;login:

THE MAGAZINE OF USENIX & SAGE

October 2002 volume 27 • number 5

inside:

SECURITY

USENIX & SAGE

The Advanced Computing Systems Association &
The System Administrators Guild

musings,

Or What I Did on My Summer Vacation

by Rik Farrow

Rik Farrow provides UNIX and Internet security consulting and training. He is the author of *UNIX System Security* and *System Administrator's Guide to System V*.

rik@spirit.com

I once imagined that I would like to spend my life attending conferences. Instead, I am feeling glad to be home, although I am also glad I did get to hang out in a couple of security conferences. And, rather than making you have to drive, ride, or fly, I will share with you parts of my experiences, and something that I think you may find very frightening.

I loathe Las Vegas. Gambling does not appeal to me, so having to walk through three casinos to reach the registration desk at Caesars Palace had me seething inside. I remembered (just in time!) that I am enlightened and cheered up enough to survive the 20-minute check-in line, then another 20-minute wait for the elevator (you'd think this was Eastern Europe, not an expensive hotel), all to attend Black Hat 2002.

The Black Hat conference is designed for security consultants, although I did see DoD types and even some faces from USENIX conferences there. The format consists of three tracks, with intermediate to moderately advanced talks about the security of software and hardware. At the low end, some guys from iDefense gave a lecture about cookies (I liked Kevin Fu's invited talk at last year's Security Symposium better). I enjoyed the explanation of Hogwash and how it had been integrated into Snort codebase as of version 9.2. And how the Honeynet Project plans to proceed with their version 2 honeynets.

Daemon9, now better known as Mark Schiffman of @stake, described his new library, libradiate, which adds to libnet (low-level networking functions for crafting/reading packet headers) with the headers necessary for 802.11B (WiFi). Schiffman demonstrated Omerta, a program that sniffs a wireless channel and disassociates any network card currently associated with an access point. He did not share the source code, a disappointment to many. He did provide other C code examples, but a show of hands revealed that there were only three C coders in the audience. Rather disappointing for a technical con.

While Schiffman rushed through his code examples, FX and Kimo, of Phenoelit (*http://www.phenoelit.de*), were explaining how to turn HP printers into port scanners, using Java code and a class loader included in networked HP printers. The audience found this very amusing (printers scanning a network!), but someone later pointed out to me that HP network printers already will scan networks looking for print servers. What I had missed was their discussion of heap buffer overflows of low-end Cisco routers. Their exploit invalidates the stored configuration and forces a reboot, at which point the router, realizing its configuration is hosed, begins broadcasting a request for a new configuration from anyone. IOS 12 and Cisco 1000, 1600, and 2600 routers are vulnerable to remote attacks, and the 2500 series to local attacks only.

Remember that I mentioned rumors about exploits to IOS in an earlier column. FX made certain that I (and Cisco) understood that they had not done any reverse engineering, just opened the router, recognized that it used a Motorola 68K processor, and used debug messages and information on the Cisco Web site to create their exploit. FX told me that he did not want to be this year's Sklyarov (the Russian arrested at DefCon 9 for explaining how to defeat Adobe's pitiful encryption in eBooks). I really wish that Cisco had succeeded in rewriting IOS as a modern embedded OS instead of abandoning the effort (as far as I have been able to find out).

Hacking has nothing to do with breaking into other people's computers, and everything to do with understanding how things work.

I ran into FX at the next conference I visited, DefCon. DefCon was a bit more subdued this year when compared to previous years, I've been told. I had just enough time to hang out the night before and the first half-day, long enough to get a feel for things and not really missing out on what I hadn't liked about the first DefCon – drunken, chain-smoking teenagers. Keep in mind that DefCon is a serious security conference, with a very low entry fee ($75). Many speakers from Black Hat also speak at DefCon but give a more technical version of their talks.

I listened to Ofir Arkin present the revised version of Xprobe, which does away with the tree structure for probes and instead focuses on a list of probe modules. The modular structure makes Xprobe easier to extend, but it also loses one of the benefits of the original tool, which was accurate TCP/IP fingerprinting with two or three packets. Being an "older guy" who has lost enough hearing (probably from loud concerts in the sixties) was a real disadvantage at DefCon, as two of the conference rooms were outdoor tents, and the roaring of the AC units attempting to keep the temperature at reasonable levels drowned out some of what the speakers said, as well as most questions.

I am sorry I missed Jennifer Granick's talk on the implications of the PATRIOT Act (and yes, it is an acronym) for security practitioners, Simple Nomad's (*http://www.nmrc.org*) talk about the Hacker Nation and how the "War on Terrorism" affects hacking in general, the two lock-picking sessions, and Richard Thieme's (*http://www.thiemeworks.com*) closing session, reminding the audience that hacking is a form of truth seeking.

Lest this last statement confuse you, remember that hacking has nothing to do with breaking into other people's computers and everything to do with understanding how things work – even if it means taking them apart first. My next trip (and why I left DefCon early) took me to San Francisco for the USENIX Security Symposium. The December issue of *;login:* will include the summaries from this conference, as well as other articles dedicated to security, and will be a great edition. I know, as I am the editor and already have some of the articles in hand.

But I don't want to make you wait quite that long. This year's symposium was great, lots of good papers and ITs, and the hall talk was great as well. Professor Felton spoke about the "Freedom to Tinker," another way of saying that reverse engineering of code is akin to US First Amendment rights. Tinkering with things is not only common (would you buy a car where the hood was sealed?) but is good for the community and economically beneficial. Tinkerers have discovered security mistakes in code, and their activities often result in better, competing products (see *http://www.freedom-to-tinker.com/*).

One hall debate led right into a special evening talk about Palladium and TCPA (Trusted Computing Platform Alliance). Tom Perrine, of San Diego Supercomputing Center, asked, rhetorically, why software was so insecure. His argument: that better and more formal design processes would make a huge difference, even when using the insecure programming languages common today (C and Perl as examples). I piped up with my common assertion that you cannot compel people to use formal design processes, but you might instead provide them with safer tools to use – that is, instead of C, using programming languages that enforce good practices, and make it close to impossible to create buffer and heap overflows or to write code that does not check user input, etc. And that this must be implemented on top of a secure operating system that can run untrusted applications in their own compartments. No one agreed

with me, although Perrine did muse about the virtues of ADA, a programming language developed by the DoD for portability and security, and KSOS, an operating system with a trusted kernel.

The EFF's Lucky Green moderated a panel discussion with Peter Biddle of Microsoft and Seth Schoen of the EFF about Palladium. Palladium is Microsoft's project for developing software and hardware for a trusted kernel (see *http://vitanuova.loyalty.org/2002-07-05.html*, under the Microsoft heading, for details). You might think that I would be happy that *someone* is thinking about hardware support in PCs for running a trusted kernel, but the Microsoft focus is of course not the same as an open source focus for security. You should read Ross Anderson's TCPA FAQ for a very detailed critique (*http://www.cl.cam.ac.uk/%7Erja14/tcpa-faq.html*). But I will give you the nutshell here.

Biddle explained how Microsoft's Palladium will work to provide a trusted operating system. Briefly, after booting the trusted kernel, special hardware calculates a hash of this trusted kernel. Then the regular operating system continues with the boot process. The trusted kernel – officially the Trusted Operating Root (TOR), unofficially the "nub" – provides a limited set of services to the operating system and other applications, particularly the ability to seal and unseal "blobs" – any set of data, be it a program, a text file, or a DVD image. The TOR relies on a bit of hardware, a secure cryptographic coprocessor (SCC or SCP) that can perform asymmetric encryption (used in digital signatures) and symmetric encryption (AES in CBC mode), and support a secure store for keys. The SCP also controls memory management, protecting certain regions of memory so that even a root user or the operating system itself cannot access protected memory. At this point, it sounds like there exists the basis for the trusted kernel and compartments that I have long advocated.

But the plan for these wonderful security features is quite different. Instead of protecting the security of your system from attacks, Palladium protects rights of copyright owners. To quote Anderson:

> TCPA and Palladium do not so much provide security for the user as for the PC vendor, the software supplier, and the content industry. They do not add value for the user, but destroy it. They constrain what you can do with your PC in order to enable application and service vendors to extract more money from you. This is the classic definition of an exploitative cartel – an industry agreement that changes the terms of trade so as to diminish consumer surplus.

To provide a few examples of how Palladium and TCPA work to enforce Digital Rights Management (DRM), imagine a system where you cannot migrate files from, say, Microsoft Office 2003 to any other software package. The TOR will not allow you to decrypt the file for the purpose of exporting it to, say, StarOffice. Organizations can configure applications so that data can never be shared, or so that files automatically and irrevocably delete themselves after some time period. No whistle-blowers "leaking" information, no email records detailing dirty deeds, and no more unlicensed copies of Microsoft software, as you *must* have a valid license to run – one that is keyed to your hardware platform using the SCP and the TOR. For the people controlling digital rights, this will be a windfall, as they control how many times you can play a DVD, prevent you from copying it (even by screen scraping), or can even charge you each time you open an application.

Instead of protecting the security of your system from attacks, Palladium protects rights of copyright owners.

We must choose between freedom (with its responsibilities) or passing over control of our computers and aspects of our lives to large corporations.

Microsoft and Intel claim that these new initiatives, once completed, will make your PC more secure, even prevent spam. But, instead of making your own computer more trustworthy for your own use, it will make it trustworthy for the use of content and application providers. Viruses will not be able to affect the TOR or Trusted Agents protected by the TOR, but they will still be able to write to files, delete files, send email – in fact, do almost everything they do today. The only exception will be those files and devices protected by the TOR (which in Palladium includes the keyboard, so no more keystroke sniffers).

Too bad these are DRM initiatives, not real security initiatives. Lucky Green pointed out to me, as does Dar Williams in his July 5 journal entry, that Intel and Microsoft felt they had no choice but to create an unbreakable system for DRM. If they failed to do so, the home entertainment system of the future might not use Intel hardware and Microsoft software. But the very success of these schemes gives each company tremendous leverage, far beyond the virtual monopolies each enjoys today.

You will still be able to run your favorite operating system on Palladium and TCPA-enabled systems. In fact, there were people at the Symposium with IBM T30 laptops that incorporate a TCPA chip. You just won't be able to use any of the features that require the chip, as these make use of a TOR and trusted hardware: for example, an encrypted link to your monitor, DVD-ROM, keyboard, etc.

The RIAA and MPA argue that flagrant copyright violations are destroying their businesses and hurting artists. Perhaps the former might one day be true, but the latter rarely is. Record companies lend money to bands, and it is unusual for the artists that provide the content for RIAA members to make a living as musicians. But providing free digital downloads can help promote artists (read about Janis Ian's experiences as a recording artist and musician, and how free downloads have helped her and Mercedes Lackey, *http://www.janisian.com/article-internet_debacle.html*).

The TCPA chip has been coined the "Fritz" chip, after Senator Fritz Hollings, who has sponsored a law that would make the selling of any computer or storage device that does not support TCPA illegal in the US (*http://www.salon.com/tech/feature/2002/03/29/hollings_bill/*).

The sky is not falling. We find ourselves at a crossroads where we must choose between freedom (with its responsibilities) or passing over control of our computers and aspects of our lives to large corporations. I believe the decision is clear, but I know my mother, as well as many of my friends, doesn't understand the issues (yet). Make yourself heard, ask for real security, and don't give up your freedom.