Crypto-Gram Newsletter

March 15, 2001

by Bruce Schneier
Founder and CTO
Counterpane Internet Security, Inc.
schneier@counterpane.com
<http://www.counterpane.com>

A free monthly newsletter providing summaries, analyses, insights, and commentaries on computer security and cryptography.

Back issues are available at <http://www.schneier.com/crypto-gram.html>. To subscribe or unsubscribe, see below.

Copyright (c) 2001 by Counterpane Internet Security, Inc.

In this issue:

- The Security Patch Treadmill
- Crypto-Gram Reprints
- Insurance and the Future of Network Security
- News
- Counterpane Internet Security News
- Harvard's "Uncrackable" Crypto
- TCP/IP Initial Sequence Number Flaw
- The Doghouse: iBallot.com
- The "Death" of IDS?
- 802.11 Security
- Comments from Readers

The Security Patch Treadmill

"Well, in our country," said Alice, panting a little,
"you'd generally get somewhere else -- if you ran very
fast for a long time, as we've been doing."
"A slow sort of country!" said the Queen. "Now here,
you see, it takes all the running you can do, to keep
in the same place."
--Through the Looking Glass, by Lewis Carroll.

Last week, the FBI announced that over the past year, several groups of Eastern European hackers had broken into at least 40 companies' Web sites, stolen credit card numbers, and in some cases tried to extort money from their victims. The network vulnerabilities exploited by these criminals were known, and patches that closed them were available -- but none of the companies had installed them. In January 2001, the Ramen worm targeted known vulnerabilities in several versions of Red Hat Linux. None of the thousands of infected systems had their patches up to date. In October 2000, Microsoft was molested by unknown hackers who wandered unchallenged through their network, accessing intellectual property, for weeks or months. According to reports, the attackers would not have been able to break in if Microsoft patches had been up to date. The series of high-profile credit card thefts in January 2000, including the CD Universe incident, were also the result of uninstalled patches. A patch issued eighteen months previously would have protected these companies.
What's going on here? Isn't anyone installing security patches anymore? Doesn't anyone care?

What's going on is that there are just too damn many patches. It's simply impossible to keep up. I get weekly summaries of new vulnerabilities and patches. One alert service listed 19 new patches in a variety of products in the first week of March 2001. That was an average week. Some of the listings affected my network, and many of them did not. Microsoft Outlook had over a dozen security patches in the year 2000. I don't know how the average user can possibly install them all; he'd never get anything else done.

Security professionals are quick to blame system administrators who don't install every patch. "They should have updated their systems; it's their own fault when they get hacked." This is beginning to feel a lot like blaming the victim. "He should have known not to walk down that deserted street; it's his own fault he was mugged." "She should never have dressed that provocatively; it's her own fault she was attacked." Perhaps such precautions should have been taken, but the real blame lies elsewhere.

Those who manage computer networks are people too, and people don't always do the smartest thing. They know they're supposed to install all patches. But sometimes they can't take critical systems off-line. Sometimes they don't have the staffing available to patch every system on their network. Sometimes applying a patch breaks something else on their network. I think it's time the industry realized that expecting the patch process to improve network security just doesn't work.

Security based on patches is inherently fragile. Any large network is going to have hundreds of vulnerabilities. If there's a vulnerability in your system, you can be attacked successfully and there's nothing you can do about it. Even if you manage to install every patch you know about, what about the vulnerabilities that haven't been patched yet? (That same alert service listed 10 new vulnerabilities for which there is no defense.) Or the vulnerabilities discovered but not reported yet? Or the ones still undiscovered?

Good security is resilient. It's resilient to user errors. It's resilient to network changes. And it's resilient to administrators not installing every patch. For the past two years I have been championing monitoring as a way to provide this resilient security. If there are enough motion sensors, electric eyes, and pressure plates in your house, you'll catch the burglar regardless of how he got in. If you are monitoring your network carefully enough, you'll catch a hacker regardless of what vulnerability he exploited to gain access. Monitoring makes a network less dependent on keeping patches up to date; it's a process that provides security even in the face of ever-present vulnerabilities, uninstalled patches, and imperfect products.

In a perfect world, systems would rarely need security patches. The few patches they did need would automatically download, be easy to install, and always work. But we don't live in a perfect world. Network administrators are busy people, and networks are constantly changing. Vigilant monitoring does not "solve" computer security, but it is a much more realistic way of providing resilient security.

The Ramen worm:
<http://www.securityfocus.com/archive/75/156624>

Security patches aren't being applied:

Best quote: "Failing to responsibly patch computers led to 99 percent of the 5,823 Web site defacements last year, up 56 percent from the 3,746 Web sites defaced in 1999, according to security group Attrition.org." I'm not sure how they know, but is scary nonetheless.

The Eastern European credit card hackers:
<http://www.sans.org/newlook/alerts/NTE-bank.htm>
<http://www.nipc.gov/warnings/advisories/2001/01-003.htm>
<http://www.fbi.gov/pressrel/pressrele01/...>
<http://www.zdnet.co.uk/news/2001/9/ns-21473.html> [link moved to http://news.zdnet.co.uk/story/0, s2084921,00.html]

Many networks have not patched BIND after January's vulnerabilities were patched:
<http://www.computerworld.com/cwi/stories/>

The Microsoft attack:
<http://www.schneier.com/crypto-gram-0011.html#7>

Patch your apps: