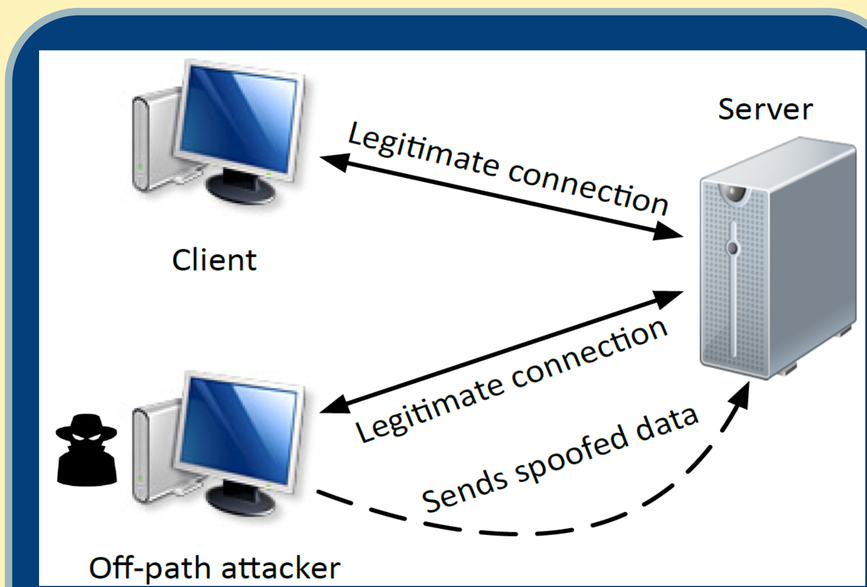
TCP Modern Side Channel Attacks

Zhiyun Qian, University of California, Riverside

Research Goals

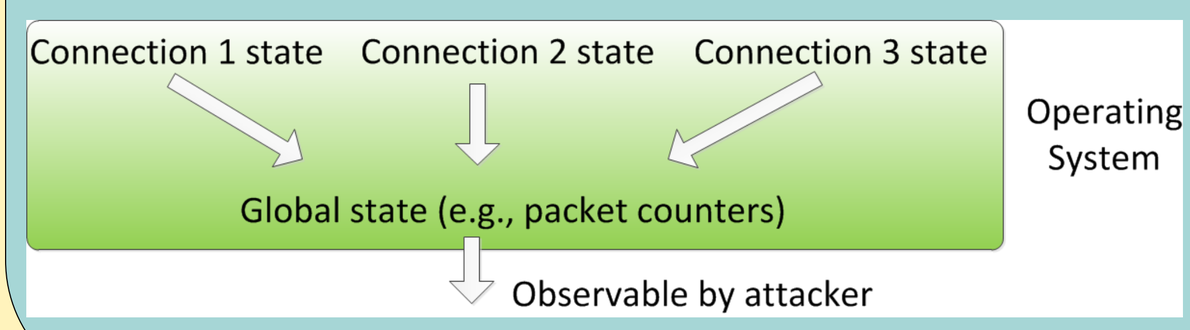
- **Understanding the root causes of TCP side channels**
  - Why do they exist and how they manifest?
  - What type of side channels are there?
- **Modeling of the exploits or vulnerabilities**
  - Is the side channel introduced in the network protocol specification or implementation?
  - Can we anticipate new or variants of existing network side channels through the model?
- **Defenses**
  - How do we systematically defend against this class of attacks? Discovery-based or prevention-based?

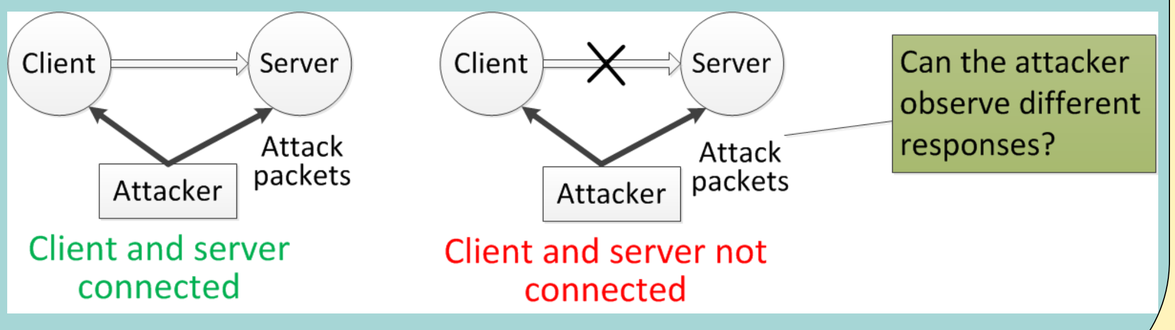


Thread model of one type of network side channel attacks where the attacker is attempting to learn state of the legitimate connection

Approach

- Identify global state shared across connections (e.g., rate limit counters) and what internal information (e.g., connection state) can impact the global state
- Understand whether the global state can be leaked to an attacker through attacker-observables such as packet counters, network traffic, or timing of the traffic





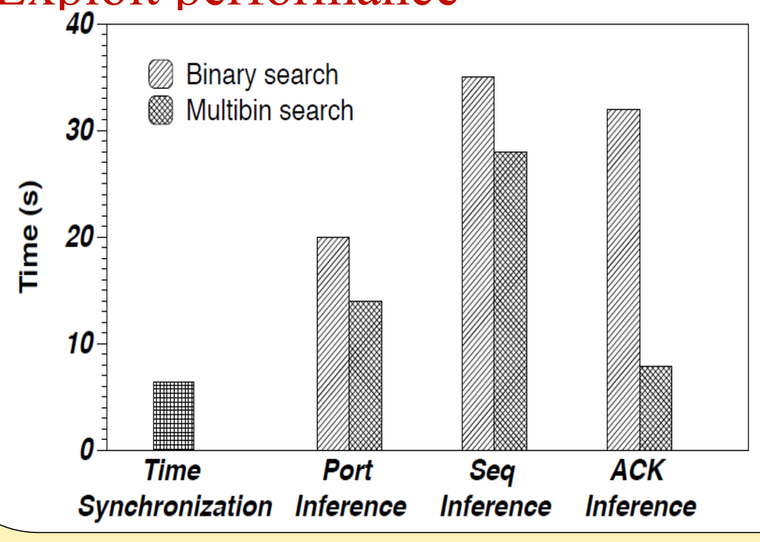
CVE-2016-5696 identified and reported

– Discover a vulnerability through a global variable (rate limit), which:
  - Enforces the maximum number of challenge ACKs per second
  - Is shared by all ongoing TCP connections

Impact: an pure off-path attacker can:

- Test if two arbitrary hosts on the Internet are communicating and on what ports
- Infer the TCP sequence number of both client and server
- Perform reset and injection attacks

Exploit performance



Node	Country	Success Rate	Avg % of rounds with loss	BW (pkts)	Time Cost(s)
62.210.x.x	FR	8/10	4.58%	4000	46.36
89.163.x.x	DE	9/10	7.97%	4000	49.08
178.62.x.x	GB	7/10	4.20%	4000	53.00
198.27.x.x	NA	10/10	1.45%	4000	59.86
192.150.x.x	NL	8/10	5.64%	4000	68.03
62.210.x.x	FR	6/10	5.85%	4000	49.57
89.163.x.x	DE	8/10	3.06%	4000	52.51
178.62.x.x	GB	8/10	8.15%	4000	78.35
198.27.x.x	NA	7/10	3.64%	4000	72.49
192.150.x.x	NL	6/10	7.14%	4000	79.42

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Biennial Principal Investigator Meeting
Jan. 9 -11th 2017
Arlington, Virginia

UNIVERSITY OF CALIFORNIA UCRIVERSIDE