the network police blotter

by Marcus J. Ranum
<mjr@nfr.net>

Marcus J. Ranum is CTO of Network Flight Recorder, Inc. He's the author of several security products and of a book on computer security (with Dan Geer and Avi Rubin) and is a part-time sysadmin.

Some More Results

My contest on "Where do packets go when they die?" was a complete failure. I got only one response, which means that my concept was clearly unfunny and uninteresting. After the spectacular success of the Haiku contest, I think I'll be hard-pressed to come up with another exciting avenue for you to show off your creative juices, but check the end of the column for details. By next issue's column I hope I'll have some printable results from the "dirty tricks" contest.

Enough Waffling, Already

For the last year I've been dancing around a set of issues that have really been bugging me: the social problems behind computer security. These have to do with media attitudes, corporate attitudes, and, most important, the attitudes of security professionals. All the pieces of the jigsaw puzzle finally clicked into place for me a couple of months ago and, as a result, I've been taking a much less forgiving position on a number of issues, primarily those related to how security bugs are discussed and how security professionals share information. Now I'm officially throwing my hat in the ring as a hard-liner on professional ethics for security practitioners — and I'm going to urge you to join me in saying "enough is enough."

A few weeks ago, I had the honor of giving a keynote talk at The Internet Security Conference (TISC) in San Jose. As usual, I wrote my presentation the night before, and allowed my talk to follow the outline of my viewgraphs, while accreting free-associated thoughts on the way. The results were unexpectedly strong, amounting to a prediction that eventually we security professionals (backed by civil litigators and law enforcement) will declare unrestricted war on hackers. I've made an MP3 version of the talk available on my USENIX Web page <*http://pubweb.nfr.net/~mjr/usenix/index.shtml*> for those of you interested in the talk. So, now I'm officially out on a limb, and I'm looking forward with distaste to the usual mature high-level debate I have come to expect from the hacker community: overflowing email boxes, Web site denial of service, problems with phone bills and my voicemail.

The Three Phases of Internet Security

In the first phase of Internet Security, we pretty much ignored the problem. This era was typified by an "It's OK, it's just fun-loving hijinks and curiosity" attitude. Back in the first phase, we had things like the gnu.ai.mit.edu server, which provided what amounted to anonymous shell accounts to the Internet at large. Not surprisingly, a lot of hostile network activity originated from that site. But in those days "dotcom" madness had not yet set in, the Internet was not yet a gold rush, and the only people who were suffering were relatively unimportant: system administrators and network managers. The attitude of the day was playful fun-loving curiosity and willingness to forgive.

In the second phase of Internet Security, we built firewalls, vulnerability-assessment tools, and intrusion-detection systems. We're still there today. This phase began in the mid to late 1980s and peaked in the early "dotcom" madness of 1992—1994, when everyone finally started installing firewalls. Network and system administrators had to become like urban homeowners: constantly checking on the state of their locks, burglar alarms, and barred windows. Today's attitude is typified by a mentality of hunkering down behind walls and defenses and hoping the bad guys will go away.

In the third phase of Internet Security, we will lash out in anger, seeking retribution. The firewalls will be supplemented with tort lawyers, and the intrusion-detection systems will become sources of evidence. I think we'll be there within a year, and it'll peak in five years. Law enforcement's efforts will fall by the wayside as people realize that they can hurt their tormentors much faster and more effectively by suing them for damages than by trying to put them in prison. Ever see *The Omega Man*? The attitude of the future will be typified by a mentality of hunkering down behind a wall with a loaded sniper rifle and the phone number of a good ambulance chaser on your speed dialer.

I'm not sure the third phase will be particularly fun, but having lived through the first two, I don't think it's going to be a whole lot worse. It might even be better, since a lot of the casual script kiddies will dry up and blow away, leaving us with only the cadre of dedicated troublemakers to deal with. Fear of litigation will also cause a lot of sites to tighten up their acts. I'm glad I'm not the system administrator at a university or anyplace with deep-pocket financing and a large body of uncontrolled and unmonitored users.

The kind of draconian monitoring requirements that lawyers will start recommending could get really ugly. The downstream-liability lawsuits you'll face if you can't deflect liability onto your users will be uglier. Other folks who are going to have problems with downstream-liability lawsuits are all those sites that distribute security exploits and hacking tools, or teach hacking techniques. Look at the kind of troubles publishers who sell "mayhem manuals" have had, multiply that by a few thousand, and that should give a rough approximation of the magnitude of pain that may be felt.

I'm a big fan of the various low-numbered amendments to the constitution, especially the first. Censorship's a bad idea. However, we've shown time and again that as a society we are willing to apply the screws to people who use their freedom of speech irresponsibly. And I'm now of the opinion that the hackers have garnered themselves enough negative attention that they're about to be on the receiving end of a little good-natured crushing. Too bad it's come to this, but I'm going to save my sympathy for someone who deserves it.

Ethics for Security Professionals

A distressingly large number of security professionals have come up through the ranks by starting as "black hat" hackers who have subsequently "gone legit." I used to believe that this happened because they saw the error of their ways and changed sides in an attempt to help improve the situation — to be part of the solution rather than the problem. Now, however, I'm convinced that the main reason they're doing so is because they've realized that they can make a ton of money, disclaim responsibility for their actions, and continue to do pretty much the same kinds of things they were doing before.

"Ethical Hacking" has been widely marketed as an essential tool in information security. Former "black hats" in several cases have managed to parlay their old collections of attack tools into millions (and even tens of millions) of dollars. Hackers whose claim to fame is a criminal record for cyber-crime can make six figures as "Ethical Hackers" working for audit firms. At the same time, their buddies are releasing a veritable flood of new tools designed to exploit vulnerabilities in commercial products, ostensibly to "illustrate the seriousness of the problem" or to "promote vendors taking security seriously." Some individuals who work as engineers for security companies spend their free time writing and distributing the very attack tools their corporate masters sell you products to protect against. Conferences like Interop, SANS, and TISC are offering classes in "how to hack" that basically train analysts in how to assess and exploit vulnerabilities in systems and networks. They know better, but the classes are sold-out successes and the money's too good to refuse.

I don't know about you, but I'm thinking this is one highly messed-up situation.

I'm not a believer in standards bodies, but I think someone needs to propose a standard of ethics for security practitioners. I'll give it a shot:

1. If I have been involved in cyber-crimes in the past, I have renounced and will denounce such activities in the future.
2. If I know individuals or groups who are involved in cyber-crimes, I will not encourage them, share information with them, or in any way aid or abet their activities.
3. I will never produce or distribute attack tools or tools designed to evade or bypass security systems.[1]
4. I will never teach others how to compromise system security; rather, I shall strive to teach them how to defend systems against compromise.

5. I will never publish designs for new attacks or new attack tools, nor will I speculate about potential vulnerabilities in future or existing systems except in the context of offering ways to prevent them.
6. If I discover a vulnerability, I will work with the author or vendor in a responsible manner to ensure that it is fixed with minimal impact on the user community. If the vendor does not act responsibly in addressing the vulnerability, I will use appropriate channels to inform the user community of the presence of the vulnerability but will not provide exploitable information except to the vendor and responsible parties.
7. If I develop security-critical software I will, at all times, be prompt in responding to or fixing vulnerabilities found in my software.
8. I will not employ individuals I believe might be cyber-criminals or ex—cyber-criminals unless I am certain that they are adhering strictly to this standard of ethics.

I welcome comments on the thoughts above! If you're in the security business, and you agree with me, please share them with others.

My belief is that if the security community doesn't clean up its act, a flurry of lawsuits will. Maybe that's wishful thinking. But I know that if I were so unwise as to develop and release an attack tool, the last thing on earth I'd do is sign my handiwork as many tool-writers do, especially not the denial-of-service tools. Guys, you're painting targets on your backs that could attract years of lawsuits downstream. At the very least, they might someday cost you a job.[2]

If I ran a security conference, the last thing I'd teach attendees is how to hack people's sites. Conferences have deep pockets. I know that if I were running a security-related Web site (actually, I do . . .) the last thing I'd do is redistribute attack tools and exploit information. Not only is that a huge disservice to the community, but I bet any lawyer you told about it would faint. You don't have a lawyer yet? Don't worry, you will.

U Help Me I Lame

Since I authored the original Internet firewalls FAQ and have posted a lot of security-related messages in the last 13+ years, I get emails about once a week from people asking for help in compromising the security of this, that, or the other. The one below is a real sample I got recently:

```
From: [Deleted]@hotmail.com
To: mjr@nfr.net
Subject: hello sir ! ! ! ! ! !
dear sir,

I have read u r "article" at http://www.hackingexposed.com/ I find it very
nice,plz. send u r next papers also to me, if possible. I am also in the
hacking,i was caught 7 times,I want Do my Carrier in HACKING if possible.I
want u to suggest me some way to a big Bully.

thanking u in an anticipation ,

u r's faithfully,
```

Lame, isn't it? This is what we're up against. Caught seven times and he still doesn't get it.

Next Up

In my next column I plan to attack a concept that has been very widely accepted in the security community — the notion of "full disclosure" in bug/vulnerability reports. It's an old idea, and a lot of people place considerable stock in it. I'm sure my popularity will hit an all-time low. In fact, I suspect that a number of people will disagree strongly with the opinions I've voiced in this column. So I'd like to make this issue's contest the "Disagree with Marcus Contest." I'll give a cool Network Police windbreaker to the person who emails me the best brief rebuttal to my position. I'll include it (or a summary if it's not brief enough) in a future column. Mail to <*mjr@nfr.net*> with the subject line "column rebuttal" if you've got something to say.

Forgive me if I'm passionate about this stuff; I've been working in this field a long time, and as far as I can tell things are getting worse faster than they're getting better. So: no more Mr. Nice Guy.

NOTES

1. I'm kind of red-faced on this one. When I was an undergraduate in 1984 I wrote a program called cloak which was designed to let me disappear from our UNIX system so I could play empire without getting caught breaking the university's "no games" policy. There are probably copies of it still out there.

2. You won't work for me, anyhow. My company is the only security-products company I know of that has a policy of not hiring cyber-criminals or even ex-cyber-criminals.