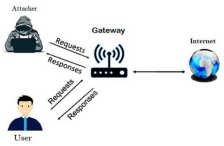
INTEGRAL UNIVERSITY
LUCKNOW - INDIA
A+ ACCREDITED BY NAAC
DOI No. 10.5281/zenodo.15113039
FEBRUARY 2025

CYBER BULLETIN

Man-in-the-Middle(MITM)Attack

1. Wi-Fi MITM Attacks

PACKET SNIFFING



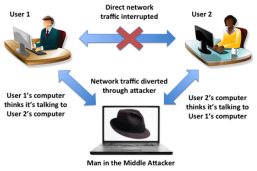
TARGET: Devices connected to unsecured public Wi-Fi network like laptops, smartphones & tablets.

IMPACT: Hackers can steal data, track online activity, send you to fake websites, or infect device with viruses.

MITIGATION: Use secure websites (HTTPS), turn on strong Wi-Fi security (WPA3/WPA2), avoid public Wi-Fi or use a VPN, block unknown devices.

2. LAN-Based MITM Attacks

ARP SPOOFING



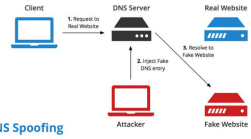
TARGET: Devices connected on a local network, including computers, routers, and servers..

IMPACT: Hackers can steal data, spy on online activities, or block internet access.

MITIGATION: Use strong network security, enable encryption (VPN, HTTPS), and monitor for unusual network activity.

3. MITM Via Fake DNS Responses

DNS SPOOFING



TARGET: Users unknowingly visiting fake websites.

IMPACT: Stolen passwords, phishing scams, malware, and financial fraud.

MITIGATION: Use secure DNS services (like Cloudflare or Google DNS), enable DNSSEC, and verify HTTPS before entering sensitive information.

4. MITM on Active Sessions

SESSION HIJACKING

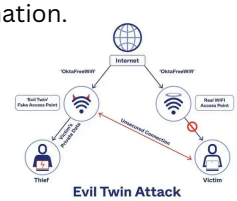
TARGET: Logged-in users on websites, apps, or banking portals.

IMPACT: Hackers can hijack sessions, act as the user, and perform unauthorized actions.

MITIGATION: Use multi-factor authentication (MFA), secure cookies, and avoid public or untrusted networks.

5. Evil Twin Attacks

ROGUE ACCESS POINTS



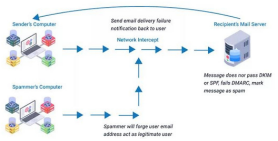
TARGET: Users unknowingly connecting to fake Wi-Fi networks controlled by attackers.

IMPACT: Hackers can steal data, capture login credentials, and inject malware into devices.

MITIGATION: Always verify Wi-Fi networks, use WPA3 encryption at home, and avoid untrusted networks.

6. Email MITM Attacks

SMTP SPOOFING



TARGET: Email communications, especially in business and financial transactions.

IMPACT: Attackers can alter invoice details, impersonate senders, or steal confidential data.

MITIGATION: Use encrypted email protocols (TLS, PGP), verify sender identities, and avoid sharing sensitive data via email.

INTEGRAL UNIVERSITY
LUCKNOW - INDIA
A+ ACCREDITED BY NAAC
DOI No. 10.5281/zenodo.15113039
FEBRUARY 2025

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
ISEA www.isea.gov.in
STAY SAFE ONLINE ऑनलाइन सुरक्षा कवच

CYBER SECURITY POSTER OF THE DAY

Use secure Wi-Fi connections when accessing social media.

#SecureWifi
#OnlineSafety

CYBER SAKCHHARTA ABHIYAN
UNDER THE AEGIS OF
CYBER AWARENESS CLUB
DEPARTMENT OF COMPUTER APPLICATION

FACULTY COORDINATORS
MR. SHUBHAM KUMAR | MR. FAIZAN MAHMOOD | MR. MOHD TALHA
STUDENTS COORDINATORS
MOHAMMAD FARHAN | SIDRA SIDDIQUI | ELMA SHARIQ
AREEBA KHAN | ANAMTA ANSARI

Prof.(Dr.) MOHAMMAD FAISAL
Head, Department of Computer Application