RAVEN ALDER

a summary of savvy backbone defense

Raven Alder is a security consultant with an ISP background, based out of Seattle. Her interests include free software, network infrastructure security, and kayaking.

raven@oneeyedcrow.net

IN RECENT MONTHS, MANY OF YOU have no doubt noticed the increasing trend toward attacks directed at routers. In the wake of this summer's "Ciscogate" disclosures at the Black Hat security conference, community interest in router and switch security has redoubled. Many more people than ever before are openly poking at Cisco IOS, and interest in Juniper and other routing vendors has also increased. Although backbone security has been a concern of ISPs for years, many of the same security lessons apply to smaller networks, corporate networks, and other devices closer to the edge. This article will discuss best practices and mitigation strategies for savvy backbone defense and will give practical guidelines that you can implement on your networks to secure them against common attacks.

There are two main sorts of attacks leveled against backbone devices—attacks against the devices themselves, and attacks against the flow of data they control. Either can be devastating if properly deployed. Most attackers seek to control a backbone as a means of traffic control or monitoring, but denial-of-service is also a common goal. By deploying a robust and well-thought-out plan of defense in depth, most of these attacks can be avoided.

Direct Attacks on the Device

Most of the early attempts to attack routers depended on accessing the device through poorly secured but legitimate channels. Malicious programs scanned the Internet looking for devices that still had default logins enabled ("cisco/cisco" was common), default Simple Network Management Protocol strings such as "public" or "private," cleartext protocols being used for authentication traffic, or other hallmarks of classic poor security. More recently, brute force programs have been attempting to guess usernames and passwords, depending on administrators to allow poor choices. It only takes one bad account to grant viewing access to much of the router's statistical data, for example. This year, we have seen for the first time a remote root exploit that targeted Cisco IOS, shoveling an enabled shell back to the attacking machine. While exploit code for this was not publicly known to

be in the wild at the time of writing, the proof of concept alone sparked a determined flurry of similar research.

To defend against these sorts of attacks, here are some best-practice recommendations:

- Treat your routers and switches as you treat all the other devices on your network—as machines which will need regular patching and maintenance. Gone are the days of "set it up and forget it." As new vulnerabilities are discovered, the responsible and security-conscious administrator will need to keep backbone software up to date to defend against new threats.
- Don't use insecure or cleartext protocols to manage your backbone devices. Log in with SSH rather than with Telnet. If you must use SNMP, use SNMPv3 rather than SNMPv1. This will reduce the chances of your authentication data being sniffed by an attacker.
- Restrict access to the routers themselves to designated management stations. The fewer people are authorized and empowered to talk to your routers, the harder it will be for an attacker. They'll have to get through your access lists first.
- Use strong passwords and a good authentication system. Don't keep default passwords. If you use centralized authentication such as TACACS+ or RADIUS, make sure that users have non-obvious usernames and strong passwords to reduce the chances of brute-forcing. Practice good change control—when an employee leaves, make sure the account is disabled.
- Practice good physical security. Many routers can be reset by a signal to the console port, and their passwords changed through a well-known five-minute sequence involving an interrupted reboot.
- Maintain a good relationship with your vendors, and watch for posts about your products to security mailing lists such as Bugtraq, VulnWatch, or any vendor-specific security mailing lists. Early warning will alert you to a new problem quickly and increase your odds of taking remediation steps before things reach critical severity.

Routing and Switching Attacks

The device advice above ought to sound very familiar—it's strikingly like best practice procedures for managing any end device on your network. However, the unique challenges of securing backbone devices really come to the forefront when you look at vulnerabilities in their handling of routing protocols and switching management traffic. Here, our concerns will center on protocol authentication, data validation, and trust relationships. The following best practice guidelines will help you secure your routing and switching traffic:

- Use protocols that do some authentication checking before accepting new information. If you're using BGP, for example, use BGP passwords to validate that the external peer sending you those new routes really is who you think.
- Prohibit routing, switching, and management protocols from being distributed out toward the LANs. An end user sitting at a desk should not see Spanning Tree traffic, under most circumstances. EIGRP neighbor announcements should not be allowed to reach a laptop LAN user. This leaks unnecessary information about your network's configuration, and may enable further and more sophisticated attacks. If you can see the traffic, you can spoof the traffic.
- Use access lists to control what traffic you will accept and what traffic you will route. Block RFC 1918 space from being advertised to you, unless you

have a specific reason to allow it. Don't allow your neighbors to advertise your own netblocks to you. If possible, implement bogon filtering.

- Take denial-of-service vulnerabilities seriously. They're not "just DoS"—a threat to availability and security ought to be a concern for just about any network administrator or security geek. In addition, some DoS vulnerabilities have later been found to be exploitable memory corruption vulnerabilities—Michael Lynn's remote root exploit for Cisco IOS was developed from such a vulnerability. The people who didn't patch for a DoS were left scrambling frantically to patch after Cisco's full advisory was published. Do patch, even if it's "just a DoS."
- Read routing-specific mailing lists such as the North American Network Operators Group (http://www.nanog.org/mailinglist.html) or its equivalent for your locale, to keep abreast of Internet events and security issues that affect the backbone.

I also highly recommend the Secure IOS Template (http://www.cymru.com/Documents/secure-ios-template.html), Secure JunOS Template (http://www.cymru.com/gillsr/documents/junos-template.pdf), Secure BGP Template (http://www.cymru.com/Documents/secure-bgp-template.html), and Secure JunOS BGP Template (http://www.cymru.com/gillsr/documents/junos-bgp-template.pdf) as excellent guides to configuration for many of these recommendations. In effect, these guides allow you to produce hardened routers, disabling unnecessary services, helping you to select stronger cryptography and passwords, and much more. Team Cymru does an excellent job in maintaining and updating these consensus documents.

In addition to taking the appropriate technical measures to support and secure your backbone infrastructure, it is also important to build a business case for maintaining the security of your backbone. Good security policies and a strong incident response plan can be invaluable in case of a backbone intrusion, and you're unlikely to get them without the support of your management. Often, this involves building a business case to explain to them why this issue is important.

Risk management procedures show that the severity of a threat to the backbone is likely to warrant some effort in defense; the possible loss of a compromised backbone is staggering. To that end, have your incident response plan ready. Know who your engineering and management contacts are within your organization in case of an event, and have the contact and contract data from your vendors available and ready. Have a plan for data transfer of patches in case your network becomes unreachable. (Some networks depend on overnight delivery, while others have a guaranteed delivery within hours from their vendors written into the service contracts.) If a severe enough event occurs, having your whole network knocked offline or clogged to unusability is a distinct possibility, and worth planning for.

By following these basic guidelines, you will not perfectly secure your backbone, but at the very least you ought to be able to improve your security posture. It's a well-known adage that "Attacks don't get worse, they only get better." By taking some of these basic precautions to protect your routers, you are more likely to be prepared to deal with these attacks.