MEN&MICE

DNS and BIND Security

Cricket Liu

Men & Mice

www.menandmice.com

Security Threats

- **Spoofing**
- **Denial of service**
- **BIND vulnerabilities**

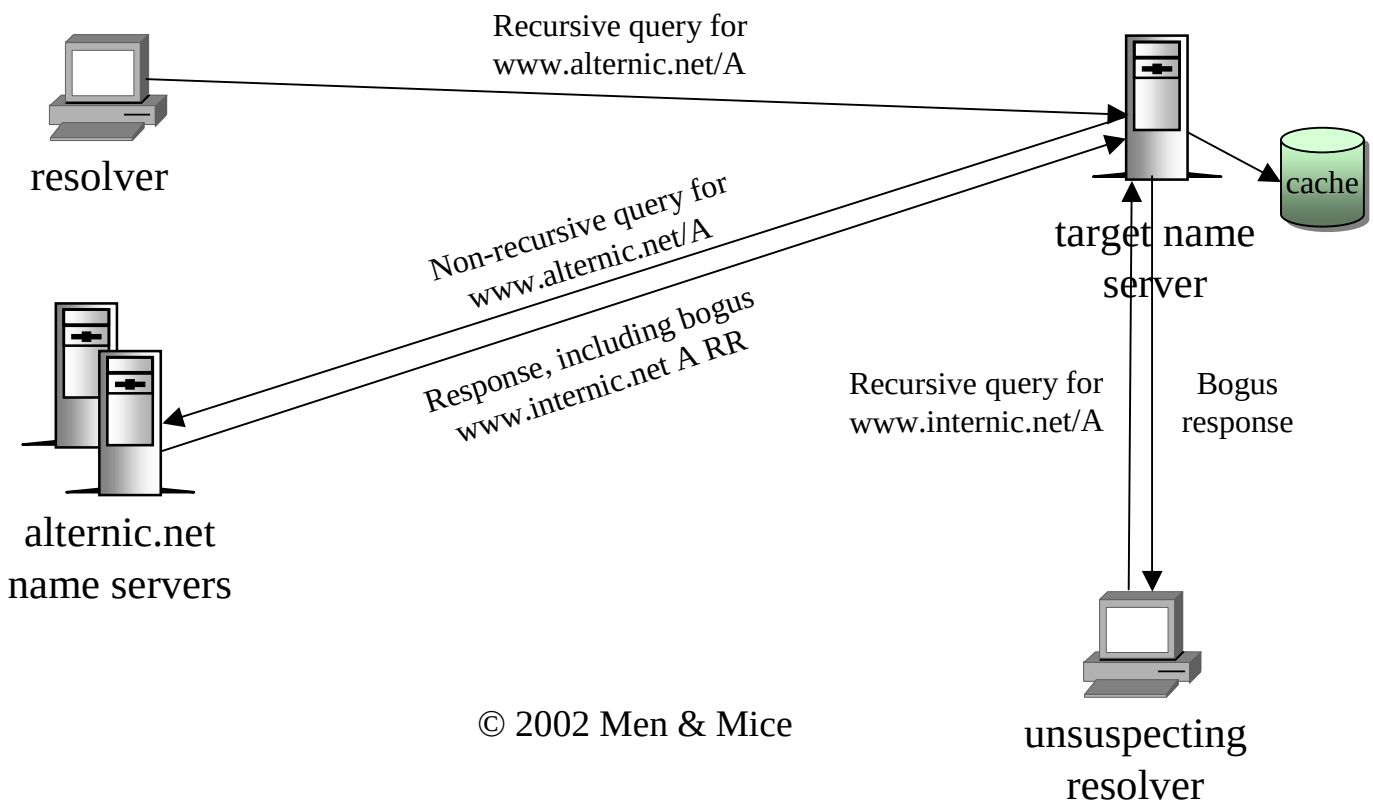
MEN&MICE

“Triggered” Cache Poisoning

- **Inducing a name server, directly or indirectly, to query a name server under your control and cache bogus records**
  - Directly
    - By sending it recursive queries
    - By spoofing responses
  - Indirectly
    - By connecting to a server (e.g., mail, web) that uses the target name server

The Kashpureff Attack

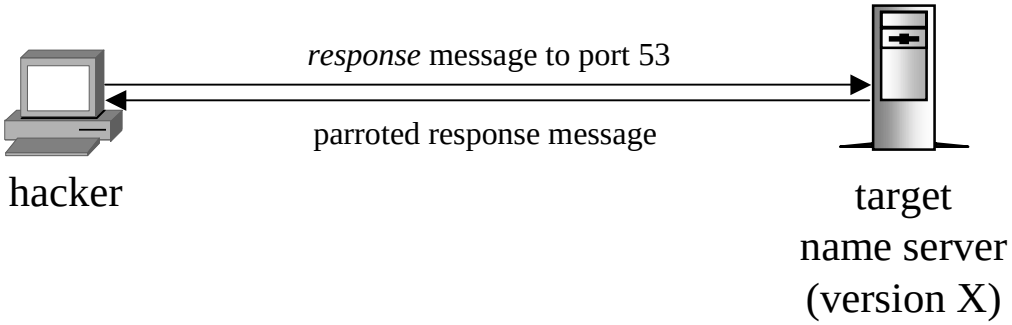
- **In July, 1997, Eugene Kashpureff used a direct triggered cache poisoning attack against the InterNIC's web site**



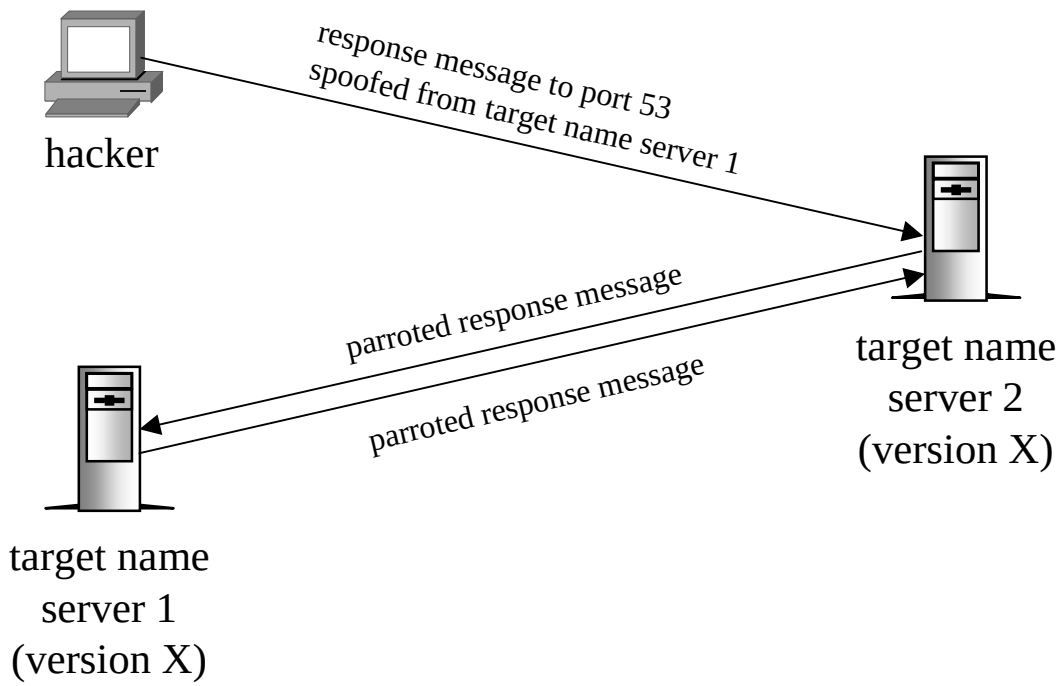
Denial of Service

- **Exploiting implementation flaws**
  - E.g., responding to responses with parroted responses
- **Overwhelming name servers**
  - E.g, with zone transfer requests

A (Real) Sample Implementation Flaw



A (Real) Sample Implementation Flaw (cont.)



MEN&MICE

(Some) BIND Vulnerabilities

- **The "TSIG bug"**
  - A buffer overflow in the TSIG code of all BIND name servers older than 8.2.3
  - Provides access to the host on which *named* runs
  - Exploited by the li0n worm
- **The "Complain bug"**
  - A buffer overflow in *nslookupComplain()*
  - Allows hackers to crash *named*
- **The "SRV bug"**
  - Improper processing of SRV records
  - Results in an infinite loop
- **The "NXT bug"**
  - Improper processing of NXT records
  - Provides access to the host on which *named* runs

MEN&MICE

DNS and BIND Security Recommendations

- **Avoid single points of failure**
- **Run a new version of BIND**
- **Disable unnecessary services and filter traffic**
- **Run *chroot()*ed**
- **Run with least privilege**
- **Don't use BIND 8's *inet* control channel**
- **Restrict queries**
- **Restrict zone transfers**
- **Restrict dynamic updates**
- **Run "split service" name servers**
- **Monitor your name servers**
- **Read**

Avoid Single Points of Failure

- **Provide multiple authoritative name servers for each zone**
  - On different subnets
  - Behind different routers
  - Connected via different leased lines
- **Provide backup master name servers**
  - Slave name servers can load from multiple master name servers
- **Provide backup name servers for resolution**
  - Most resolvers can query as many as three name servers

Run a New Version of BIND

- **All versions of BIND older than 8.2.3 have widely known vulnerabilities**
- **Run a new version of BIND**
  - 8.3.1 or 8.2.5
  - 9.2.0

MEN&MICE

ISC's Matrix of BIND Vulnerabilities

Summary

The following table summarizes the vulnerability to the bugs mentioned for all versions of BIND distributed by ISC. Upgrading to BIND version 8.2.3 or higher is strongly recommended for all users of BIND.

version	zxfr	sigdiv0	srv	nxt	sig	naptr	maxdname	solinger	fdmax	complain	infoleak	tsig
4.8											+	
4.8.1							-				+	
4.8.2.1							-				+	
4.8.3							-				+	
4.9.3							-			+	+	
4.9.4							-			+	+	
4.9.4 p1							-			+	+	
4.9.5			-		+	+	+			+	+	
4.9.5 p1			-		+	+	+			+	+	
4.9.6			-		+	+	+			+	+	
4.9.7			-		-	+	+			+	+	
4.9.8			-		-	+	+			-	-	
8.1			-		+	+	+	+	+	-	+	
8.1.1			-		+	+	+	+	+	-	+	
8.1.2			-		-	+	+	+	+	-	+	
8.2	-	+	+	+	+	+	+	+	+	-	+	+
8.2 p1	-	+	+	+	+	+	+	+	+	-	+	+
8.2.1	-	+	+	+	+	+	+	+	+	-	+	+
8.2.2	+	+	+	-	-	+	+	-	-	-	+	+
8.2.2 p1	+	+	+	-	-	+	+	-	-	-	+	+
8.2.2 p2	+	+	+	-	-	-	-	-	-	-	+	+
8.2.2 p3	+	+	+	-	-	-	-	-	-	-	+	+
8.2.2 p4	+	+	+	-	-	-	-	-	-	-	+	+
8.2.2 p5	+	+	+	-	-	-	-	-	-	-	+	+
8.2.2 p6	+	-	+	-	-	-	-	-	-	-	+	+
8.2.2 p7	-	-	-	-	-	-	-	-	-	-	+	+
8.2.3	-	-	-	-	-	-	-	-	-	-	-	-
8.2.4	-	-	-	-	-	-	-	-	-	-	-	-
8.2.5	-	-	-	-	-	-	-	-	-	-	-	-
9.0.0		-	-	-	-	-	-	-	-	-	-	-
9.1.0		-	-	-	-	-	-	-	-	-	-	-
9.1.1		-	-	-	-	-	-	-	-	-	-	-
9.1.2		-	-	-	-	-	-	-	-	-	-	-
9.1.3		-	-	-	-	-	-	-	-	-	-	-
9.2.0		-	-	-	-	-	-	-	-	-	-	-

Vulnerable: '+', Not Vulnerable: '-', Feature does not exist: ' '

Disable Unnecessary Services and Filter Traffic

- **Disable all unnecessary services on the hosts that run your name servers**
- **A possible minimal set of network services**
  - DNS
  - SSH
  - NTP
- **Filter traffic to and from your name servers**

From	Source Port	To	Destination Port	Protocol	Purpose
Any	Any	Name server	53	UDP or TCP	Queries from the Internet
Name server	53	Any	Any	UDP or TCP	Responses from your name server
Name server	Any	Any	53	UDP or TCP	Queries from your name server
Any	53	Name server	Any	UDP or TCP	Responses from your name server

MEN&MICE

Run *chroot()*ed

- **Running your name server *chroot()*ed helps minimize the damage caused by a breach**
  - A successful hacker would only have access to the directory the name server *chroot()*ed to
- **BIND 9 name servers are much easier to run *chroot()*ed**
  - They read */etc/passwd* before *chroot()*ing
  - They don't use *named-xfer*
- **If your OS supports *chroot()*, run your name server *chroot()*ed**

Run with Least Privilege

- **BIND name servers can give up root privilege after listening on port 53**
- **Like using *chroot()*, this helps minimize the damage a breach causes**
  - A successful hacker would only have access to the host as the user *named* runs as
  - Typically, this is a special user created just to run *named*

Don’t Use BIND 8’s *inet* Control Channel

- **Under BIND 8, *inet* control channels are inherently insecure**
  - The name server uses source IP addresses to authenticate commands
  - So don’t use *inet* control channels; use *unix*
- **Under BIND 9, *inet* control channels are secure(r)**
  - The name server uses cryptography to authenticate commands
  - But you should still restrict the IP addresses that can send commands

MEN&MICE

Restrict Queries

- **Most name servers shouldn't accept queries from just any IP address**
  - A caching-only name server, for example, should only accept queries from the IP addresses of resolvers it serves
  - An authoritative-only name server must accept queries from any IP address, but shouldn't accept any recursive queries
  - A name server should never accept queries from some networks
    - Private networks (unless they're yours)
    - Experimental networks
    - Multicast networks

Restrict Queries (cont.)

- **Based on the function of each of your name servers, restrict the queries it will accept to authorized sources**
- **Blackhole private, experimental and multicast networks**
  - See *http://www.cymru.com/~robt/Docs/Articles/secure-bind-template.html* for a nice list

Restrict Zone Transfers

- **Zone transfers reveal entire zones (duh) and burden your name server**
- **Restrict zone transfers to slave name servers and other authorized software**
  - Preferably by TSIG key rather than IP address
  - Remember to deny all zone transfers from slaves that aren't used as master name servers

MEN&MICE

Restrict Dynamic Updates

- **A dynamic updater has near-complete control over a zone**
  - He can delete every record in the zone except for the SOA record and one NS record and add entirely different records
- **Restrict dynamic updates as much as possible**
  - To individual IP addresses or, preferably, TSIG keys
- **If possible, “sandbox” dynamically updated domain names in a separate zone**

MEN&MICE

Run “Split Service”

- **If possible, run separate “delegated” and “resolving” name servers**
  - “Delegated” name servers have one or more zones delegated to them
  - “Resolving” name servers have one or more resolvers configured to query them
- **On a “delegated” name servers, disable recursion**
- **On a “resolving” name server, restrict queries to the IP addresses of authorized resolvers**

Monitor Your Name Servers

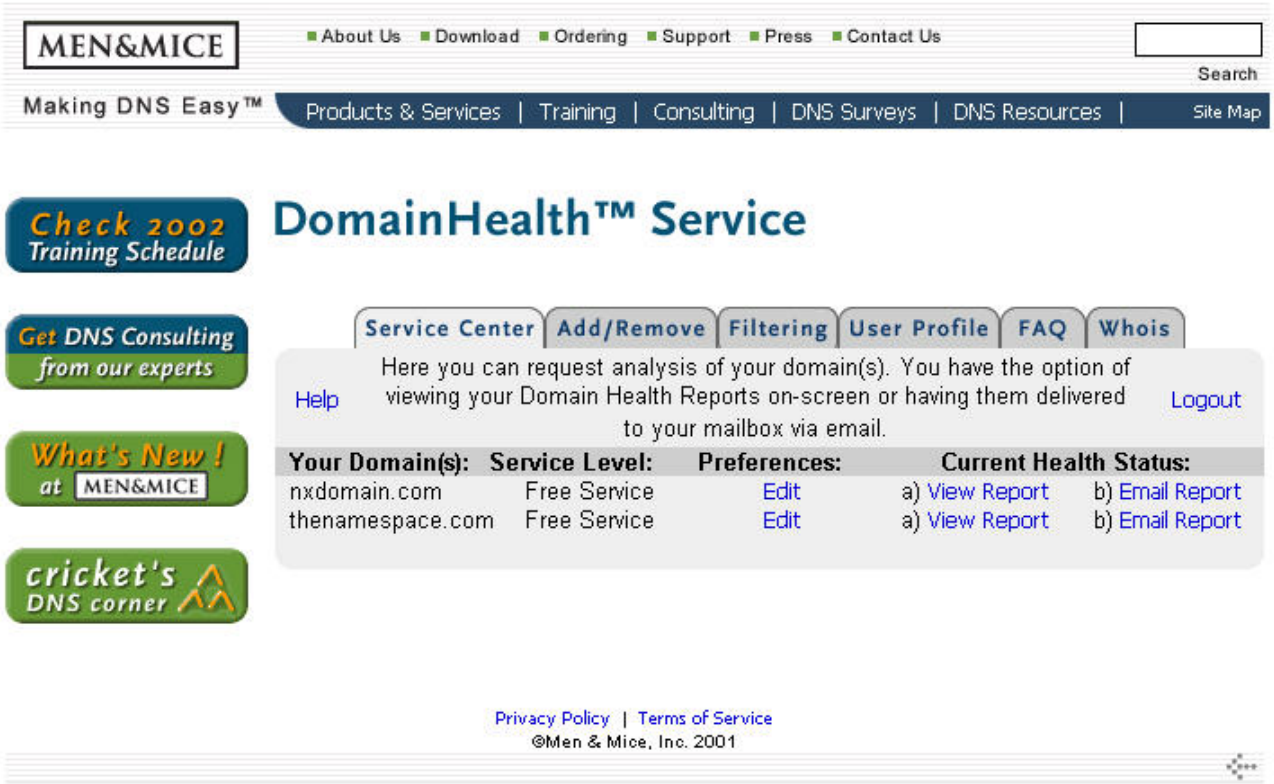
- **Aggregate your name servers' *syslog* output on a loghost**
  - Use a log file monitoring tool like *swatch* to alert staff of important log messages
- **Use Men & Mice's DomainHealth™ service**
  - For monitoring the health of your name servers from the Internet

DomainHealth™ Service

- **Commercial service available at *www.DNS-Health.menandmice.com***
- **Queries your name servers and analyzes the results**
  - Detects nearly 200 configuration errors and vulnerabilities
  - Produces a report describing results, including links to explanations
  - Runs periodically or on demand

MEN&MICE

DomainHealth™ Service (cont.)



MEN&MICE

Domain Health™ Service (cont.)

DomainHealth™ Service

Service Center | Add/Remove | Filtering | User Profile | FAQ | Whois

Help

Here you can see the health status of your domain as it was the last time it was scanned.

Logout

Health status for the domain "thenamespace.com"

Date of analysis:	2/26/2002 4:45:21 PM (GMT)
Serial number:	2002011600
Primary name server:	bigmo.nxdomain.com.
Primary mail server:	bigmo.nxdomain.com.
Number of records:	7 (4 NS, 1 MX, 1 A, 1 CNAME, 0 PTR, 0 Other)
Number of errors:	2
Number of warnings:	3

Printer Friendly Version

The zone is in fair condition
You should be aware of these issues:
* The delegation information for the zone is incorrect.

Report: (To get details on an error message, simply click on a corresponding hyperlink.)

Legend:

- Error - Warning - Click this icon to set the filtering options for the message

Read

- **Subscribe to *bind-users* or *bind9-users***
  - *bind-users* is gatewayed to *comp.protocols.dns.bind*
  - Subscribe by sending mail to *bind-users-request@isc.org* or *bind9-users-request@isc.org* with “subscribe” in the body
- **Subscribe to Bugtraq**
  - Subscribe at *http://www.securityfocus.com/cgi-bin/subscribe.pl*
- **Monitor CERT advisories and the ISC’s BIND security page**
  - *http://www.cert.org/advisories*
  - *http://www.isc.org/products/BIND/bind-security.html*

A Commercial Break

- **For information on Men & Mice's DNS security assessment service, or to request a quote, see *http://www.menandmice.com/8000/8520_consulting_assess.html***
- **For Men & Mice's full-day class on DNS and BIND security, see *http://www.menandmice.com/8000/8000_dns_training.html***