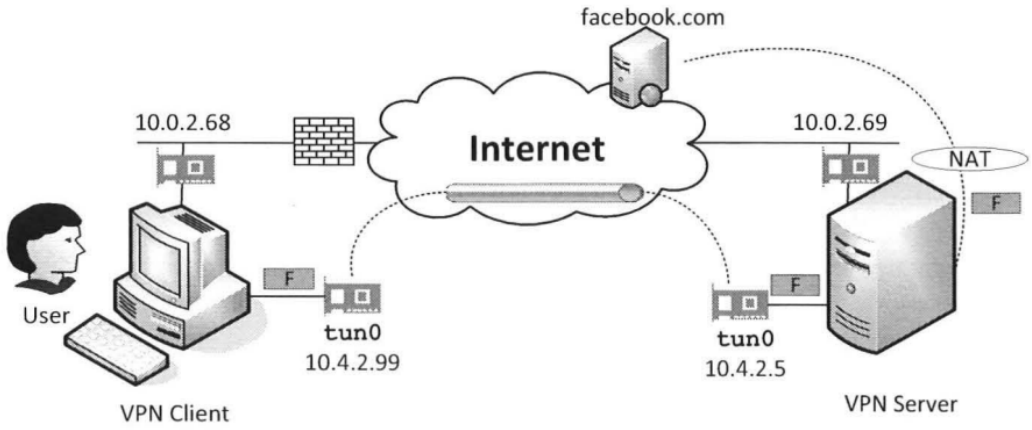


Figure 19.10: Bypassing firewall using VPN

Usinf VPN you can bypass Egress filtering

To bypass ingress filtering use NAT inside the VPN

The Heartbleed Bug and Attack

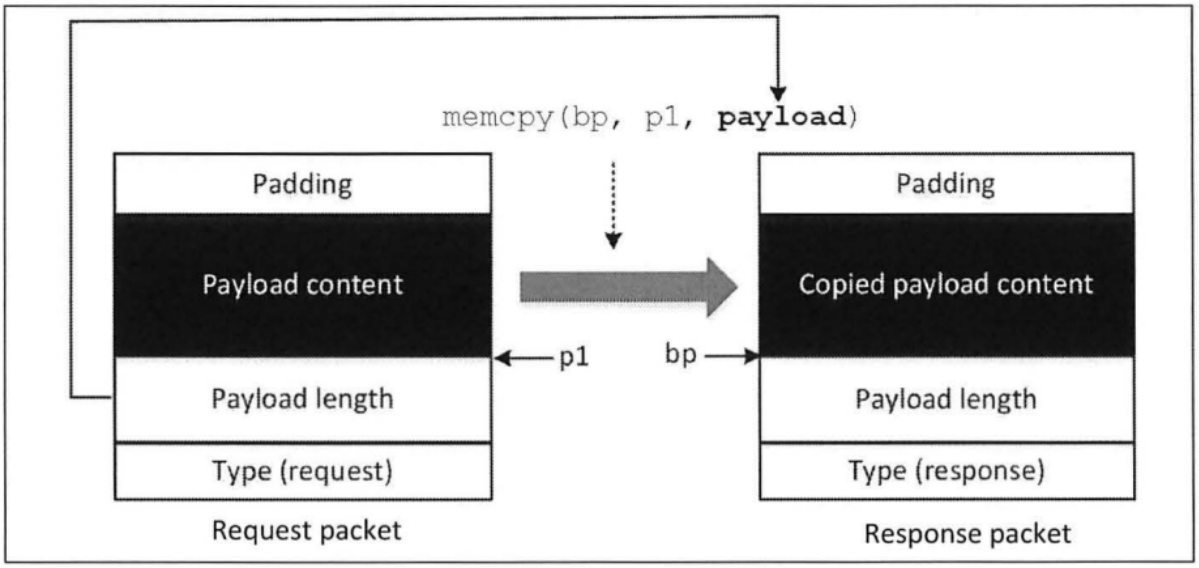


Figure 20.1: How the Heartbeat protocol copies the payload

Heartbleed is a security vulnerability in the OpenSSL implementation, affecting the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. These protocols establish secure channels between communicating applications, ensuring the protection of transmitted data. OpenSSL, being an open source project widely used on the Internet, provides a robust toolkit for TLS/SSL protocols.

The vulnerability arises from an implementation flaw in **OpenSSL's TLS/SSL heartbeat extension, designed to implement the keep-alive feature of TLS**. In normal operation, when a client and server are not actively sending data, the channel may be broken by firewalls or either side. The Heartbeat extension introduces a protocol where a sender sends a Heartbeat packet (request) to the receiver, and the receiver responds with the same payload.

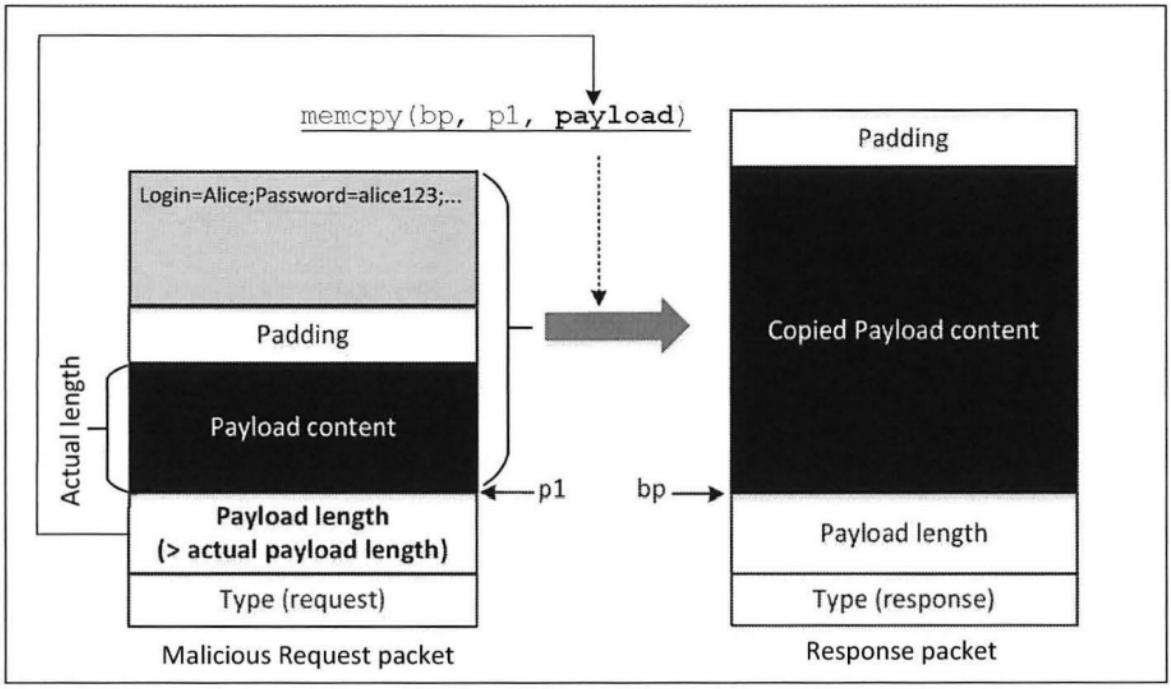


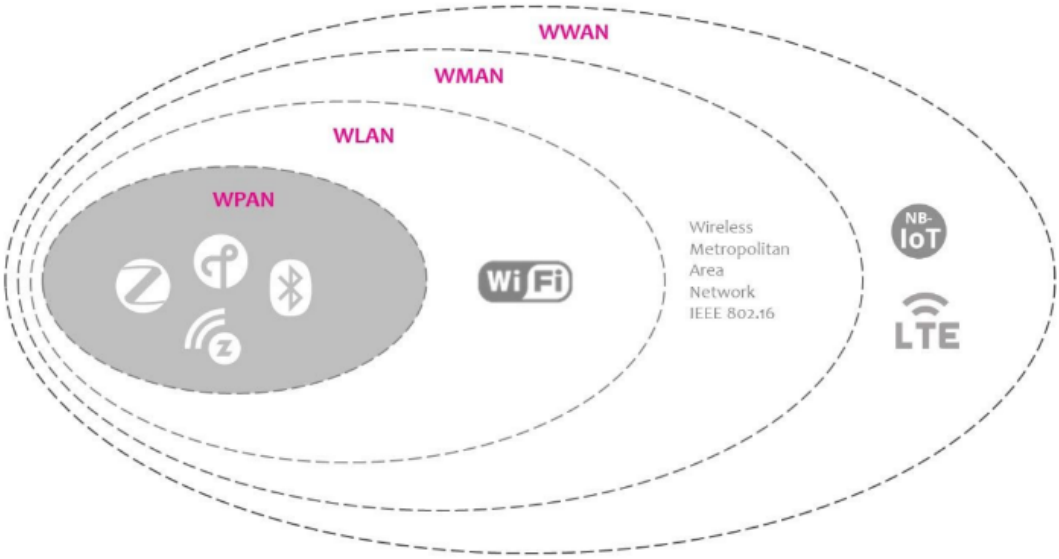
Figure 20.2: How the HeartBleed attack works

However, the flaw occurs in how the response packet is constructed. Developers assumed that the declared payload size in the packet matches the actual size, but attackers can exploit this by sending a Heartbeat request packet with a declared payload size larger than the actual payload. When the packet reaches the receiver, the memcpy() function copies more data into the response packet than exists in the request packet.

This copying extends beyond the payload region, accessing adjacent memory that may store sensitive information like passwords or credit card numbers. Essentially, attackers can use a Heartbleed attack to dump the server's memory contents, gaining unauthorized access to confidential data.

In practical terms, an attacker crafts a malicious Heartbeat request, manipulates the payload size, and sends it to a vulnerable server. The server, unaware of the discrepancy, copies extra data into the response packet, inadvertently leaking sensitive information to the attacker. To understand the real-world implications, the text suggests setting up a web server and conducting a controlled Heartbleed attack to observe and assess the severity of the vulnerability.

Wireless Network Security



Wireless Networking Technologies Overview: WWAN, WLAN, and WPAN

1. WWAN (Wireless Wide Area Network):

- **Definition:** A WWAN is a large-scale wireless network covering a vast geographic area, typically utilizing cellular network technologies such as LTE, GSM, or CDPD.
- **Purpose:** It facilitates communication between devices, often sensors, by transmitting small data packets over mobile telecommunication networks.

2. WLAN (Wireless Local Area Network):

- **Definition:** A WLAN is a flexible data communication system that employs radio waves, connecting wireless users to a wired network using wireless access points.
- **Characteristics:**
  - Backbone network may use cables.
  - Range can vary from a single room to an entire campus.
  - Technologies include Wi-Fi based on IEEE 802.11 standards.

- Easy installation without the need for extensive cabling.

3. WPAN (Wireless Personal Area Network):

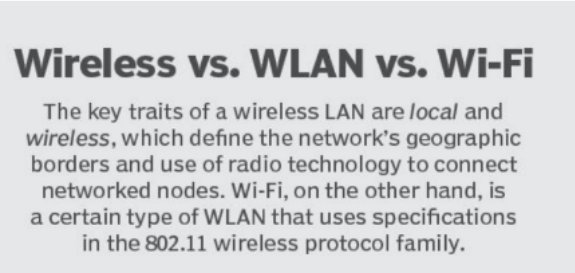
- **Definition:** A WPAN connects devices within a small area, typically within a person's reach, with a range of about 30 feet.
- **Use Cases:** Interconnecting compatible devices near a central location, such as a desk.
- **Technologies:**
  - Bluetooth (Bluetooth radio and Bluetooth Low Energy)
  - ZigBee
  - Z-Wave
  - Thread

Evolution of WLAN:

- **802.11 Standard:** Introduced in 1997, operating at 2.4 GHz with a throughput of 1 to 2 Mbps.
- **Current Standard (IEEE 802.11B):** Introduced in the early 2000s, operates at 2.4 GHz with a maximum speed of 11 Mbps.
- **Advantages of WLAN:**
  - Simplified installation, eliminating the need for extensive cabling.
  - Utilizes various wireless technologies, including Wi-Fi.

Wi-Fi (Wireless Fidelity):

- **Definition:** Wi-Fi is a trademark name used to brand WLAN devices adhering to IEEE 802.11 standards.
- **Technology Basis:** **Devices with the Wi-Fi trademark operate based on IEEE 802.11 standards.**
- **Usage:** Commonly associated with wireless internet access in homes, businesses, and public places.



Evolution of Wi-Fi Security Standards: WEP, WPA, WPA2, and WPA3

1. WEP (Wired Equivalent Privacy):

- **Introduction:** WEP was the initial security protocol for Wi-Fi networks.
- **Issues:** Vulnerable to various attacks, weak encryption.

2. WPA (Wi-Fi Protected Access):

- **Introduction:** Wi-Fi Alliance introduced WPA in October 2002.
- **Nature:** Subset of draft IEEE 802.11i requirements.
- **Limitation:** Unable to support computationally intensive AES encryption.

3. WPA2 (Wi-Fi Protected Access 2):

- **Timeline:** Introduced with the ratification of IEEE 802.11i in June 2004.
- **Features:**
  - Interoperable equipment supporting IEEE 802.11i requirements.
  - Stronger security with support for AES encryption.
- **Certification:** Wi-Fi Alliance initiated WPA2 certification after IEEE 802.11i ratification.

4. WPA3 (Wi-Fi Protected Access 3):

- **Introduction:** Announced by Wi-Fi Alliance in 2018.
- **Purpose:** Designed as a replacement for WPA2.
- **Improvements:**
  - Enhanced security protocols.
  - Protection against offline dictionary attacks.
  - Individualized data encryption for personal and open networks.

Security Protocol Evolution Summary:

- **WEP: Initial but insecure.**
- **WPA: Introduced as a subset with limitations.**
- **WPA2: Ratified with stronger security features, including AES.**
- **WPA3: Announced as a replacement with enhanced security measures.**

Wireless Networking Components and IEEE 802.11 WLAN Overview:

1. Wireless Networking Components:

- **Wireless Client/Station:** Devices like laptops, tablets, cell phones, Bluetooth devices.
- **Access Point:** Cell towers, Wi-Fi hotspots, wireless routers.
- **Transmission Medium:** Carries signals.

2. IEEE 802.11 WLAN Components:

- **STA (Stations):**
  - *Types:* Client or AP (Access Point).
- **BSS (Basic Service Set):**
  - *Definition:* Group of stations communicating together.
- **ESS (Extended Service Set):**
  - *Definition:* Set of connected BSS.
- **DS (Distributed System):**

- *Definition:* Connects APs in ESS.

3. Stations (STA):

- *Types:* Wireless Access Point (WAP), Clients (workstations, computers, laptops, printers, smartphones).
- *Interface:* Each station has a wireless network interface controller.

4. Service Set:

- *Definition:* Group of wireless network devices sharing a Service Set Identifier (SSID).
- *Types:* Basic Service Set (BSS) or Extended Service Set (ESS).

5. SSID (Service Set Identifier):

- *Identification:* Assigned by a network administrator.
- *Broadcast:* Usually broadcasted by wireless access points.
- *Usage:* WLAN users select an SSID when connecting to a network.

6. BSSID (Basic Service Set Identifier):

- *Identification:* MAC address of the access point.
- *Tracking:* Identifies access points and their associated clients.
- *Dynamic:* Can change as users move within network coverage.

7. IEEE 802.11 WLAN Components (Advanced):

- **Basic Service Set (BSS):**
  - *Types:* Independent BSS (ad hoc) and Infrastructure BSS.
- **Wireless Network Architectural Modes:**
  - *Modes:* Infrastructure mode and Ad-hoc mode (Independent mode).
- **Extended Service Set (ESS):**
  - *Definition:* Set of all connected BSS.
- **Distribution System (DS):**
  - *Function:* Connects access points in ESS.

8. Wireless Network Modes:

- **Infrastructure Mode:**
  - *Connection:* Clients connect to a central device (Access Point).
- **Ad-hoc Mode (IBSS):**
  - *Connection:* Clients connect directly to each other.
  - *Advantage:* Rapid deployment without existing infrastructure.

IEEE 802.11 is a set of standards for implementing wireless local area networking (WLAN) communication. Commonly known as Wi-Fi, it defines how devices communicate wirelessly within a network. Key aspects include:

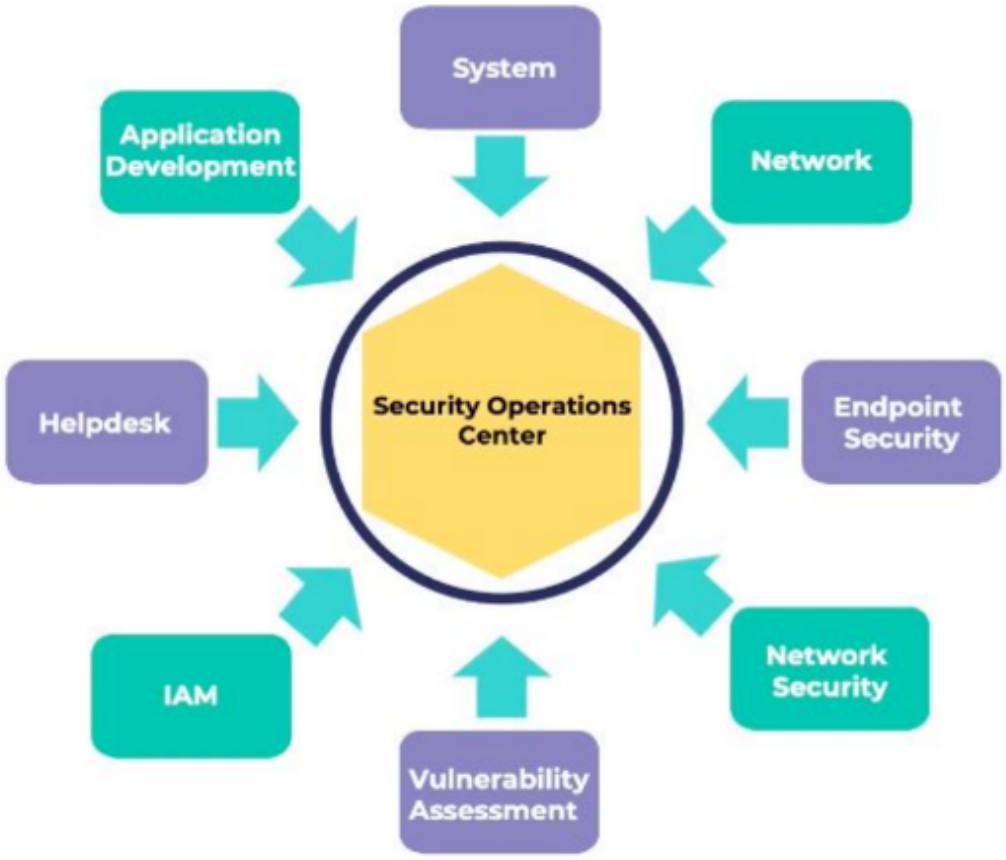
1. **Standards:** IEEE 802.11 has various amendments, each denoted by letters (e.g., 802.11b, 802.11n, 802.11ac), defining different capabilities and enhancements.
2. **Components:**
   - **STA (Station):** Devices like laptops or phones.
   - **BSS (Basic Service Set):** A group of STAs communicating.
   - **ESS (Extended Service Set):** Multiple BSS connected together.
   - **DS (Distribution System):** Connects different parts of an ESS.
3. **Modes:**
   - **Infrastructure Mode:** Devices connect through an access point.
   - **Ad-hoc Mode:** Devices connect directly to each other.
4. **Identifiers:**
   - **SSID (Service Set Identifier):** Network name.
   - **BSSID (Basic Service Set Identifier):** MAC address identifying an access point.
5. **Architectural Concepts:**

- **Service Set:** A group of devices sharing the same network.
- **Distribution System:** Connects access points within an Extended Service Set.

6. **Evolution:**
    - **Amendments:** Updates and improvements to the standard.
    - **Wi-Fi Alliance:** Ensures interoperability and certifies devices.
    - **Current Standards:** Include Wi-Fi 6 (802.11ax) and Wi-Fi 6E (802.11ax extended to 6 GHz).

IEEE 802.11 provides the foundation for wireless communication, enabling the widespread use of Wi-Fi for various applications, from home networks to public hotspots.

Security Operations Center (SOC)



Security Operations Centers (SOC) play a crucial role in managing and responding to cybersecurity threats. Here are key activities and objectives associated with SOC operations:

SOC Operations:

1. **Collects logs from Available resources:** Gathers data from various sources such as firewalls, IDS/IPS, proxies, applications, and more.
2. **Preparation and preventive maintenance:** Conducts routine maintenance, incident response planning, testing, and stays current with cybersecurity developments.
3. **Continuous and proactive monitoring:** Monitors security events around the clock, analyzing and correlating millions of daily events.
4. **Alert ranking and management:** Prioritizes and manages alerts to focus on critical threats.

5. **Threat response:** Responds to and mitigates identified threats promptly.
6. **Recovery and remediation:** Implements recovery plans and remediates vulnerabilities after incidents.
7. **Log management:** Manages and analyzes logs for security insights.
8. **Root cause investigation:** Investigates the root causes of security incidents.
9. **Security refinement and improvement:** Constantly refines security measures based on incident insights.
10. **Compliance management:** Ensures compliance with regulatory requirements.

SOC Objectives:

1. **Preparation, planning, and prevention:**
    - Asset inventory.
    - Routine maintenance and preparation.
    - Incident response planning.
    - Regular testing.
    - Staying current.
2. **Monitoring, detection, and response:**
    - Continuous, around-the-clock security monitoring.
    - Log management.
    - Threat detection.
    - Incident response.
3. **Recovery, refinement, and compliance:**
    - Recovery and remediation.
    - Post-mortem and refinement.
    - Compliance management.

Key Objectives for SOC:

- Manages and coordinates the response to cyber threats and incidents.

- Monitors the cybersecurity posture and reports deficiencies.
- Coordinates with regulatory bodies.
- Performs threat and vulnerability analysis.
- Maintains an internal database of cybersecurity incidents.
- Provides alerts and notifications of general and specific threats.
- Provides regular reporting to management and cyber incident responders.

Additional Objectives:

- Reducing response time for security incidents.
- Proactive security monitoring based on predefined security metrics.
- Raising awareness of information security.
- Correlating system, application, network, server, and security logs consistently.
- Automating compliance requirements, including vulnerability assessment and risk management.
- Integrating change control into the SOC process.
- Identifying security attack vectors and classifying incidents.
- Building disaster recovery plans.
- Constructing comprehensive reporting dashboards aligned with security metrics.
- Collaborating with national CERT (Computer Emergency Response Team).
- Aligning SOC processes with existing ISO27001 security policies.
- Building physical and virtual teams for 24×7 monitoring.
- Developing forensics capabilities for incident reconstruction.
- Proactively monitoring network and security infrastructure devices.

SOC Team

SOC Manager

L3/SOC Lead

L2 Security Analyst

L1 Security Analyst

Modern Day SOC roles

L1 Security Analyst

- 24/7 Eyes-on-Glass monitoring
- Analysis of triggered alerts (usually following a Playbook)
- Raising tickets for validated incidents
- Follow-up with incident response team for remediation
- Drafting shift hand-overs
- Assist L2/L3 in reporting

L2 Security Analyst

- Deep dive analysis of escalated alerts
- Assist in Incident Remediation
- Assist L1 in alert analysis
- Maintaining and improving SOPs and processes
- Troubleshoot basic SIEM issues

SOC Lead

1. Installing, updating, upgrading SIEM solution.
2. On-boarding log sources and working on log source issues.
3. Create and fine-tune content in SIEM – Correlation Rules, Dashboards, Reports, Lists etc.
4. Interact with SIEM vendor TAC (support) to fix any issues with SIEM.
5. Install, Manage and build content in SIEM.
6. Mentor L1 and L2 security analyst.
7. Assist in analysis that requires involvement of multiple teams.
8. Evaluate new solutions for SOC team.
9. Create Playbooks for all alerts.
10. Schedule shift rooster.

SOC Manager

1. Define the scope, vision and direction for the SOC team.
2. Supervise the team, provide technical guidance, and manage financial activities.
3. Oversee the activity of the SOC team members, including hiring, training, and assessing staff.
4. Develop and Improve processes and procedures for SOC team.
5. Ensure compliance to Service Level Agreements (SLA), process adherence.
6. Create compliance reports, support the audit process, measure SOC performance metrics.
7. Vendor Management.
8. Report on security operations to business leaders.

Threat Intelligence Brief Description:

Definition:

Threat intelligence is information gathered, analyzed, and interpreted to understand potential cybersecurity threats. It involves collecting data on cyber threats, assessing their credibility, and providing actionable insights to enhance an organization's cybersecurity posture.

Key Elements:

1. **Data Collection:**
   - Gathering information from diverse sources such as the dark web, government agencies, and cybersecurity vendors.
2. **Analysis and Interpretation:**
   - Analyzing data to identify patterns and trends.
   - Converting raw data into actionable insights.
3. **Information Sharing:**
   - Collaborating with others to share threat intelligence.

- Participating in Information Sharing and Analysis Centers (ISACs) or Organizations (ISAOs).

4. **Proactive Measures:**
    - Using threat intelligence to implement proactive cybersecurity measures.
    - Adjusting security policies and enhancing incident response plans.

Benefits:

1. **Proactive Defense:**
    - Anticipating and defending against emerging threats.
2. **Improved Incident Response:**
    - Enhancing the speed and effectiveness of incident response.
3. **Informed Decision-Making:**
    - Providing decision-makers with valuable insights.
4. **Reduced Impact of Attacks:**
    - Minimizing the potential impact of cyber attacks.
5. **Collaboration:**
    - Facilitating collaboration between organizations.

SOC Workflow

A Security Operations Center (SOC) plays a crucial role in an organization's cybersecurity strategy. The SOC workflow encompasses a series of processes designed to identify, prevent, detect, respond to, and recover from security threats. Below is an overview of key SOC processes:

1. **Threat Identification:**

- **Objective:** Identify potential threats and vulnerabilities.
- **Activities:**
    - Continuous monitoring of network and system activities.

- Analyzing logs and alerts to identify anomalies.
- Utilizing threat intelligence feeds.

2. **Threat Detection:**

- **Objective:** Detect security incidents promptly.
- **Activities:**
  - Real-time monitoring of security alerts.
  - Conducting correlation and analysis of security events.
  - Utilizing security information and event management (SIEM) systems.

3**. Threat Prevention:**

- **Objective:** Implement measures to prevent identified threats.
- **Activities:**
  - Deploying firewalls, intrusion prevention systems (IPS), and other preventive tools.
  - Implementing security policies and access controls.

4**. Incident Response:**

- **Objective:** Rapidly respond to and mitigate security incidents.
- **Activities:**
  - Activating incident response plans.
  - Containing and isolating affected systems.
  - Conducting forensics analysis to understand the scope.

5. Investigation and Analysis:

- **Objective:** Understand the nature and impact of security incidents.
- **Activities:**
  - In-depth analysis of incident details.
  - Correlating data to identify the root cause.
  - Collaborating with internal and external stakeholders.

6. Communication:

- **Objective:** Effective communication internally and externally.
- **Activities:**
  - Notifying relevant stakeholders about security incidents.
  - Collaborating with law enforcement, if necessary.
  - Keeping leadership and teams informed.

7. Recovery:

- **Objective:** Restore affected systems to normal operation.
- **Activities:**
  - Implementing recovery plans.
  - Applying patches and updates.
  - Validating system integrity.

8. Documentation:

- **Objective:** Maintain detailed records for future reference and analysis.
- **Activities:**
  - Documenting incident details, responses, and resolutions.
  - Creating post-incident reports for analysis and improvement.

9. Continuous Improvement:

- **Objective:** Enhance SOC capabilities based on lessons learned.
- **Activities:**
  - Conducting post-incident reviews.
  - Updating incident response plans.
  - Implementing new technologies and strategies.

10. Training and Awareness:

- **Objective:** Keep SOC teams updated on the latest threats and technologies.

- **Activities:**
  - Providing ongoing training for SOC analysts.
  - Conducting simulated exercises for skill reinforcement.

SOC Deployment Models:

Security Operations Centers (SOCs) are deployed using different models to meet the unique needs of organizations. Here are three common SOC deployment models:

1. **In-House Deployment:**
   - **Pros:**
     - Dedicated Staff: Internal team with in-depth knowledge of the organization's environment.
     - Better Environment Understanding: Staff understands the intricacies of the internal network.
     - Efficient Correlation: Easier collaboration between internal groups.
     - Local Log Storage: Logs are stored locally, providing control over data.
   - **Cons:**
     - Larger Up-Front Investment: Requires significant initial capital investment.
     - ROI Pressure: Internal teams may face pressure to demonstrate return on investment.
     - Talent Challenges: Finding and retaining competent staff can be challenging.
2. **Managed Deployment:**
   - **Pros:**
     - Quick Start: Rapid deployment with reduced capital expenditure.

    - Staff Efficiency: Requires fewer internal staff, including for managing security appliances.
- **Cons:**
    - Limited Environment Knowledge: External team may lack a deep understanding of the organization's environment.
    - Data Mishandling: External handling of sensitive data and security appliances.
    - Archiving Challenges: Lack of archiving capabilities for historical data.

3. **Hybrid Deployment:**
    - **Pros:**
        - Sufficient Visibility: Balances centralized and distributed approaches for comprehensive visibility.
        - Quick Detection and Response: Achieves quicker detection and response times.
        - Reduced Backlog: Helps in managing and reducing incident backlog.
        - Intel Sharing: Facilitates sharing threat intelligence.
    - **Cons:**
        - Costly: Can be more expensive due to third-party involvement.
        - External Handling: Involves external parties in critical security operations.

Security Information and Event Management (SIEM)

SIEM is about looking at what’s happening on your network through a larger lens than can be provided via any one security control or information source.

1. D**efinition:**
    - SIEM is a comprehensive platform designed to manage security incidents effectively.
    - **It involves the collection of system logs and event data from various IT components across an organization's environment.**
    - **The primary goal is to identify unusual or suspicious activities that may indicate a security threat.**
    - SIEM reports real-time alerts when it detects potentially harmful events.
2. **Terminology Origins:**
    - SIEM incorporates various terms and concepts:
        - LMS: Log Management System
        - SIM: Security Information Management
        - SLM/SEM: Security Log/Event Management
        - SEC: Security Event Correlation
    - Over time, SIEM has become the generalized term for managing information generated from security controls and infrastructure.
3. **How SIEM Works:**
    - **SIEM solutions collect and store logs and event data from diverse components within an enterprise network.**
    - **Event Story Creation: Utilizes threat intelligence, predefined rules, and advanced analytics to detect security incidents in real-time.**
    - **Alert Categorization: Classifies alerts into categories like malware, failed logins, successful logins, and other potentially harmful activities.**
    - **Reporting and Response: Generates reports and facilitates a timely response to potential security incidents.**
    - **Performs SIM (Security Information Management) and SEM (Security Event Management) functions.**

4. **Common Uses of SIEM:**

- **Security Monitoring:** Continuous monitoring of security events to identify anomalies.
- **Advanced Threat Detection:** Utilizes sophisticated methods to detect and respond to advanced security threats.
- **Forensics and Incident Response:** Aids in investigating incidents and responding effectively.
- **Compliance Auditing and Reporting:** Supports organizations in meeting regulatory compliance requirements through auditing and reporting capabilities.

SIEM Architecture

1. Log Management Process:

- **Data Collection (Log Aggregation):** Gathers data from various sources, including security controls, infrastructure components, and business information.
- **Log Processing:**
  - Log Parsing: Converts logs into a standardized format for easier analysis.
  - Log Normalization and Categorization: Ensures consistency in log formats.
  - Log Enrichment: Adds contextual information to enhance log data.
  - Log Indexing: Organizes logs for efficient storage and retrieval.
- **Data Management:**
- **Log Monitoring:**
- **Log Correlation:**
- **Log Retention (Log Filtering, Summarization):** Manages the retention and storage of logs based on filtering and summarization.

2. Log Sources:

- Security Controls:
  - Intrusion detection
  - Endpoint security (antivirus, etc.)
  - Data loss prevention
  - VPN concentrators
  - Web filters
  - Honeypots
  - Firewalls
- Infrastructure:
  - Routers
  - Switches
  - Domain controllers
  - Wireless access points
  - Application servers
  - Databases
  - Intranet applications
- Infrastructure Information:
  - Configuration
  - Locations
  - Owners
  - Network maps
  - Vulnerability reports
  - Software inventory
- Business Information:
  - Business process mappings

- Points of contact
- Partner information

3. Log Parsing:

- Log entries often vary in format, making standardized parsing necessary.
- Normalization involves breaking down log messages into a consistent, normalized format.
- Enables SIEM to interpret logs from different devices.

4. Event Correlation:

- Correlation matches events from various systems to identify patterns and behaviors.
- Combines events from different sources to uncover hidden patterns.
- Matches events against business-specific information.
- Automates detection of unusual network activities.

5. Searches, Pivoting, and Cross-Correlation:

- Normalized log entries allow for effective search across logs from diverse devices.
- Correlates events across different devices and time periods.
- Supports automated correlation based on specific criteria.
- Enables the creation of summarizations and reports for analysis.

6. SIEM Deployment Models:

- Traditional SIEM
- Cloud SIEM, Self-Managed
- Self-Hosted, Hybrid-Managed
- SIEM as a Service

These deployment models cater to various organizational needs, offering flexibility and scalability in SIEM implementation.