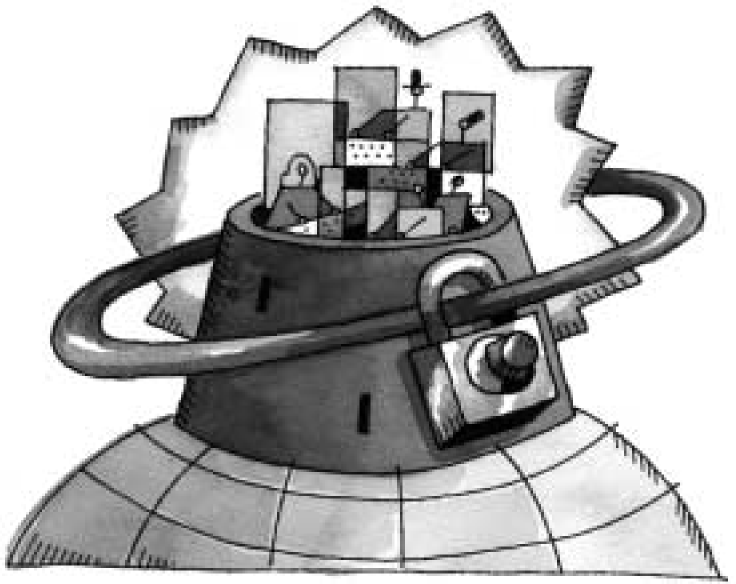
;login:
THE MAGAZINE OF USENIX & SAGE
December 2002 • volume 27 • number 6

Focus Issue: Security

Guest Editor: Rik Farrow



inside:

USENIX & SAGE
The Advanced Computing Systems Association &
The System Administrators Guild

the case for network infrastructure security

"The network is the computer." – Sun Microsystems, ca. 1984

"The network is the network, the computer is the computer. Sorry about the confusion." – Anonymous

by George M. Jones

George Jones is a network security architect for UUNET. In previous lives he worked at BankOne, CompuServe, and Ohio State University. He has been noodling around with Emacs since '79, UNIX since '85, and security things since '97. What a long strange trip it's been.

gmj@pobox.com

What Does "Network Security" Mean?

What do you mean when you say "network security"? Firewalls? Intrusion detection systems? Anti-virus software? Authentication systems? System and application hardening? These are all fine and even necessary elements of "current best practice" if you're running a small office network or even a medium-sized corporate intranet.

But what if you're running a global Internet backbone with over 4700 routers, announcing over 60% of all routes, and have over 600 routers and switches in 25 hosting data centers? What does "network security" mean when you *are* the network and have no perimeter?

Chances are that in your world, you are closer to the first scenario. It is the premise of this article that while many of the solutions for smaller networks don't scale, many of the problems in the larger networks do apply generally, and that ignoring them may result in widespread disruption of service.

The main goal for large networks is availability. The bits should keep flowing, preferably to the right place. While integrity and confidentiality are important problems, it is assumed that these are handled "at the end of the pipe" by VPNs, host-based controls, good security policy and practice, etc. Assuring availability is a larger problem than it might at first seem. Let's take a look at some (relatively) recent problems.

Some Real Problems

DDoS Attacks

The greatest foreshadowing (not counting the Morris Worm of '88) of what could go wrong occurred in February 2000. Distributed Denial of Service (DDoS) attacks were launched, disabling Yahoo, eBay, Amazon.com, and others [lem01]. These attacks were made possible because hackers were able to "own" many poorly protected hosts across the Internet. Since then, DDoS defense has been a hot topic with governments, researchers, standards bodies, and network operators. A few products have even come on the market to address the problem. Still, there are no generally accepted solutions, technical or social, that adequately address the issue. In 2001, Code Red and Nimda demonstrated the speed with which worms can spread (and that we clearly have not solved the problem of insecure hosts). A paper [sta02] presented at the 2002 USENIX Security Symposium, titled "How to Own the Internet in Your Spare Time," demonstrates the current magnitude of the problem and suggests solutions, both technical and social.

The bottom line: DDoS attacks have already caused some disruption of service and have the potential to do far greater damage. Solutions are needed.

Bugs That Enable Hacking of the Network

Here is a sampling of some "recent" bugs that enable hacking of network infrastructure.

SNMP VULNERABILITIES

In February 2002, CERT announced vulnerabilities [cer02] that had been discovered in SNMP trap and request handling.[1] SNMP is the most widely used protocol for managing and monitoring network infrastructure. The root of the problem was our old friend the buffer overflow. In this case it was in the ASN.1 encoding/decoding that underlies SNMP. There are apparently very few ASN.1 implementations, so the result was that most SNMP implementations were vulnerable. A single malformed packet could cause the device to crash, or at least disable the IP stack. Imagine your core routers all suddenly rebooting.

NTP BUGS

In April 2001, a buffer overflow was discovered in certain UNIX-based NTP (Network Time Protocol) daemons [sec01]. Exploit code was published. Cisco published their own advisory in May 2002 [cis02]. The Cisco advisory stated that they were unable to reproduce the problem. Sources known to this author were able to exploit the vulnerability in IOS. Moral #1: Bugs can be "out there" a long time before they are exploited. Moral #2: Don't believe everything you read. Moral #3: Trust, but verify.

TELNET BUFFER OVERFLOWS

Going back a little further, to December 2000, we see that all problems are not related to buffer overflows in routers. A memory leak in the Telnet process on catalyst switches [cis00] caused them to reboot. Bye-bye desktops. Bye-bye Web servers . . .

SSH VULNERABILITIES

But you are being good. You're not using Telnet with its clear-text passwords. You use SSH to manage your devices. Have we got a vulnerability or two for you . . .[cis01]

Conflicting Priorities

Commercial vendors and network operators have conflicting priorities.[2] Vendors are interested in selling new equipment and software. Network operators are interested in operating networks. Vendors tend to focus effort on developing new products (which invariably have new bugs). Network operators focus on operating networks. Vendors tend to view bug fixing as a distraction from new product development and sales. Network operators view bug fixes in existing products as essential to operating networks. Vendors tend to see their job as done when the bug is fixed in the latest release. Network operators see their job as done when the bug fix is deployed across all devices (including old/obsolete ones) in their operating networks.

Operations

Operational realities can adversely affect security, even if technical solutions are known and available.

ANTIQUATED CODE REVS REQUIRED

It is sometimes the case that antiquated code revs are required for production. This may be true, for instance, if the vendor has produced a "special" to address unique

[1] SNMP has been rumored to stand for "Security Not My Problem."

[2] The author acknowledges that this may be "unfair," since it portrays an external view of vendors as seen from the engineering/security trenches.

needs of a particular customer or if the customer has policies against running "bleeding edge" releases (as is the case in industries such as utilities and banking).

UPGRADES NOT POSSIBLE

Sometimes, in the real world, it is just not possible to upgrade code quickly. Maybe "the network guy" quit or was laid off, and consultants are not immediately available. Maybe the IT department has other priorities (i.e., the risk of a bug in networking infrastructure is not perceived as high). Maybe the vendor has not produced a fix for the bug in question, or it is not available on the old hardware that is still doing just fine at meeting the business needs it was purchased to address. "If it ain't broke . . ."

PEOPLE/REAL-WORLD ISSUES

This does not touch the non-technical yet very real issues of staffing and training. At the present time the entire telecommunications sector is experiencing serious financial difficulty, with all the attendant impact on priorities and funding.

Configuration

In defense of vendors, it can be argued that the majority of vulnerabilities in networking infrastructure are due to incomplete configuration or misconfiguration. Vendors are supplying the right knobs. They just need to be set correctly. That's where tools such as the Router Audit Tool [jon02a] come in.

SURVEY SAYS . . .

A quick survey of 471 routers across the Internet that showed up in traceroutes to 94 Web servers showed that 81 of them (17%) accepted connections from arbitrary sources on either port 22 (SSH), 23 (Telnet) or 80 (HTTP). This is bad – no filters on administrative access. Of those, 38 (8%) were listening on port 22, 57 (12%) were listening on 23, and thankfully only 5 (1%) answered on 80.[3]

Some Potential Problems

We have seen a sampling of things that are problems today. Now, let's take a look at Network Nightmares: The Next Generation.

Same Old Same Old

If past performance can be used to predict future behavior, we can project that:

- Vendors will continue to release new products.
- These products will, with non-zero probability, have bugs.
- Consumers will buy and deploy these buggy products.
- The numbers of deployed networks,[4] systems, and users will continue to increase.
- The product of the probability of bugs and the number of deployed systems will increase. In absolute terms, there will be more vulnerabilities.
- The number of trained (and employed) systems and network security administrations will not increase at the same rate. The result will be more misconfigured or unconfigured systems.

More Spew

The eBay/Yahoo attacks of February 2000 [lem01] may only have been the tip of the iceberg, as demonstrated in Staniford et al. [sta02]. Real and crippling DDoS attacks on major sites and networks are a distinct possibility.

[3] Thanks to Pete White for suggesting this survey method.

[4] From 1/5/00 to 3/5/02, the number of advertised routes grew from 76,182 to 110,842, a 45% increase, even in the face of a down economy. Source: *http://www.employees.org/~tbates/cidr-report.html.*

References and Resources

References

[ahm00] “Network Infrastructure Insecurity,” Rauch Ahmad: *http://www.blackhat.com/presentations/bh-asia-00/jeremy-dave/jeremy-dave-asia-00-network.ppt*.

[cer02]“Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP),” CERT/CC: *http://www.cert.org/advisories/CA-2002-03.html*.

[cis00] “Cisco Catalyst Memory Leak Vulnerability,” Cisco Systems: *http://www.cisco.com/warp/public/707/catalyst-memleak-pub.shtml*.

[cis01] “Multiple SSH Vulnerabilities,” Cisco Systems: *http://www.cisco.com/warp/public/707/catalyst-memleak-pub.shtml*.

[cis02] “Cisco Security Advisory: NTP Vulnerability,” Cisco Systems: *http://www.cisco.com/warp/public/707/NTP-pub.shtml*.

[eff02] EFF Homepage, Electronic Frontier Foundation: *http://www.eff.org/*.

[jon02a] “The Router Audit Tool and Benchmark,” George M. Jones et al., Center for Internet Security: *http://www.cisecurity.org*.

[jon02b] “Network Security Requirements for Devices Implementing Internet Protocol,” George M. Jones, editor: *http://www.port111.com/docs/netsec-reqs.html*.

[lem01] “DDoS Attacks – One Year Later,” Robert Lemos: *http://zdnet.com.com/2100-11-527990.html?legacy=zdnn*.

[sec01] “Ntpd Remote Buffer Overflow Vulnerability,” SecurityFocus: *http://online.securityfocus.com/bid/2540/info/*.

[sta02] “How to 0wn the Internet in Your Spare Time,” Stuart Staniford, Vern Paxon, and Nicholas Weaver: *http://www.icir.org/vern/papers/cdc-usenix-sec02/*.

[yas01] “Latest Hacker Target: Routers,” Rutrell Yasin: *http://www.internetweek.com/story/INW20011217S0004*.

[yro02] “Your Rights Online,” Slashdot: *http://www.slashdot.org/yro/*.

Do You Know Where Your Routes Are?

Attacks on routing infrastructure (routers, routing protocols) have been a matter of great speculation for some time [ahm00, yas01]. Should they materialize, they could result in denial of service or misrouted traffic on a large scale. Does your intrusion detection system alert you when someone advertises a more specific route for your address blocks, or when someone logged in to your router, set up a tunnel, and policy routed all traffic for a single customer down the tunnel?

Sed Quis Custodiet Ipsos Custodes?

Juvenal asked, “But who watches the watchmen?” This is a question we need to ask again as we design and legislate confidentiality out of our systems. Networks provide aggregation points that are natural targets for those who would practice surveillance. See [eff02] and [yro02] for a list of current abuses and privacy threats mixed with some strong opinions and wild ravings.

Short-Term Solutions

What can you do *today* to improve the security of your network?

- Be vigilant. Be clued. The first and best line of defense for any network is network/security admins doing things like: staying on top of current vulnerabilities, being aware of current best practices and tools, implementing fixes as needed, watching logs, etc.
- Patch, patch, patch. Vendors routinely put out patched versions of code to fix newly discovered problems. Running old/unpatched code is inviting trouble. Check your vendor advisories.
- Harden network infrastructure using current best practices and tools. See the resources section for some suggestions.

Medium-Term Solutions

What can you do in “medium” term to improve the security of your network?

- Policy. You do have a policy even though you may not have written it down. Why does your network exist? Who can use it and for what? Who manages it? How are changes made? Having clear, documented answers to these questions backed by those in charge of the organization provides a foundation for all other standards, requirements, practices, etc.
- Standards and requirements. What features do you need to be able to implement your policy? Does your current infrastructure support them? Can you clearly communicate them to your vendors? Some areas to consider (addressed more fully by the author in [jon02b]) include:
    - device management
    - user interface
    - IP stack (RFC compliance, disable services/ports, DoS tracking, traffic monitoring/sampling, rate limiting . . .)
    - packet filtering
    - event logging
    - authentication, authorization, and accounting (AAA)
    - layer-2 issues (VLAN isolation).
- Industry participation. Work with others to define the important problems and generate solutions. This could range from policy and legislative work, to generat-

ing industry-wide consensus on required security features, helping to define standards and best practices, and developing tools to ensure their application.

Long-Term Solutions

What can be done in the long term to improve the security of your network?

- Cooperation and communication. Staniford et al. [sta02] suggest a network analog to the Center for Disease Control (CDC) for network issues. There have been some attempts to form such an organization (e.g., www.first.org). The big question is how to ensure participation.
- Consensus. Consensus must be achieved about what the "right" solutions are.
- Conformance. Vendors must be convinced to conform to the consensus solutions. The strongest incentive for conformance would be to have many customers making conformance a condition of purchase in contracts.
- Compliance certification. Once vendors are convinced and implement the requested features, there will be a need for testing and certification. It is likely that larger organizations will do this "in house," while smaller organizations will need to rely on some external testing entity.
- Coercion ("Send lawyers, guns, and money"). In the end (maybe sooner than we would think/like), we will have lawyers, legislators, insurance companies, and auditors telling us how to run and secure networks.

The Big Question

The big question, assuming this assessment of the problem is correct, is whether anything will be done before we have a major network outage. Can we, as a community, proactively address the issues raised here, or will it take a major disruption of services for "Network Security" to be recognized as an important priority? Time will tell.

Resources for Securing Cisco Routers

"Hardening Cisco Routers," Thomas Akin: *http://www.oreilly.com/catalog/hardcisco/.*

"Improving Security on Cisco Routers," Cisco Systems: *http://www.cisco.com/warp/public/707/21.html.*

"The Router Audit Tool and Benchmark," George M. Jones et al., Center for Internet Security: *http://www.cisecurity.org.*

"Securing Cisco Routers Step-by-Step," John Stewart and Joshua Wright: *http://www.sansstore.org* (forthcoming).

Rob Thomas' Security Articles, Rob Thomas: *http://www.cymru.com/~robt/Docs/Articles/* (articles/guides to securing IOS, JunOS, BGP, DoS tracking, etc.).

Thanks to the whole UUNET net-sec team (past and present) for feedback.