# Report On Common Network Security Threats

The contemporary digital landscape is characterized by an escalating array of cyber threats that compromise the foundational pillars of information security: confidentiality, integrity, and availability. This report provides a detailed analysis of three pivotal network security threats—Denial-of-Service (DoS), Man-in-the-Middle (MITM), and spoofing. An examination of their mechanics and real-world impacts reveals that while each threat has a distinct objective, they are often interconnected, with spoofing frequently serving as a foundational vector for more complex DoS and MITM campaigns. The analysis demonstrates that a resilient defense posture cannot rely on isolated countermeasures but must adopt a multi-layered, proactive strategy that combines robust technical controls with continuous monitoring and human-centric security awareness.

A high-level comparison of these threats is provided in the table below to frame the subsequent discussion.

| Threat | Primary Objective | Core Technique | Primary Impacted CIA Principle |
| --- | --- | --- | --- |
| **Denial-of-Service (DoS)** | Service Disruption | Traffic Overwhelming / Resource Exhaustion | Availability |
| **Man-in-the-Middle (MITM)** | Data Interception & Alteration | Communication Interception | Confidentiality & Integrity |
| **Spoofing** | Impersonation & Deception | Falsified Identity | Confidentiality & Integrity |

## 1. Foundational Concepts in Network Security

To comprehend the nature of network security threats, it is necessary to first understand the core principles they are designed to subvert. The field of information security is fundamentally defined by the **CIA triad**—Confidentiality, Integrity, and Availability—a model that forms the basis for the development of secure systems and the identification of vulnerabilities.

* **Confidentiality** ensures that information remains private and is disclosed only to authorized entities. This is achieved by controlling access and protecting data from unauthorized viewing, whether intentional or accidental.
* **Integrity** refers to the assurance that data has not been improperly modified or destroyed. It involves guarding against unauthorized changes to information to ensure its authenticity and non-repudiation.
* **Availability** guarantees that systems, data, and services are accessible to legitimate users when they are needed. This is a crucial principle for any organization that provides direct services to customers, as availability can be disrupted by both natural events and cyberattacks.

The relationship between vulnerabilities and threats is a central theme in cybersecurity. A **vulnerability** is a weakness in a system's design or a human-related flaw, such as outdated software or an employee susceptible to deception.

**Threat** is a malicious event that exploits a vulnerability to cause harm.The potential for loss, or

**risk**, can be understood as a function of the threat and the vulnerability, but this calculation must also account for the safeguards in place to mitigate potential damage.A proactive approach to network security, therefore, is an active process of risk management, where the implementation of robust safeguards directly reduces the potential for loss even when threats and vulnerabilities are present.

## 2. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks

### 2.1. Defining the Threat

A **Denial-of-Service (DoS) attack** is a cyberattack that aims to make an online service unavailable by overwhelming it with an excessive volume of traffic or resource requests.5 This attack is characteristically launched from a single computer.In contrast, a

**Distributed Denial-of-Service (DDoS) attack** originates from multiple, geographically dispersed sources simultaneously, making it far more effective and difficult to defend against.These multiple sources typically form a **botnet**, a network of compromised computers or devices, referred to as "bots" or "zombies," that are under the attacker's remote command 2.2. Attack Mechanics and Vectors

DDoS attacks are highly diverse, with thousands of vectors that can be broadly categorized :

* **Volumetric Attacks:** The most common type, these attacks aim to saturate the target's network bandwidth with a massive flood of data. A notable vector,  
  **SYN flooding**, specifically exploits the TCP three-way handshake. The attacker sends a high volume of SYN packets to a server but never responds to the SYN-ACK packets, leaving the server with open connections that consume its resources and prevent legitimate users from connecting. Other examples include UDP and ICMP floods.
* **Protocol-Based Attacks:** These attacks target weaknesses in the network (Layer 3) and transport (Layer 4) layers of the OSI model, aiming to exhaust server resources beyond simple bandwidth.  
  **Slowloris attack** is a classic example, where an attacker sends slow, partial HTTP request headers to keep connections open for an extended period, which exhausts the server's connection resources.
* **Application-Layer Attacks:** These attacks target specific application resources like servers or CPUs with a high volume of requests, aiming to make a service unresponsive.  
  **HTTP/S Flood** imposes high requests per second on a server to keep it busy and prevent it from serving legitimate users.

### 2.3. Impact Analysis

The primary impact of a successful DDoS attack is a severe compromise of service availability.For an organization, this can lead to significant financial losses due to interrupted transactions, decreased customer engagement, and loss of productivity. Beyond financial consequences, these attacks can cause severe reputational damage and erode customer trust in an organization's ability to provide reliable services.In some cases, DDoS attacks are used as a distraction to draw security teams' attention away while attackers attempt other forms of cyber intrusion, such as data exfiltration or fraud.

### 2.4. Real-World Case Studies

* **The Dyn DDoS Attack (2016):** This landmark attack, peaking at 1 Tbps, targeted the DNS provider Dyn and disrupted services for major platforms like Twitter, Reddit, and Netflix across Europe and North America.The attack was executed using the Mirai botnet, which leveraged vulnerable Internet of Things (IoT) devices with weak security to launch a massive, multi-vector volumetric barrage of UDP, LDAP reflection, DNS reflection, NTP reflection, and UDP fragmentation attacks.
* **The GitHub DDoS Attack (2018):** GitHub was hit with a record-setting 1.35 Tbps attack that exploited a vulnerability in the memcached caching system. The attack used a UDP
* amplification technique where a small request (15 bytes) could trigger a massive response (up to 750kB), an amplification factor of over 51,200x. The attack demonstrated a clear progression in attacker methodology from raw brute force to achieving maximum impact with minimal resources. GitHub's response, which involved routing traffic through a cloud-based scrubbing center, successfully mitigated the attack within 15 minutes.

| Attack Vector | Description | Impact | Mitigation Strategy |
| --- | --- | --- | --- |
| **Volumetric Attacks** | Overwhelming target bandwidth with high-volume traffic (e.g., UDP/ICMP floods). | Saturates network infrastructure, causing service unavailability. | Increase bandwidth, rate limiting, BGP Anycast, traffic scrubbing centers. |
| **SYN Flood** | Bombarding a server with SYN requests without completing the TCP handshake. | Fills server's connection table, preventing new, legitimate connections. | TCP SYN cookies, server configuration to clear half-open connections faster. |
| **Slowloris Attack** | Sending small, partial HTTP headers to keep connections open indefinitely. | Exhausts server's connection resources, leaving no room for legitimate traffic. | Rate limiting, connection timeouts, specialized application-layer firewalls. |
| **DNS Amplification** | Using spoofed DNS queries to trigger large DNS responses to a victim. | Magnifies attack traffic volume, overwhelming the victim's resources. | DNSSEC, source port randomization, DDoS scrubbing services. |

## 3. Man-in-the-Middle (MITM) Attacks

### 3.1. Defining the Threat

A **Man-in-the-Middle (MITM) attack** is a cyberattack in which a malicious actor secretly intercepts and potentially alters communications between two parties without their knowledge. The attacker inserts themselves into the communication channel, intercepting sensitive data such as credit card numbers, login credentials, or other private information.

### 3.2. Attack Mechanics and Vectors

* **SSL Stripping:** This is a sophisticated MITM technique that downgrades a secure HTTPS connection to an unencrypted HTTP connection. This is achieved by exploiting the fact that most internet connections initially start as HTTP before being redirected to HTTPS. The attacker intercepts this initial request, establishes a secure HTTPS connection with the legitimate server on behalf of the user, and maintains an insecure HTTP connection with the user, all without the user's knowledge.
* **ARP and DNS Spoofing:** These are foundational vectors for enabling MITM attacks. **ARP spoofing** involves linking an attacker's MAC address to a legitimate IP address on a local network, tricking devices into sending traffic intended for a host (like a router) to the attacker's machine.  
  **DNS spoofing**, also known as DNS cache poisoning, works by corrupting DNS records to redirect a user's traffic to a fraudulent website controlled by the attacker. A user may type in the correct URL but be redirected to a fake site that appears legitimate, where the attacker can then steal their login credentials.
* **Wi-Fi Eavesdropping:** Public Wi-Fi hotspots, which often have fewer security protocols than home or work networks, are a common attack vector for MITM attacks. Attackers can either compromise a public router to intercept traffic or create a malicious, fake public Wi-Fi network to lure unsuspecting users and harvest their personal data.
* **Session Hijacking:** This attack exploits session tokens, which are temporary pieces of data used to identify a user who has logged into a website.An attacker who intercepts a valid session cookie can impersonate the legitimate user, gaining unauthorized access to their account without needing a password.

### 3.3. Impact Analysis

The primary impact of an MITM attack is the compromise of sensitive data in transit. This can lead to severe consequences, including financial fraud, identity theft, and the theft of intellectual property. Beyond data theft, the ability to alter communications can lead to a user or organization taking a completely different set of actions than intended.

## 4. Spoofing Attacks: The Foundation of Deception

### 4.1. Defining the Threat

Spoofing is a deceptive technique in which a malicious actor impersonates a trusted source—such as a website, email address, or network device—to deceive a victim and gain unauthorized access or steal data. It is a foundational tactic in social engineering attacks, as it exploits human psychology and the victim's inherent trust in a known entity.

### 4.2. Key Spoofing Types and Their Roles

**IP Spoofing:** This involves sending data packets with a forged source IP address to disguise the attacker's true identity or to impersonate a legitimate host.

* **DNS Spoofing:** This involves modifying DNS records to redirect users to a fraudulent website that is often a replica of a legitimate site. This attack can be a direct enabler for phishing and MITM, as it ensures the victim believes they are interacting with a legitimate service while their data is being funneled to the attacker.
* **Email Spoofing:** This is one of the most common forms of social engineering, where an email sender's address is forged to make a message appear as though it came from a trusted source. It is a central component of phishing campaigns, as it tricks recipients into opening malicious links, downloading malware, or revealing sensitive information.

### 4.3. The Interconnected Nature of Threats

A nuanced analysis of network security threats reveals that DoS, MITM, and spoofing are rarely isolated events but are instead deeply interconnected and often used in a blended, multi-stage approach. Spoofing is not just a threat on its own but also a foundational vector that enables more complex and damaging attacks.

* For instance, IP spoofing is critical to the success of many DDoS attacks. By forging the source IP address, attackers can hide their identity and launch reflection/amplification attacks that amplify their impact and direct the flood of responses toward a victim.29 Without spoofing, it would be far simpler to trace the attack's origin and block the malicious traffic at the source.
* Similarly, DNS and ARP spoofing are explicit, step-by-step components of many MITM attacks. The attacker leverages these spoofing techniques to trick a user's device into sending network traffic to the attacker's machine, thereby establishing the crucial "man-in-the-middle" position.

This interdependency means that a defense strategy that only focuses on mitigating a single threat type in isolation is fundamentally flawed. Modern attacks are designed to be complex and multi-vector, complicating both detection and mitigation.

## 5. Multi-Layered Mitigation and Proactive Defense Strategies

Effective defense against these interconnected threats requires a multi-layered approach that secures the network, data, and the human element. The most resilient security postures do not simply react to threats but actively manage risk by anticipating and preventing them.

### 5.1. Technical Countermeasures

**Network Infrastructure Hardening:** This involves reinforcing a network's capacity and defenses to withstand attacks. Key measures include increasing bandwidth, deploying firewalls and Intrusion Prevention Systems (IPS) to filter malicious traffic, and using packet filtering to identify IP inconsistencies that may indicate a spoofing attack.

**Data and Communication Encryption:** Protecting data in transit is paramount. This includes using Virtual Private Networks (VPNs) on public networks and ensuring all public-facing services use HTTPS. For protection against SSL stripping, the implementation of  
**HTTP Strict Transport Security (HSTS)** is critical, as it forces the browser to always use a secure HTTPS connection, blocking any attempts to fall back to an unencrypted HTTP connection.

**Authentication Controls:** Strong, unique passwords and Multi-Factor Authentication (MFA) are essential to prevent credential theft and unauthorized access. MFA requires users to provide a second form of verification, greatly reducing the risk of a successful attack even if a password is stolen.

### 5.2. Proactive and Cloud-Based Mitigation

For large-scale, hyper-volumetric attacks like DDoS, on-premise defenses are often insufficient. Cloud-based solutions provide a scalable and robust defense.

* **DDoS Traffic Scrubbing:** Cloud-based solutions employ "traffic scrubbing centers," which are specialized data centers designed to analyze and filter out malicious traffic before it reaches the target network.
* **BGP Anycast Routing:** This routing technique advertises the same IP address from multiple locations, distributing incoming traffic across a wider surface area. In the event of a DDoS attack, this allows high volumes of traffic to be rerouted to multiple scrubbing centers, absorbing the attack's impact. GitHub's rapid defense against the 2018 attack was a textbook example of leveraging this type of automated, cloud-based solution to minimize service disruption.

### 5.3. Organizational and Human-Centric Defenses

Technology alone is not a sufficient defense. The human element remains a significant vulnerability, particularly for threats like spoofing that rely on deception.

* **Security Awareness Training:** Employees are the first line of defense against social engineering and phishing attacks that often use spoofing as a vector. Training should focus on recognizing suspicious links, identifying malicious emails, and understanding the risks associated with unsecured public Wi-Fi.
* **Adopting a Zero-Trust Framework:** A zero-trust security framework assumes no user or device can be trusted by default, regardless of their location. All access must be continuously validated, which helps to mitigate the impact of compromised credentials and devices and minimizes the risk of a successful MITM or spoofing attack.

| Attack Vector | Goal | Technical Mitigation Measures | Human-Centric Countermeasures |
| --- | --- | --- | --- |
| **Email Spoofing** | Phishing, Malware Delivery | Email authentication protocols (SPF, DKIM, DMARC), anti-spoofing software. | Security awareness training to spot suspicious headers and links, hanging up and calling back for sensitive requests. |
| **DNS Spoofing** | Credential Theft, Malware Distribution | DNSSEC, trusted DNS servers, Intrusion Detection Systems (IDS). | Verifying URLs before clicking, typing URLs directly into the browser. |
| **SSL Stripping** | Data Interception | HTTP Strict Transport Security (HSTS), use of VPNs. | Avoiding public Wi-Fi networks, checking for 'https' in the URL before submitting data. |
| **ARP Spoofing** | Data Interception, DoS | ARP spoofing detection software, static ARP entries. | Education on local network vulnerabilities, vigilance for suspicious activity. |

## 6. Conclusion and Future Outlook

The analysis of DoS, MITM, and spoofing attacks reveals an evolving and increasingly interconnected threat landscape. Attackers are moving beyond simple, brute-force tactics and are leveraging vulnerabilities and human psychology in sophisticated, multi-vector campaigns. The recent rise of hyper-volumetric attacks, exemplified by the Dyn and GitHub incidents, underscores the need for proactive, automated, and cloud-based defense solutions that can absorb and mitigate threats at a massive scale.

However, technology alone is not a sufficient defense. The foundational nature of spoofing as a deceptive vector highlights that a resilient security posture must be multi-layered. A truly secure network infrastructure must be complemented by a security-aware culture, continuous employee training, and the adoption of principles like a zero-trust framework. The future of network security will be defined not by a single technological silver bullet, but by continuous adaptation, vigilance, and a holistic defense posture that addresses the full spectrum of technical and human vulnerabilities.

#### Works cited

1. Executive Summary — NIST SP 1800-26 documentation - NCCoE, accessed September 13, 2025, <https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html>
2. What is the CIA Triad and Why is it important? - Fortinet, accessed September 13, 2025, <https://www.fortinet.com/resources/cyberglossary/cia-triad>
3. The Essential Network Security Principles for IT Leaders: Designing a Robust Security Program - Cato Networks, accessed September 13, 2025, <https://www.catonetworks.com/network-security/principles/>
4. Vulnerabilities, Threats & Risk Explained - Splunk, accessed September 13, 2025, <https://www.splunk.com/en_us/blog/learn/vulnerability-vs-threat-vs-risk.html>
5. www.cloudflare.com, accessed September 13, 2025, <https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/#:~:text=DoS%20attacks%20typically%20function%20by,computer%20to%20launch%20the%20attack.>
6. Denial of Service (DoS) guidance - NCSC.GOV.UK, accessed September 13, 2025, <https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection>
7. What Is a Distributed Denial-of-Service (DDoS) Attack? | F5, accessed September 13, 2025, <https://www.f5.com/glossary/distributed-denial-of-service-ddos-attack>
8. DDOS attacks and the GitHub case » IRIS-BH, accessed September 13, 2025, <https://irisbh.com.br/en/ddos-attacks-and-the-github-case/>
9. What Is a Distributed Denial of Service (DDoS) Attack? - NetScout Systems, accessed September 13, 2025, <https://www.netscout.com/what-is-ddos>
10. What Is a SYN Flood Attack? | F5, accessed September 13, 2025, <https://www.f5.com/glossary/syn-flood-attack>