

SOLUTION NOTE

## A Checklist for Guarding Against Cache Poisoning Attacks

Cricket Liu, Vice President of Architecture

1. **Use forwarders.** The recent spoofing attacks against name servers are an object lesson in the importance of not allowing all of your internal name servers to query name servers on the Internet directly. If your internal name servers turn out to be vulnerable to a well-known DNS spoofing attack, you may be able to address it by securing or upgrading your forwarders. If you don't use forwarders, be prepared to upgrade all of your internal name servers. Yuck.
2. **Run the latest version of BIND on your forwarders.** The Microsoft DNS Server, as well as older BIND name servers, don't protect themselves against cache poisoning attacks as well as BIND 9 does. Your forwarders are directly exposed to the Internet, so run the most robust name server code there.
3. **If possible, split your external authoritative name servers and forwarders.** External authoritative name servers need to accept queries from almost any address, but forwarders don't. If you split these name servers into two camps, you can protect each: On the external authoritative name servers, disable recursion. On the forwarders, allow only queries from your internal address space.
4. **If you split your external name servers and forwarders,** filter traffic to and from your forwarders. Using either firewall- or router-based filters, ensure that Internet name servers can't send queries to your forwarders. This will probably require "stateful" filtering of UDP datagrams, to allow only solicited DNS messages (i.e., responses to queries) from Internet name servers to your forwarders.
5. **If you can't split your authoritative name servers and forwarders, restrict recursion as much as possible.** Only allow recursive queries if they come from your internal address space. Oh, that requires the ability to apply an ACL to recursive queries, which you can't do with the Microsoft DNS Server. BIND 9's views may come in handy here, allowing you to separate your name server's role as an authoritative name server and as a forwarder into separate views, each with its own configuration. The authoritative view would have recursion disabled, and only internal clients could access the internal view.



For more information on securing your name servers, see *O'Reilly & Associates' DNS and BIND*.

### Infoblox Product Warranty and Services

The standard hardware warranty is for a period of one year. The system software has a 90-day warranty that will meet published specifications. Optional service products are also available that extend the hardware and software warranty. These products are recommended to ensure the appliance is kept updated with the latest software enhancements and to ensure the security and availability of the system. Professional services and training courses are also available from Infoblox. Information in this document is subject to change without notice. Infoblox Inc. assumes no responsibility for errors that appear in this document.