DNS and BIND Security

Cricket Liu
Men & Mice
www.menandmice.com
Security Threats

• Spoofing
• Denial of service
• BIND vulnerabilities
“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

![Diagram of the Kashpureff Attack]
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

response message to port 53
parroted response message

hacker

name server (version X)

target
A (Real) Sample Implementation Flaw (cont.)

**Diagram:**
- Hacker
  - Sues spoofed DNS request to port 53 from Target Name Server 1
- Target Name Server 1
  - Responds with a parroted response message to the hacker
- Target Name Server 2
  - Receives a parroted response message from Target Name Server 1
  - Responds with a parroted response message to the hacker

© 2002 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
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
## ISC’s Matrix of BIND Vulnerabilities

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.

<table>
<thead>
<tr>
<th>version</th>
<th>zxfi</th>
<th>sigdiv0</th>
<th>srv</th>
<th>nxt</th>
<th>sig</th>
<th>naptr</th>
<th>maxdname</th>
<th>solinger</th>
<th>f.dmax</th>
<th>complain</th>
<th>info.leak</th>
<th>tsig</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.8</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4.8.1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4.8.2.1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4.8.3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4.9.3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4.9.4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4.9.4p1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4.9.5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4.9.5p1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4.9.6</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4.9.7</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4.9.8</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8.1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8.11</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8.12</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8.2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8.2p1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8.2.1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8.2.2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8.2.2p1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8.2.2p2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8.2.2p3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8.2.2p4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8.2.2p5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8.2.2p6</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8.2.2p7</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8.3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8.4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8.5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>9.0.0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>9.1.0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>9.1.1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>9.1.2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>9.1.3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>9.2.0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>From</th>
<th>Source Port</th>
<th>To</th>
<th>Destination Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Name server</td>
<td>53</td>
<td>UDP or TCP</td>
<td>Queries from the Internet</td>
</tr>
<tr>
<td>Name server</td>
<td>53</td>
<td>Any</td>
<td>Any</td>
<td>UDP or TCP</td>
<td>Responses from your name server</td>
</tr>
<tr>
<td>Name server</td>
<td>Any</td>
<td>Any</td>
<td>53</td>
<td>UDP or TCP</td>
<td>Queries from your name server</td>
</tr>
<tr>
<td>Any</td>
<td>53</td>
<td>Name server</td>
<td>Any</td>
<td>UDP or TCP</td>
<td>Responses from your name server</td>
</tr>
</tbody>
</table>
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

© 2002 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
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
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
DomainHealth™ Service (cont.)

DomainHealth™ Service

Here you can request analysis of your domain(s). You have the option of viewing your Domain Health Reports on-screen or having them delivered to your mailbox via email.

<table>
<thead>
<tr>
<th>Your Domain(s)</th>
<th>Service Level</th>
<th>Preferences</th>
<th>Current Health Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>nxdomain.com</td>
<td>Free Service</td>
<td>Edit</td>
<td>a) View Report b) Email Report</td>
</tr>
<tr>
<td>thenamespace.com</td>
<td>Free Service</td>
<td>Edit</td>
<td>a) View Report b) Email Report</td>
</tr>
</tbody>
</table>

Privacy Policy | Terms of Service
©Men & Mice, Inc. 2001
Domain Health™ Service

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

<table>
<thead>
<tr>
<th>Health status for the domain &quot;thenamespace.com&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of analysis:</td>
</tr>
<tr>
<td>2/26/2002 4:45:21 PM (GMT)</td>
</tr>
<tr>
<td>Serial number:</td>
</tr>
<tr>
<td>2002011600</td>
</tr>
<tr>
<td>Primary name server:</td>
</tr>
<tr>
<td>bigmc.nxdomain.com.</td>
</tr>
<tr>
<td>Primary mail server:</td>
</tr>
<tr>
<td>bigmc.nxdomain.com.</td>
</tr>
<tr>
<td>Number of records:</td>
</tr>
<tr>
<td>7 (4 NS, 1 MX, 1 A, 1 CNAME, 0 PTR, 0 Other)</td>
</tr>
<tr>
<td>Number of errors:</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>Number of warnings:</td>
</tr>
<tr>
<td>3</td>
</tr>
</tbody>
</table>
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](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.cert.org/advisories)
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

© 2002 Men & Mice