COMPUTER SECURITY ALERT

THE NEWSLETTER FOR INFORMATION PROTECTION PROFESSIONALS

*We're going at OS development completely backwards – see page 3*

August 2002

COMPUTER SECURITY INSTITUTE
600 HARRISON STREET
SAN FRANCISCO
CALIFORNIA 94107
TEL: (415) 947-6320

# INSIDE INFORMATION



# Hat-Hackers Show New Attacks

**by Rik Farrow**

*Black Hat Briefings runs alongside DefCon in Las Vegas each year. Put together by Jeff Moss, aka "Dark Tangent", the latest Briefing was held late this past July*

As you read this account of Black Hat 2002, remember that most of the speakers are security consultants who are presenting their research about weaknesses found in current software and hardware products--including Open Source.

It's quite easy to get upset about some of what you are about to read. But the purpose behind the talks is to improve security by revealing where it is weak today.

Richard Clarke, the administration's computer security advisor, led off the program. Clarke has come a long way in his understanding of the real issues behind computer and network security weaknesses since a speech that I heard in December 2001. But this time, he described software vendors as irresponsible for delivering such buggy software, and called for protection of hackers who discover and responsibly disclose security problems in software. Clarke said that software makers must provide patches that are both easy to install and that have already been tested for compatibility with the major applications used on most computers.

Clarke also stated that operating systems should be shipped with network services disabled by default, so that they can be enabled only when the user or system administrator needs those services. This statement got Clarke a round of applause.

## Fuzzing and decompiling

I had looked forward to hearing Halvar Flake's presentation on the use of graphs to aid in binary analysis. Flake's specialty is reverse engineering--the decompilation of programs with the goal of understanding their flow and purpose. When the source code to a program is not available, security researchers have used two techniques while searching for security bugs: fuzzing (or stress testing) and decompiling code. Fuzzing has a problem in that it is impossible to know if all possible code paths have been tested. Decompilation, on the other hand, is just plain difficult to do.

Flake described a set of tools he developed that work with a commercial product (IDA) to provide flow diagrams to programs being reverse engineered. IDA comes with a graphing tool, but Flake determined that the tool would not work well for his own purposes, so he wrote a better one. Flake's tool allows the programmer to collapse parts of the flow tree once they have been tested, for example. Another version marks the paths taken through code with color, showing if all possible paths have been reached yet. Such tools show great promise in testing commercial code for undiscovered problems. While reverse engineering is not required for Open Source software, Flake's graphing techniques, such as following variables through a program and marking program branches as tested, could be useful there as well.

While Flake was presenting, Roelof Temmingh and Haroon Meer, both of Sensepost (sensepost.com) described a new Trojan that uses Internet Explorer to run an HTTP

*continued on page 8*

tunnel designed to penetrate firewalls with an outgoing connection, and avoid IDS as well. Later that day, I caught part of Maximiliano Caceres (CORE, corest.com) presentation on a replacement for the shellcode 'traditionally' used in remote attacks on UNIX and Linux systems. Instead of actually attempting to invoke /bin/sh, the UNIX shell, Caceres described a technique for proxying system calls, so that the attacker runs commands on the remote system that actually get carried out, via system calls, on the local (victim) system. Quite a clever (and scary) concept, the current version requires that both the attacking and victim OS be the same version.

I next listened to Mike Schiffman describe a new library he had written. Schiffman, once known as Daemon9, and now an @stake employee, had previously written the first widely used SYN flood tool, firewalk, and later libnet, a tool used for writing other security and attack tools aimed at TCP/IP networks. His new library, libradiate, helps C programmers build 802.11b (WiFi) packets. During the talk, Schiffman demonstrated a tool named Omerta, that disassociates current sessions with a wireless access point. Black Hat had four different access points set up, and once Schiffman determined the channel used for his lecture hall, he ran Omerta. Audience members quickly acknowledged that they had been knocked off the wireless network. He did not share the source code for Omerta, something that had some attendees miffed--but probably a good thing. I also spent some time listening to Dan Veeneman, an expert in wireless networks (including not only wireless, but cellular and satellite networks as well).

### Snorting hogwash

After Flake's presentation, Jed Haile, one of the Snort (snort.org) developers, was my second favorite of the day. Haile had been working on turning snort, the Open Source IDS, into a tool that could do more than monitor networks looking for attacks. Hogwash uses snort, but instead of merely sending alerts, Hogwash can drop packets, or even alter packet contents. If this sounds a lot like an application gateway-based firewall to you, you would be close. Hogwash does work with ipfilter, the Linux firewall software, but is not intended to act as an organization's firewall. Instead, Hogwash sits inline on a network to remove or modify packets that represent part of an attack. Hogwash will be used with the second generation of the Honeynet Project.

The Black Hat organizers really set up an aggressive schedule, starting at 8 am each day and ending at 6 in the evening. As if that were not enough, Hacker Court was scheduled during the reception. Hacker Court is the invention of a group of security consultants, including Carole Fennell, Brian Martin, and Jon Klein, designed to demonstrate to an audience some of how different a court and jury appears to the world of technical experts. Essentially, while evidence submitted to Black Hat or USENIX audiences can be expected to stand on its own merits, the same evidence would be totally inappropriate, and likely ineffective, when presented to a judge and jury. The goal becomes translating dry, technical facts into something that a jury can understand and believe.

Making the court even more realistic, two law enforcement officers, Don Cavender (FBI) and Jesse Kornblum (Air Force OSI) presented the government's evidence, and Richard Salgado, Trial Attorney for the US Department of Justices Computer Crime and Intellectual Property Section, handled the prosecution. The actual evidence was manufactured by Jon Klein, but modeled on an actual case. The defense team included Jennifer Granick, Litigation Director of the Public Interest Law and Technology Director at Stanford, and someone who has actually defended people charged with computer crimes.

While the demonstration was intended to be serious, it was also very entertaining. Richard Thieme (thiemeworks.com) gave a hilarious impromptu performance as the owner of the victim company, RATCO. The jury, mostly members of the press, were permitted to leave at any time, and to drink while "in the box". Cavender, with a straight face, described portions of an IRC (Internet Relay Chat) log used in evidence, including interpretations of the various smiley faces. The defense pointed out that the same logs showed that an enemy of the defendant (Brian Wilson) was actually a much more likely suspect. In the end, Wilson was acquitted of two charges, but convicted of a third charge, having password cracking software on his home system.

I missed the beginning of the second morning's presentation. After the parties the previous night, 8am is just too early to get started. And I did spend a lot of time talking to people in the halls outside of the lectures. I missed hearing about SPIKE, a fuzzing tool written by Dave Aitel (immunitysec.com). I did listen to Nicolas Fischback and Sebastien Lacoste-Seris discuss threats to IP backbone security. Some threats, such as the lack of real security to BGP4, were familiar. The discussion of MPLS, a protocol used to create virtual circuits over IP networks, was new to me, but the advice (use IPsec for encryption of data over MPLS) was excellent.

After lunch, I listened to a fired up Lance Spitzer (sun.com) talk about the Honeynet Project (project.honeynet.org). Spitzer described the version 1 Honeynets, then went on to explain how version 2 will be better. Part of the improvement will be the use of Hogwash, instead of a blocking firewall, to prevent an attacker who has broken into a honeynet system from successfully attacking other systems. Another innovation is a new, covert, logging channel. The logging channel actually was based on a rootkit, and sends packets with forged headers to a silently sniffing IDS system for logging.

I had missed listening to FX and Kimo of Phenoelit (phenoelit.de), as their talk conflicted with the Honeynet Project. I met up with FX and Kimo later at DefCon, and found out what I had missed. FX explained how to exploit Cisco routers and HP printers. Of the two, the audience was most enthralled with the HP printer attack, that sends a Java program to a networked HP printer, that, in turn, begins scanning the local network. But for me, the attack against Cisco routers was much more interesting. FX carefully explained

*continued on page 6*

*continued from page 8*

how they had gone about designing their example attacks without reverse engineering Cisco's IOS. Instead, they used debugging error messages and public documents on the Cisco Web site to create heap overflow attacks that could be used to completely subvert Cisco 1500, 1600, and 2600 series routers remotely, and 2500 series routers locally. It is likely that similar attacks would work against high end Cisco routers and switches as well. Cisco, who has known about similar issues for some time, needs to replace IOS, an aged, embedded OS, with a newer operating system.

There was a lot more, including Rain Forest Puppy explaining new attacks on Novell Netware, Ofir Arkin (atstake.com) on VoIP attacks, Thomas Akin (crossrealm.com) on Cisco router forensics, and David Litchfield (ngssoftware.com) on Microsoft SQL Server bugs. Perhaps appropriately for the last talk of the day, someone asked Litchfield, perhaps best known recently for exposing 26 Oracle vulnerabilities in February 2002, what the next big target will be. Litchfield paused, thoughtfully staring into space, then said, "LDAP and Active Directory". No one doubts that there will be more Microsoft vulnerabilities, more UNIX/Linux vulnerabilities, so almost anything could have been said at this point--but it does make me wonder.

***they used debugging error messages and public documents on the Cisco web site to create heap overflow attacks.***

The next morning, I checked in at DefCon 10. Where Black Hat includes a nice lunch every day, the Alexis Hotel sells slices of pizza and bottles of water or beer for lunch. Two of the lecture "halls" are in tents, and the roar of the air conditioning made it difficult to hear speakers. I did listen to Ofir Arkin's talk about his next scanning tool (Xprobe v2), being very glad that he was mostly reading his slides. But at DefCon, the real conference is not in the lecture rooms, but wandering the grounds, meeting and talking with some of the thousands of people there. Like the first DefCon I ever attended (DefCon 1), there were still phone phreaks there but they are now using wireless technology. DefCon can best be described as a self-organizing anarchy, but the Black Hat organization runs this conference as well as anyone could manage to herd cats--or thousands of hackers and hangers on.

If you can't afford Black Hat, you can hear similar lectures (under appropriate circumstances, like a seat near the speakers) at DefCon, as well as being entertained by the attendees. Not for the weak at heart, and not for me either, as I had to turn around and head off to the USENIX Security Symposium, and a much more sedate crowd.

*Rik Farrow is a security consultant and CSI's technical editor. Reach him at rik@spirit.com*

## DC INSIDER

# Beltway insecurity

**by Michael J. Zuckerman**

Suddenly, cyber security is a big deal here in the Nation's Capital.

After years of getting short shrift–alternately derided as hyperbole or lost in the media's insatiable love-hate relationship with hackers–"Cyber" is being taken seriously as a component of Homeland Security. This could be a very good thing or a very bad thing. To know for sure will require a break in the current news cycle. The annual Congressional August recess should take care of that, enabling cooler heads and clearer thinking to prevail when the federal government goes back to work after Labor Day.

I know, the rest of the nation views the Beltway crowd as too greedy, self-involved or just plain dumb to "get it" when complex issues are at stake. And I'm not challenging any time-tested notions about our government. However, in my experience, their shortcomings have as much to do with inertia (Physics 101: "A body at rest will stay at rest until acted upon by an outside force") as anything else. They just need that "outside force" to get them into action.

On Thursday, June 27 The *Washington Post*, with revelatory gusto, discovered cyber security in a 3,200-word story that began atop the front page. The story reported some recent developments, but covered familiar ground about known threats and vulnerabilities. By Friday and on into the weekend the network news programs followed the story and kept it percolating into the long July 4th holiday.

By the time Congress got back, the buzz was making cyber security part of Homeland Security.

Nowhere in the president's proposal to create a Department of Homeland Security is there a single reference to cyberspace or responding to terrorist attacks that might originate on the Internet.

By contrast, the plan devotes a section to "chemical, biological, radiological or nuclear" threats and envisions one of five "Under Secretaries" to head the Chem-Bio, Rad, Nuke section or agency. Yet nowhere in the $37.7 billion plan does Cyber get so much as an Ass'Sect. IT "trade groups" rose in protest over this slight, demanding a Homeland bureaucrat to represent their interests.

Members of Congress and the administration offered assurances that cyber security would not be overlooked. But this is an election year. And complex, sensitive issues have a way of getting more complicated by the vagaries and local interests of politicians. What right-thinking pol concerned by local lay-offs resulting from a troubled economy and corporate corruption, is going to green light a plan for a new Department of Homeland Security that will gobble up 22 existing agencies, move people around, take away jobs and generally change things just as an election is on the horizon?