Problem Statement for Cross-Layer Vulnerabilities due to Forged ICMP Errors

ZHAOXI LI
Tsinghua university

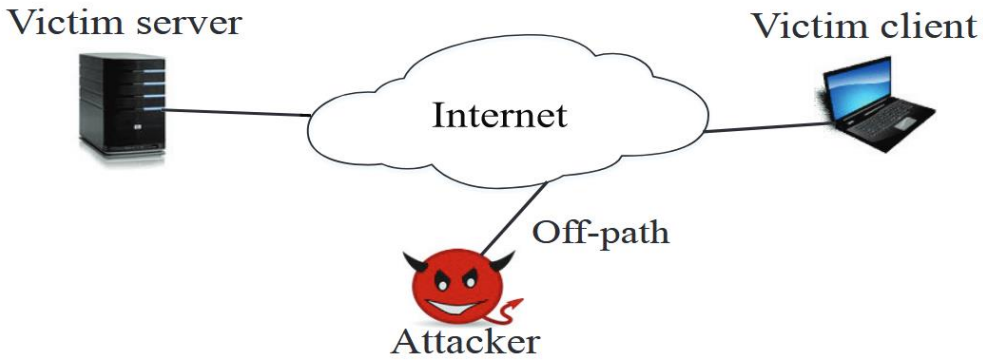
July 2025

The Importance and Challenge of ICMP

- ICMP: The Internet's Essential Feedback Mechanism
  - Report network issues
  - Enables diagnostics like traceroute.
  - Crucial for efficiency, like Path MTU Discovery (PMTUD).
- The Inherent Challenge: Validation is Weak
  - ICMP messages can be easily forged.
  - Receivers lack context to verify authenticity, especially with stateless protocols like UDP.

Threat Model: The Off-Path Attacker

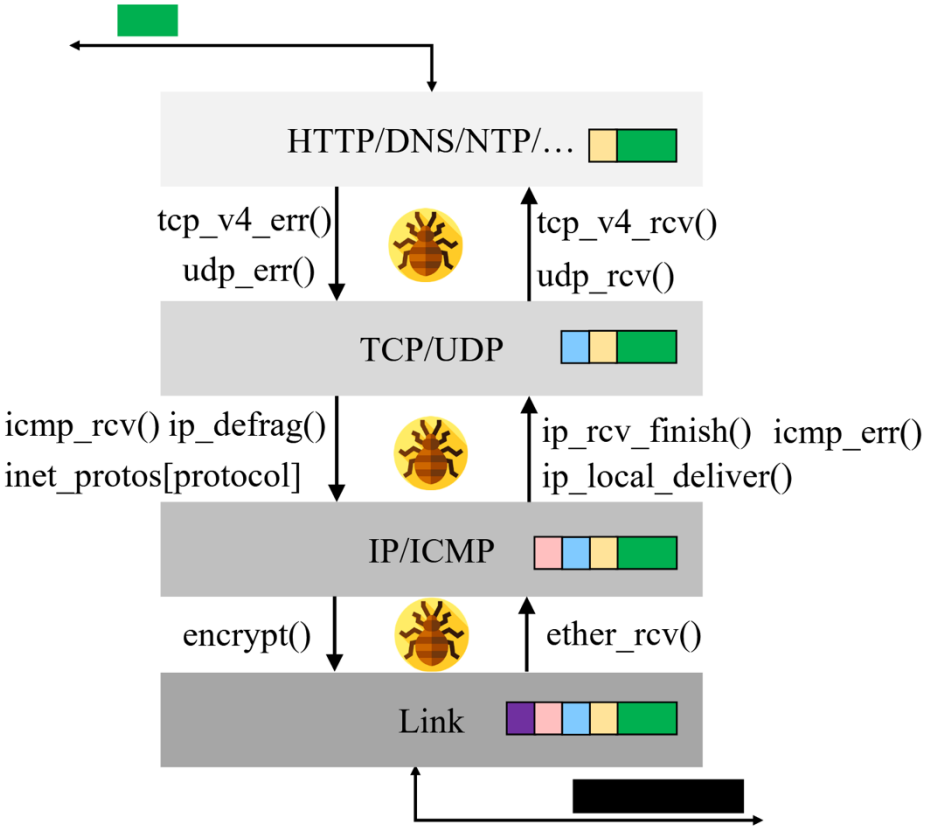
- Adversary is Off-Path:
  - Not on the direct communication path between client and server.
  - Cannot eavesdrop on, modify, or drop legitimate traffic.
- Attacker's Capability:
  - Can inject spoofed IP packets into the network.
- Why this is a significant threat:
  - The attacker can be anywhere on the internet.
  - Difficult to detect and trace.



Core Problem

Forged ICMP Induces Cross-Layer Vulnerabilities.

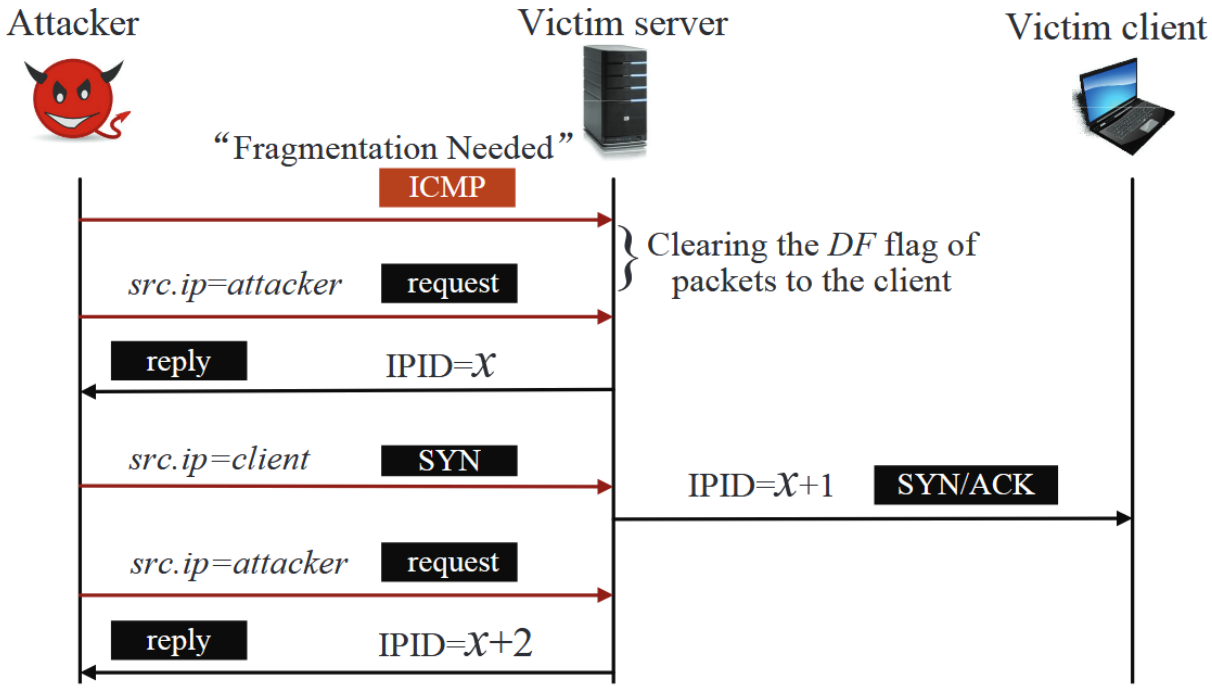
- Forged ICMP errors deceive the victim's TCP/IP stack.
  - This triggers unintended cross-layer interactions.
  - The stack misinterprets the network state, leading to vulnerabilities.
- Four Classes of Vulnerabilities:
  - Information Leakage
  - Ambiguity on Shared Variables (State Desynchronization)
  - Semantic Gaps
  - Identity Deception



Information Leakage

A lower-layer field unintentionally exposes upper-layer secrets.

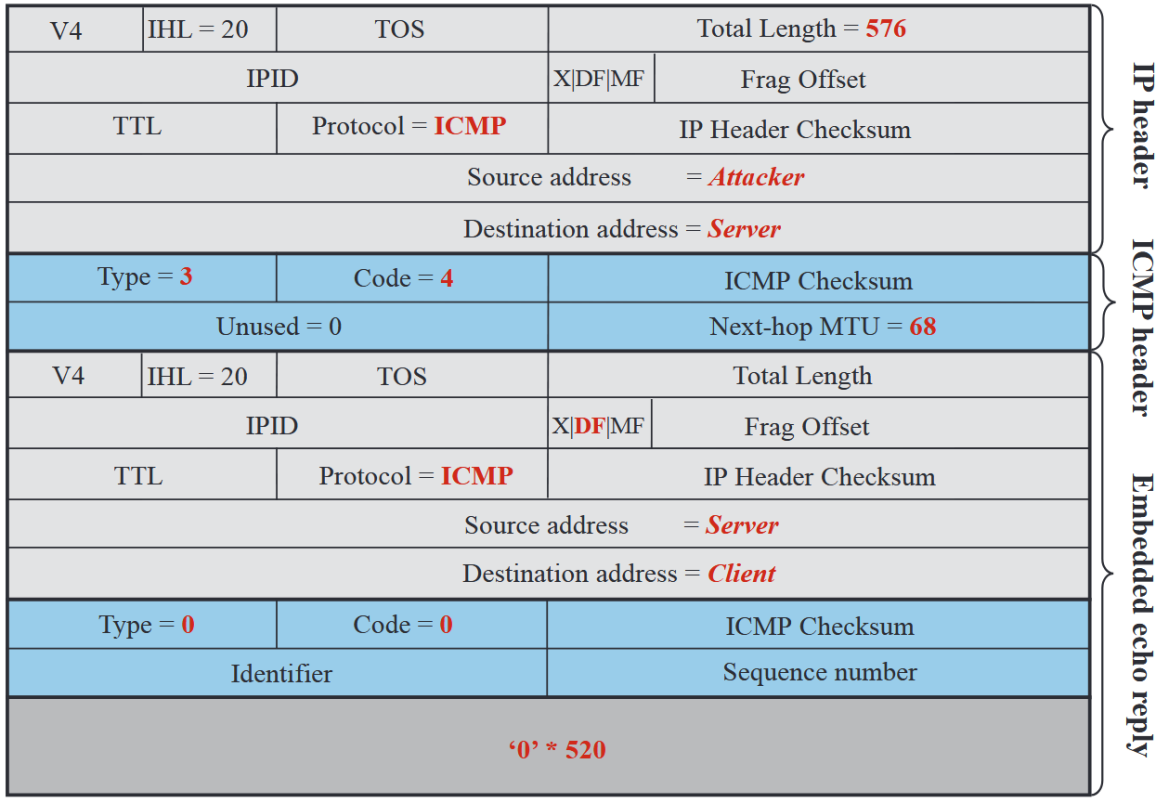
- IP Identification (IPID) Side Channel
  - A forged ICMP error forces the victim's IP layer to change its IPID generation policy.
  - This creates a side channel where the IPID counter, an IP-layer field, now leaks information about TCP-layer events.
  - By observing IPID increments, the attacker can infer TCP sequence numbers.



[1] Feng, X., Fu, C., Li, Q., Sun, K., and K. Xu, "Off-path TCP exploits of the mixed IPID assignment"

Information Leakage

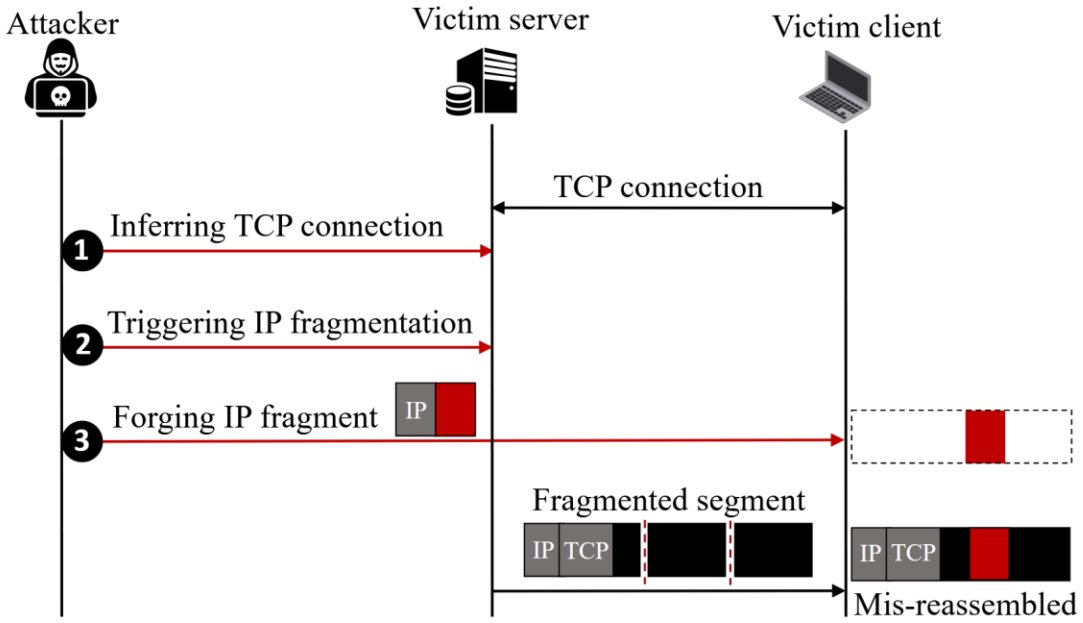
- The Embedded Payload
  - The attacker embeds a complete ICMP Echo Reply packet as the payload of forge packet.
  - The source/destination of the embedded packet are reversed
- How it Works
  - The server simply process message ,doesn't validate whether it actually sent this specific echo reply.
  - It applies the error's context and clears the DF flag for that destination.
  - Allowing attacker monitor predicable IPID counter to infer TCP sequence number .



Ambiguity on Shared Variables

Protocol layers have an inconsistent view of a shared resource.

- IP Fragment Injection Attack
  - A forged ICMP error desynchronizes the Path MTU value between the IP and TCP layers.
  - This causes TCP to generate segments that are unexpectedly fragmented.
  - The attacker can then inject a malicious IP fragment, which is incorrectly reassembled with legitimate ones.

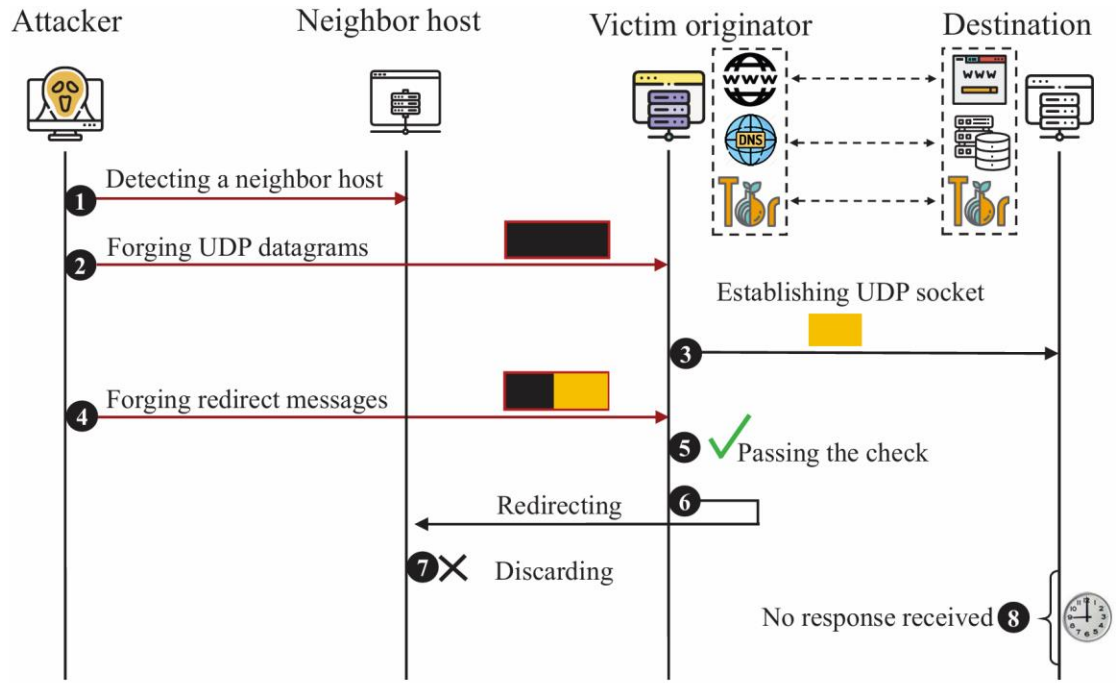


[2] Feng, X., Li, Q., Sun, K., Xu, K., Liu, B., Zheng, X., Yang, Q., Duan, H., and Z. Qian, "PMTUD is not Panacea: Revisiting IP Fragmentation Attacks against TCP"

Semantic Gaps

A protocol receives a control message that it cannot fully validate.

- ICMP Redirect Traffic Hijacking
  - The attacker forges a UDP datagram and a corresponding ICMP Redirect message.
  - The victim's stack checks the embedded header in the ICMP message, finds a matching (but forged) flow, and accepts the redirect.
  - This semantic gap in validation leads to traffic being hijacked.

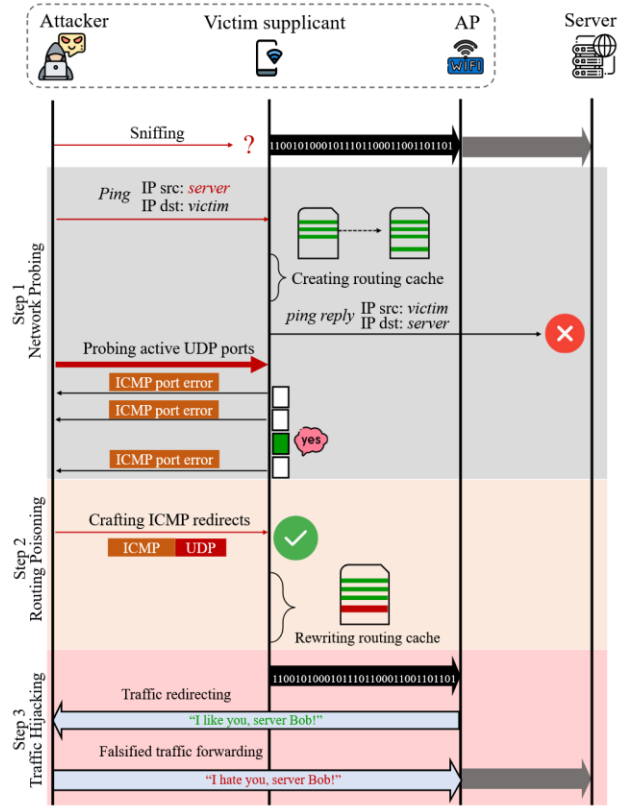


[3] Feng, X., Li, Q., Sun, K., Qian, Z., Zhao, G., Kuang, X.,Fu, C., and K. Xu, "Off-Path Network Traffic Manipulation via Revitalized ICMP Redirect Attacks"

Identity Deception

Lack of source authentication allows an attacker to impersonate a trusted network entity, like a router or Access Point.

- Wireless Network Routing Cache Poisoning
  - An attacker impersonates the AP and sends a forged ICMP Redirect to a victim on a Wi-Fi network.
  - The message contains a crafted UDP payload to bypass validation checks.
  - The victim accepts the redirect, poisoning its routing cache and making the attacker its new gateway.
  - All subsequent traffic, is redirected through the attacker, who can intercept or manipulate it."



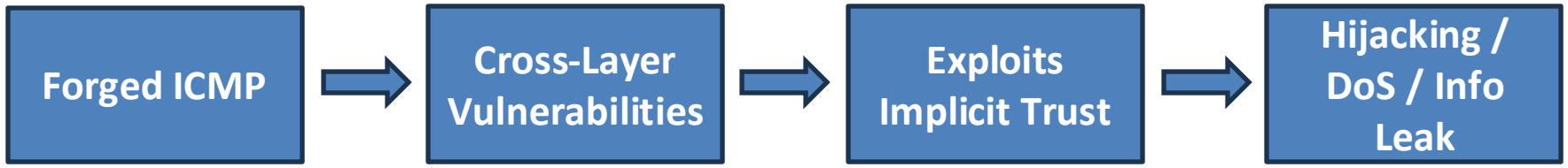
[4] Feng, X., Li, Q., Sun, K., Yang, Y., and K. Xu, "Man-in-the-middle attacks without rogue AP: when WPAs meet ICMP redirects"

Mitigation Directions

- Enhance Data Provenance Validation:
  - Introduce stronger authentication for control messages (e.g., cryptographic signatures).
- Enforce Stronger Lower-Layer Checks:
  - Infrastructure (routers, firewalls) should perform more rigorous validation before passing control messages up the stack.
- Adopt Fine-grained, Explicit Trust Models:
  - Move away from implicit trust between layers and require explicit validation for cross-layer interactions.

Conclusion & Next Steps

- **Problem:** The implicit trust between protocol layers is being exploited by forged ICMP messages.
- **Impact:** This leads to severe vulnerabilities that compromise communication integrity and user privacy.
- **Call to Action:** The IETF community should carefully consider these cross-layer interaction risks in the design and implementation of current and future protocols.



Next Step

- Collaboration is welcome!
- Your comments and suggestions are welcome!

Thanks!