;login:

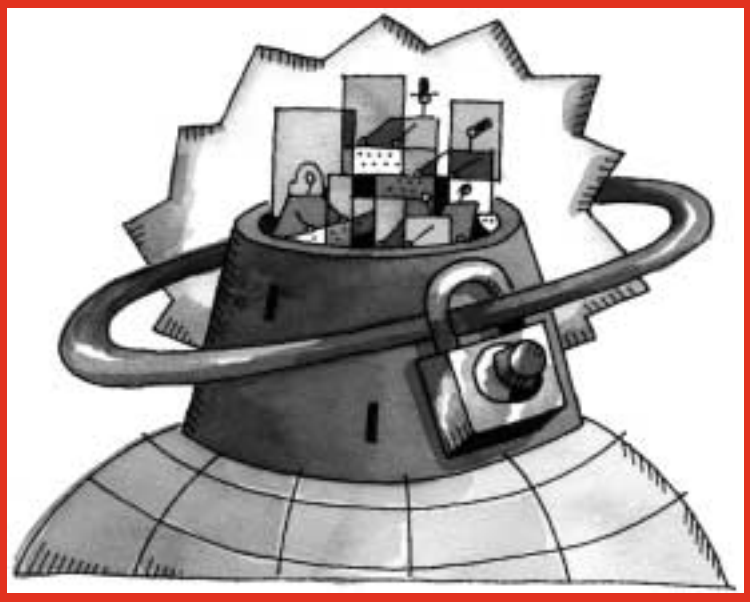
THE MAGAZINE OF USENIX & SAGE

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

secure from what?

by Peter H. Salus

Peter H. Salus is a member of the ACM, the Early English Text Society, and the Trollope Society, and is a life member of the American Oriental Society. He is Chief Knowledge Officer at Matrix NetSystems. He owns neither a dog nor a cat.

peter@matrix.net

The 11th Security Symposium took place in the San Francisco Marriott, August 5–9. I was struck by several things: how much interest there was in the concept of "security," and how little that concept had changed since 1988, when I attended the First Security Workshop in Portland, Oregon.

The keynote this year was by Whitfield Diffie, the co-inventor of the Diffie-Hellman protocol for public key cryptography a quarter-century ago. Whit posed the question, "What is security?" and responded that it was "prevention of adverse consequences from illegitimate acts of human beings." Not bad. But it struck me, as it has before, that we spend too much time considering intrusions and break-ins, on encryption, passwords, and firewalls.

Back in 1998, Bill Cheswick gave a wonderful talk at SANE in Maastricht, involving castles with moats, the Great Wall of China, siege warfare, and sneak attacks.

Nowadays, tens of thousands of enterprises depend on the Internet. They are as vulnerable to cutting off that service as ancient and medieval cities were to sieges. Preventing access to their customers and suppliers would be as disastrous to the modern corporation as lack of access to food and water was to the besieged. And this is exactly what SYN floods and DDoS attacks do: they render Internet communication impossible to the besieged.

Diffie pointed out that the goal of security is not retaliation, but denial of success. Thus, preventing others from obtaining secrets is important. Losing secret information is a vulnerability. But so is the inability to use information. The proliferation of the Internet, Diffie pointed out, leads to increasing power, increasing digitization, and a need for security remote from the individual.

There was much more in Diffie's keynote, and there was a lot of food for thought. Which may be yet more important.

The Plan 9 guys gave a great paper on security in Plan 9 resulting from constraints on privileged execution of server processes through "factotum." If you weren't in SF, read the paper.

I then toddled off to hear Ed Felten of Princeton speak on the "Freedom to Tinker," the law's impact on technologies being of increasing concern. Felten understands the freedom to tinker as vital to our ability to understand, discuss, repair, and modify the technological devices that we own.

When I was a kid, I liked to take things apart: an alarm clock, a toaster, etc. I'll bet most of us did. Taking things apart (and, as time went on, putting them back together) brought about understanding. I'm willing to state that my ability to explore and understand has, over time, benefited others, too.

Felten made the point that "Tinkering is socially important." He's right.

On Thursday, I went to listen to Stuart Staniford, Vern Paxson, and Nicholas Weaver talk about the ways that script kiddies wreak mischief. While valuable, I found the most important point of the paper buried at the end: while he has advocated it in the past, Paxson makes an increasingly salient point in advocating a sort of CDC for cyberspace, an organization whose mission is to track and monitor various forms of cyber-disease and attack.

With the attention being paid to "homeland security" these days, $10 to $25 million a year to map, track, dissect, and analyze the matrix seems almost trivial.

Paul Kocher's "Illusions of Security" had a number of good points embedded in it: security does not equal functionality; "Most commercial products have negligible probability of being very secure against creative attackers"; "There are too many people designing secure systems who have never broken one" (refer to Felten's right to tinker); and "There is a shrinking ratio of engineers to problems."

On Friday morning, I listened to Pam Samuelson's excellent presentation on the DMCA. Again, Felten came to mind. While Jack Valenti and the TV/video, music, and film industries may have a lot of money, they're wrong-headed. Preventing reverse-engineering is like passing a law against taking apart an alarm clock.

I keep having this bizarre ahistorical fantasy in which Petrarch sues Chaucer and Milton and Shakespeare for "reverse-engineering" the sonnet.

Lots of things to think about, hence a fine conference.