Denial of Service

- Attacks that prevent legitimate users from doing their work
- By flooding the network
- Or corrupting routing tables
- Or flooding routers
- Or destroying key packets

How Do Denial of Service Attacks Occur?

- Basically, the attacker injects some form of traffic
- Most current networks aren't built to throttle uncooperative parties very well
- All-inclusive nature of the Internet makes basic access trivial
- Universality of IP makes reaching most of the network easy

An Example: SYN Flood

- Based on vulnerability in TCP
- Attacker uses initial request/response to start TCP session to fill a table at the server
- Preventing new real TCP sessions
- SYN cookies and firewalls with massive tables are possible defenses

Normal SYN Behavior

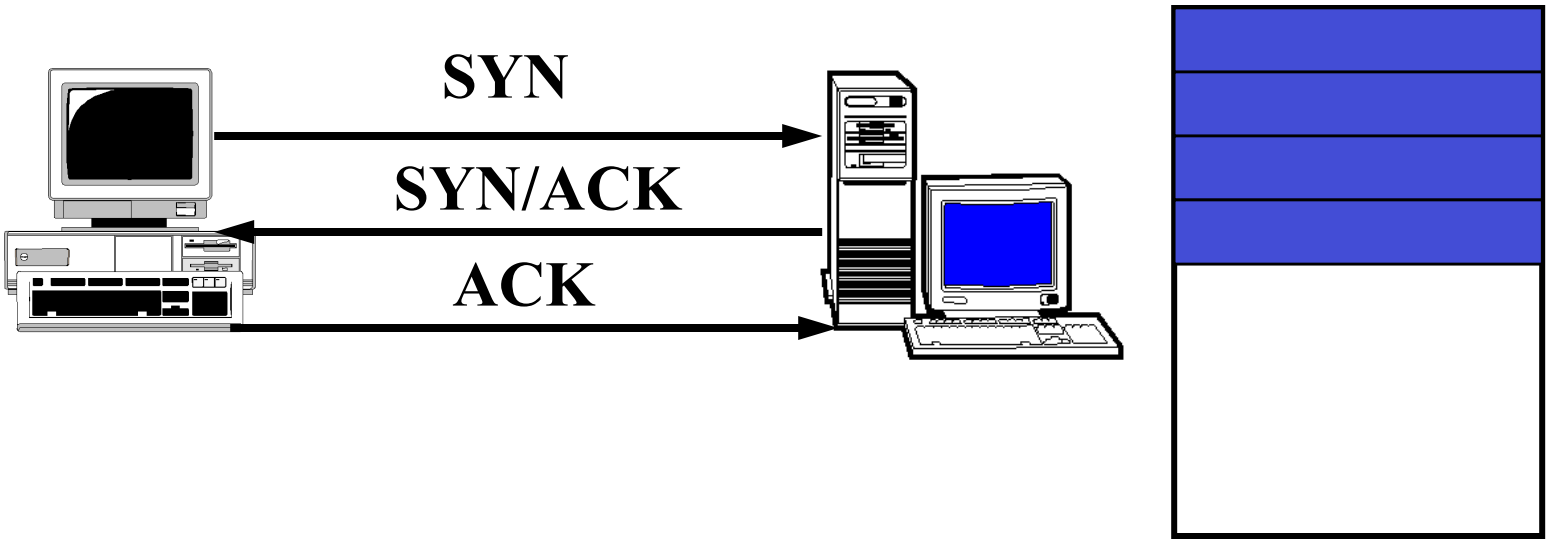
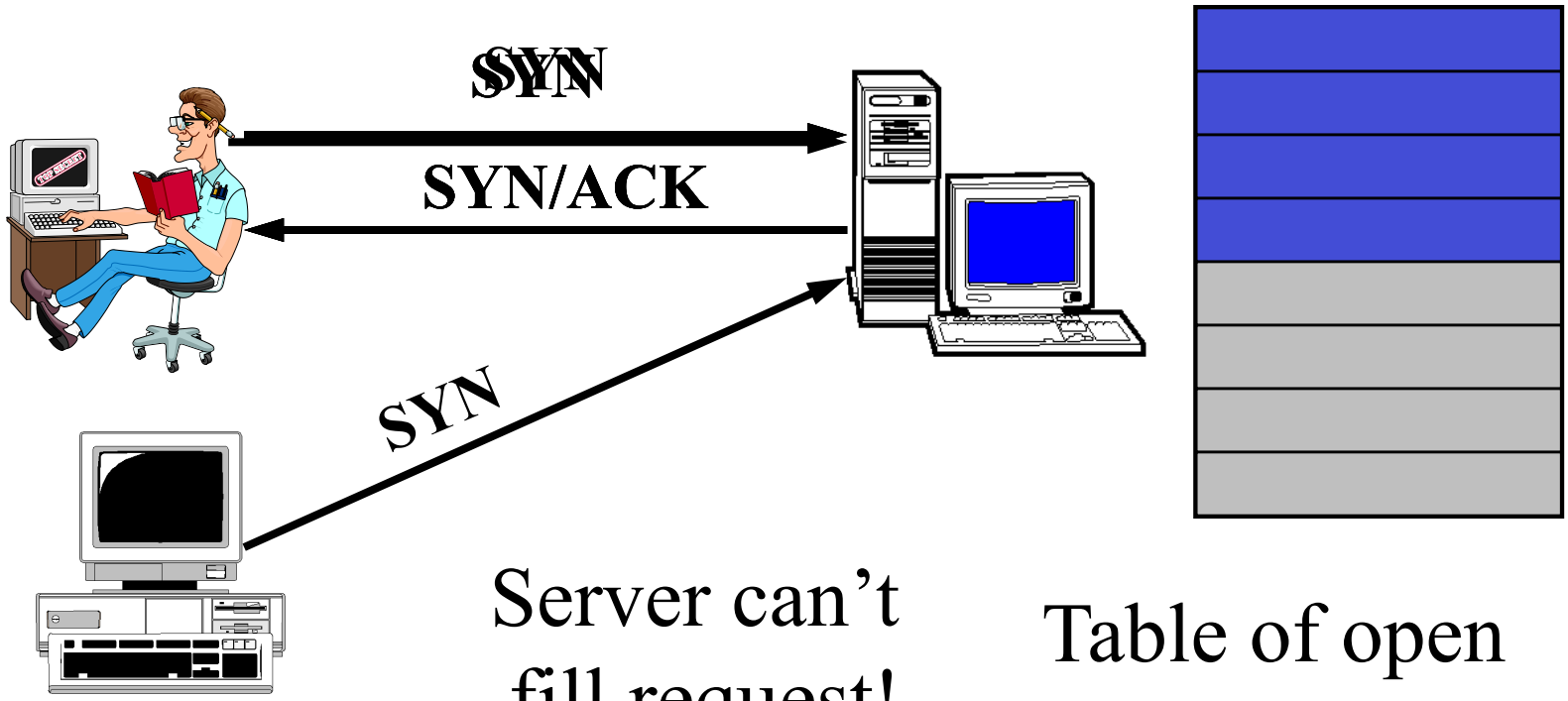


Table of open TCP connections

A SYN Flood



Server can't fill request!

Table of open TCP connections

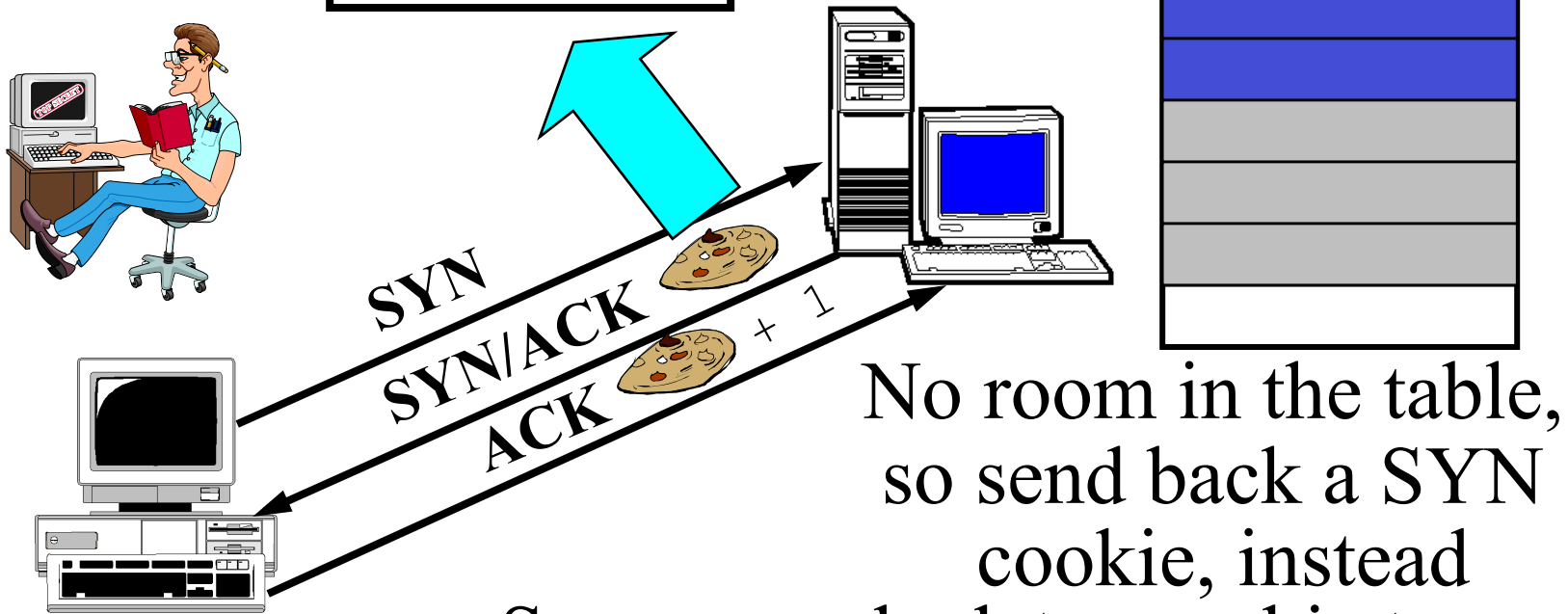
SYN Cookies

And no changes to TCP protocol itself

SYN/ACK number is secret function of various information

Client IP address & port, server's IP address and port, and a timer

KEY POINT: Server doesn't need to save cookie value!



No room in the table, so send back a SYN cookie, instead

Server recalculates cookie to determine if proper response

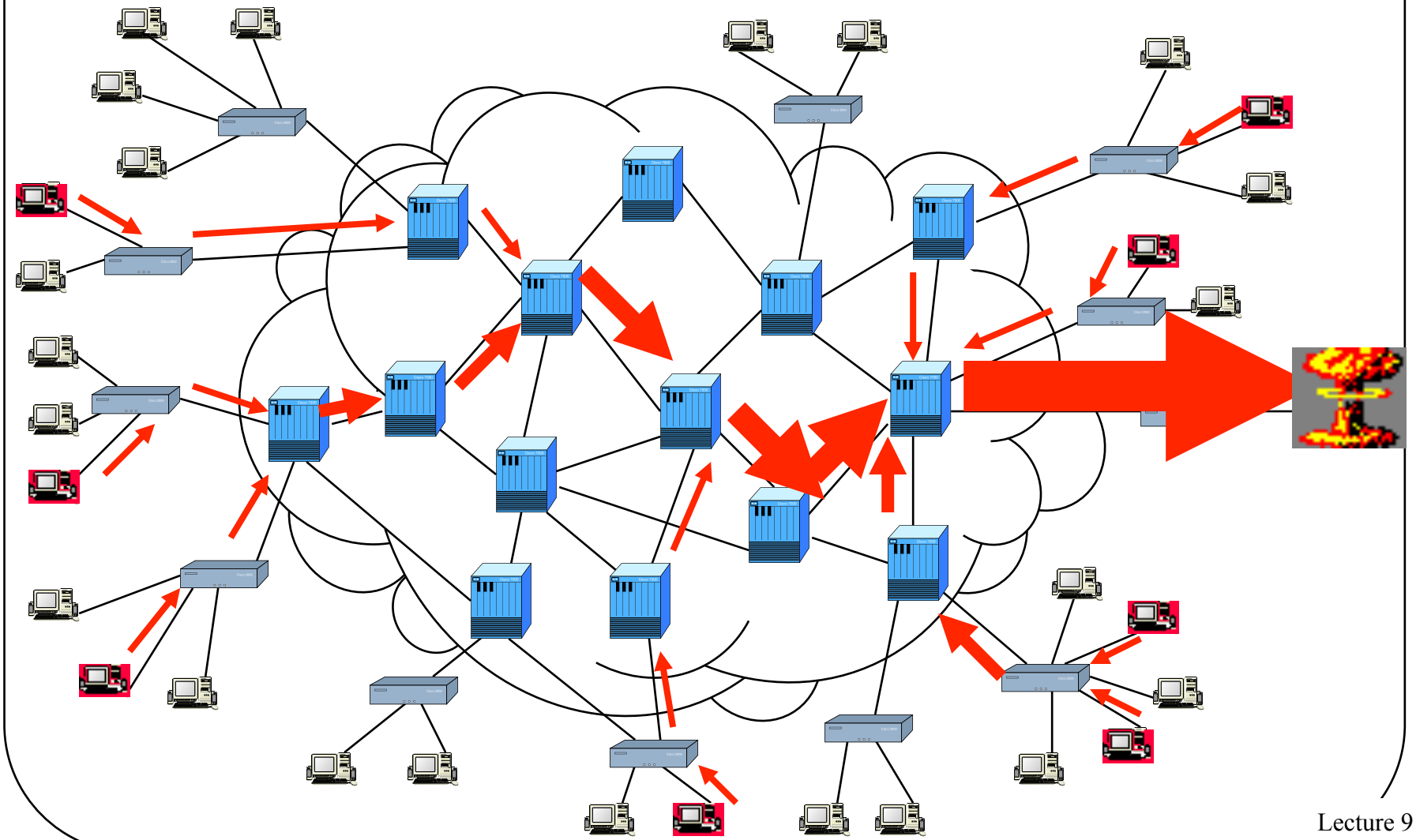
General Network Denial of Service Attacks

- Need not tickle any particular vulnerability
- Can achieve success by mere volume of packets
- If more packets sent than can be handled by target, service is denied
- A hard problem to solve

Distributed Denial of Service Attacks

- Goal: Prevent a network site from doing its normal business
- Method: overwhelm the site with attack traffic
- Response: ?

The Problem



Why Are These Attacks Made?

- Generally to annoy
- Sometimes for extortion
- Sometimes to prevent adversary from doing something important
- If directed at infrastructure, might cripple parts of Internet

Attack Methods

- Pure flooding
  - Of network connection
  - Or of upstream network
- Overwhelm some other resource
  - SYN flood
  - CPU resources
  - Memory resources
  - Application level resource
- Direct or reflection

Why “Distributed”?

- Targets are often highly provisioned servers
- A single machine usually cannot overwhelm such a server
- So harness multiple machines to do so
- Also makes defenses harder

How to Defend?

- A vital characteristic:
  - Don't just stop a flood
  - ENSURE SERVICE TO LEGITIMATE CLIENTS!!!
- If you deliver a manageable amount of garbage, you haven't solved the problem
- Nor have you if you prevent a flood by dropping all packets

Complicating Factors

- High availability of compromised machines
  - Millions of zombie machines out there
- Internet is designed to deliver traffic
  - Regardless of its value
- IP spoofing allows easy hiding
- Distributed nature makes legal approaches hard
- Attacker can choose all aspects of his attack packets
  - Can be a lot like good ones

Basic Defense Approaches

- Overprovisioning
- Dynamic increases in provisioning
- Hiding
- Tracking attackers
- Legal approaches
- Reducing volume of attack
- None of these are totally effective