Off-Path TCP Exploit: How Wireless Routers Can Jeopardize Your Secrets

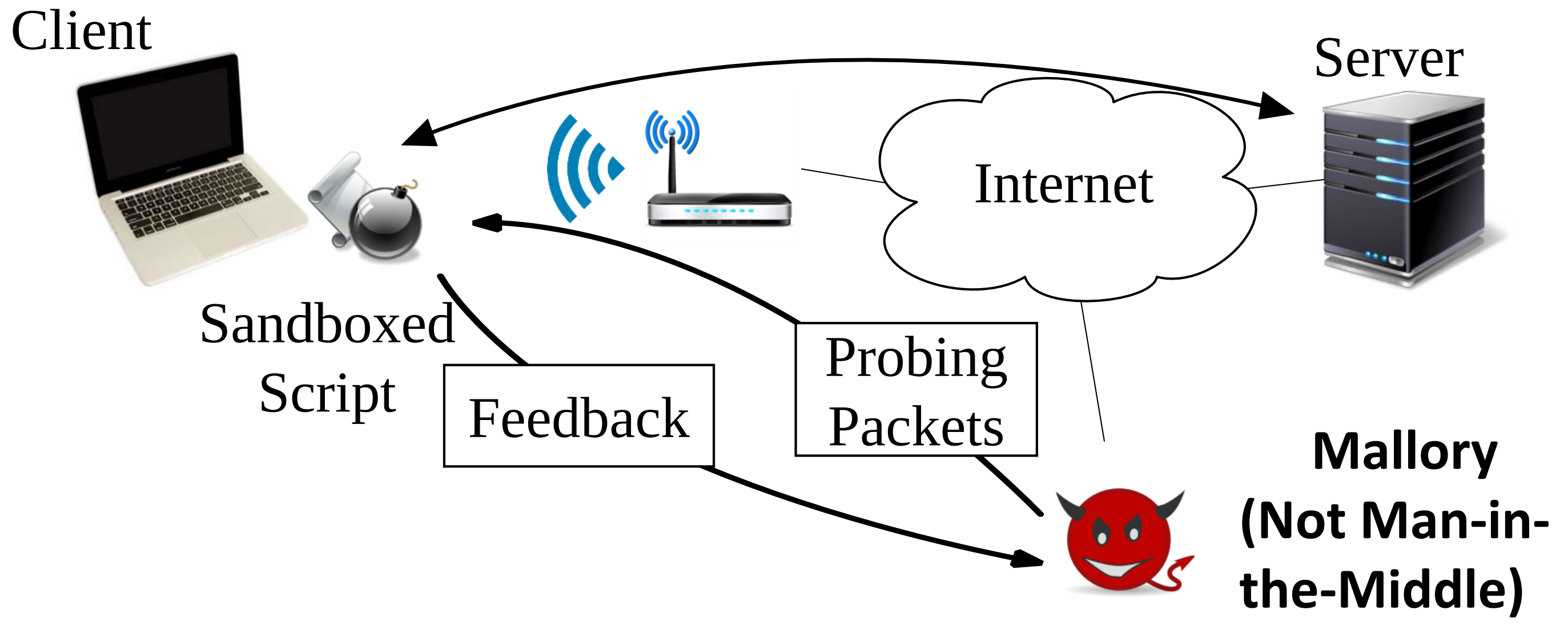
Weiteng Chen & Zhiyun Qian
University of California, Riverside

Vulnerability Overview

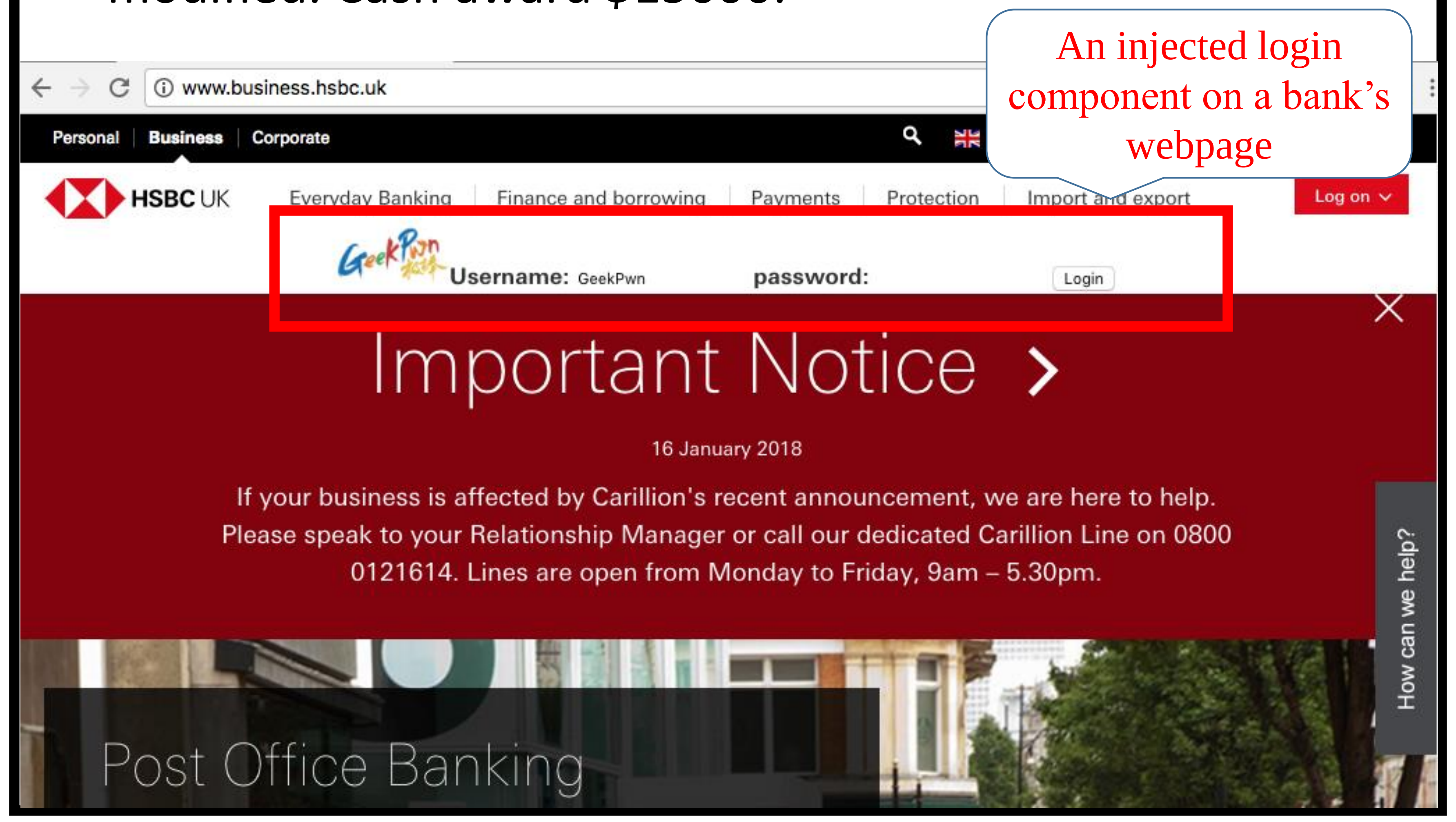
We report a nearly ***impossible-to-fix network side channel vulnerability*** rooted in the "half-duplex" design of all generations of IEEE 802.11 protocols.

It allows a blind off-path attacker to hijack chosen TCP connections, as long as one end-host is connected to the Internet via Wi-Fi.

Threat Model



- Mallory can hijack connections between the client and server by injecting malicious HTTP payload.
- Client browser caches will be permanently poisoned.
- Demoed at Geekpwn 2017 -- a banking homepage is modified. Cash award $15000.



An injected login component on a bank's webpage

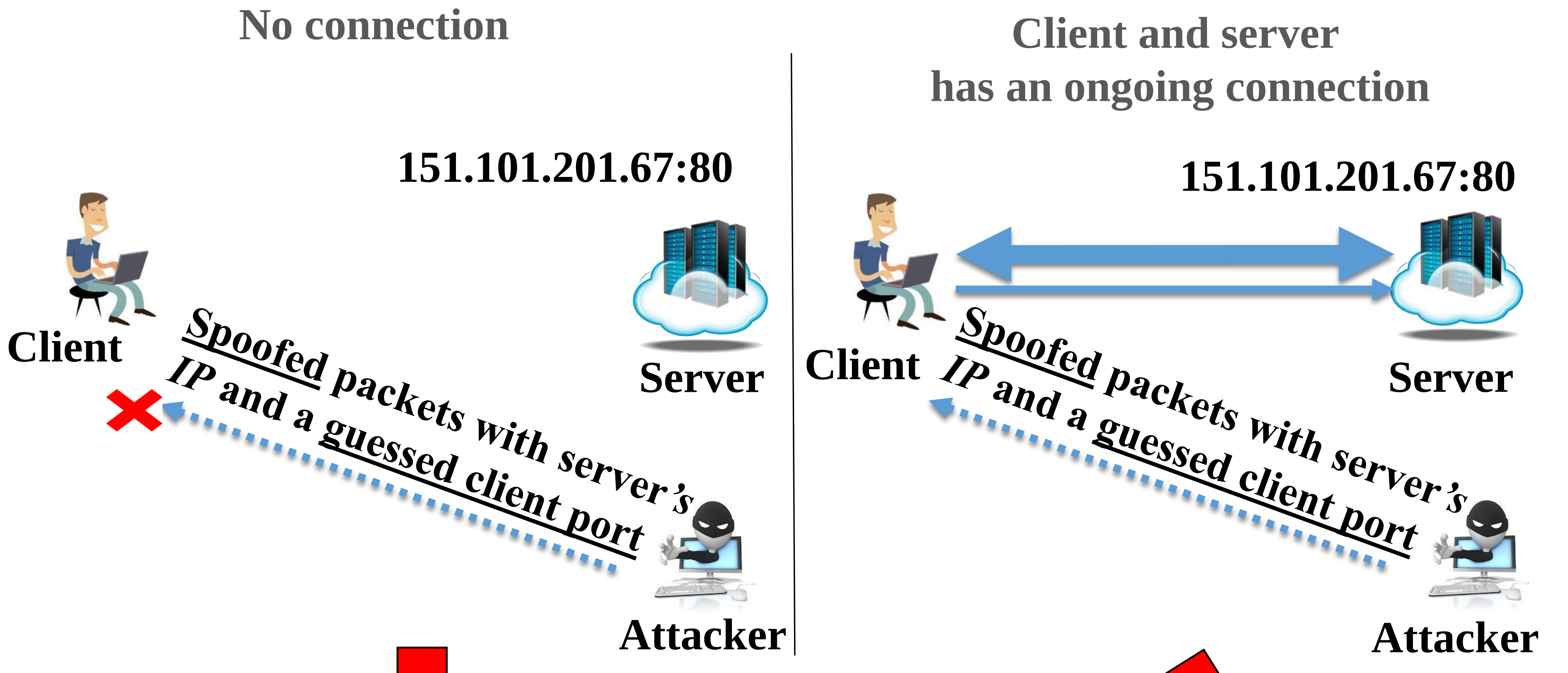
Important Notice >

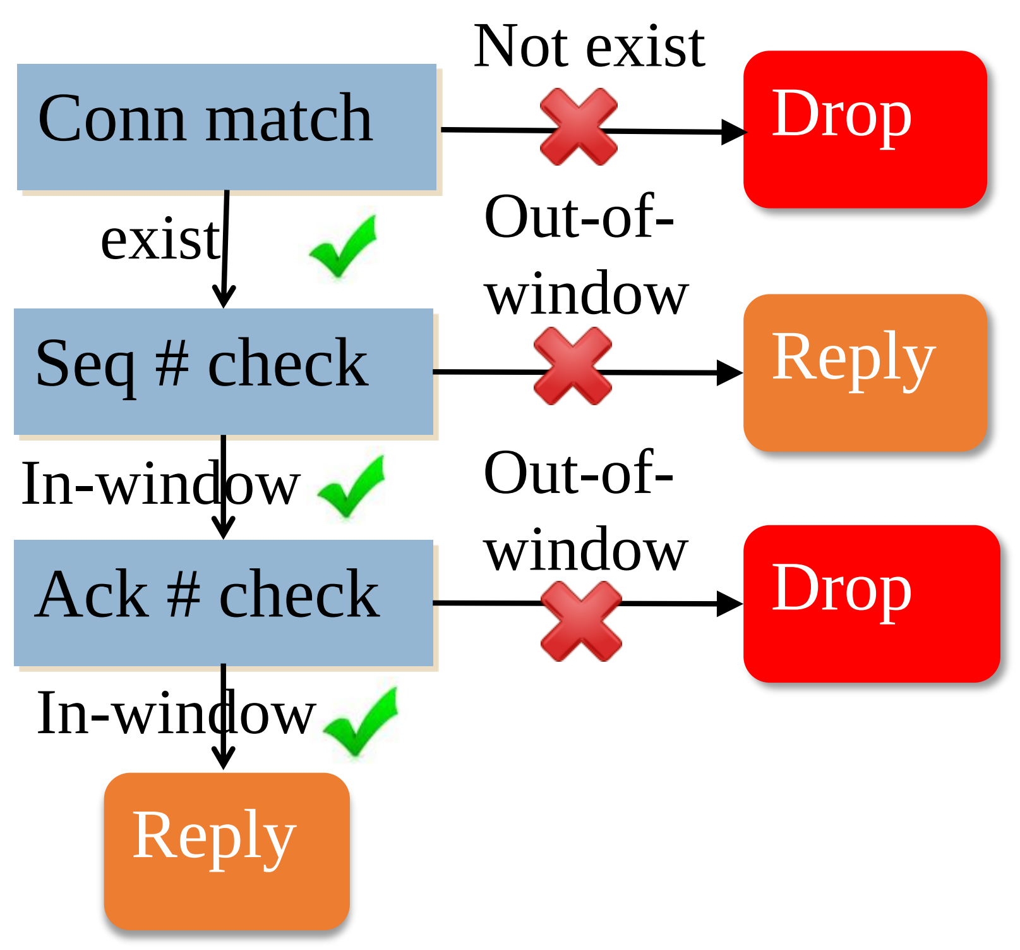
16 January 2018

If your business is affected by Carillion's recent announcement, we are here to help. Please speak to your Relationship Manager or call our dedicated Carillion Line on 0800 0121614. Lines are open from Monday to Friday, 9am – 5.30pm.

Post Office Banking

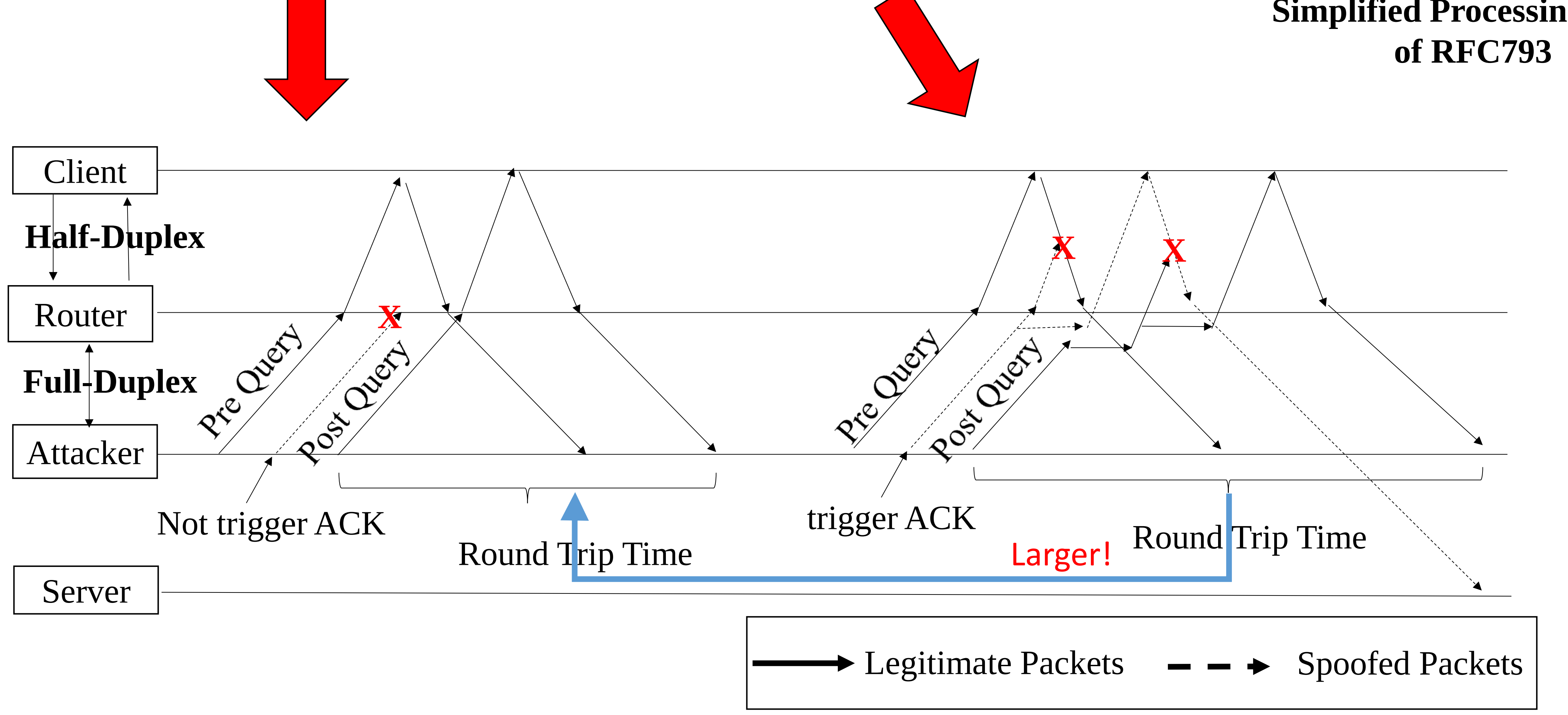
Connection Inference


No connection
151.101.201.67:80
Client
Server
Spoofed packets with server's IP and a guessed client port
Attacker
Client and server has an ongoing connection
151.101.201.67:80
Client
Server
Spoofed packets with server's IP and a guessed client port
Attacker



Simplified Processing Logic of RFC793

- Depending on whether the guessed port number matches an ongoing connection, the client will behave differently i.e., with/without replies.
- By leveraging the side channel we discovered, the attacker can indirectly observe the difference indirectly through timing.
- Sequence and acknowledgement number inference is almost the same as port number inference.



Wireless Timing Side Channel

- The *half-duplex* nature of Wi-Fi creates a "shared resource" among uplink and downlink traffic – only one direction can transmit at the same time.
- Probing strategy: A spoofed probing packet along with a pre-probe query and post-probe query
- Not trigger ACK → little contention → small RTTs
- Trigger ACK → high contention → large RTTs
- The signal is amplifiable: More probing packets → more contention → larger RTTs

Results

- Local experiment

OS	Success Rate	Avg time cost
Linux	10/10	188.80s
MacOS	10/10	48.91s
Windows	10/10	43.42s

- Remote experiment – RTT = 20ms

MacOS	9/10	304.18s

Conclusion

- A timing side channel in Wi-Fi which indirectly affects TCP in all OSes, as long as the host is behind Wi-Fi
- Demo of the threat.
- Reported to IEEE 802.11 working group --- **impossible to fix.**