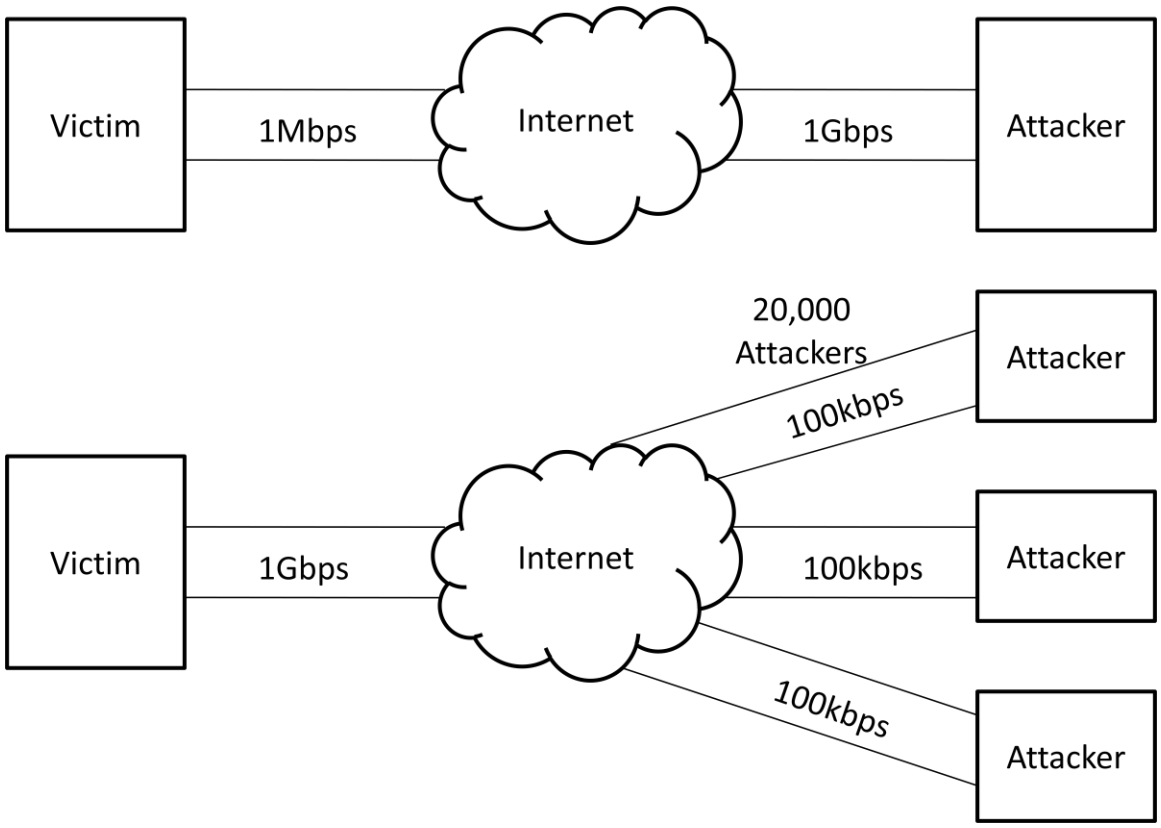
Denial of Service Attack

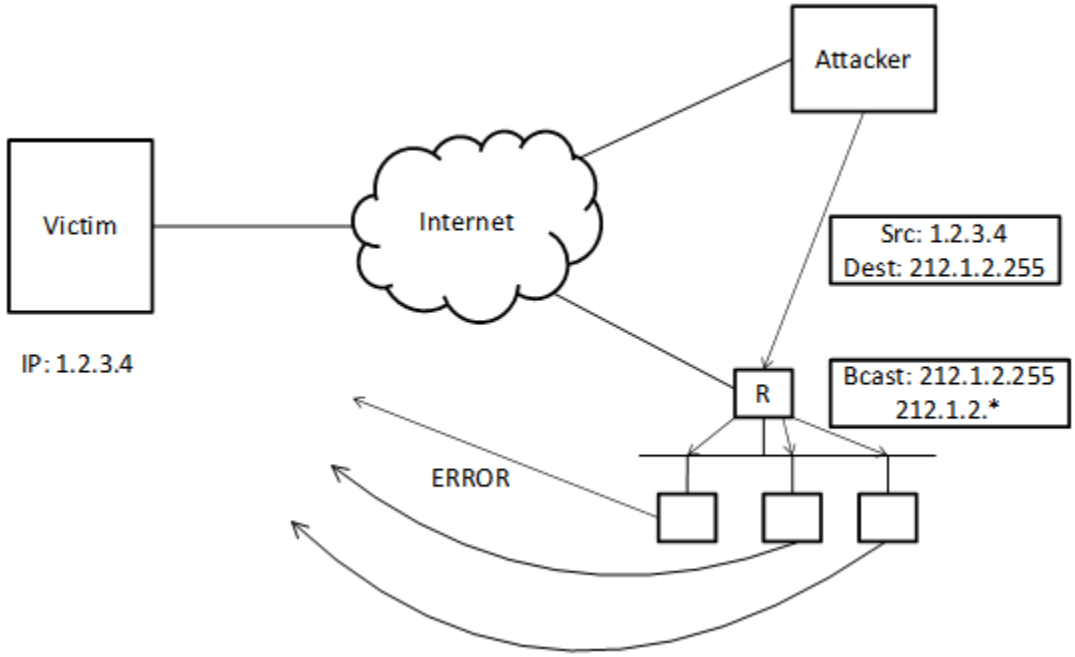
- Crashing Program
- Resource Exhaustion
    - Network bandwidth
    - Memory
    - OS resources
    - Disk
    - CPU

Some Network DoS Attacks



More attacker machines => Harder to distinguish attackers

SMURF Attack



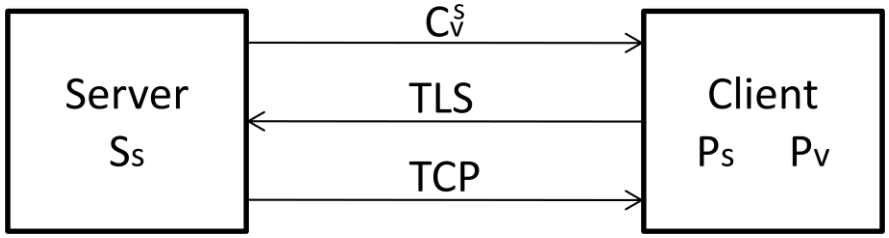
CPU DoS

- Algorithmic Complex Attacks
  Example: Hash Table
  i = hash(x);
  append (bucket[i], x);
- Hash function is typically fixed & public
  ⇨ Easy for an attacker to find collisions

Attack

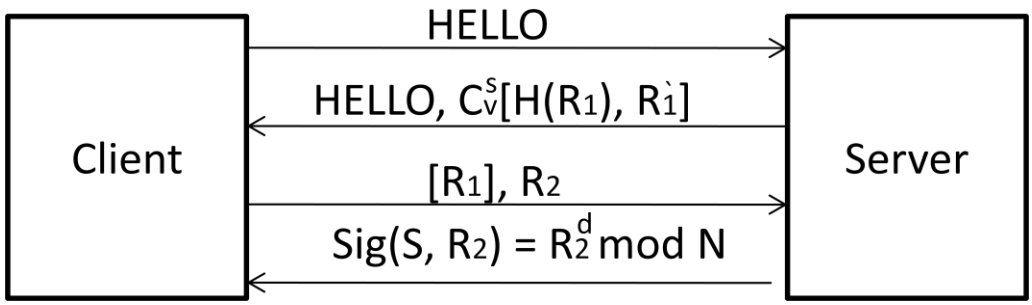
1) Choose many inputs X_1, …, X_n that all hash to 0
2) Interact with server to cause it to insert X_1, …, X_n into its hash table
3) Force server to do HT lookups

TLS / SSL



TLS guarantees:

- Secrecy
- Authenticity
- Server identity



Verify certificate and R_1

Verify signature

- Modular exponentiation is slow
- Typical Desktop ≈ 100 s/sec

Client Puzzles

Problem:

- Doesn't distinguish real from attacker
- Must be configured system
- Discriminates against slow clients

CPU Puzzles vs Memory Puzzles

Top end machine	3GHz	2GB
Phone	0.1GHz	128MB
	30	16