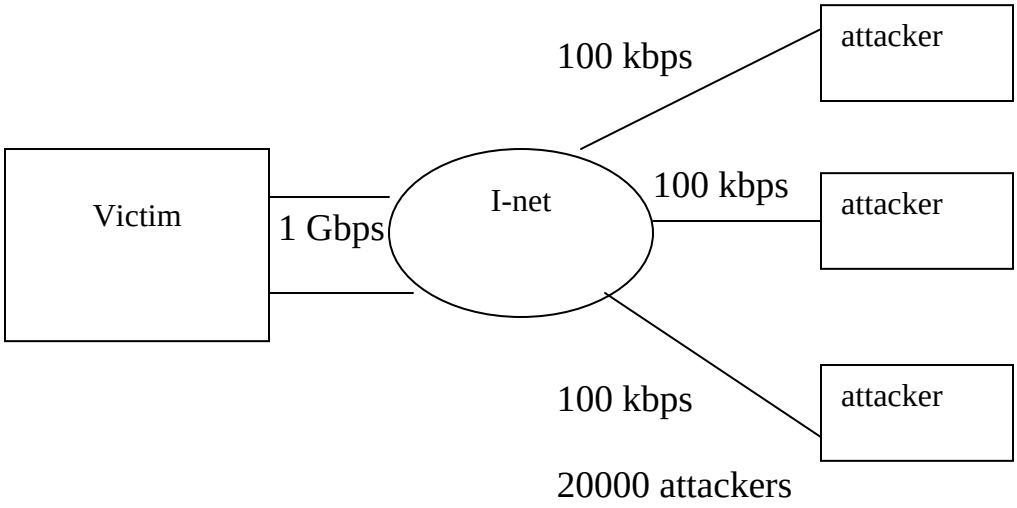
Class Note for CSE 509 (4/17)

Denial of Service Attacks

- Crashing program
- Resource exhaustion
  - Network bandwidth
  - Memory
  - OS resources
  - Disk
  - CPU

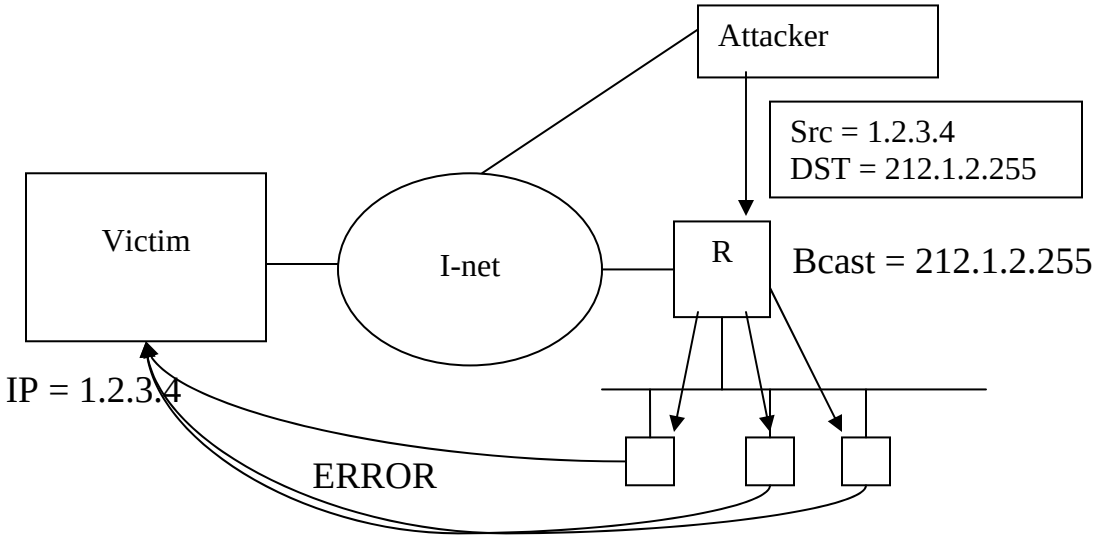
1. Some network Dos attacks



20000 attackers

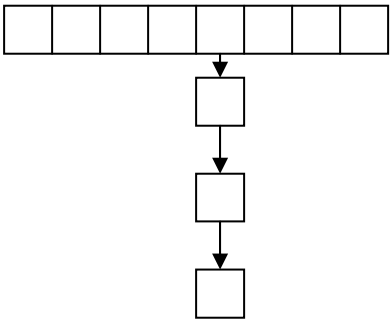
more attacker machines ➔ hard to distinguish attackers

2. Smurf attack



3. CPU Dos

- Algorithmic complexity Attacks
  - Example : Hash Tables
    i = hash(x)
    append(bucket[i], x)

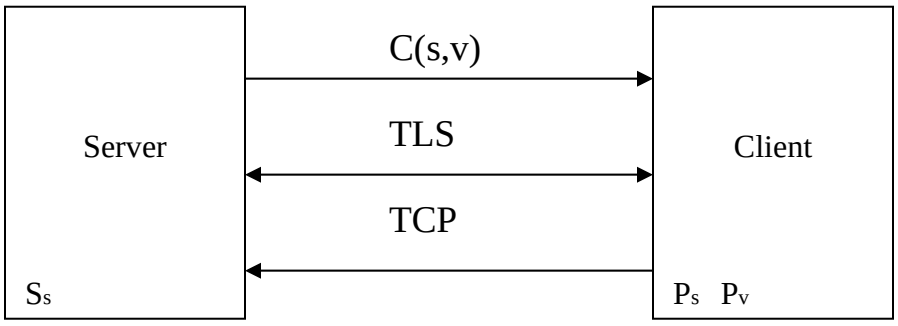


hash function is typically fixed and public
→ easy for an attacker to find collisions.

Attack (input: x1, … xn)

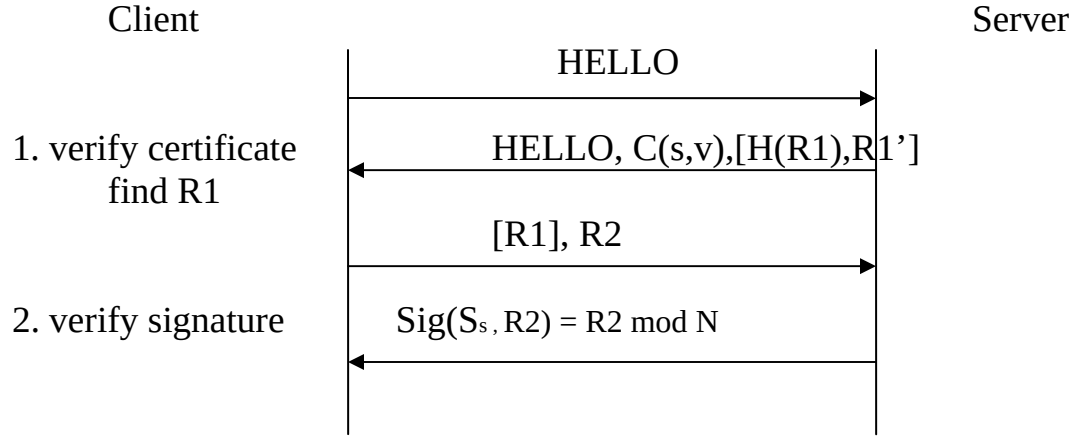
1). Choose many inputs that all hash to 0
2). Interact w/ server to cause it to insert x1,…xn into its hash table
3). Force server to do hash table lookups

4. TLS/SSL



TLS guarantees

- secrecy
- authenticity
- server identity



- modular exponentiation is slow
- typical Desktop == 100 sig/sec

Client puzzles

- problems
  - Does not distinguish real from attacks
  - Must be configured / system

CPU puzzles vs memory puzzles

	CPU	Memory
TOP end machine	3 GHz	2 GB
Phone	.1 GHz	128MB
	<30>	<16>