CSE 484 (Winter 2008)

Network Security

Tadayoshi Kohno

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

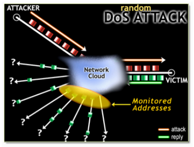
Goals for Today

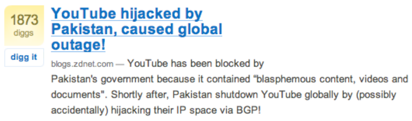
- Network Security Attacks
  - Routing
  - IP
  - TCP
  - DNS
- Key points:
  - Failures at interaction between layers
  - Asymmetry between attacker and defender
  - Some attacks designers never considered
  - All motivations for existing security decisions (SSL/TLS, filter certain types of packets,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

- 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]

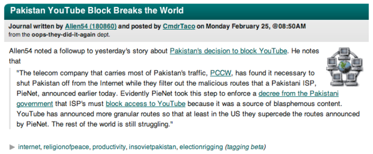



1873 diggs

digg it

YouTube hijacked by Pakistan, caused global outage!

blogs.zdnet.com — YouTube has been blocked by Pakistan's government because it contained "blasphemous content, videos and documents". Shortly after, Pakistan shutdown YouTube globally by (possibly accidentally) hijacking their IP space via BGP!


Pakistan YouTube Block Breaks the World

Journal written by Allen54 (180860) and posted by CmdrTaco on Monday February 25, @08:50AM
from the **oops-they-did-it-again** dept.

Allen54 noted a followup to yesterday's story about Pakistan's decision to block YouTube. He notes that

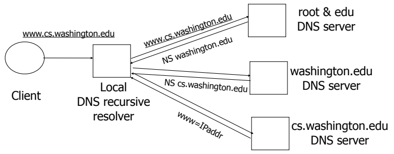
> "The telecom company that carries most of Pakistan's traffic, PCCW, has found it necessary to shut Pakistan off from the Internet while they filter out the malicious routes that a Pakistani ISP, PieNet, announced earlier today. Evidently PieNet took this step to enforce a decree from the Pakistani government that ISP's must block access to YouTube because it was a source of blasphemous content. YouTube has announced more granular routes so that at least in the US they supercede the routes announced by PieNet. The rest of the world is still struggling."

▶ internet, religionofpeace, productivity, insovietpakistan, electionrigging *(tagging beta)*

DNS Issues

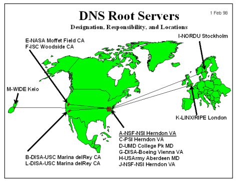
DNS: Domain Name Service

DNS maps symbolic names to numeric IP addresses
(for example, www.cs.washington.edu ↔ 128.208.3.88)



DNS Root Name Servers

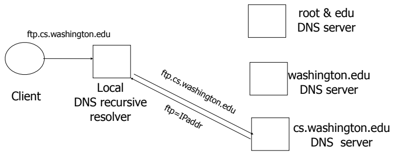
- Root name servers for top-level domains
- Authoritative name servers for subdomains
- Local name resolvers contact authoritative servers when they do not know a name
  •



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

Cached Lookup Example


ftp.cs.washington.edu

Client

Local
DNS recursive
resolver

root & edu
DNS server

washington.edu
DNS server

cs.washington.edu
DNS server

ftp.cs.washington.edu

ftp=IPaddr

DNS Vulnerabilities

- DNS host-address mappings are <u>not</u> 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)

Defenses Against DNS Spoofing

- Double-check reverse DNS
  - Modify rlogind, rshd to query DNS server and check if symbolic address maps to numeric address
  - Cache poisoning still an issue
- Authenticate entries in DNS tables
  - Hard to do; need public-key infrastructure

See <u>http://cr.yp.to/djbdns/notes.html</u>

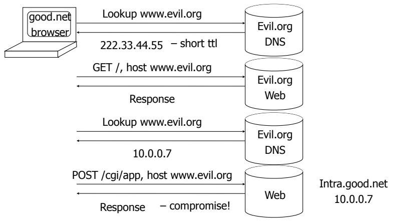
Other DNS Risks

- 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

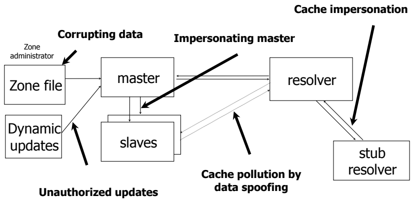
JavaScript/DNS Intranet attack (I)

- 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

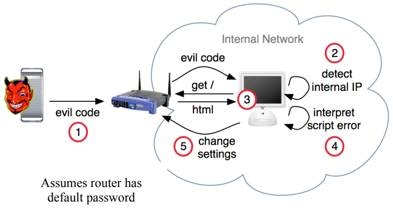
JavaScript/DNS Intranet attack (II)



DNS Vulnerabilities: Summary

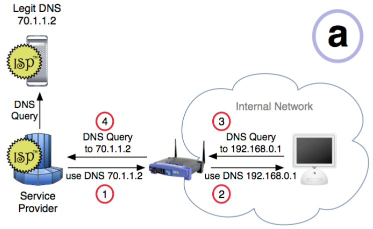


Drive-by pharming

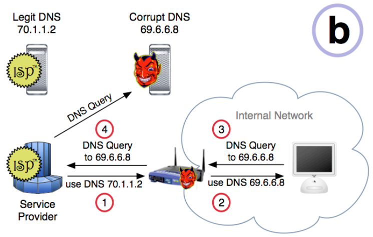


Assumes router has
default password

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

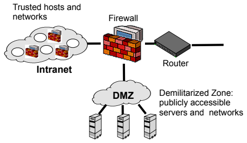
DNSSEC

- 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)

Firewalls and Network Defense

Firewalls

- ◆ Idea: separate local network from the Internet

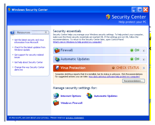

Trusted hosts and networks
Firewall
Intranet
Router
DMZ
Demilitarized Zone: publicly accessible servers and networks

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!

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


Windows Security Center

Security Center
Help protect your PC

Resources
- Get the latest security and virus information from Microsoft
- Check for the latest updates from Windows Update
- Get support for security-related issues
- Get help about Security Center
- Change the way Security Center alerts me

Security essentials
Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.
What's new in Windows to help protect my computer?

Firewall ON

Automatic Updates ON

Virus Protection CHECK STATUS

Symantec AntiVirus reports that it is installed, but its status is unknown. Click Recommendations for suggested actions you can take. How does antivirus software help protect my computer?

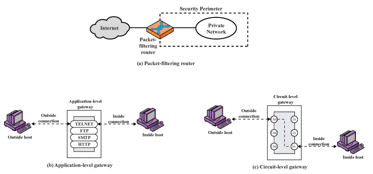
Manage security settings for:

At Microsoft, we care about your privacy. Please read our privacy statement.

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

Firewall Types: Illustration



(a) Packet-filtering router

(b) Application-level gateway

(c) Circuit-level gateway

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

Packet Filtering Examples

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

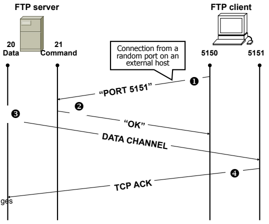
	action	ourhost	port	theirhost	port	comment
B	block	*	*	*	*	default

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

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

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

Example: FTP (borrowed from Wenke Lee)



❶ Client opens command channel to server; tells server second port number

❷ Server acknowledges

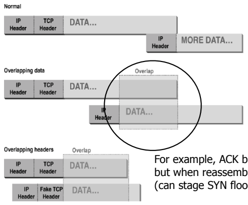
❸ Server opens data channel to client's second port

❹ Client acknowledges

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

Abnormal Fragmentation

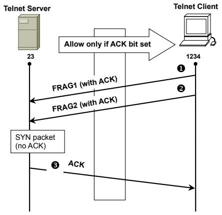


For example, ACK bit is set in both fragments, but when reassembled, SYN bit is set
(can stage SYN flooding through firewall)

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



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