Research Report: Common Network Security Threats
DoS/DDoS, Man-in-the-Middle (MITM), and Spoofing

Date: August 31, 2025
Author: Generated by ChatGPT (GPT-5 Thinking)

Abstract—This report surveys three fundamental network security threats—Denial of Service (DoS/Distributed DoS), Man-in-the-Middle (MITM), and Spoofing. For each, we explain how the attack works, typical impact on confidentiality, integrity, and availability (CIA), representative real-world incidents, and layered mitigations spanning people, process, and technology.

1. Introduction

Modern networks face a constant barrage of attacks that aim to disrupt availability, steal data, or subvert trust. Understanding how cornerstone threats work—and how they are mitigated—helps teams design resilient systems and incident response plans. This report focuses on DoS/DDoS (availability), MITM (confidentiality/integrity), and Spoofing (impersonation and redirection).

2. Denial of Service (DoS/DDoS)

2.1 How it works

A DoS attack tries to exhaust a target's resources (bandwidth, CPU, memory, connections) so legitimate users cannot be served. DDoS distributes this across many compromised hosts (botnets), amplifying effect via reflection/amplification (e.g., DNS, NTP) or layer-7 HTTP floods. IoT botnets (default credentials, weak update hygiene) have made massive attacks routine.

2.2 Impact

• Service and API outages; degraded performance
• Collateral costs: autoscaling bills, SLA violations, incident response load
• Reputational damage and downstream supply-chain effects (e.g., DNS providers)

2.3 Real-world examples

• Mirai botnet (2016) overwhelmed DNS provider Dyn, disrupting access to Twitter, Netflix and others [1][2].
• Cloudflare mitigated a record 26M HTTPS requests/second flood in 2022; larger waves (71M rps; multi-Tbps) were observed in 2024 [3][4].
• AWS reported new HTTP/2 Rapid Reset-style DDoS patterns beginning August 2023 and protected customers via AWS Shield [5].

2.4 Mitigations

• Edge capacity + scrubbing: Anycast CDNs/WAFs, DDoS protection services; automatic detection and rate-limiting.
• Protocol hardening: HTTP/2 abuse protections; SYN cookies; connection limits; request validation; caching.
• Upstream cooperation: BCP 38/ingress filtering to prevent spoofed-source reflection; peering with scrubbing centers.
• Architectural resilience: Multi-region failover, DNS failover, autoscaling with cost-guardrails, circuit breakers.
• Playbooks and drills: Thresholds, runbooks, contact trees, pre-approved controls (rate limits, WAF rules).

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

3.1 How it works

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

3.1 How it works

An adversary interposes on a communication path to eavesdrop or modify traffic. Common vectors include rogue Wi-Fi APs, ARP poisoning on LANs, BGP/DNS hijacking at the control plane, or subverting the PKI trust model (malicious/compromised CAs or local root certs). TLS aims to prevent MITM, but is undermined if trust anchors are compromised or users are coerced to install interception CAs.

3.2 Impact

- Credential/session theft; injection of malware or ads; silent tampering of data in transit
- Loss of confidentiality and integrity; regulatory exposure

3.3 Real-world examples

- DigiNotar CA compromise (2011): attackers issued fraudulent certificates (e.g., *.google.com), enabling MITM; the CA later collapsed [6].
- Lenovo Superfish (2015): adware installed a non-unique root CA, enabling HTTPS interception on affected laptops [7][8].
- Kazakhstan (2019): authorities attempted nationwide HTTPS interception via a government root CA; academics later documented the interception campaign [9][10].

3.4 Mitigations

- End-to-end encryption done right: TLS 1.2+ with strong cipher suites, HSTS, certificate pinning (where feasible), DNSSEC + DoT/DoH for resolvers.
- PKI hygiene: CA monitoring, Certificate Transparency (CT) logs, rapid revocation, short-lived certs, hardware-backed keys.
- Network protections: WPA3/802.1X; switch port security; ARP inspection; DHCP snooping; secure BGP (RPKI/ROV) with route monitoring.
- User/endpoint hardening: disable trust of user-added roots; EDR; VPN on untrusted networks; MDM policies; phishing-resistant MFA (FIDO2).

4. Spoofing (IP/ARP/DNS/Email)

4.1 How it works

Spoofing is the forgery of an identity or binding—IP source spoofing (packet headers), ARP spoofing (LAN mapping), DNS hijack/poisoning (name→IP), or email domain spoofing (SMTP). Attackers use spoofing to redirect users to impostor services, inject themselves in the path, or bypass ACLs.

4.2 Impact

- Redirection to phishing/malware; credential theft; session hijack
- Cache poisoning at resolvers; traffic blackholing or interception via BGP/DNS hijack

4.3 Real-world examples

- Amazon Route 53 DNS/BGP hijack (2018) redirected MyEtherWallet traffic via rogue prefixes to steal cryptocurrency [11][12].
- Syrian Electronic Army (2013) changed registrar/DNS for major media and Twitter, redirecting domains [13].

4.4 Mitigations

- Anti-spoofing at ISPs/edges (BCP 38/84); uRPF; source validation.
- LAN protections: Dynamic ARP Inspection; static ARP for critical assets; network segmentation.
- DNS protections: DNSSEC for zones; registrar lock; 2FA with registrars; monitored NS/DS records; resolver validation.
- Email authentication: SPF, DKIM, DMARC with quarantine/reject policies; brand indicators (BIMI) where applicable.
- Routing security: RPKI/ROV; route monitoring/alerting; diverse transit/anycast; max-prefix limits.

5. Defense-in-Depth & Operations

5. Defense-in-Depth & Operations

• Layered controls across endpoints, network, identity, and application reduce single points of failure.
• Security observability: flow logs, WAF/IDS, DNS logs, CT log monitors, BGP monitoring; baselines and SLOs for availability.
• Incident response: pre-built playbooks for DDoS, MITM suspicion, and DNS/BGP hijack; communication plans; law-enforcement/ISP contacts.
• Continuous testing: chaos/traffic drills, tabletop exercises, red/blue/purple teaming.

6. Conclusion

DoS/DDoS, MITM, and spoofing remain evergreen threats because they exploit foundational assumptions of the Internet. Combining robust architecture (capacity, diversity, failover) with strong cryptography, PKI vigilance, and operational readiness greatly reduces risk and blast radius.

References

[1] Cloudflare, “Inside the infamous Mirai IoT Botnet: A Retrospective Analysis,” 2017.
[2] Wikipedia, “DDoS attacks on Dyn,” updated 2025.
[3] Cloudflare, “Cloudflare mitigates 26M rps DDoS attack,” 2022.
[4] Cloudflare, “Bigger and badder: how DDoS attack sizes have evolved,” 2024.
[5] AWS Security Blog, “How AWS protects customers from DDoS events,” 2023.
[6] ENISA, “Operation Black Tulip: Certificate authorities lose authority,” 2011.
[7] CISA Alert TA15-051A, “Lenovo Superfish Adware Vulnerable to HTTPS Spoofing,” 2015/2016.
[8] Lenovo Security Advisory LEN-2015-010, “SuperFish Vulnerability,” 2015.
[9] F5 Labs, “Kazakhstan Attempts to MITM Its Citizens,” 2019.
[10] ACM IMC, “Investigating Large Scale HTTPS Interception in Kazakhstan,” 2020.
[11] Internet Society, “Amazon’s Route 53 BGP Hijack,” 2018.
[12] ThousandEyes, “Anatomy of a BGP Hijack on Amazon’s Route 53,” 2018.
[13] The Guardian, “Twitter and New York Times … SEA hack,” 2013.