

QUIC/HTTP3 MitM Handshake Attacks

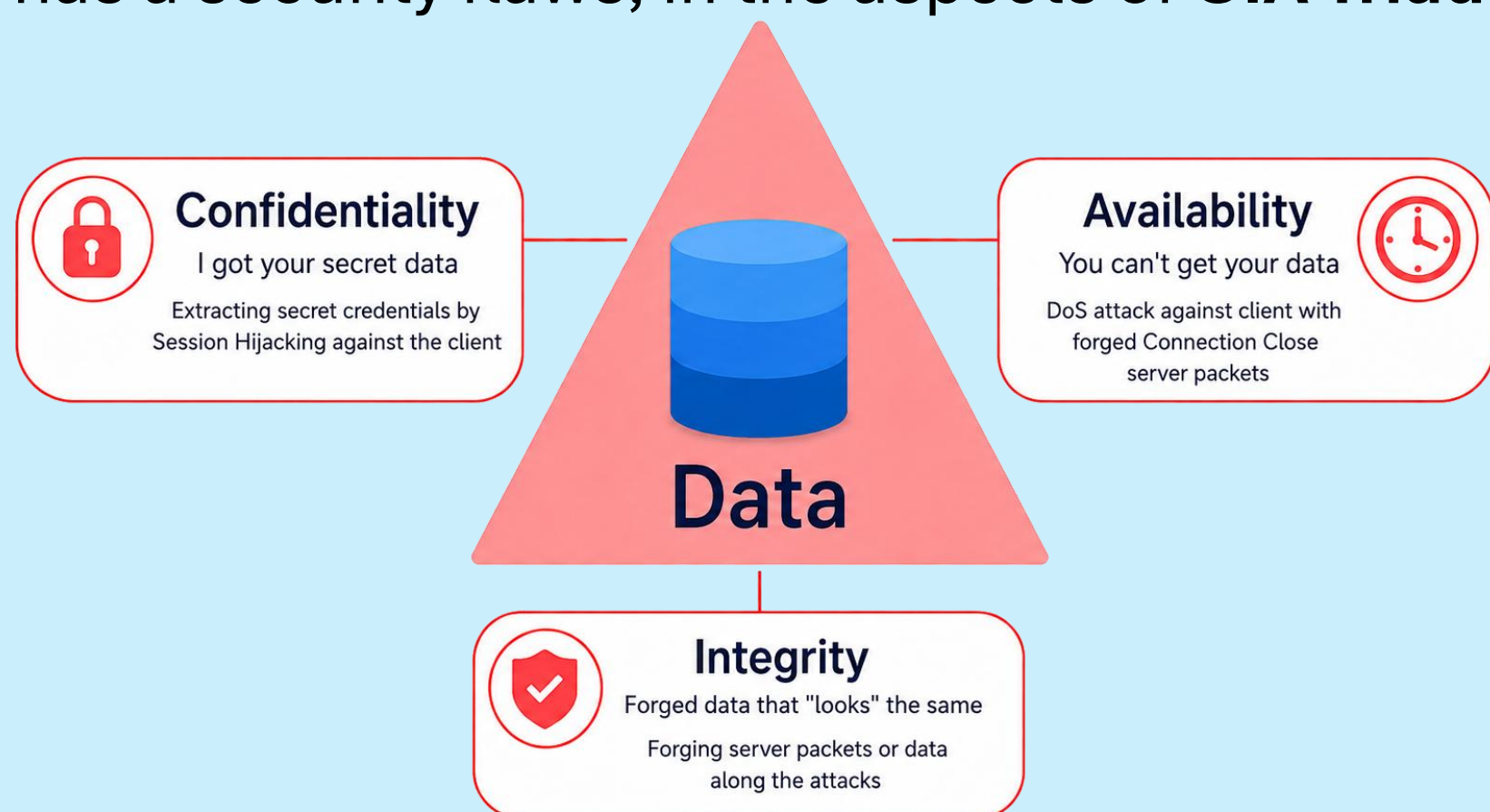
Gil Sait and Paz Wolf Supervised by Sorana Fraier

Introduction

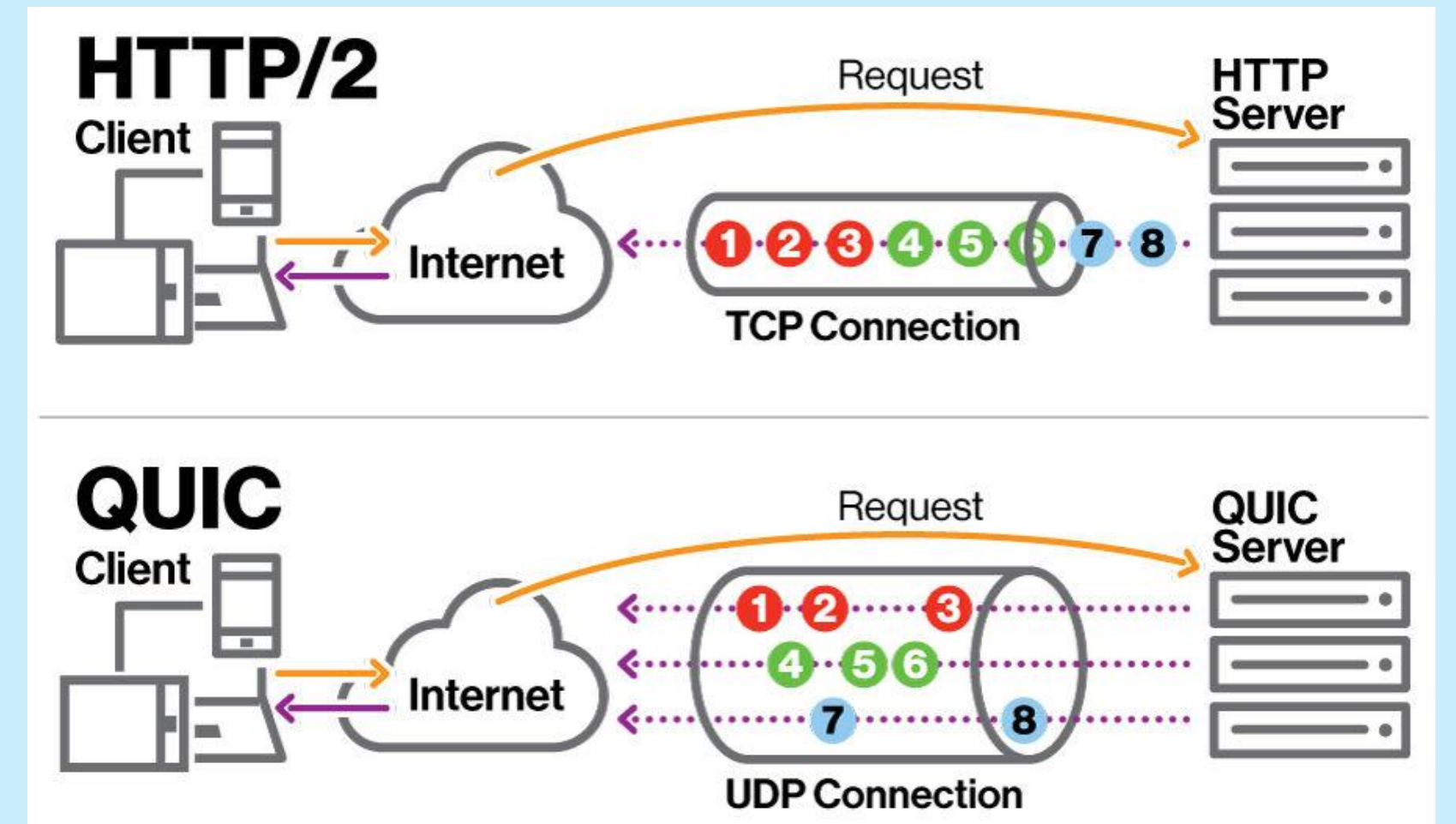
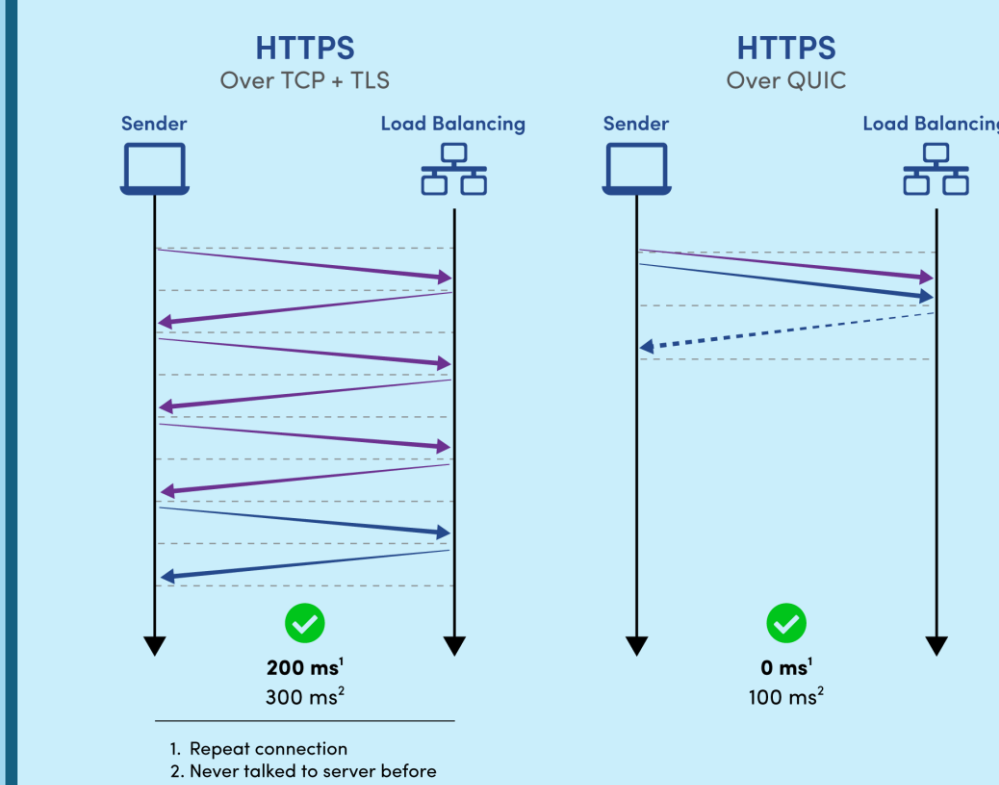
- QUIC replaces **TCP+TLS** for **HTTP3** with better performance.
- Security is integrated with TLS 1.3, but the **QUIC** handshake and semantics provides new attack surface.
- We demonstrate **handshake-based attacks** with a LAN adversary Man-in-The-Middle (**MITM**) model.

Goals

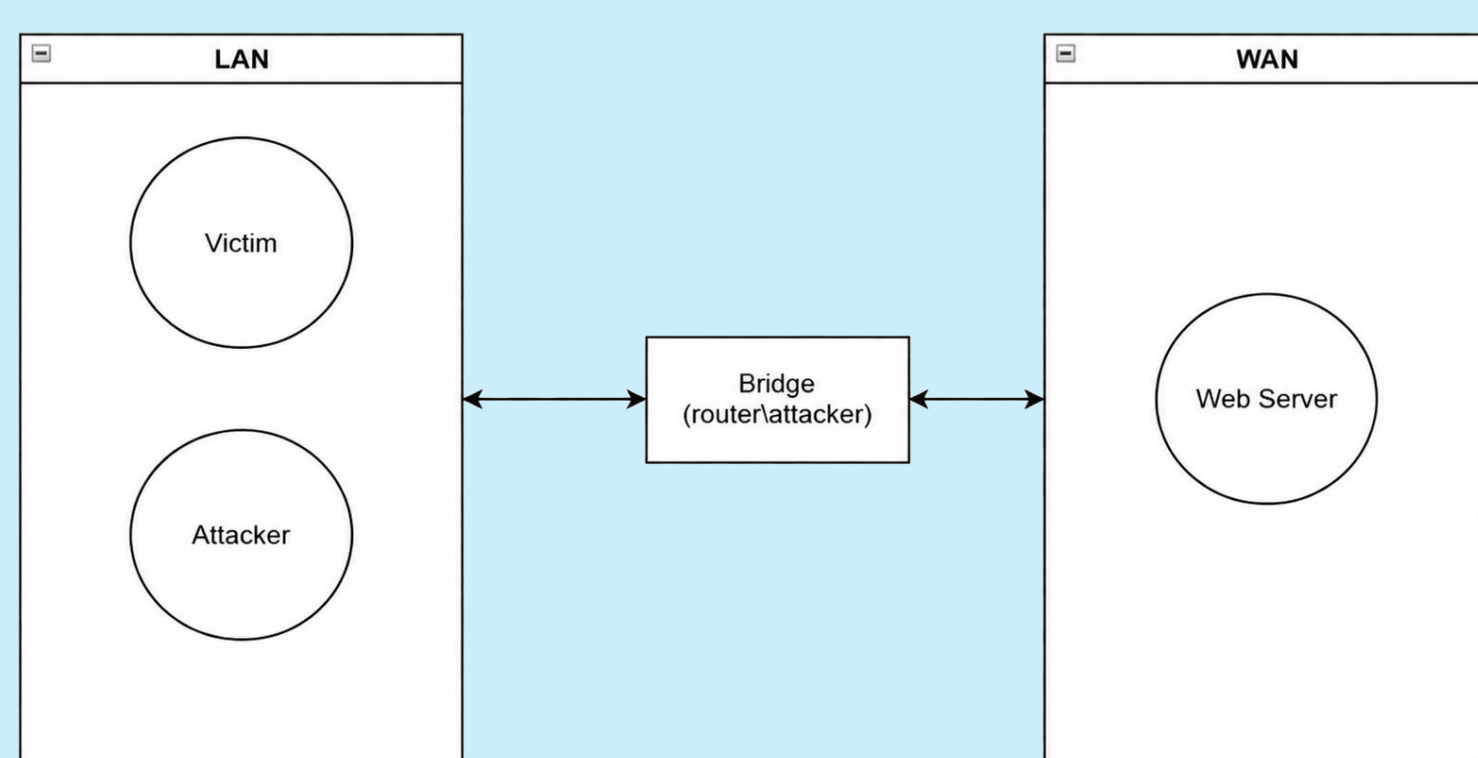
Implementing a Proof-of-Concept (**PoC**) to show **QUIC** still has a security flaws, in the aspects of **CIA Triad**:



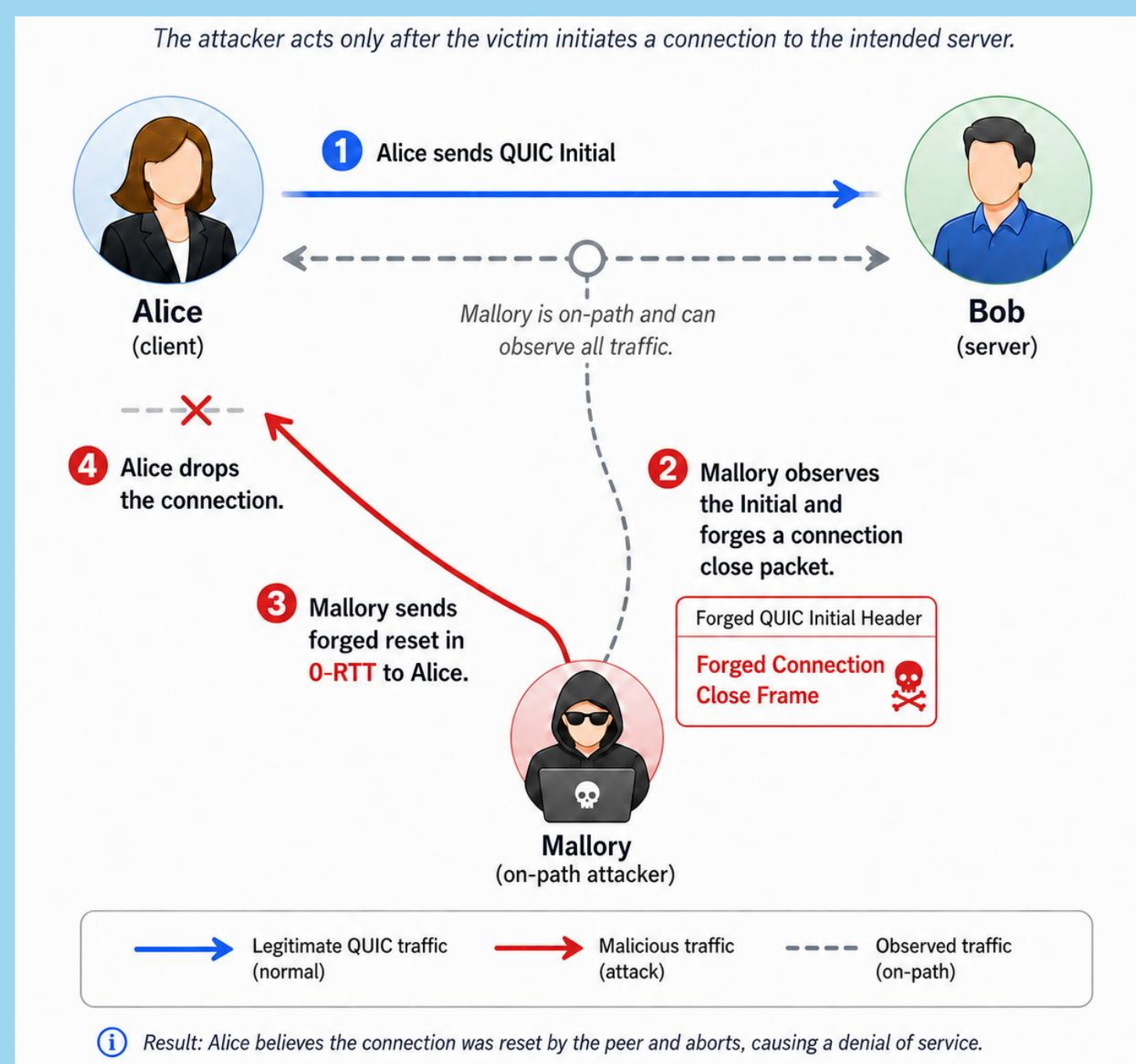
QUIC vs TCP



Threat Model & Setup



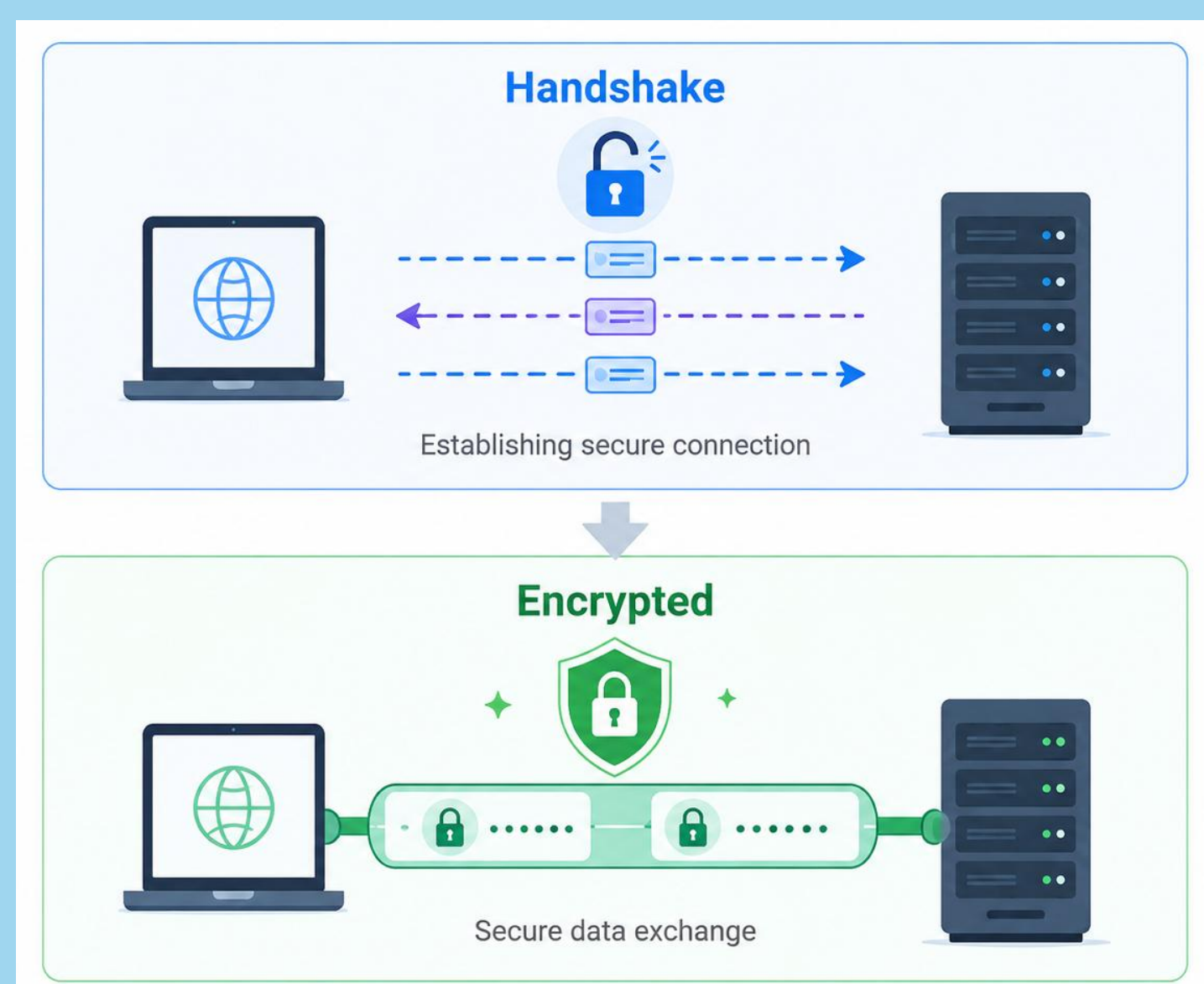
DoS Attack



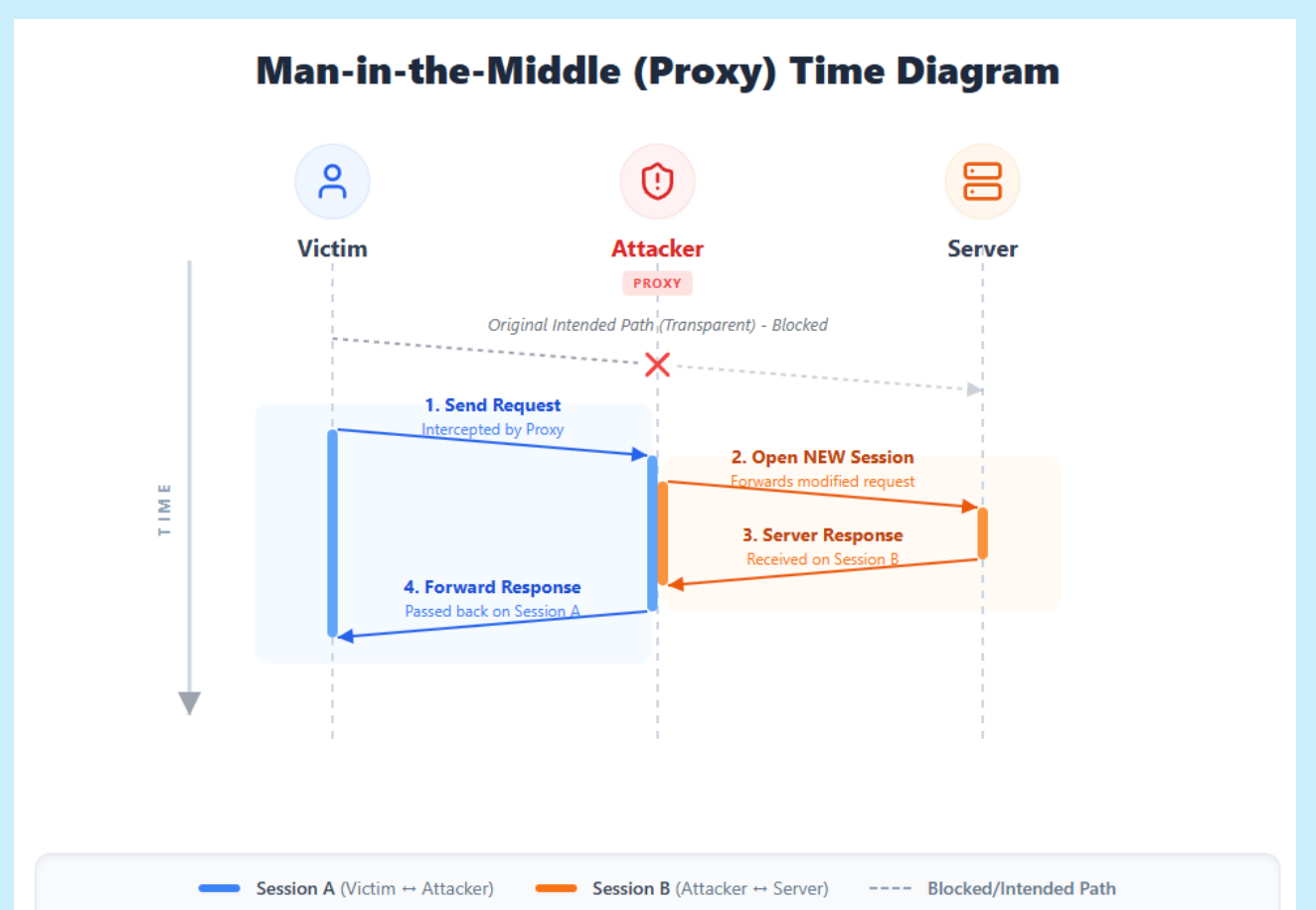
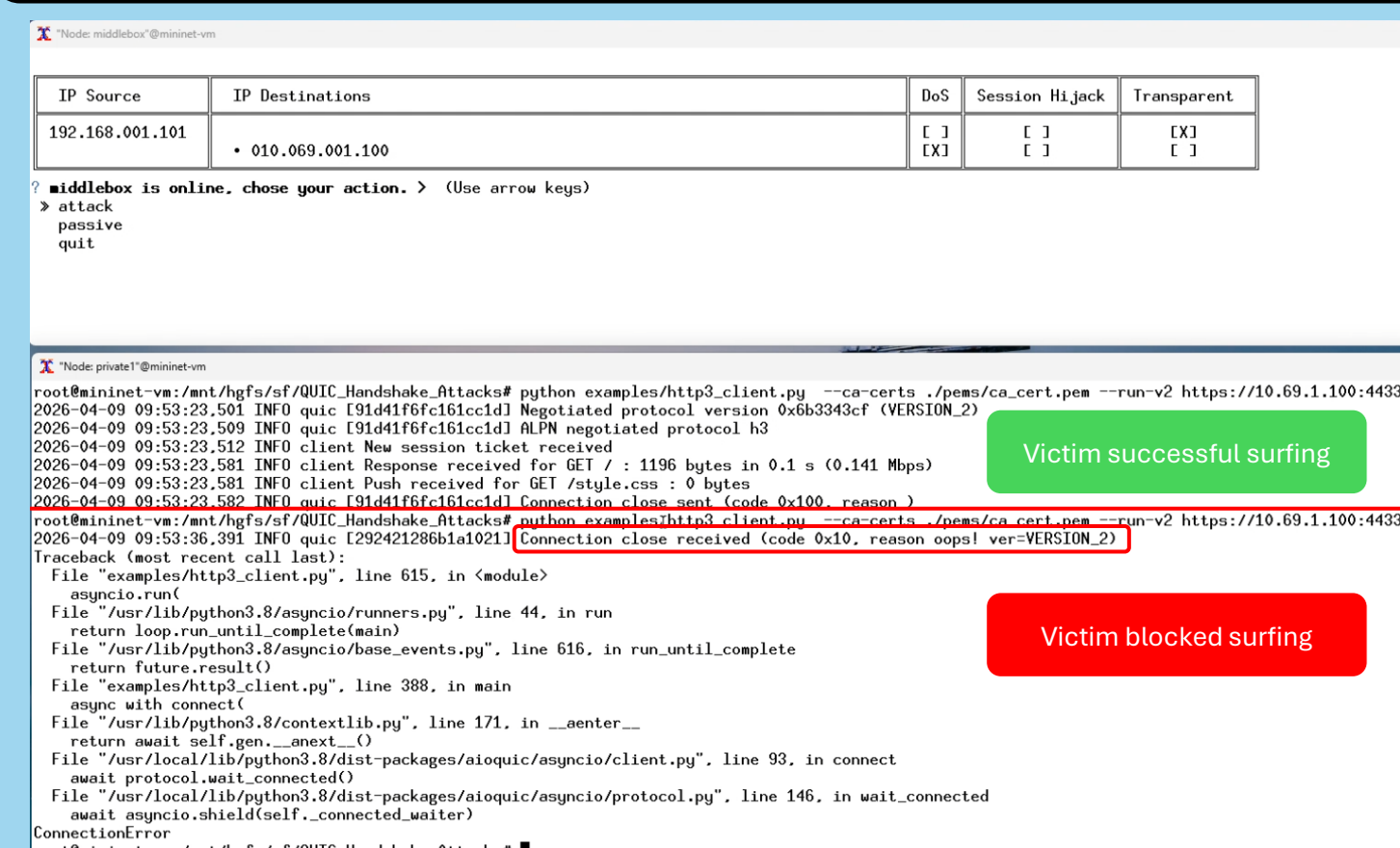
Session Hijack Attack

- The attacker can reply to the client **QUIC** handshake as if he is the real server and can open a new **QUIC** connection with the real server as if he is the real client.
- Our attack requires that the attacker has a Transport-Layer-Security (**TLS**) certificate that the victim can verify.
- Now the attacker can give the victim or the server false info, or he can spy on the data transmitted both ways.

Security status



Attacker vs Victim POV



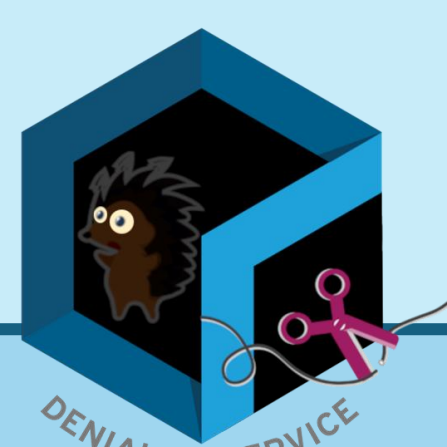
MiTM Mitigations

- ARP spoofing: Use manual DHCP or bind DHCP in switch + VLANs
- DNS poisoning/spoofing: using verification and encryption for DNS and using trusted DNS servers.
- WIFI attacks: Avoid using unsecured free Wi-Fi networks with weird behaviours.



DoS Mitigations

- Ignore connection_close packets before verifying server certificate
- After detecting connection_close in INITIAL packet:
 - change network interface (WIFI/cellular)
 - fall back to TCP/HTTP2



Session Hijack Mitigations

- strong MFA (authenticator / SMS)
- SSH/VPN tunnel
- client certificates
- proof-of-possession tokens
- Not using/accepting 0RTT handshakes
- certificate pinning

