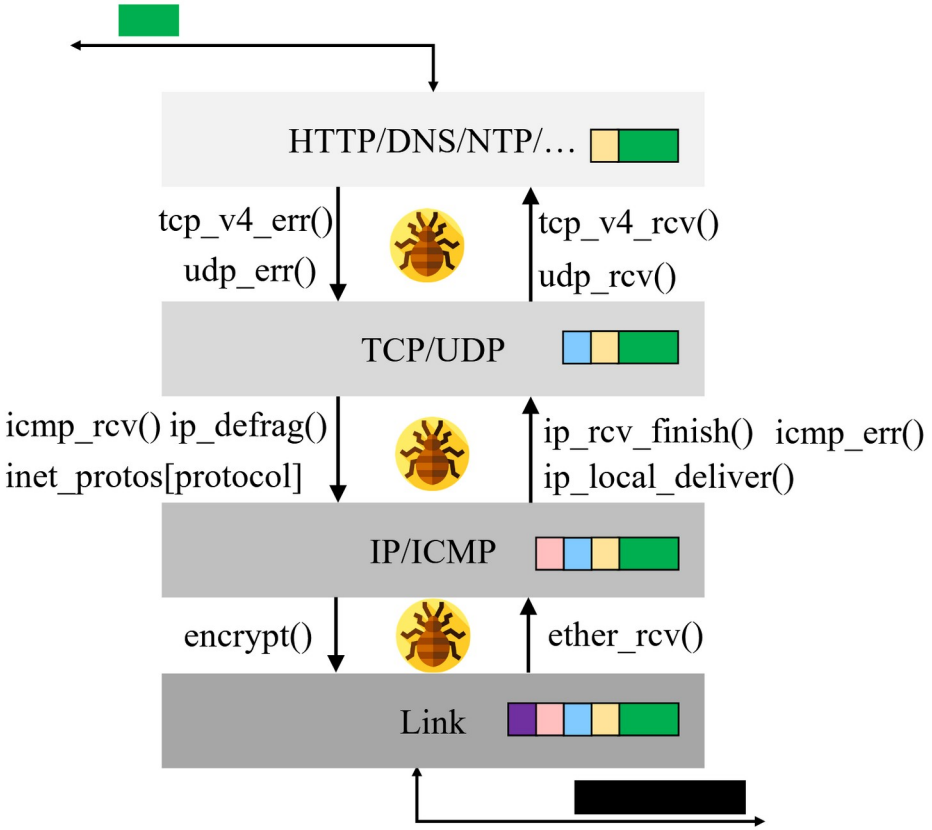
Problem Statement for Cross-Layer Vulnerabilities due to Forged ICMP Errors
&
Enhancing ICMP/ICMPv6 Error Message Authentication Using Challenge-Confirm Mechanism

Presenter: AO WANG & ZHAOXI LI

INTAREA
IETF 125, March 2026, Shenzhen

Problem Background

- ICMP: The Internet's Essential Feedback Mechanism
- The Inherent Challenge: **Validation is Weak**
- Forged ICMP errors deceive the victim's TCP/IP stack.
  - triggers unintended cross-layer interactions.
  - The stack misinterprets the network state.
- Four Classes of Cross-layer Vulnerabilities:
  - Information Disclosure
  - State Desynchronization
  - Semantic Validation Deficiencies
  - Source Authentication Failures

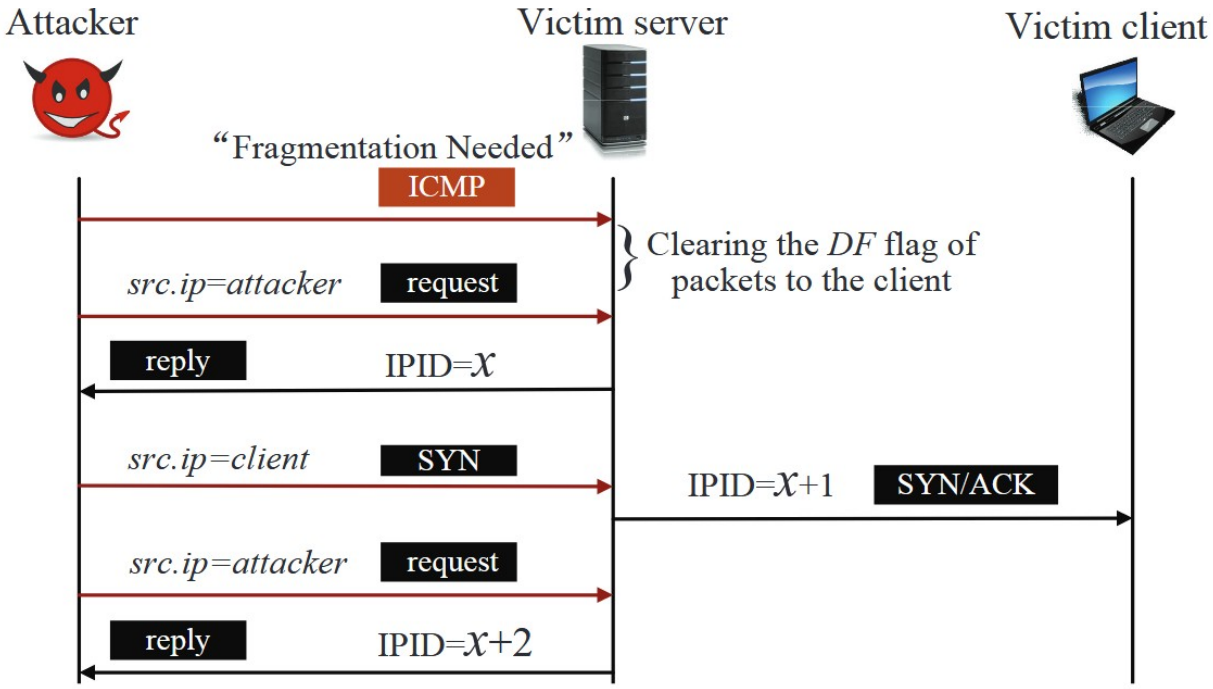


[1] Feng, X., Li, Q., Sun, K. U. N., Xu, K., and Wu, J., “Exploiting cross-layer vulnerabilities: Off-path attacks on the tcp/ip protocol suite” Communications of the ACM

Information Disclosure

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.

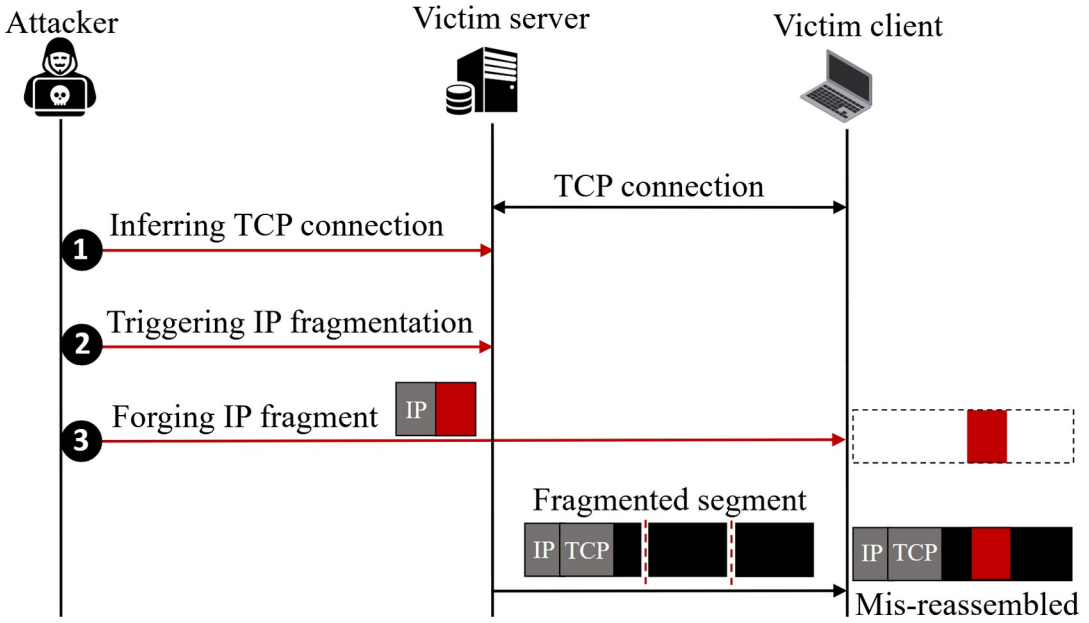


[2] Feng, X., Fu, C., Li, Q., Sun, K., and K. Xu, "Off-path TCP exploits of the mixed IPID assignment" CCS'2020

State Desynchronization

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.

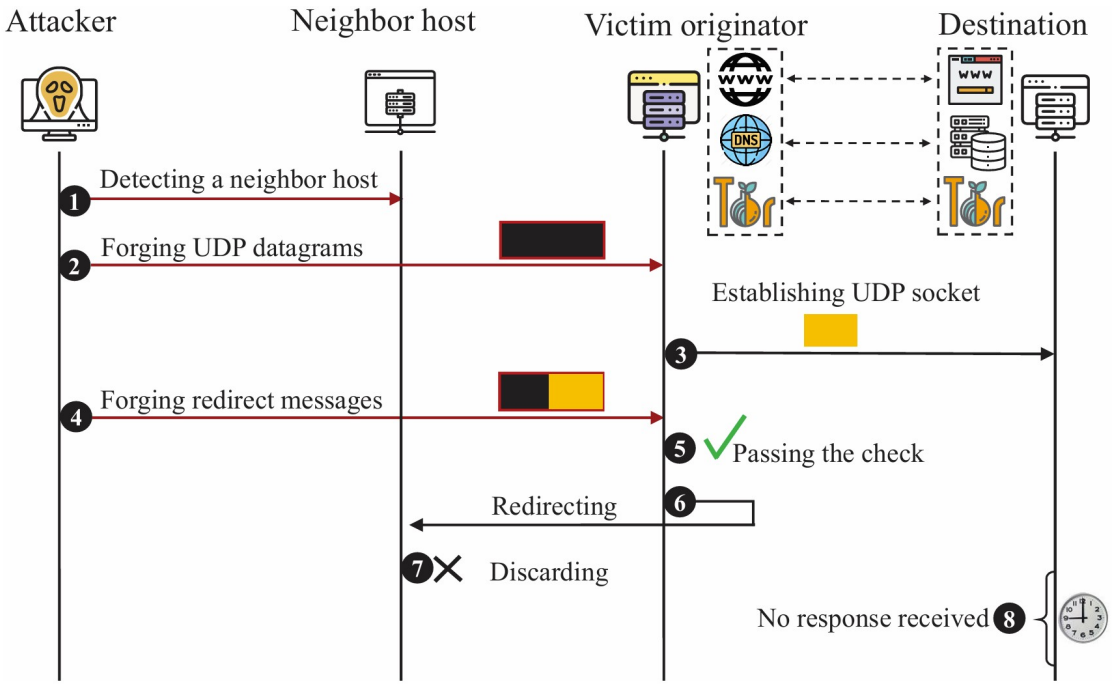


[3] Feng, X., Li, Q., Sun, K., Xu, K., Liu, B., Zheng, X., Yang, Q., Duan, H., and Z. Qian, "PMTUD is not Panacea: Revisiting IP Fragmentation Attacks against TCP " NDSS'2022

Semantic Validation Deficiencies

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.

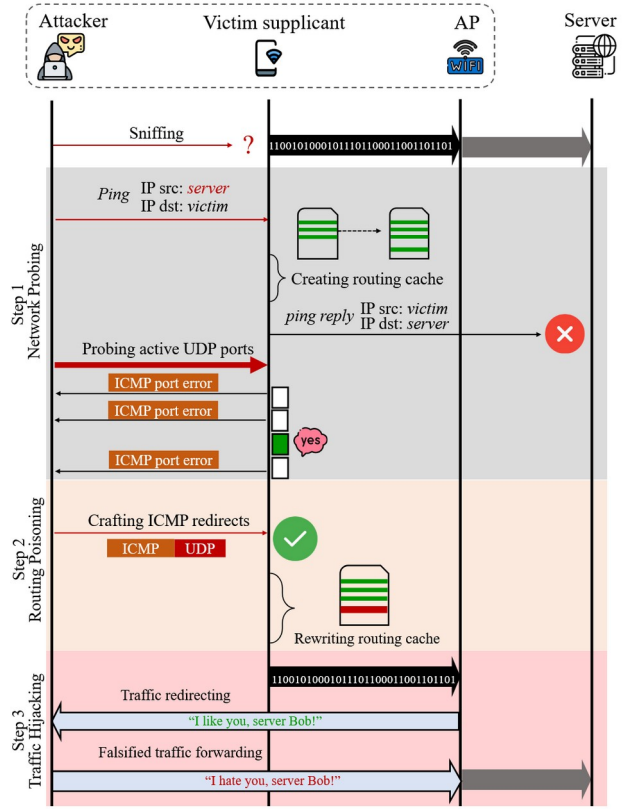


[5] Feng, X., Li, Q., Sun, K., Qian, Z., Zhao, G., Kuang, X.,Fu, C., and K. Xu, "Off-Path Network Traffic Manipulation via Revitalized ICMP Redirect Attacks“ Security'2022

Source Authentication Failures

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."



[5] Feng, X., Li, Q., Sun, K., Yang, Y., and K. Xu, "Man-in-the-middle attacks without rogue AP: when WPAs meet ICMP redirects" SP'2023

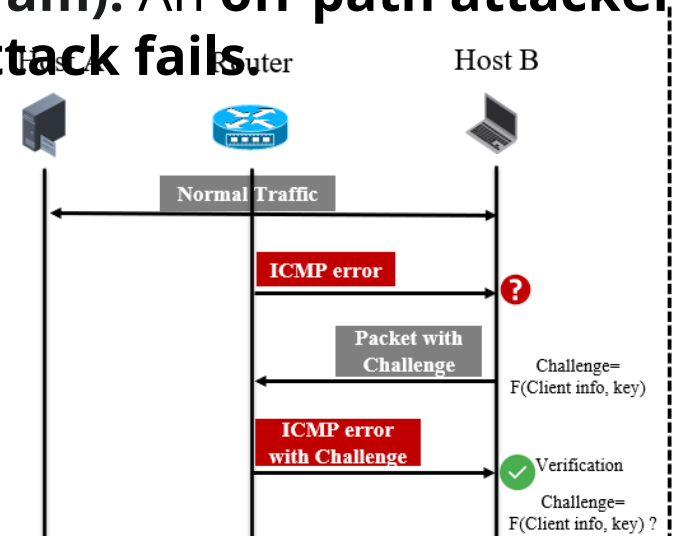
How to solve ?

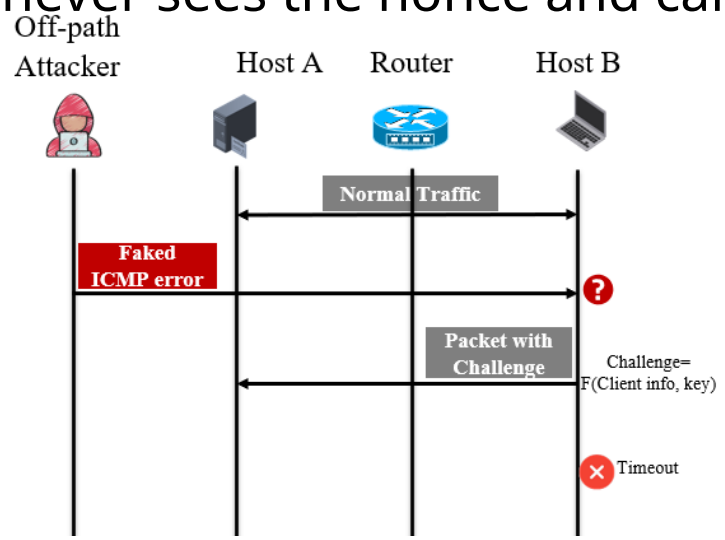
Challenge-Confirm Mechanism

- ICMP error messages for stateless traffic are easily forged by off-path attackers.
- **How it Works:**
  - **Challenge**: On receiving an ICMP error, Host B embeds a **stateless, computed nonce** in the next outgoing packet for that flow.

    Nonce = Hash(secret_key, flow_info)
  - **Verification:**
    - **(Left):** A **real on-path router** sees and reflects the nonce, proving it's on the path. **Success.**
    - **(Right Diagram):** An **off-path attacker** never sees the nonce and cannot forge a valid response. **Attack fails.**

Real ICMP Error Messages





Forged ICMP Error Messages

Updates

Updates since IETF 122

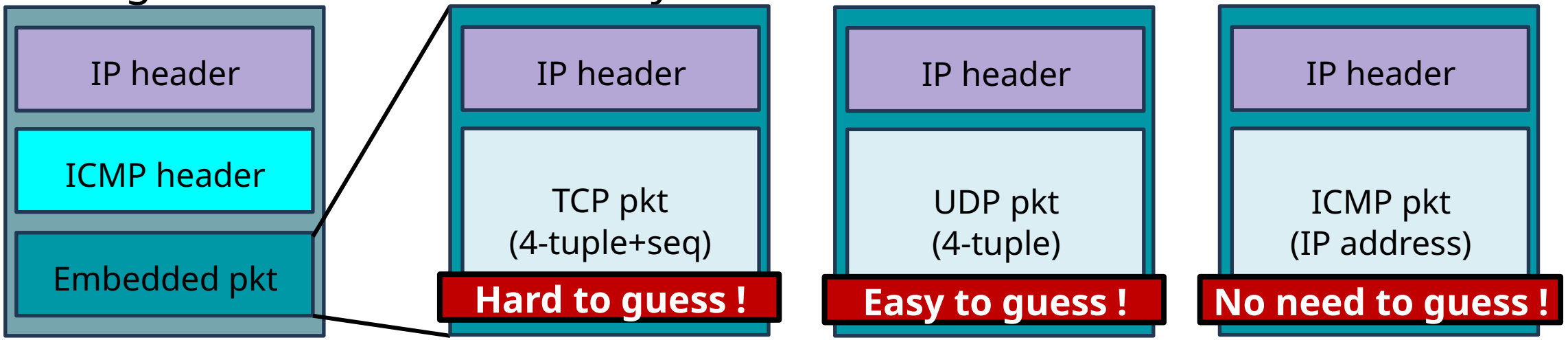
- **Question 1: State Storage**
  - **Eliminated**: The SYN-cookie style challenge generation method directly eliminates the need for random number storage.

- **Question 2**: **Amplification Attack**
  - **Not So Much**: Challenges are carried in next packets being sent, the only extra overhead is an IP option.

- **Question 3: Packet Lost**
  - **Rare**: We conducted tests on cloud servers in multiple countries and regions and found that no server directly filter packets with challenges.

Updates since IETF 123 & 124

- **Question 1:** "Why not just check the embedded packet?"
  - That check only works for stateful TCP, because its headers contain secrets (like sequence numbers) that are hard for an attacker to guess.
  - But for stateless UDP & ICMP, the headers have no secrets. They are trivial to forge. This is the vulnerability we fix.



  - **Clarified.** The draft now better emphasizes that the mechanism's primary value is for stateless protocols (UDP, ICMP).

Updates since IETF 123 & 124

- **Question 2: "Story-Based" Document Style**
  - **Rewritten** : We have rewritten the document to be a direct technical specification.
- **Question 3: Multi-path Routing：** What if the packet takes a different path?
  - **In a Single Event:**
    - The challenge will miss the original router.
    - The host receives no confirmation and **ignores that specific ICMP error.**
  - **What Happens Next? (The Stateless Recovery):**
    - Our mechanism is **stateless**. It doesn't remember the path failure.
    - If the application sends another packet that hits the same problematic path again, a **new ICMP error is generated.**
    - This **restarts the process**: a new, independent challenge will be sent.
  - **Action**: A new section rewritten is added to discuss the Multi-path Routing problem.

Next Step

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

Thanks!