TuDoor Attack: Systematically Exploring and Exploiting Logic Vulnerabilities in DNS Response Pre-processing with Malformed Packets

Xiang Li [1] Wei Xu [1] Baojun Liu [1] Mingming Zhang [1 3] Zhou Li [2 ✉] Jia Zhang [1 3]
Deliang Chang [5] Xiaofeng Zheng [1 5] Chuhan Wang [1] Jianjun Chen [1 3] Haixin Duan [1 3 4 ✉] Qi Li [1 ✉]

[1] Tsinghua University [2] University of California, Irvine [3] Zhongguancun Laboratory [4] Quan Cheng Laboratory [5] QI-ANXIN Technology Research Institute ✉ Corresponding Author(s)

UCI Samueli
School of Engineering
University of California, Irvine

DNS Resolution and Packet

- Translate human-friendly domain names into machine-readable IP addresses and vice versa.
- **Multiple resolver roles:** stub, forwarder, recursive, and authoritative.
- **Iterative resolution process:** C/S style, recursive resolution, and caching.

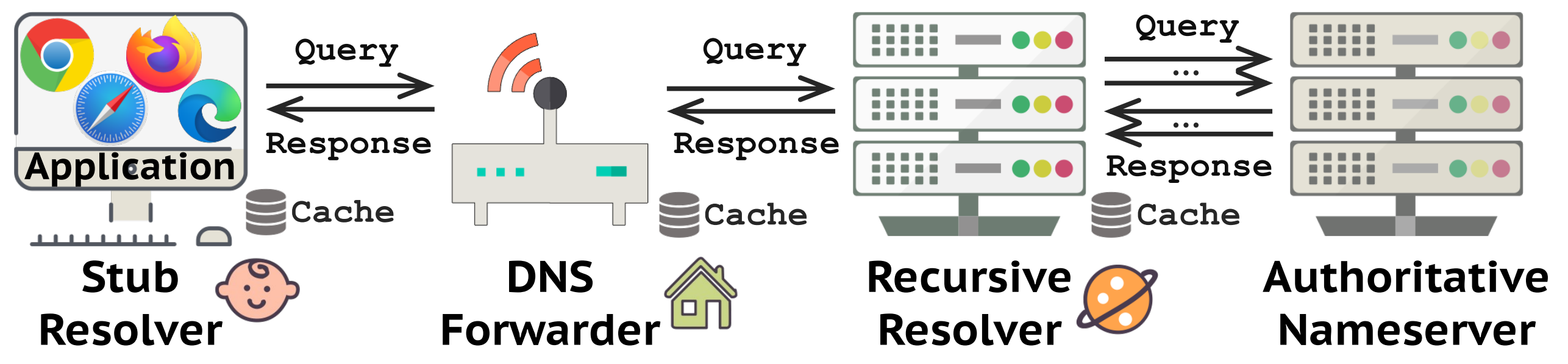
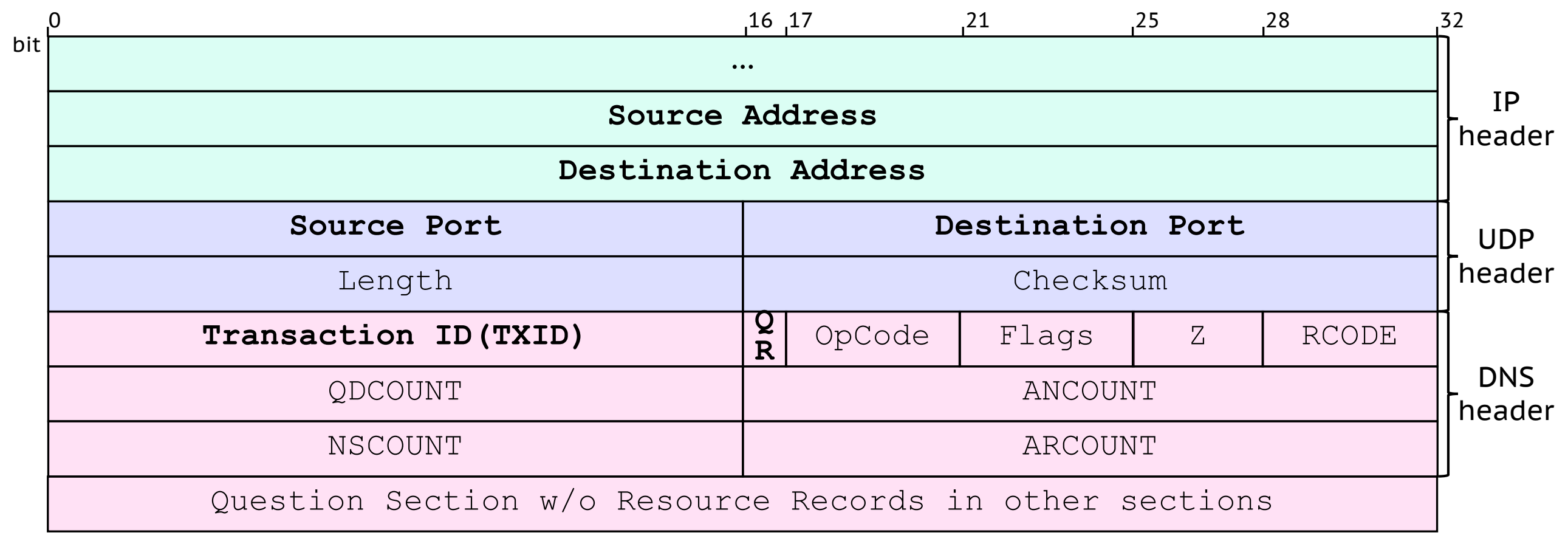


Figure 1. General DNS resolver roles and domain name resolution process.

- Communicating primarily over **UDP**.
- **DNS packet:** a 12-byte DNS header and a DNS body.
- **Two important fields:** `TxID` for authentication and `QR` indicating a query (0) or response (1).



bit 0	16	17	21	25	28–32	
...						IP header
Source Address						
Destination Address						
Source Port	**Destination Port**					UDP header
Length	Checksum					
Transaction ID(TXID)	**QR**	OpCode	Flags	Z	RCODE	DNS header
QDCOUNT	ANCOUNT					
NSCOUNT	ARCOUNT					
Question Section w/o Resource Records in other sections						

Figure 2. DNS packet format on UDP.

DNS Cache Poisoning Attacks

- **Injecting forged responses** into resolvers' cache and hijacking domains and traffic.
- DNS cache poisoning attacks **continue to be proposed** after multiple mitigation solutions.

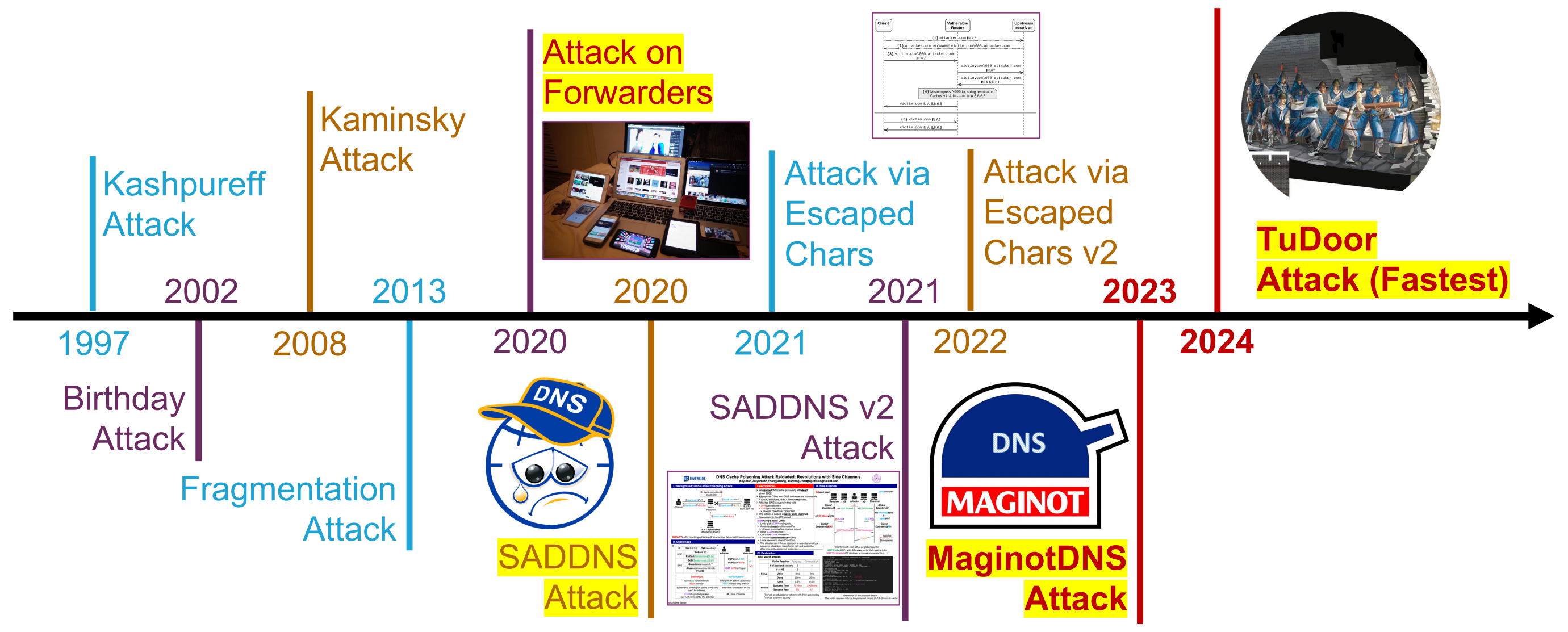


Figure 3. Timeline of DNS cache poisoning attacks.

TuDoor Attack [1]

- New powerful **DNS-related attacks:** cache poisoning, DoS, and resource consuming.
- **TuDoor in the DNS Wall:** a very covert side-channel like 突门 in the Great Wall.
- **Exploiting vulnerabilities** in **DNS response Pre-processing** with malformed packets.

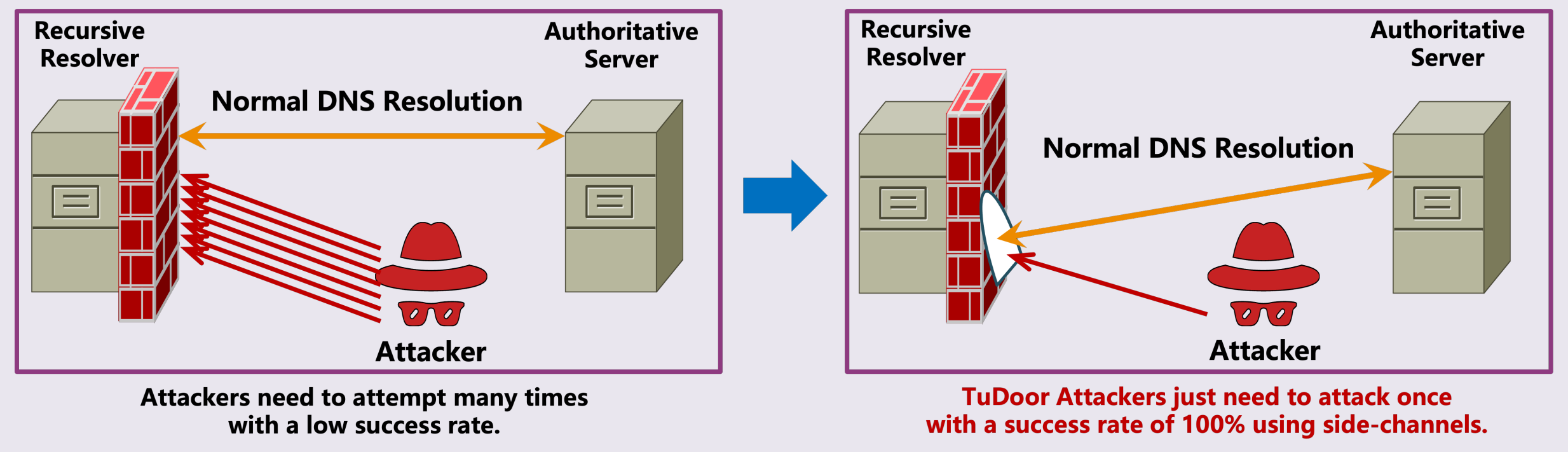

Recursive Resolver
Authoritative Server
Normal DNS Resolution
Attacker
Attackers need to attempt many times with a low success rate.
Recursive Resolver
Authoritative Server
Normal DNS Resolution
Attacker
TuDoor Attackers just need to attack once with a success rate of 100% using side-channels.

Figure 4. TuDoor attack model.

Analysis of DNS Response Pre-processing

- DNS response pre-processing **never been studied** thoroughly, leaving potential threats.
- **What we did:** constructing **state machines** for response pre-processing and finding bugs.

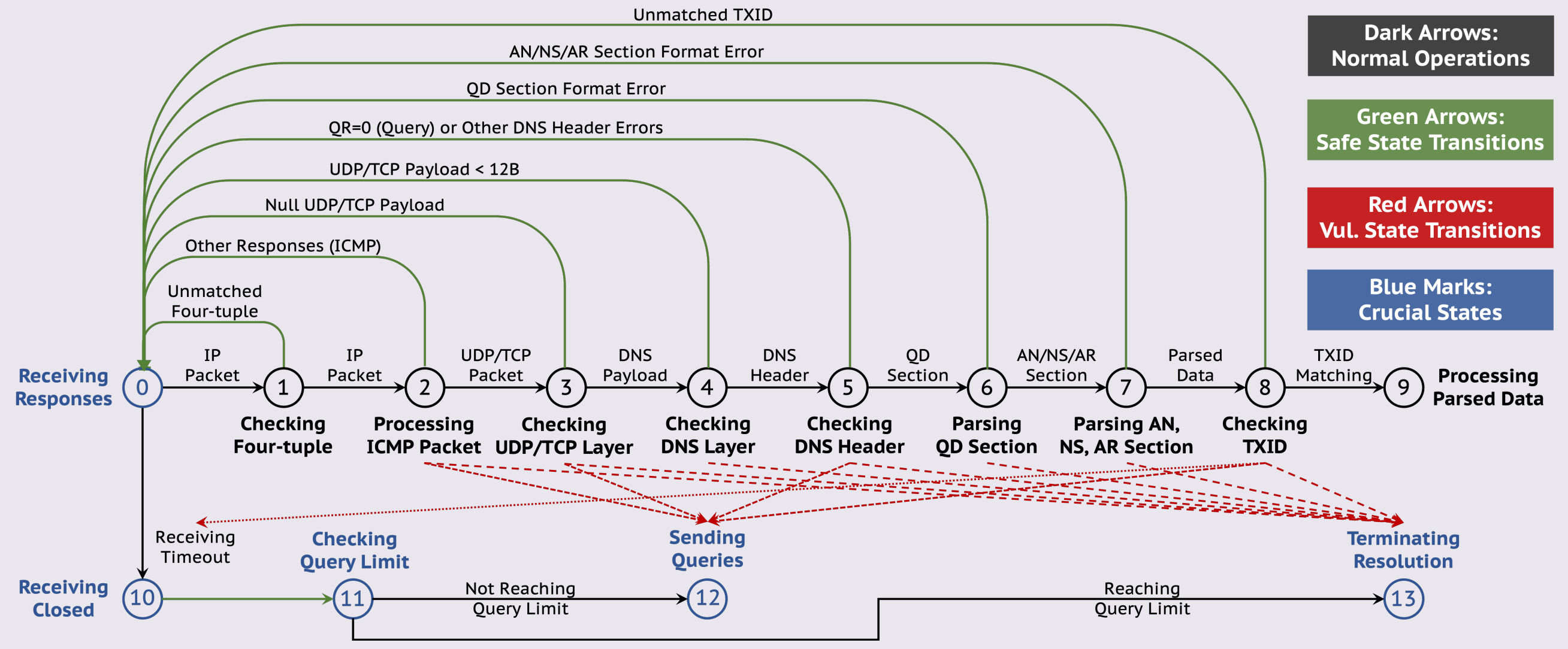


Figure 5. General state machine model of DNS response pre-processing (Except for the red dotted arrows).

Vulnerable State Transitions

- **28 DNS software:** 8 recursive, 10 forwarders, 6 stub, and 4 DNS libraries (**24 vulnerable**).

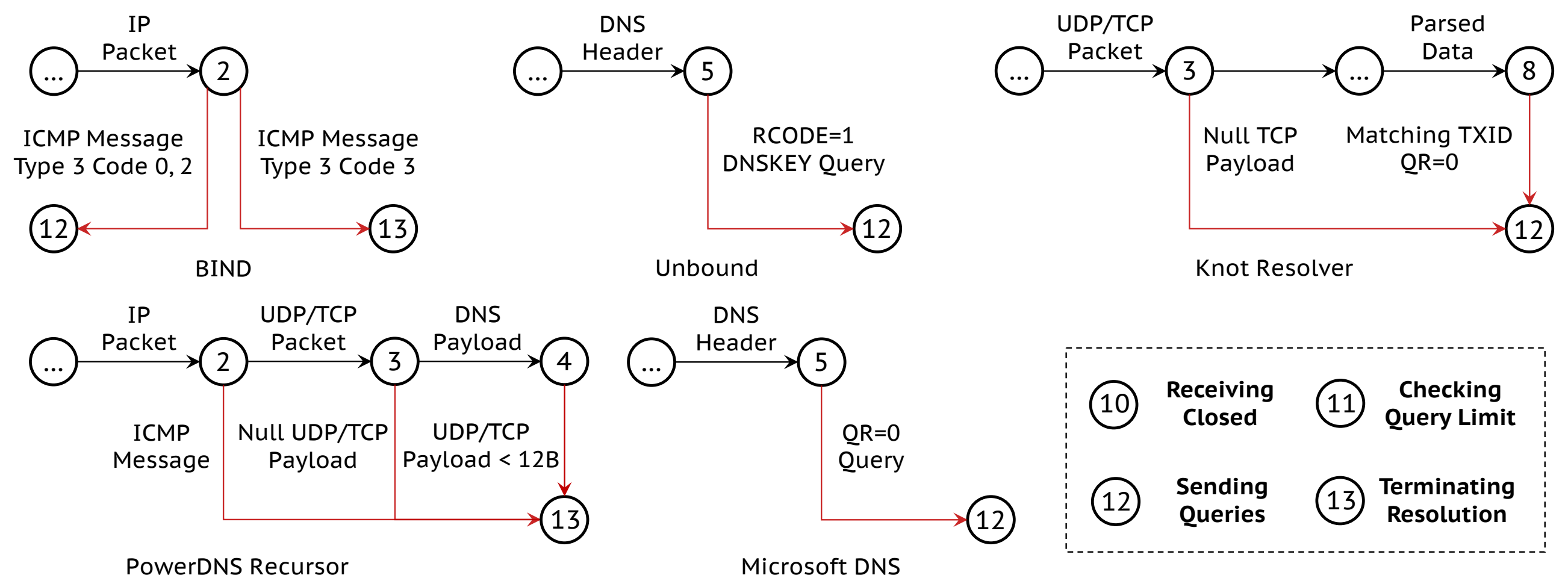


Figure 6. Part of vulnerable state transitions with red lines.

TuDoor Attack Example (1/3): DNS Cache Poisoning

- Exploiting one **new side-channel vulnerability** to locate the source port with 2,500 packets and brute-force 65,536 TxIDs (The **fastest DNS cache poisoning attack** on Microsoft DNS).
- **Attack time:** avg. **425ms**, **200 – 1,000 times faster** than prior attacks under the same conditions.

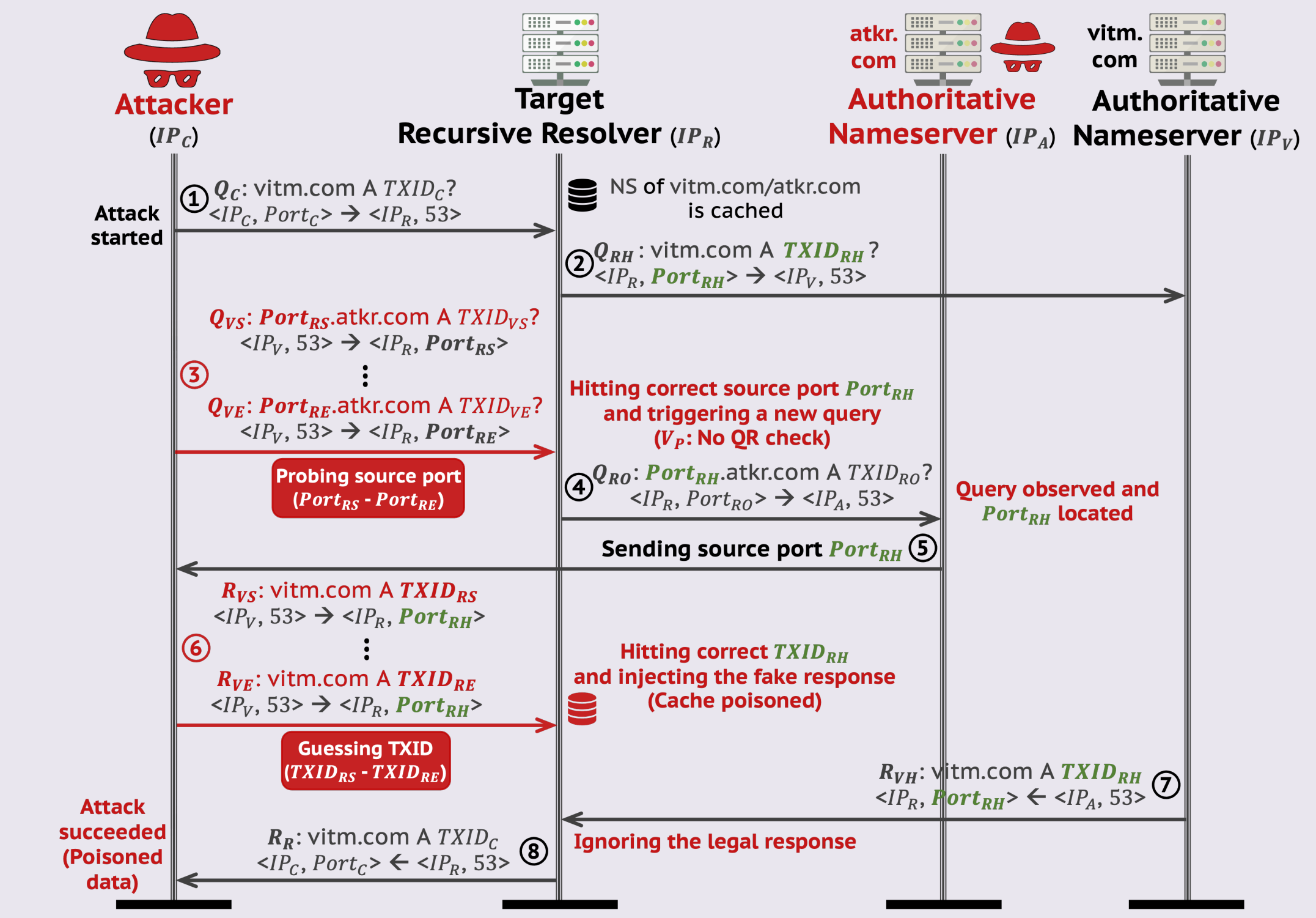

Attacker (IP_C)
Target Recursive Resolver (IP_R)
atkr. com Authoritative Nameserver (IP_A)
vitm. com Authoritative Nameserver (IP_V)
Attack started
① Q_C: vitm.com A $TXID_C$? <IP_C, $Port_C$> → <IP_R, 53>
NS of vitm.com/atkr.com is cached
② Q_{RH}: vitm.com A $TXID_{RH}$? <IP_R, $Port_{RH}$> → <IP_V, 53>
③ Q_{VS}: $Port_{RS}$.atkr.com A $TXID_{VS}$? <IP_V, 53> → <IP_R, $Port_{RS}$>
Q_{VE}: $Port_{RE}$.atkr.com A $TXID_{VE}$? <IP_V, 53> → <IP_R, $Port_{RE}$>
Probing source port ($Port_{RS}$ - $Port_{RE}$)
Hitting correct source port $Port_{RH}$ and triggering a new query (V_P: No QR check)
④ Q_{RO}: $Port_{RH}$.atkr.com A $TXID_{RO}$? <IP_R, $Port_{RO}$> → <IP_A, 53>
Query observed and $Port_{RH}$ located
Sending source port $Port_{RH}$ ⑤
⑥ R_{VS}: vitm.com A $TXID_{RS}$ <IP_V, 53> → <IP_R, $Port_{RH}$>
R_{VE}: vitm.com A $TXID_{RE}$ <IP_V, 53> → <IP_R, $Port_{RH}$>
Guessing TXID ($TXID_{RS}$ - $TXID_{RE}$)
Hitting correct $TXID_{RH}$ and injecting the fake response (Cache poisoned)
R_{VH}: vitm.com A $TXID_{RH}$ <IP_R, $Port_{RH}$> ← <IP_A, 53> ⑦
Ignoring the legal response
Attack succeeded (Poisoned data)
R_R: vitm.com A $TXID_C$ <IP_C, $Port_C$> ← <IP_R, 53> ⑧

Figure 7. Attack steps of DNS cache poisoning.

Vulnerable Population and Mitigation Solution

- **Vulnerable:** **24/28** DNS software, **18/42** public services, and **423k (23.1%)** open resolvers.
- **Mitigation:** improving poor DNS response pre-processing implementations.
- **Disclosure:** **14 vendors** confirmed TuDoor with **33 CVEs** assigned.
- **Detection & online tool:** https://test.tudoor.net.

Figure 8. Part of vulnerable DNS vendors.

References

[1] Xiang Li, Wei Xu, Baojun Liu, Mingming Zhang, Zhou Li, Jia Zhang, Deliang Chang, Xiaofeng Zheng, Chuhan Wang, Jianjun Chen, Haixin Duan, and Qi Li.
TuDoor Attack: Systematically Exploring and Exploiting Logic Vulnerabilities in DNS Response Pre-processing with Malformed Packets.
In *Proceedings of 2024 IEEE Symposium on Security and Privacy*, IEEE S&P '24, 2024.