Threats: Network Level

Ian Welch
NWEN 405
Week 10

Example

- Twitter and Facebook under attack.
- August 9th, 2009.
- http://youtu.be/IFPoDzXTwSo

Denial of Service Attacks

- Access is not the aim.
- Prevent legitimate users of a service from using the service.
- Financial incentive and extortion.
- Countermeasures aim to dilute the effect of the attack or redirect it.

Classifying Denial of Service Attacks

- Three dimensions:
  - What is the target of the attack?
  - What layer of the networking protocol is being attacked?
  - What is the source of attack?
  - What type of amplification is being used?

Targets

- Bandwidth Attacks
  - Flooding to exhaust network resources (at host or link level)
- Computational Resource Attacks
  - Consuming CPU, disk resources etc.
- Communication Path Attacks
  - Disrupting communication through attacks upon routing of messages etc.

Network Layer

- IP layer
  - ICMP (Smurf attack)
- Network layer
  - TCP/IP (SYN and SYN/ACK attack)
- Application layer
  - DNS, email, web applications etc.

Amplification

- Traffic amplification
  - Attacker sends a small attack message and this amplified by a third-party into a larger attack message.
  - Or, attacker sends a small number of messages that are amplified into a large number of messages.
- Impact amplification
  - Attacker sends a small message that requires the target to consume large amounts of resources.

Source

- Attacker
  - Single host/network launching an attack.
  - Easy to trace back to attacker, unlikely to be able to generate enough traffic.
- Distributed denial-of-service attack
  - Multiple hosts/networks working together to launch an attack (usually 3rd party compromised hosts in botnet).
- Distributed reflected denial-of-service attack
  - Multiple hosts/networks that can be duped into being source of attack (usually because misconfigured).

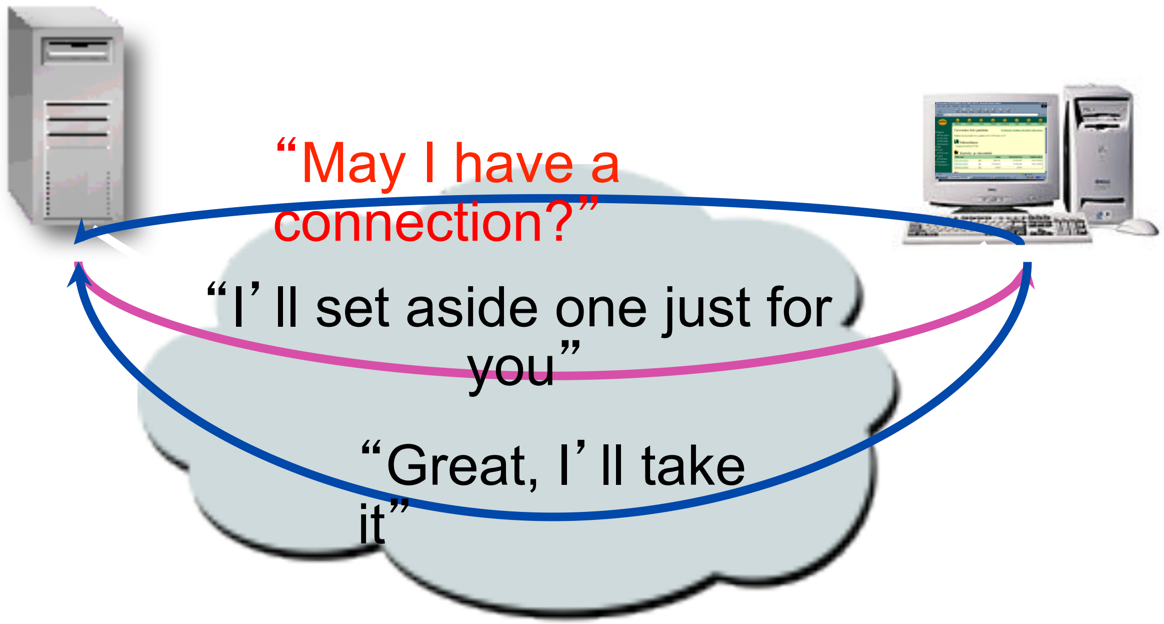
IP Layer

Smurf

- Send ICMP EchoRequest with spoofed source address to network broadcast address.
- All hosts on network respond with EchoReply to the victim.
- Floods network links (bandwidth attack).
- Traffic amplification (all hosts on network reply).
- Source (distributed reflected denial-of-service).
- Fixed since 1999.
- http://en.wikipedia.org/wiki/Smurf_attack

TCP/IP attack

Normal TCP Connection Set-up

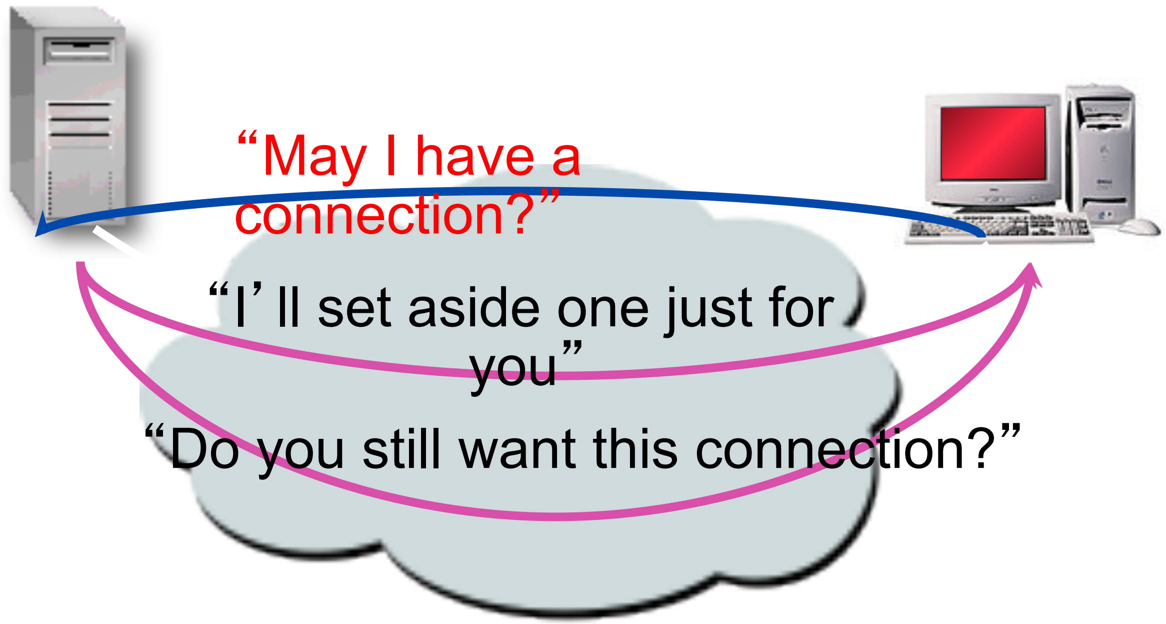


“May I have a connection?”

“I’ll set aside one just for you”

“Great, I’ll take it”

Abnormal TCP Connection Set-up



"May I have a connection?"

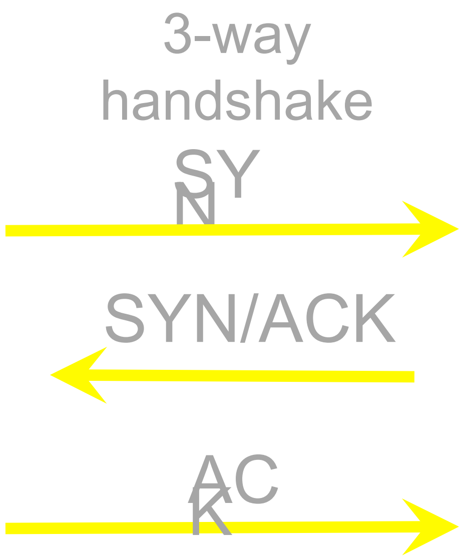
"I' ll set aside one just for you"

"Do you still want this connection?"

- Connection Setup Incomplete

SYN Flooding

- Server receives more incomplete connection requests than it can handle (Computational Resource Attack) preventing new connections
- Source code published on Internet
- Prevents completion of 3-way TCP handshake by withholding ACK flag

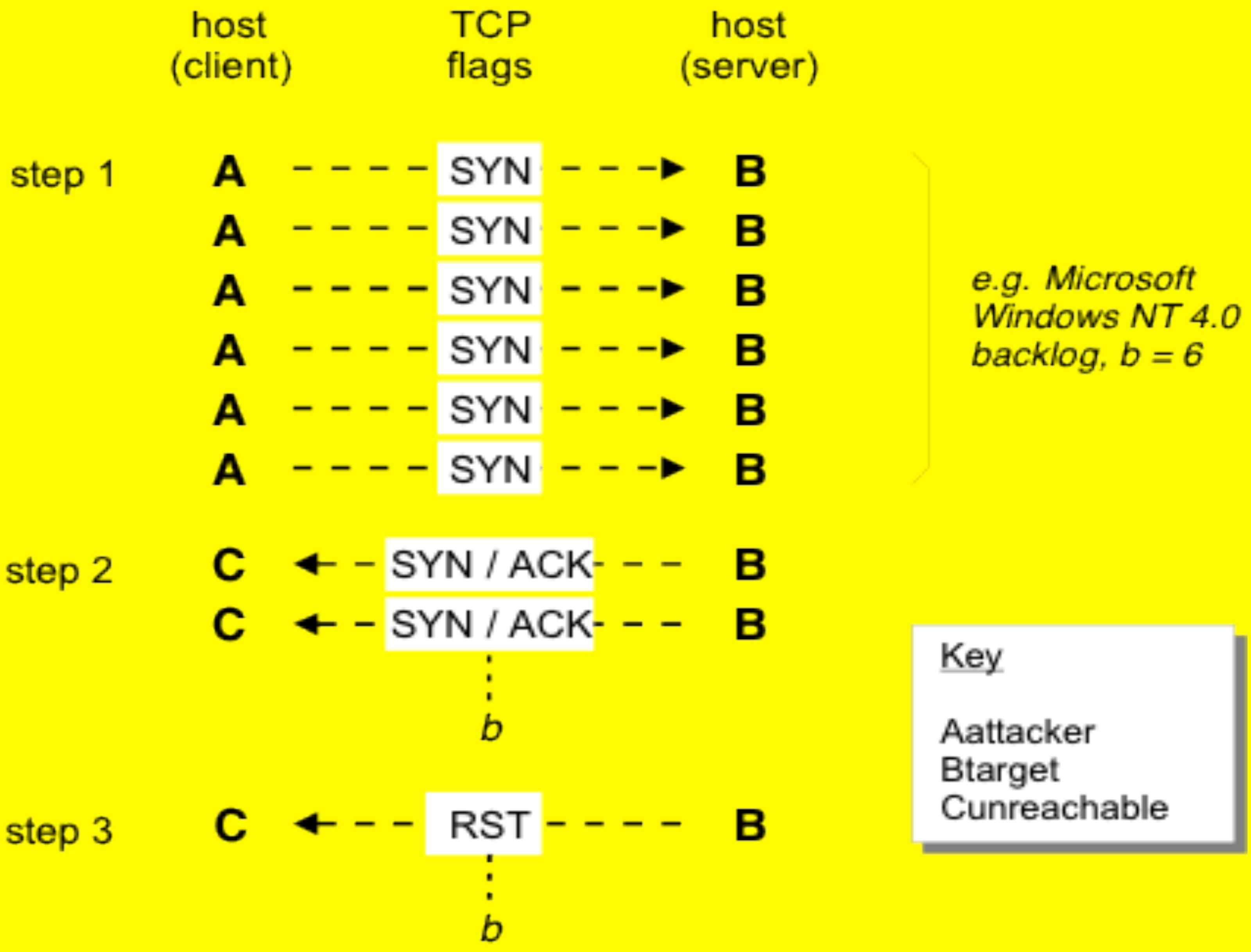


3-way handshake

SY
N

SYN/ACK

AC
K



host (client) | TCP flags | host (server)

step 1
A - - - - SYN - - - -▶ B
A - - - - SYN - - - -▶ B
A - - - - SYN - - - -▶ B
A - - - - SYN - - - -▶ B
A - - - - SYN - - - -▶ B
A - - - - SYN - - - -▶ B

e.g. Microsoft Windows NT 4.0 backlog, b = 6

step 2
C ◀- - SYN / ACK- - - B
C ◀- - SYN / ACK- - - B
b

step 3
C ◀- - - RST - - - - - B
b

Key

Aattacker
Btarget
Cunreachable

TCP SYN Flood Attack

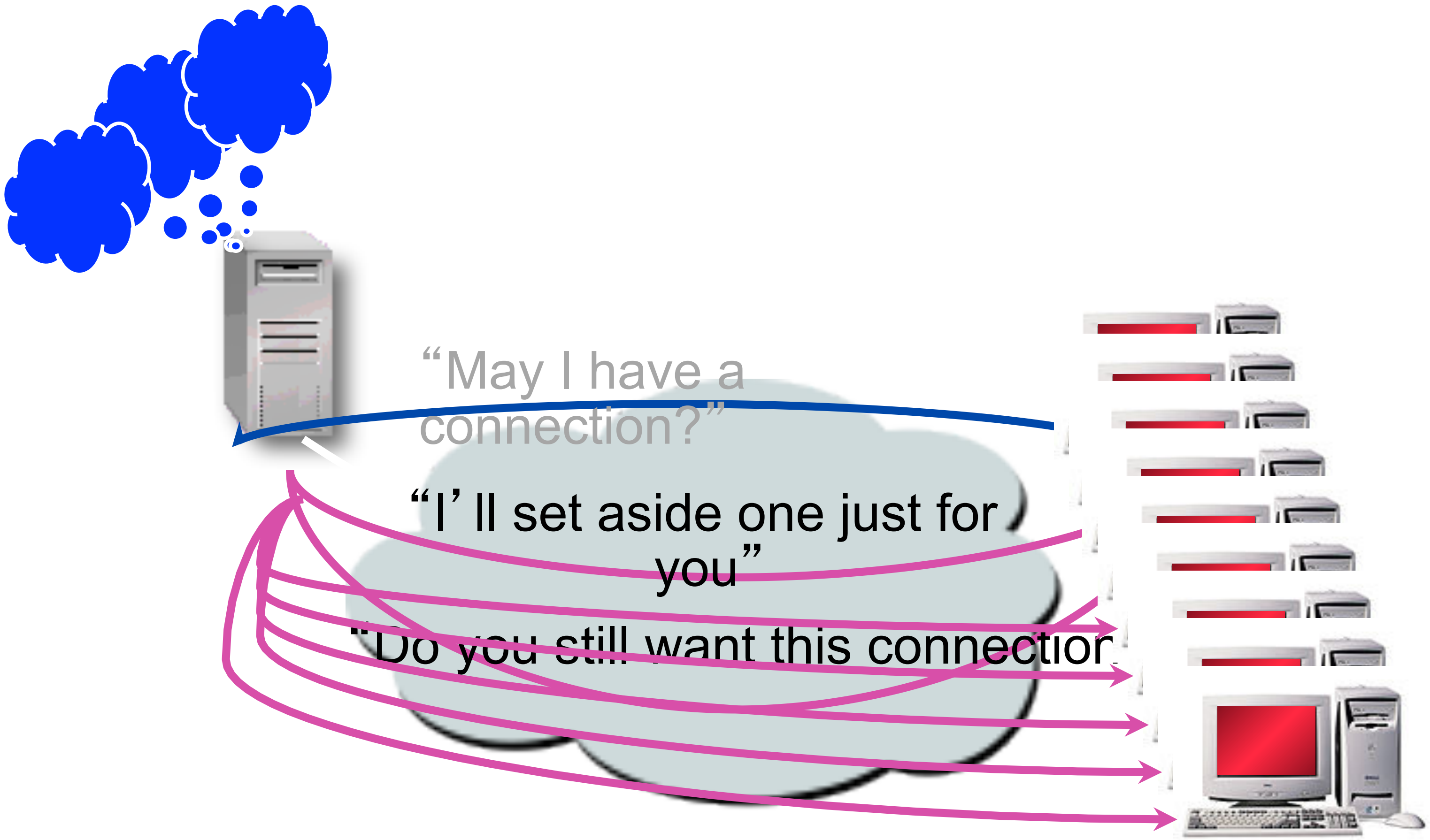
SYN Flooding

- Server rejects subsequent requests until existing requests time out → 75 secs creating denial of service
- Timeout allows attack to use fewer packets than a brute force attack (impact amplification)
- Attacking host must spoof source IP address to routable but unreachable host to prevent RST packets
- Randomisation of (unreachable) source address assists in hiding attacker’ s location.

SYN Flooding

- Source of attack can be:
  - Attacker’s own host or network.
  - Distributed denial-of-service.
- See http://en.wikipedia.org/wiki/SYN_flooding
- Counteracted by:
  - Random dropping of connections.
  - Use of cookies allowing you to cope with very large numbers of connections.

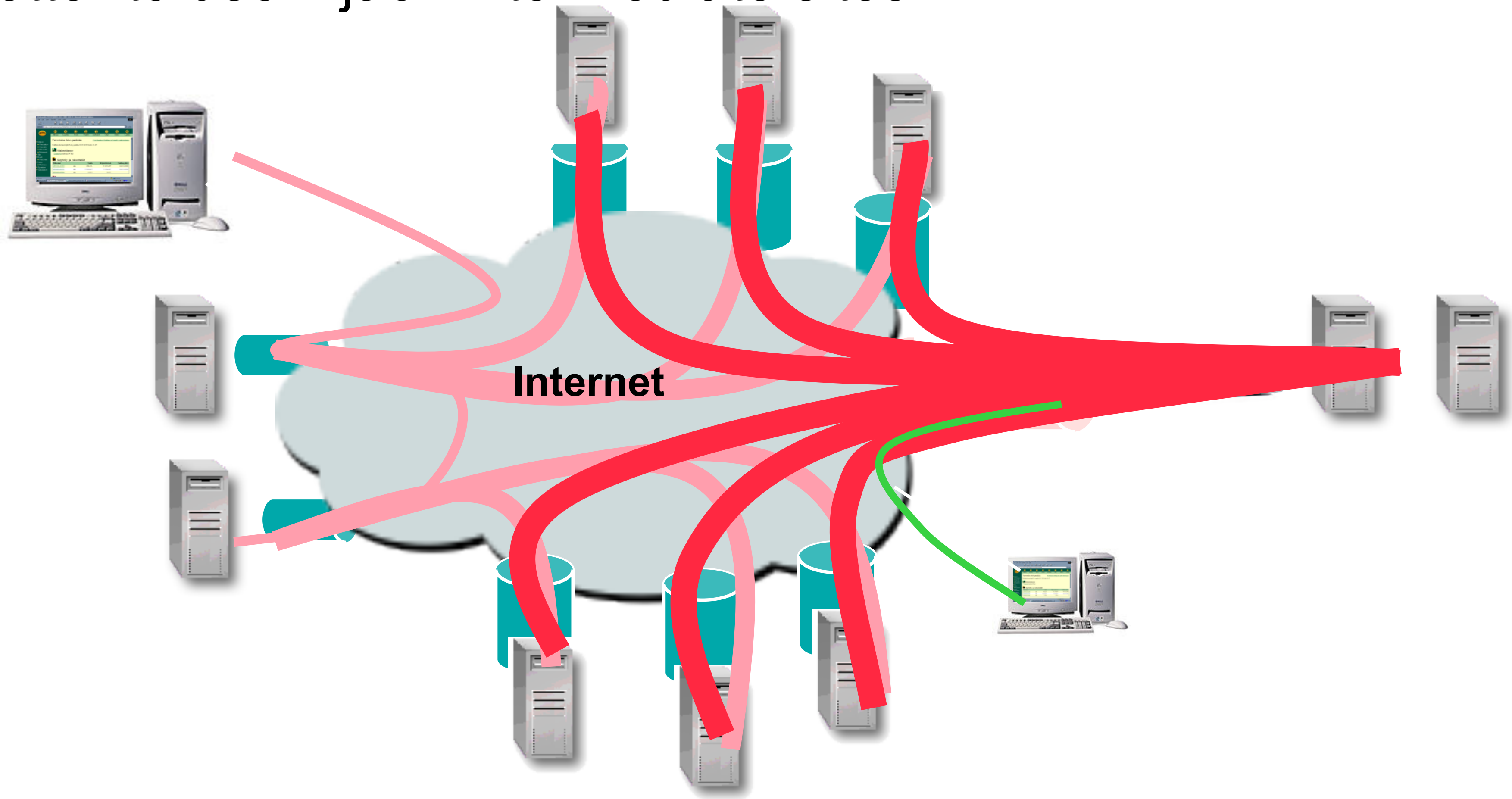
Source: Attacker


“May I have a connection?”
“I’ ll set aside one just for you”
“Do you still want this connection

- Over time, other requests will not be serviced
- System locks up, does not really die - just impaired

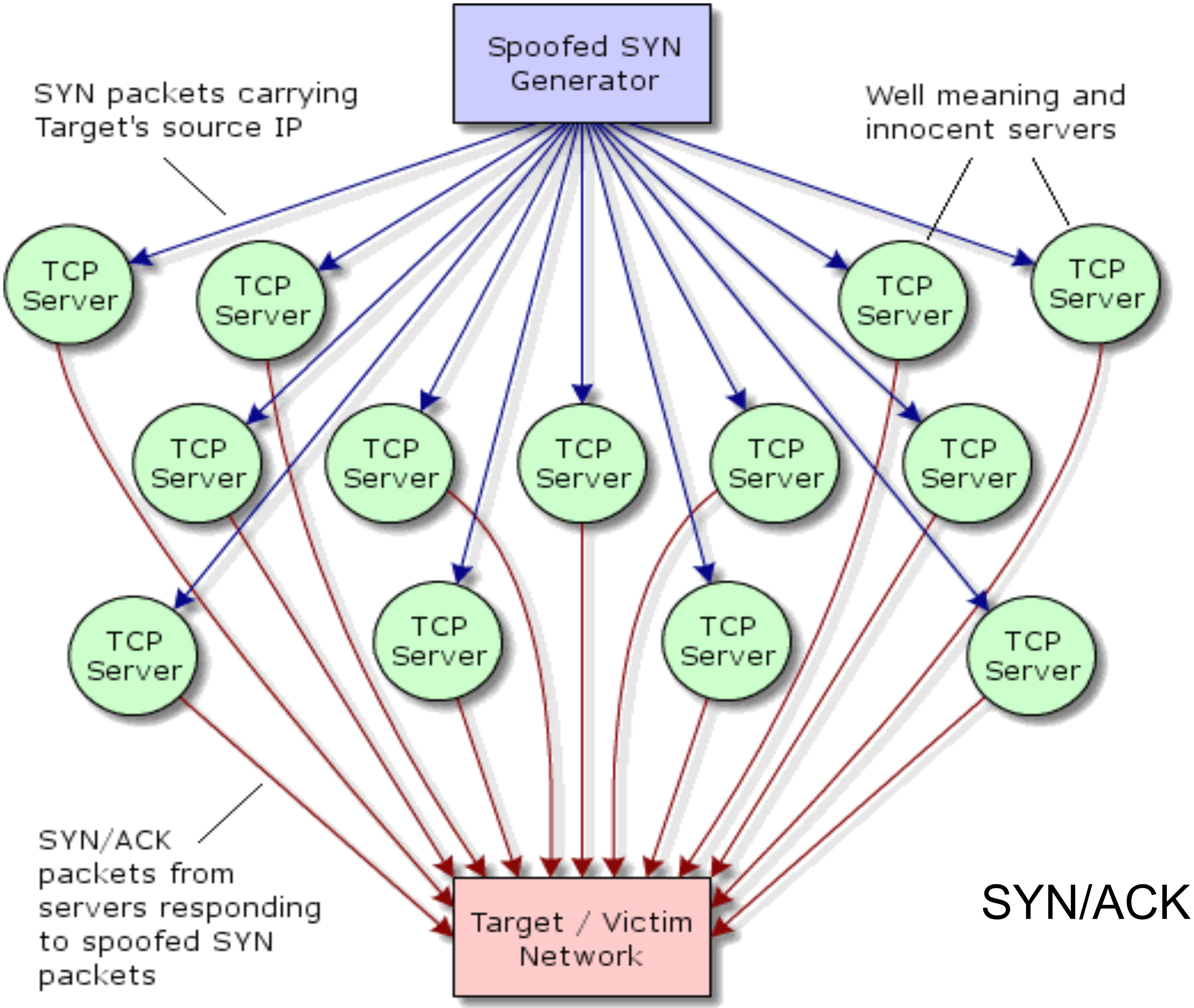
Source: Distributed DOS

- Multiple users are difficult to co-ordinate and can be traced
- Better to use hijack intermediate sites



SYN/ACK attack

- In normal operation, server receiving SYN packet to establish connection will respond with SYN/ACK packet
- Malicious user may fake source IP address of original SYN packet, causing server to send SYN/ACK packet to victim host
- Single malicious user can send same SYN packet to many servers - overwhelms victim with SYN/ACK packets
- Doesn’t require infected hosts because behaviour *is what TCP/IP is supposed to do*.
- Consumes server resources (computational attack).
- Doesn’t amplify work done by attackers (no amplification).
- May occur on any port, making many traditional firewall defenses problematic (because they filter by port number).
- Source is spread across the Internet (distributed reflection denial-of-service).



SYN/ACK attack

Example of Impact Amplification

- Low rate (Shrew) TCP Denial-of-Service attacks are new and exploit the RTO (minimum Retransmission TimeOut) property of TCP
- Basically a periodic short-burst attack which causes all TCP flows to back off and enter retransmission timeout state
- While TCP's congestion control algorithm is highly robust its implicit assumption of end-system cooperation results in vulnerability to short burst non-responsive flows
- Difficult to detect because of low flows.

Application-level attacks

Application-level Denial of Service

- Applications:
  - Network services, for example DNS, email or web servers.
  - Hardware infrastructure with a management interface accessible via a network, for example CISCO routers.
  - Applications and application-level resources, for example web applications or databases.
- Knowledge of the application or service's implementation allows attacker to multiply effect of a request to a service (amplification attacks).
  - Send small number of large packets, small volume of requests causes big effect via buffer overflow.
  - Request large files, small request with big payoff in bandwidth.
  - Request complex operations, small request leading to expensive computation, use up local resources such as disk space or memory.

Attack on DNS

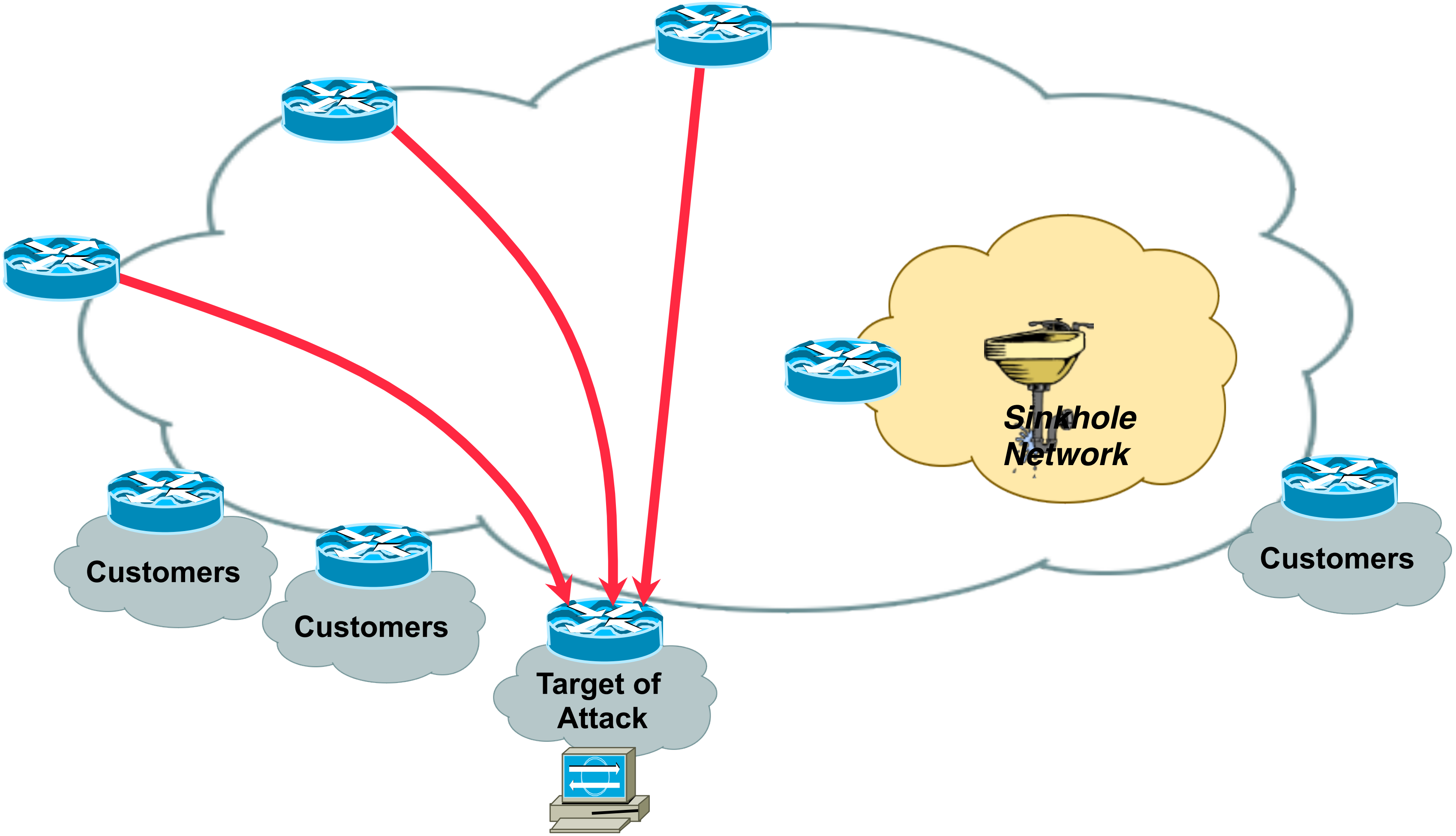
- Misconfigured DNS servers will honour requests from machines not on their own network (distributed reflection denial-of-service).
- 2001, theregister.com attacked.
- DNS request (25 bytes) resulted in mail server information for aol.com being returned (500 bytes) (traffic amplification)
- Request IP was spoofed address for theregister.com.
- Overloaded links (bandwidth attack).

Web Application

- Imagine a large forum application.
- Contains millions of messages.
- Allows performing searches involving wildcards and multiple fields.
- Attacker creates complicated search that consumes large amounts of CPUs everytime that search takes place.
- Attacker writes a script to launch this request over and over again.
- Amplification effects allows system to be taken down with only a dozen or so hosts.

Mitigating effects and preventing attacks

Sinkholes for Attack Traffic



Sinkhole Network

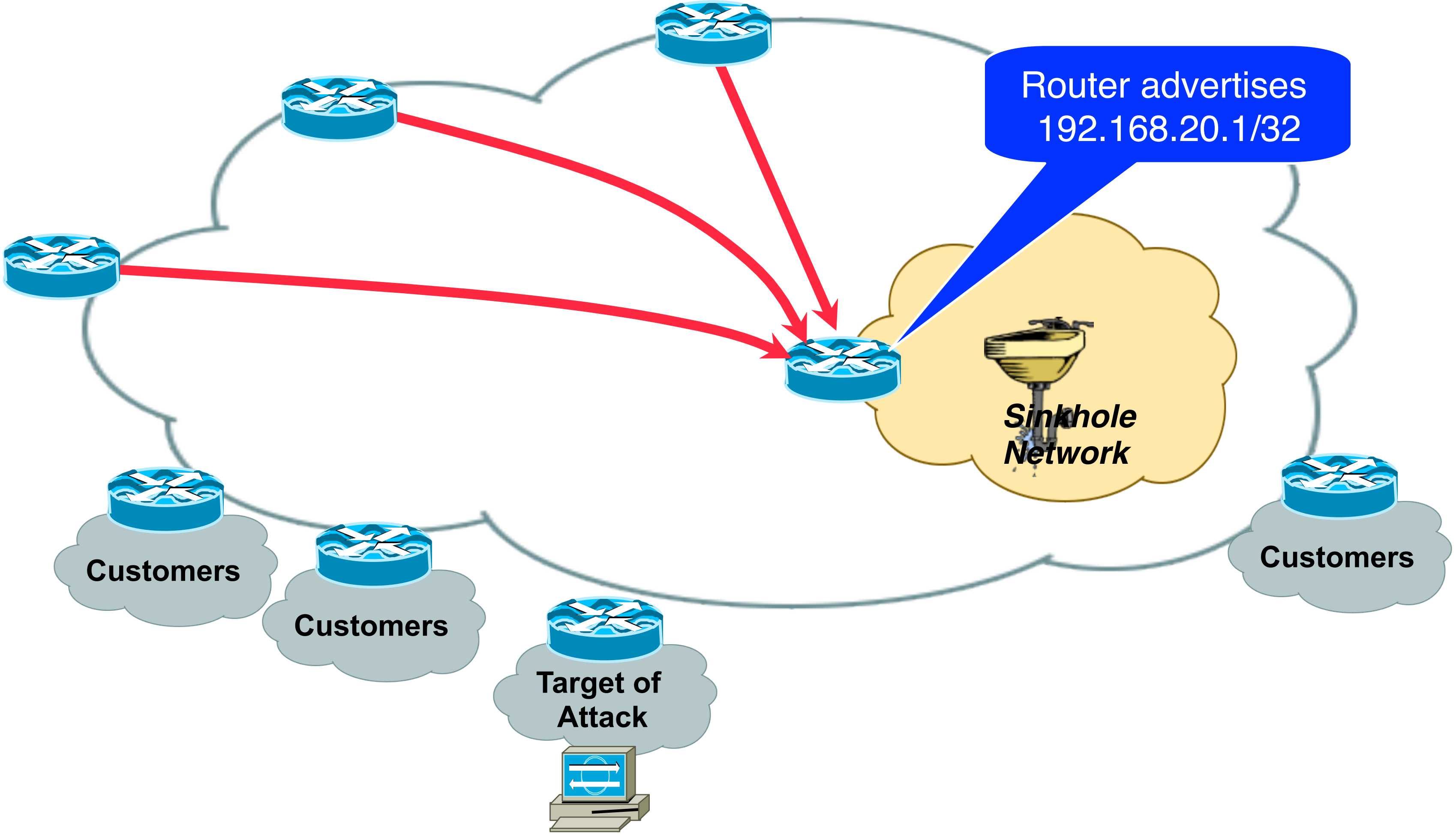
Customers

Customers

Customers

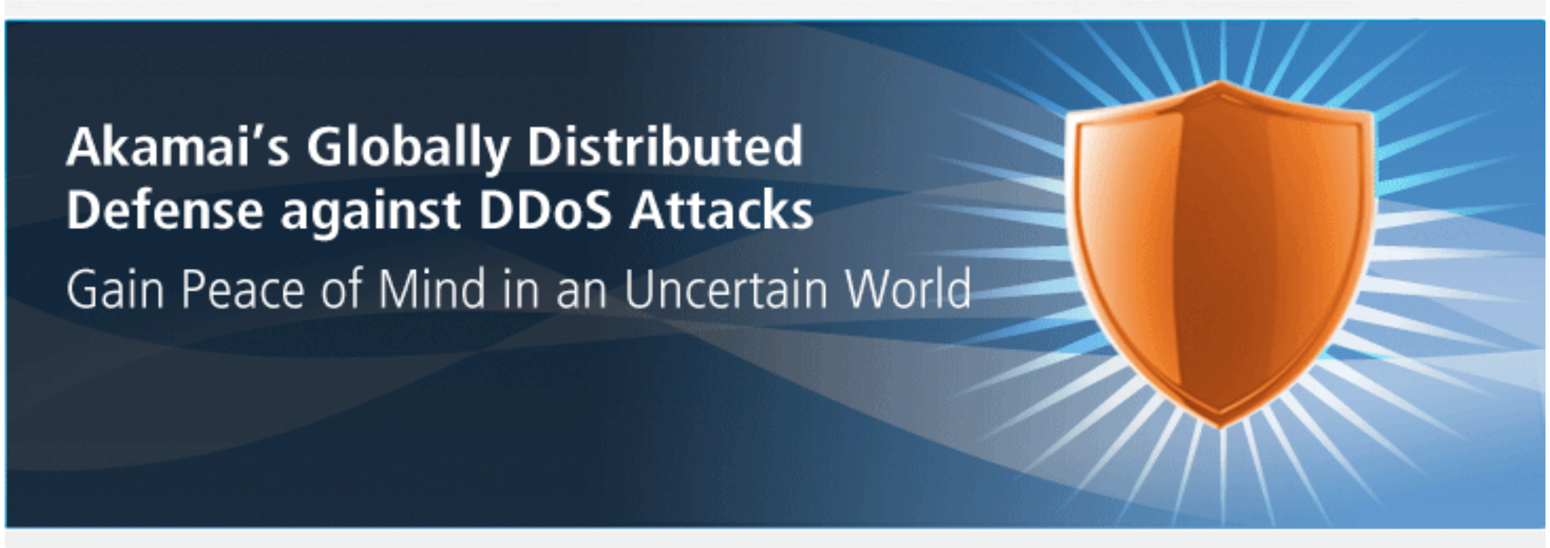
Target of Attack

Sinkholes for Attack Traffic



Some Specific DOS Attack Prevention Measures

- Spread the load.
  - Akamai content distribution network.
  - 84,000 servers across the world.



Akamai's Globally Distributed
Defense against DDoS Attacks
Gain Peace of Mind in an Uncertain World

Some Specific DOS Attack Prevention Measures

- Filter packets entering and leaving your network (ingress and egress filtering).
- Anti-virus on your machine to stop them being used as a botnet.