CSE 484 and CSE M 584 (Winter 2009)

Networks

Tadayoshi Kohno

Thanks to Dan Boneh, Dieter Gollmann, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Goals for Today

- Finish symmetric crypto
- Network Security Attacks
  - Routing
  - IP
  - TCP
  - DNS
- Key points:
  - Failures at interaction between layers
  - Asymmetry between attacker and defender
  - Some attacks designers never considered
  - All motivations for existing security decisions (SSL/TLS, filter certain types of packets, check inputs, etc).

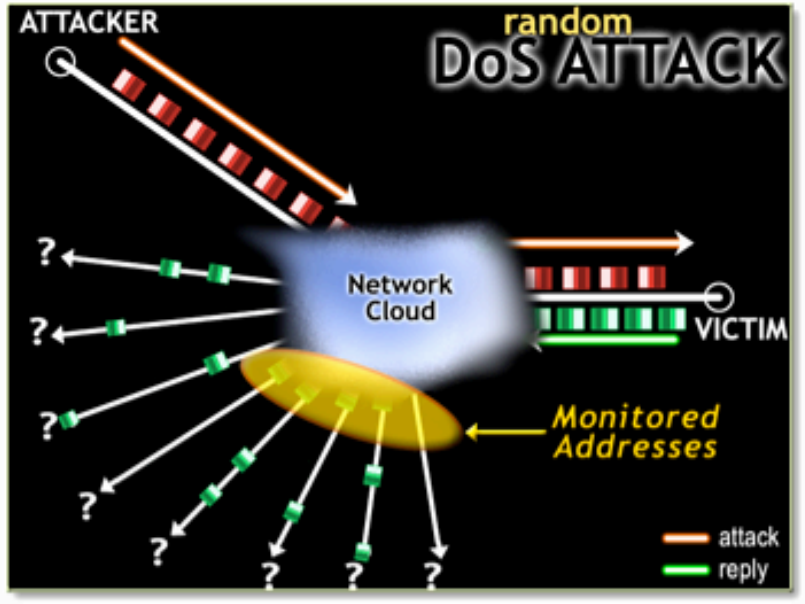
User Datagram Protocol (UDP)

- UDP is a connectionless protocol
  - Simply send datagram to application process at the specified port of the IP address
  - Source port number provides return address
  - Applications: media streaming, broadcast
- No acknowledgement, no flow control, no message continuation
- Denial of service by UDP data flood

- http://www.caida.org/publications/presentations/2004/ucsd_network_telescope/ucsd_network_telescope_bbn.pdf

Network Telescope: Denial-of-Service Attacks

- Attacker floods the victim with requests using random spoofed source IP addresses
- Victim believes requests are legitimate and responds to each spoofed address
- We observe 1/256th of all *victim responses* to spoofed addresses [MSV01]

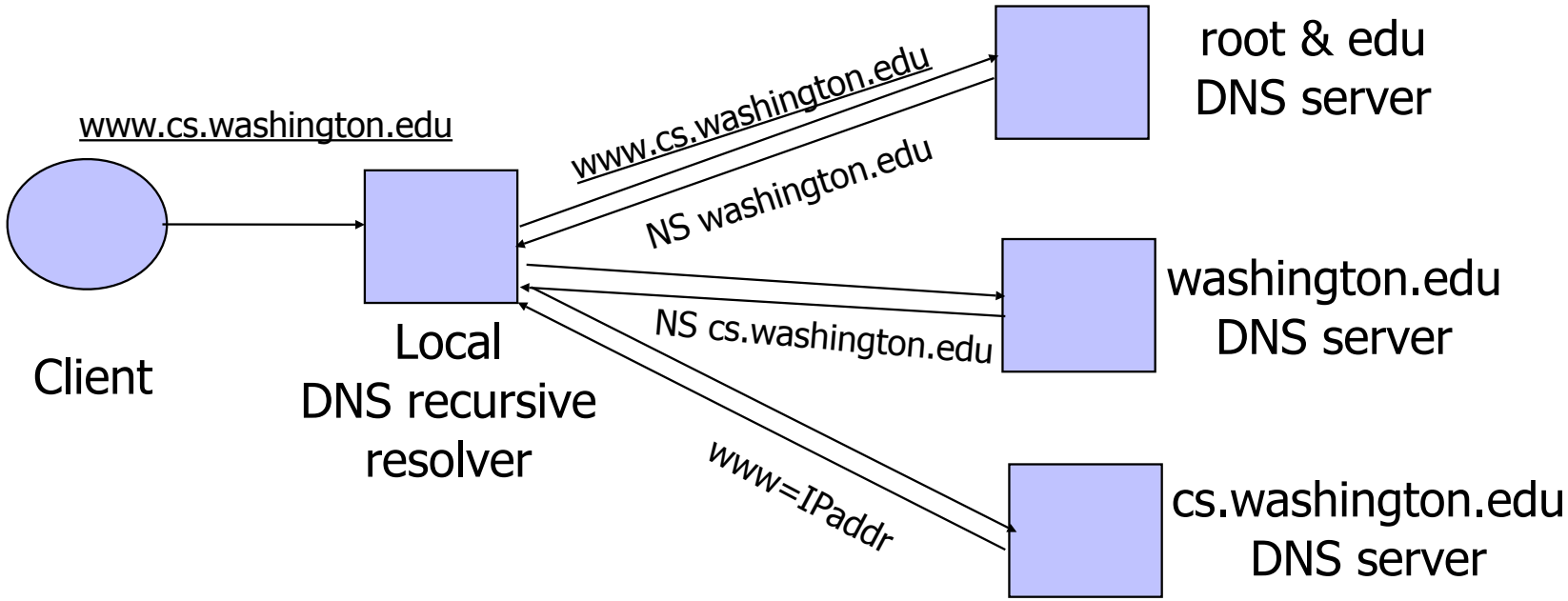


DNS Issues

DNS: Domain Name Service

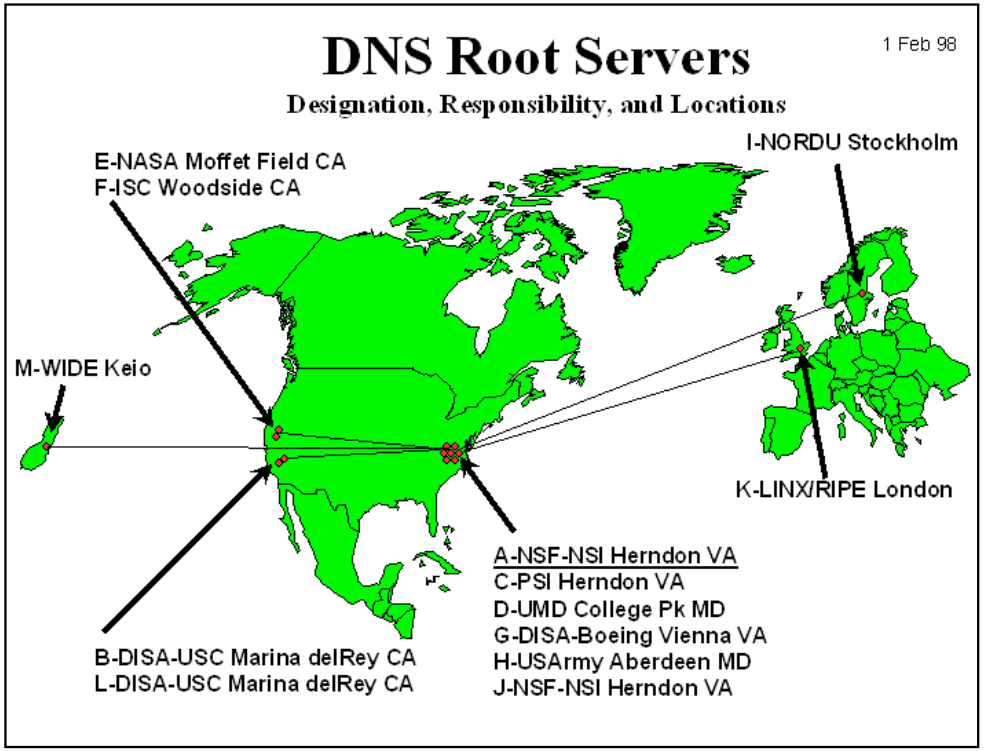
DNS maps symbolic names to numeric IP addresses

(for example, www.cs.washington.edu ↔ 128.208.3.88)



DNS Root Name Servers

- Root name servers for top-level domains
- Authoritative name servers for subdomains
- Local name resolvers contact authoritative servers when they do not know a name
  - Oct 2002: 14GB per 24 hours, 1768 queries per second



Feb 6: DoS attack on root DNS servers

DNS Caching

- DNS responses are cached
  - Quick response for repeated translations
  - Other queries may reuse some parts of lookup
    - NS records for domains
- DNS negative queries are cached
  - Don’t have to repeat past mistakes
    - For example, misspellings
- Cached data periodically times out
  - Lifetime (TTL) of data controlled by owner of data
  - TTL passed with every record

DNS Vulnerabilities

- DNS host-address mappings are not authenticated
- DNS implementations have vulnerabilities
  - Reverse query buffer overrun in old releases of BIND
    - Gain root access, abort DNS service…
  - MS DNS for NT 4.0 crashes on chargen stream
    - telnet ntbox 19 | telnet ntbox 53
- Denial of service is a risk
  - Oct ’02: ICMP flood took out 9 root servers for 1 hour

Reverse DNS Spoofing

- Trusted access is often based on host names
  - E.g., permit all hosts in .rhosts to run remote shell
- Network requests such as rsh or rlogin arrive from numeric source addresses
  - System performs reverse DNS lookup to determine requester's host name and checks if it's in .rhosts
- If attacker can spoof the answer to reverse DNS query, he can fool target machine into thinking that request comes from an authorized host
  - No authentication for DNS responses and typically no double-checking (numeric → symbolic → numeric)

Other DNS Risks

- DNS cache poisoning
  - False IP with a high time-to-live will stay in the cache of the DNS server for a long time
  - Basis of pharming
- Spoofed ICANN registration and domain hijacking
  - Authentication of domain transfers based on email addr
  - Aug ’04: teenager hijacks eBay’s German site
  - Jan ’05: hijacking of panix.com (oldest ISP in NYC)
    - "The ownership of panix.com was moved to a company in Australia, the actual DNS records were moved to a company in the United Kingdom, and Panix.com's mail has been redirected to yet another company in Canada."
- Misconfiguration and human error

Home / News

Network Solutions Under Large Scale DDoS Attack, Millions of Websites Potentially Unreachable

Jan 23, 2009 2:55 PM PST | Comments: 0 | Views: 10,429

By CircleID Reporter

Comment | Print

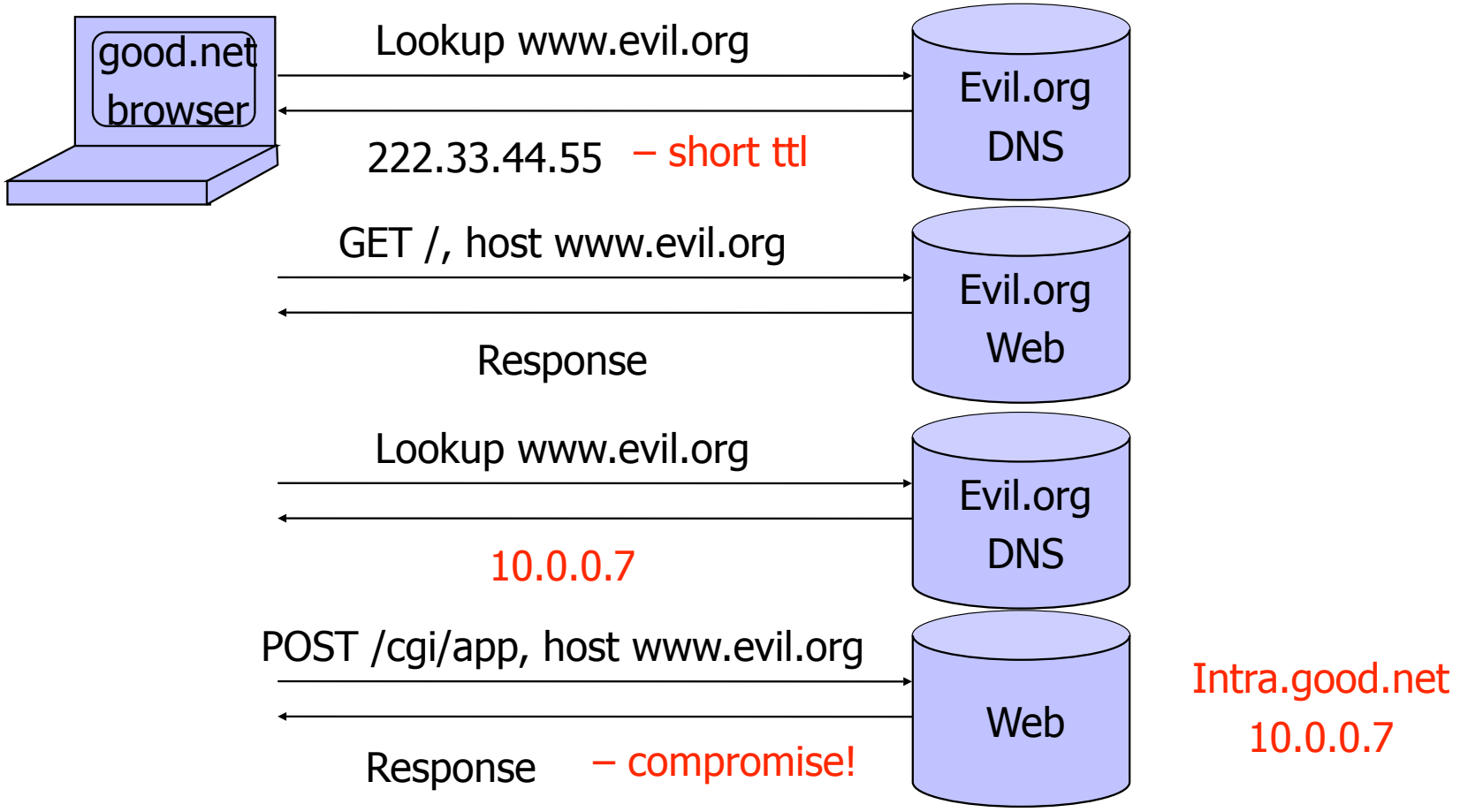
Update Received from Network Solutions Jan 23, 2009 7:27PM PST

"DNS queries for web sites should be responding normally. Thank you all for your understanding. As always, we will continue to work to take measures to prevent these and other types of technical issues caused by third parties that may impact our customers."

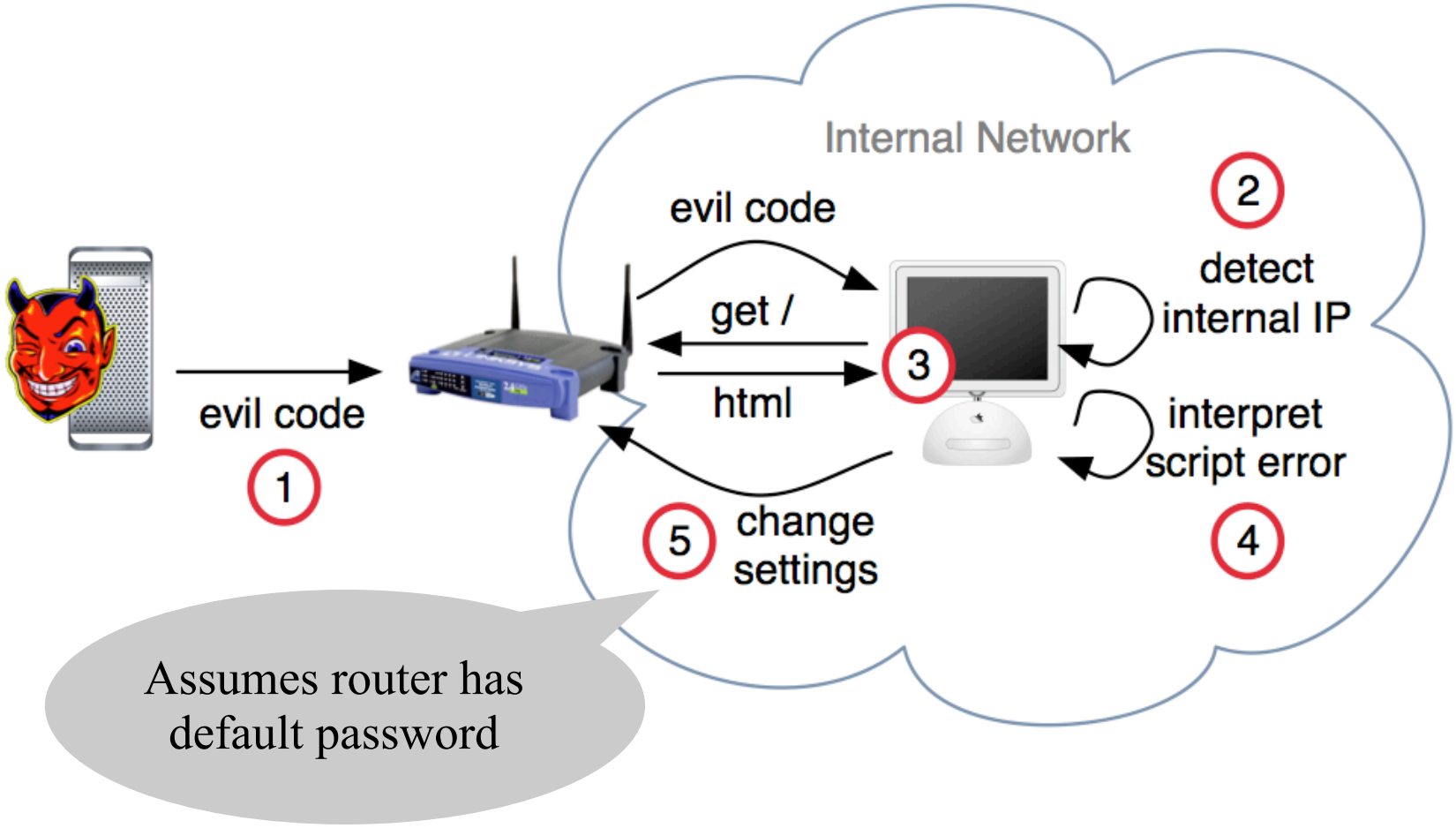
JavaScript/DNS Intranet attack (I)

- Consider a Web server intra.good.net
  - IP: 10.0.0.7, inaccessible outside good.net network
  - Hosts sensitive CGI applications
- Attacker at evil.org gets good.net user to browse www.evil.org
- Places Javascript on www.evil.org that accesses sensitive application on intra.good.net
  - This doesn't work because Javascript is subject to "same-origin" policy
  - … but the attacker controls evil.org DNS

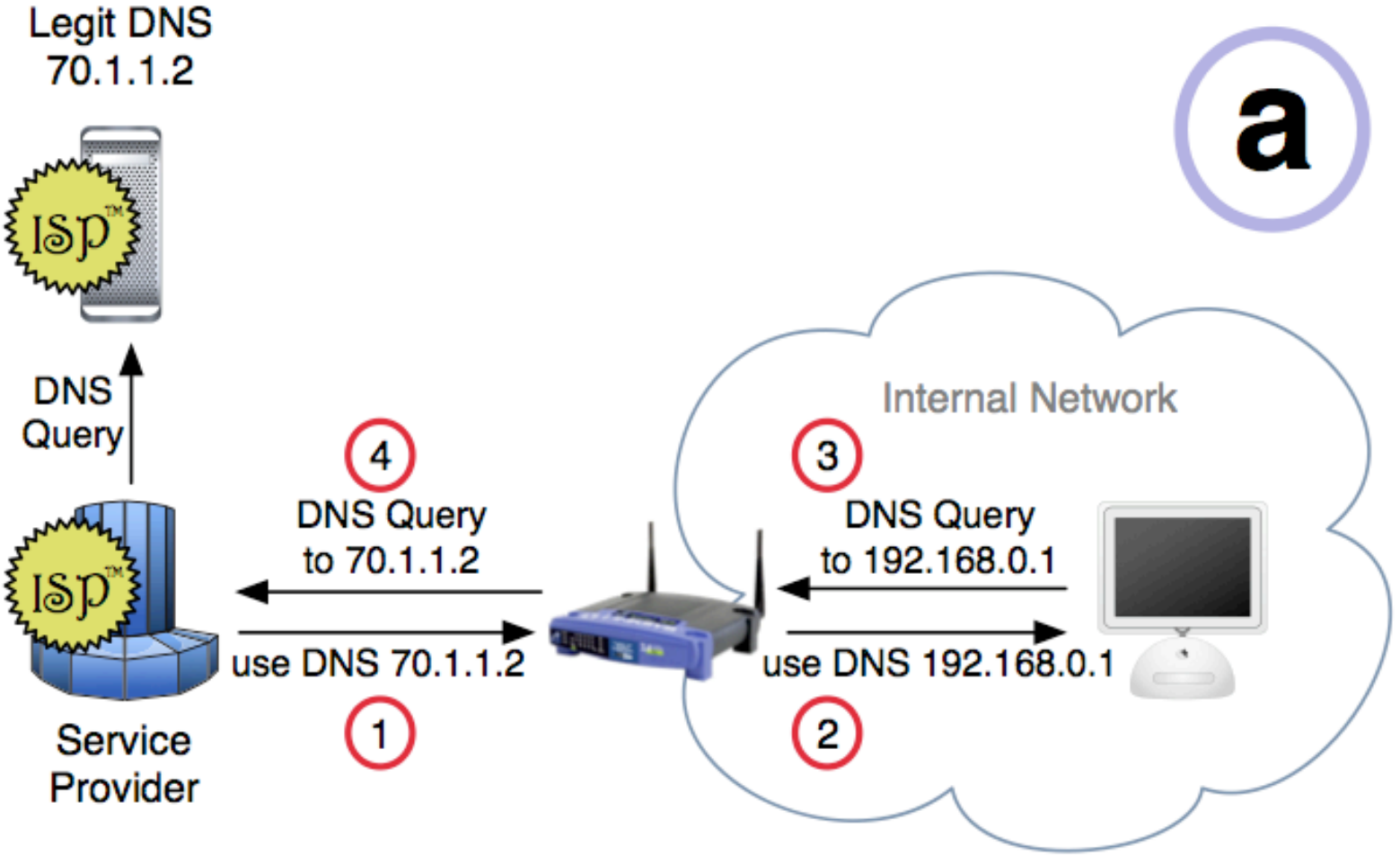
JavaScript/DNS Intranet attack (II)



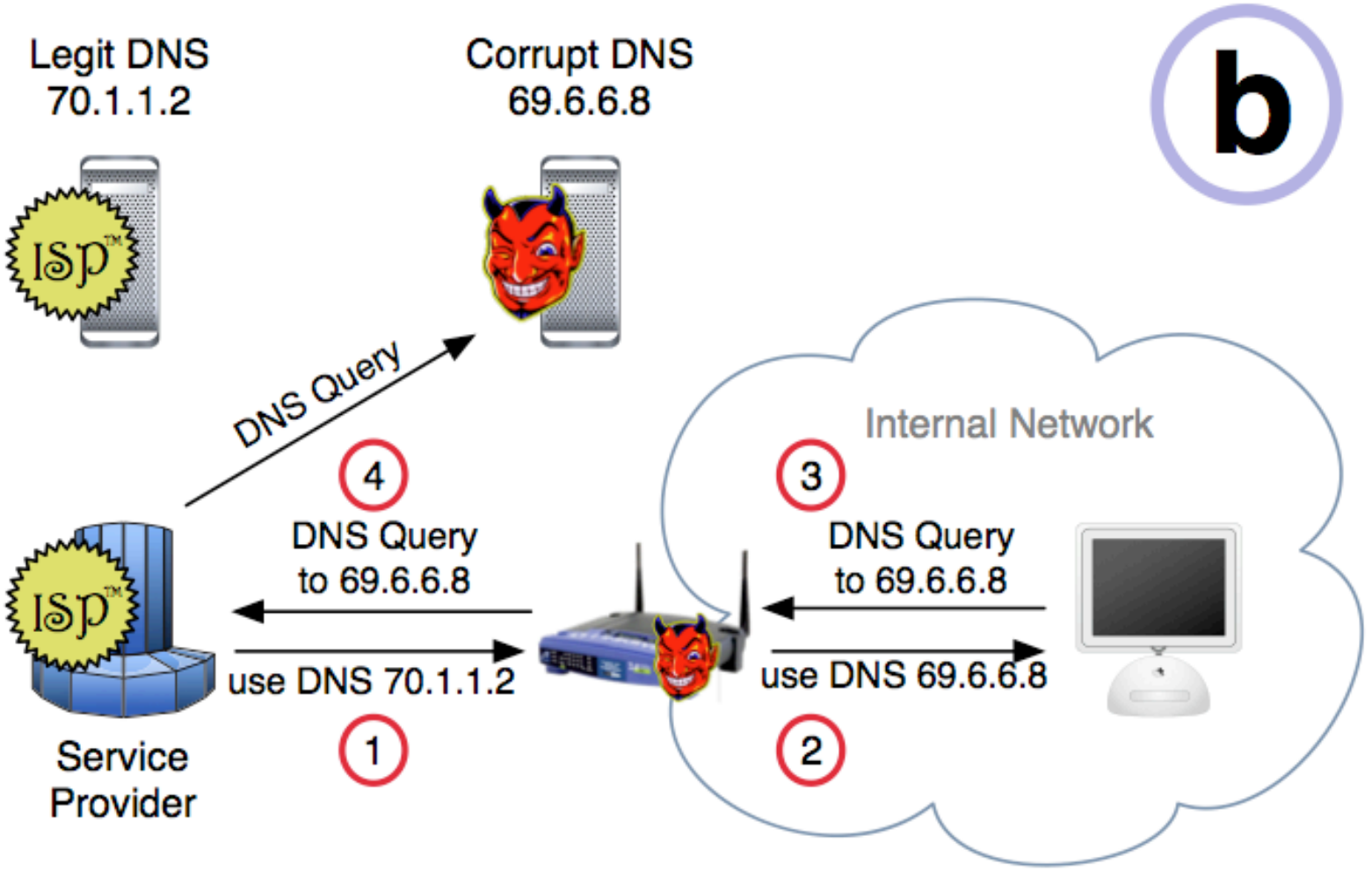
Drive-by pharming



Reference: http://www.cs.indiana.edu/pub/techreports/TR641.pdf



Reference: http://www.cs.indiana.edu/pub/techreports/TR641.pdf



Reference: http://www.cs.indiana.edu/pub/techreports/TR641.pdf

DNSSEC

- Goals: authentication and integrity of DNS requests and responses
- PK-DNSSEC (public key)
  - DNS server signs its data (can be done in advance)
- SK-DNSSEC (symmetric key)
  - Encryption and MAC: $E_k(m, MAC(m))$
  - Each message contains a nonce to avoid replay
  - Each DNS node shares a symmetric key with its parent
  - Zone root server has a public key (hybrid approach)
- http://www.secure64.com/news-reasons-to-deploy-dnssec

Kaminsky Details DNS Flaw at Black Hat Talk

LAS VEGAS, NEV. -- Roughly 85 percent of Fortune 500 companies have patched their networks to fix a security flaw that lets cyber criminals redirect visitors to counterfeit or malicious Web sites, but Internet users still remain at grave risk due to the large number of infrastructure providers that have not yet addressed the issue, a prominent security researcher warned today.

The data comes from a talk presented here at the Black Hat security conference in Las Vegas by **Dan Kaminsky**, the Seattle based IOActive researcher who discovered a fairly trivial way that bad guys could corrupt records found in the domain name system (DNS) and fill them with inaccurate information.

First instance of new DNS exploit reported

By **William Jackson** **Jul 31, 2008**

An AT&T DNS server may have been compromised with malicious code that exploits a vulnerability reported earlier this moth in the Domain Name System.

Reports are coming in that an AT&T Domain Name System (DNS) server may have been compromised with malicious code that exploits a vulnerability reported earlier this month. This apparently is the first instance of the exploit in the wild.

Related Links

DNS flaw unfixed as experts argue protocol

DNS vulnerability update: Patch now!

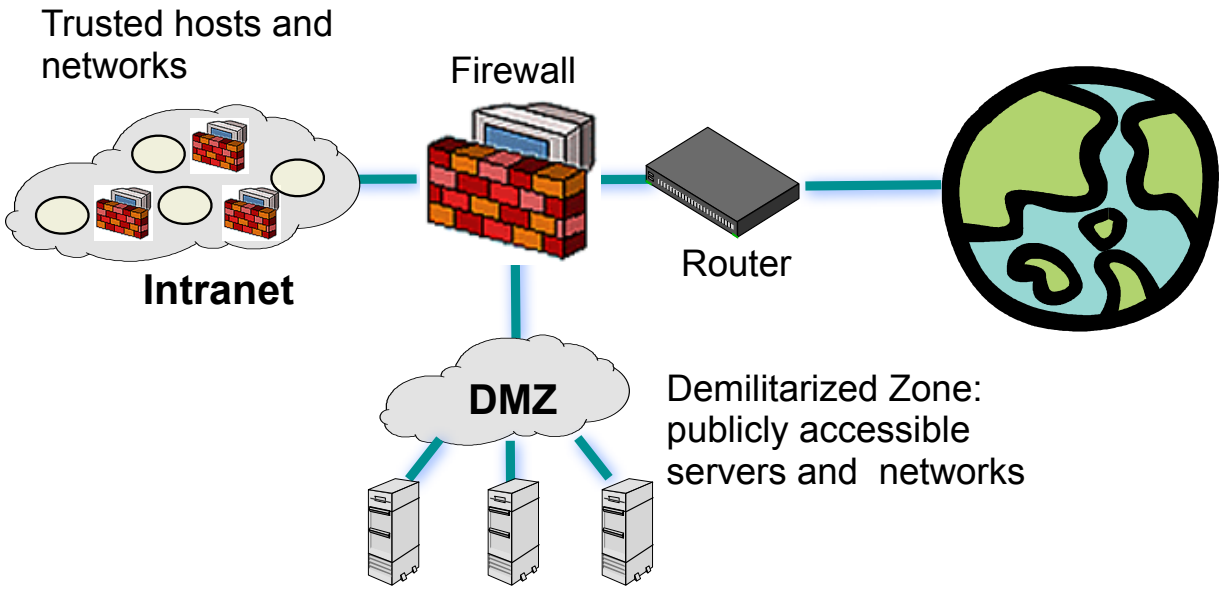
Massive patch coming for DNS vulnerability

Editor' Desk | Darkness in the cloud

Firewalls and Network Defense

Firewalls

- Idea: separate local network from the Internet



slide

Castle and Moat Analogy

- More like the moat around a castle than a firewall
  - Restricts access from the outside
  - Restricts outbound connections, too (!!)
    - Important: filter out undesirable activity from internal hosts!

slide

Firewall Locations in the Network

- Between internal LAN and external network
- At the gateways of sensitive subnetworks within the organizational LAN
  - Payroll's network must be protected separately within the corporate network
- On end-user machines
  - "Personal firewall"
  - Microsoft's Internet Connection Firewall (ICF) comes standard with Windows XP

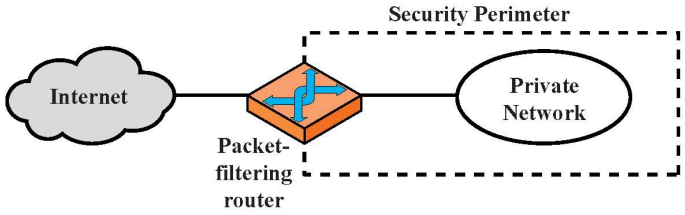
slide

Firewall Types

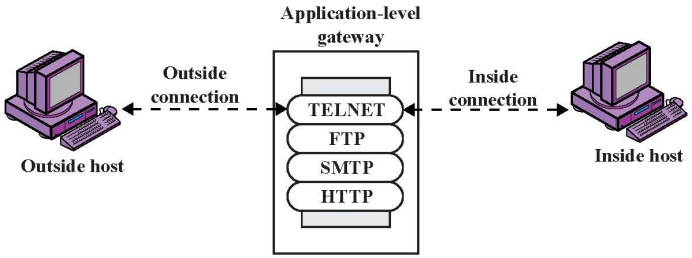
- Packet- or session-filtering router (filter)
- Proxy gateway
  - All incoming traffic is directed to firewall, all outgoing traffic appears to come from firewall
  - Application-level: separate proxy for each application
    - Different proxies for SMTP (email), HTTP, FTP, etc.
    - Filtering rules are application-specific
  - Circuit-level: application-independent, "transparent"
    - Only generic IP traffic filtering (example: SOCKS)
- Personal firewall with application-specific rules
  - E.g., no outbound telnet connections from email client

slide

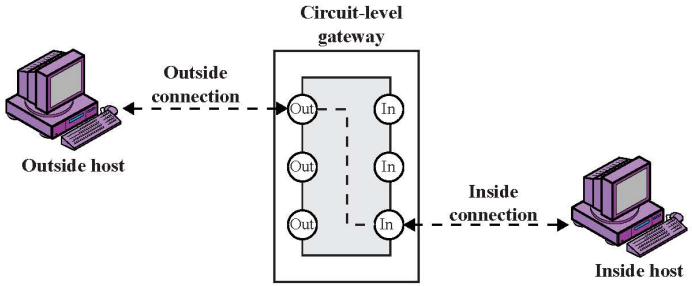
Firewall Types: Illustration



(a) Packet-filtering router



(b) Application-level gateway



(c) Circuit-level gateway

slide

Packet Filtering

- For each packet, firewall decides whether to allow it to proceed
  - Decision must be made on per-packet basis
    - Stateless; cannot examine packet's context (TCP connection, application to which it belongs, etc.)
- To decide, use information available in the packet
  - IP source and destination addresses, ports
  - Protocol identifier (TCP, UDP, ICMP, etc.)
  - TCP flags (SYN, ACK, RST, PSH, FIN)
  - ICMP message type
- Filtering rules are based on pattern-matching

slide

Packet Filtering Examples

A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

D

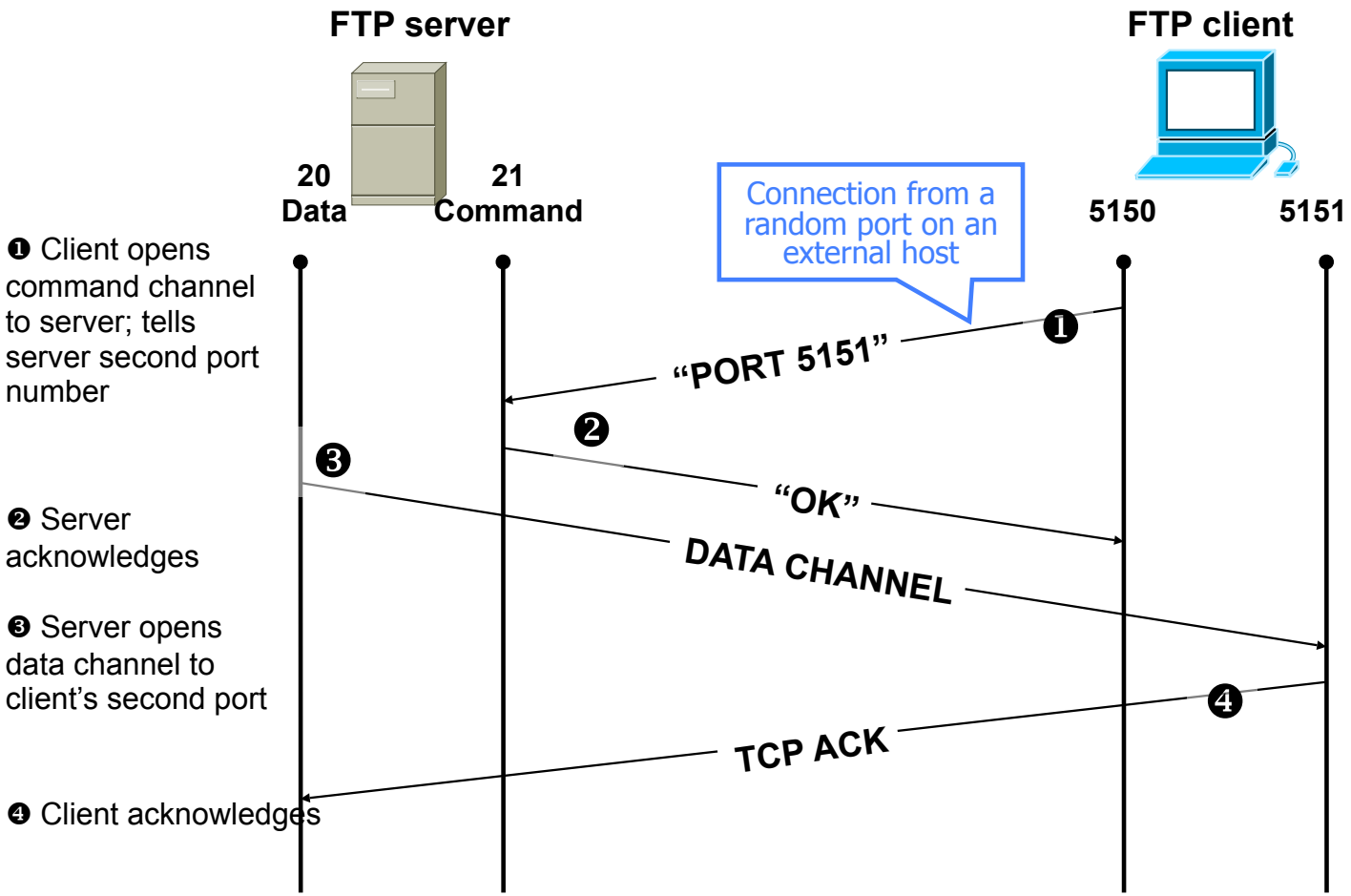
action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

slide

Example: FTP (borrowed from Wenke Lee)



slide

FTP Packet Filter

The following filtering rules allow a user to FTP from any IP address to the FTP server at 172.168.10.12

```
access-list 100 permit tcp any gt 1023 host 172.168.10.12 eq 21
access-list 100 permit tcp any gt 1023 host 172.168.10.12 eq 20
  ! Allows packets from any client to the FTP control and data ports
access-list 101 permit tcp host 172.168.10.12 eq 21 any gt 1023
access-list 101 permit tcp host 172.168.10.12 eq 20 any gt 1023
  ! Allows the FTP server to send packets back to any IP address with TCP ports > 1023

interface Ethernet 0
 access-list 100 in     ! Apply the first rule to inbound traffic
 access-list 101 out    ! Apply the second rule to outbound traffic
!
```

Anything not explicitly permitted by the access list is denied!

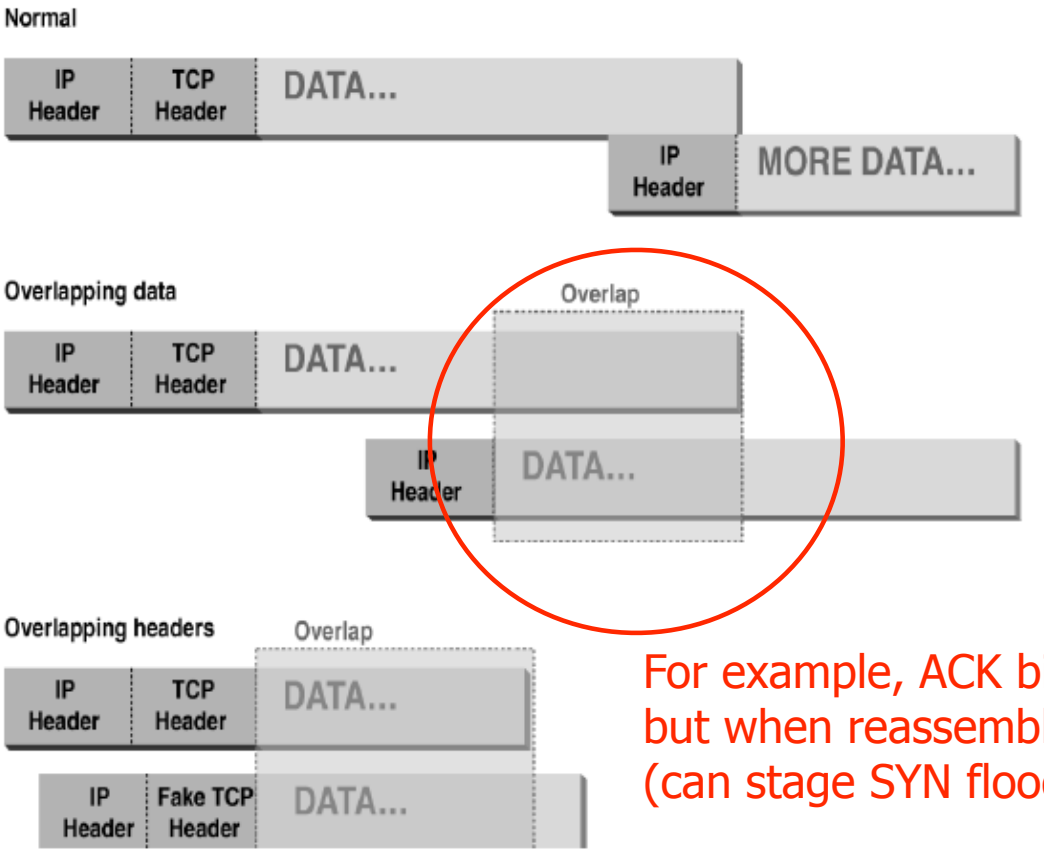
slide

Weaknesses of Packet Filters

- Do not prevent application-specific attacks
  - For example, if there is a buffer overflow in URL decoding routine, firewall will not block an attack string
- No user authentication mechanisms
  - … except (spoofable) address-based authentication
  - Firewalls don't have any upper-level functionality
- Vulnerable to TCP/IP attacks such as spoofing
  - Solution: list of addresses for each interface (packets with internal addresses shouldn't come from outside)
- Security breaches due to misconfiguration

slide

Abnormal Fragmentation



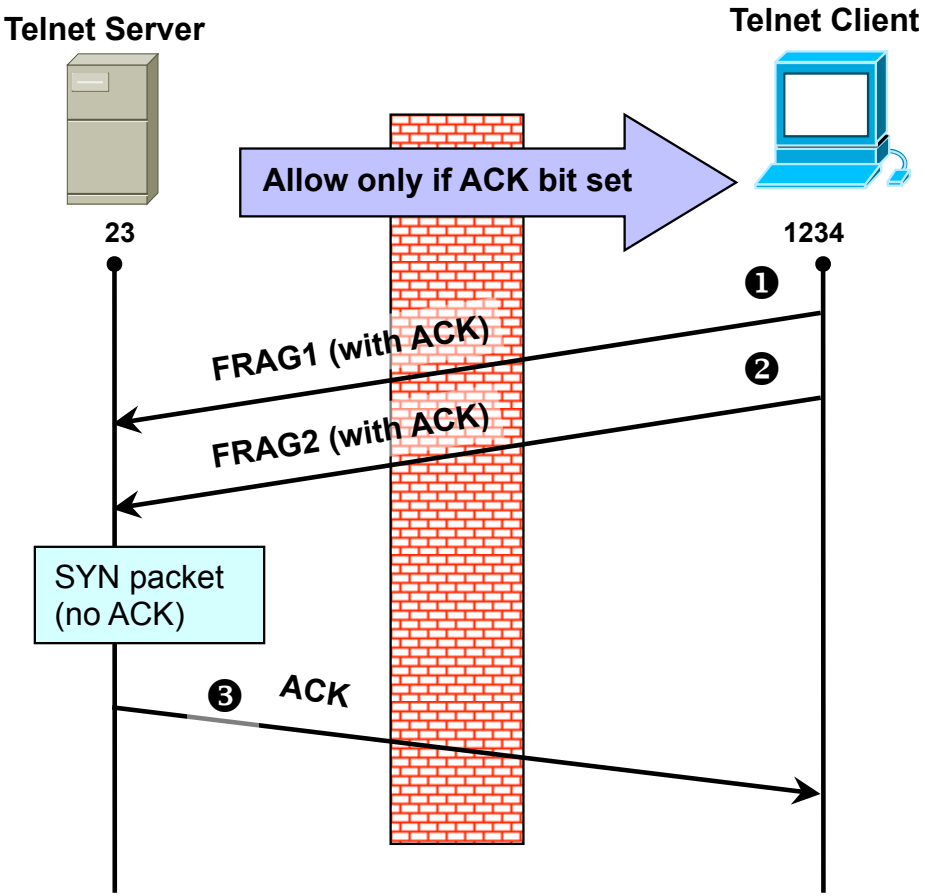
For example, ACK bit is set in both fragments, but when reassembled, SYN bit is set (can stage SYN flooding through firewall)

slide

Fragmentation Attack (borrowed from Wenke Lee)

❶,❷ Send 2 fragments with the ACK bit set; fragment offsets are chosen so that the full datagram re-assembled by server forms a packet with the SYN bit set (the fragment offset of the second packet overlaps into the space of the first packet)

❸ All following packets will have the ACK bit set



slide

More Fragmentation Attacks

- Split ICMP message into two fragments, the assembled message is too large
  - Buffer overflow, OS crash
- Fragment a URL or FTP "put" command
  - Firewall needs to understand application-specific commands to catch this

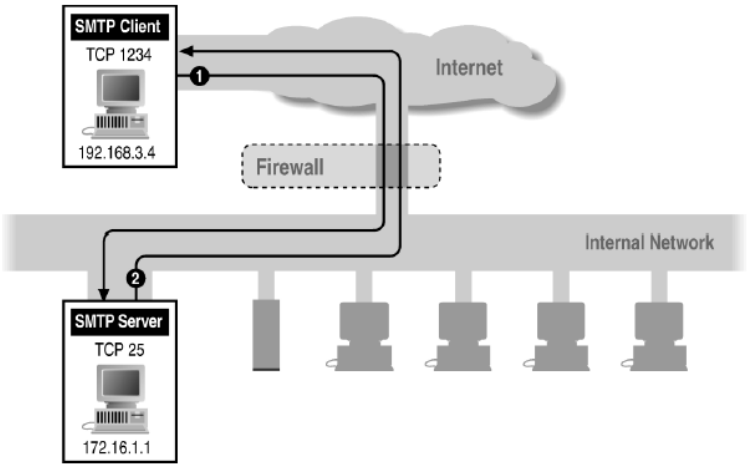
slide

Stateless Filtering Is Not Enough

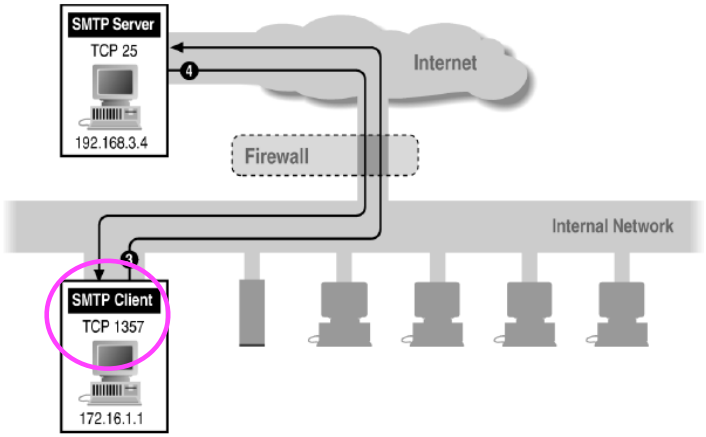
- In TCP connections, ports with numbers less than 1024 are permanently assigned to servers
  - 20,21 for FTP, 23 for telnet, 25 for SMTP, 80 for HTTP…
- Clients use ports numbered from 1024 to 16383
  - They must be available for clients to receive responses
- What should a firewall do if it sees, say, an incoming request to some client's port 5612?
  - It must allow it: this could be a server's response in a previously established connection…
  - …OR it could be malicious traffic
  - Can't tell without keeping state for each connection

slide

Example: Variable Port Use



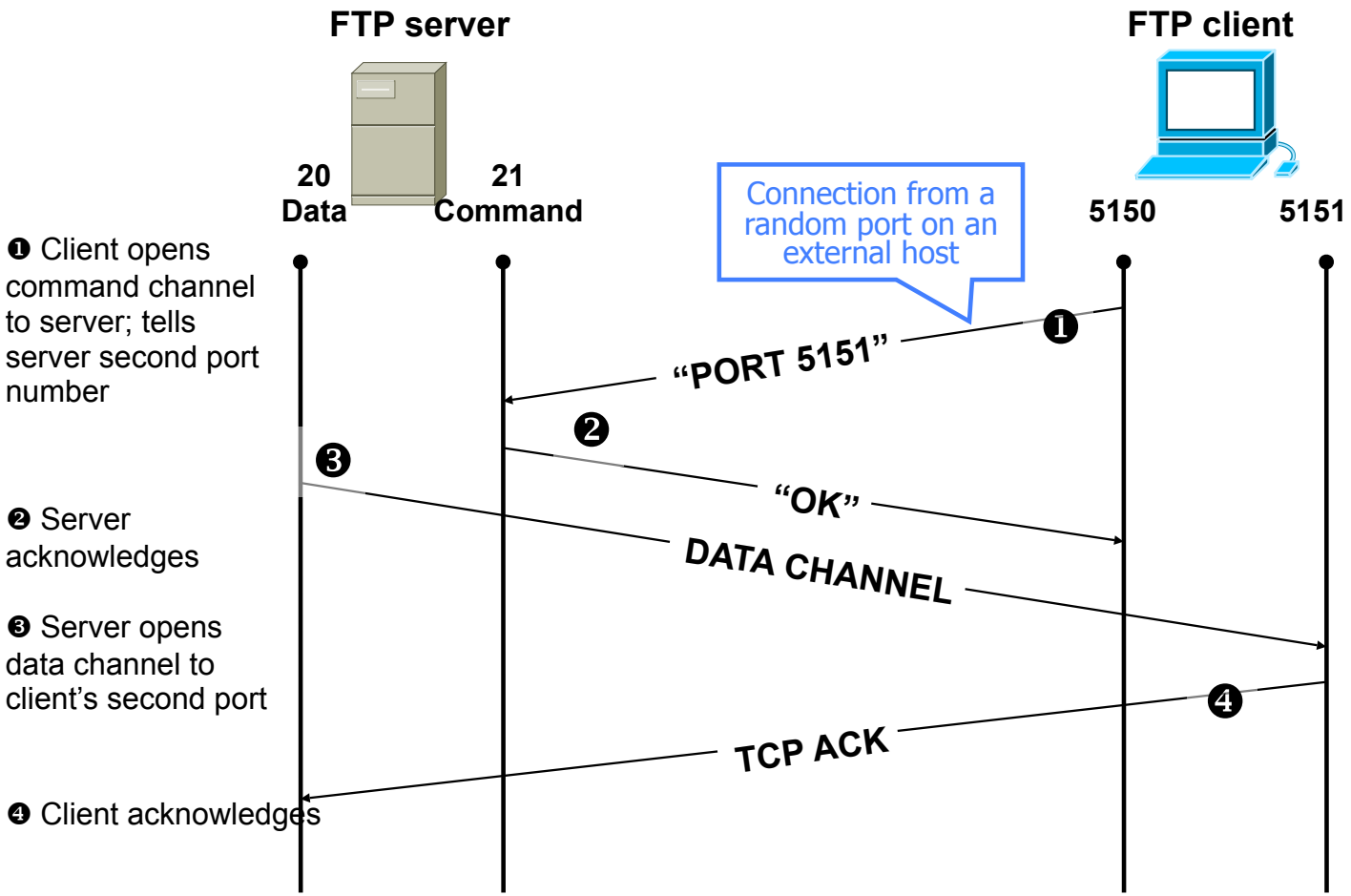
Inbound SMTP



Outbound SMTP

slide

Example: FTP (borrowed from Wenke Lee)



slide