letters to the editor

Wireless Security: A Discussion

Note from Rob Kolstad: This article summarizes an email discussion between Marcus Ranum and Bill Cheswick after Marcus had an "interesting experience" at the USENIX Security Conference. Thanks to both of them for allowing us to share it publicly in order to foster discussion.

MARCUS RANUM:

I had an interesting experience at the USENIX Security Conference, and I'd like to share it here for discussion. Like many conference attendees, I took advantage of the wireless network so I could check my email, update my Web site, etc. At virtually every USENIX conference, someone sets up dsniff and collects passwords as they cross the wireless, and this latest conference was no exception. For the past few years I've basically chosen to ignore the snoopers because, frankly, I hoped they'd grow up and go away. This year I finally got sick and tired of it, and confronted one of the snoopers who had emailed me my own password.

What bothered me most about this experience was that the folks who do the snooping are security practitioners. When I raised the issue, the immediate response was surprising. Basically, I got the exact same set of excuses that crackers have been using for years: "I wasn't abusing the information," "it was for my own research/curiosity," etc. I'm afraid I lost my temper quite badly in the face of what seemed to me to be a lack of clarity on the part of the security community regarding basic issues such as whether or not we're justified in doing exactly the same things as the "bad guys" as long as we're the "good guys." I think the whole situation was further exacerbated by the fact that the whole issue was not in my opinion taken adequately

seriously by the USENIX Board members at the conference.

So I think the whole incident becomes a microcosm of today's security experience. It motivates me to ask questions like:

- What is the difference between the good guys and the bad guys if their actions are largely the same?
- Why do we place the onus of self-defense on the victim, instead of demanding ethical behavior from the perpetrator?

I felt that my privacy was being violated, and, more to the point, I was going to be forced to waste time installing security measures because of someone's "harmless curiosity." Indeed, I find it ironic (if not outright contradictory) that USENIX, which is normally a haven for privacy advocates, would tolerate this behavior over a lengthy period of time.

BILL CHESWICK:

I just returned from the San Diego USENIX Security Conference, reliably one of the top security conferences of the year; this year's was no exception. The keynote in particular was one of the best security talks I have heard in years (and I hear a lot of security talks); there were several excellent papers; and most of the hall track meetings alone were worth the trip.

I had several things to accomplish at this conference, including preparation for an invited talk I was asked to give at the last moment. These activities were curtailed when I was accused of being legally and ethically on the wrong side concerning the use of the dsniff program.

The incident precipitated swirls of hallway conversations about the legalities and ethics of using dsniff. This is not your average crowd of I-am-not-a-lawyer-buts as they debated the ethics and legalities of password sniffing. Not only has this crowd assisted in numerous law enforcement cases, many have advised lawyers, courts, and the US Congress on such matters.

Much of what many of us have done is "ahead of the law" (to quote one lawyer), and since Leviticus (and Numbers, adds Dan Geer) and the New Testament appear to be mute on the topic, we have traditionally had to grope our own way towards personal and societal rules for using the Internet. Concerning the legality of using dsniff, the IANALBs appeared to cover the spectrum from "illegal" to "not covered." Several laws appear to be involved, and it looks like a courtroom toss-up to me.

I have given a lot of thought to the ethics of various Internet experiments and practices I have adopted over the years. I believe that this is an especially important thing to do, given this novel medium and the nascent state of case law. I have used sniffed passwords to make an important point in a number of my talks in the past. I am still satisfied with the ethics of doing so, despite the lecture I received, but the point is not important enough to fight for. I have agreed not to display sniffed passwords publicly, for any reason, in the future, and did not do so at the invited talk.

I think USENIX's response was measured and proper. They asked us nicely not to sniff the network, and I, for one, complied. That is about all they can do without closing the network or implementing extremely invasive procedures. I expect that future conferences will include similar requests.

Marcus raises several specific issues. Some are matters of basic law; the rest deal with our community's position on the forefront of a new technology.

Marcus asks, "Are individuals justified in doing exactly the same things as the 'bad guys' as long as we're the 'good guys'?" The problem here is in the question. We are not doing "the same things as the "bad guys." The bad guys break into systems, compromise their integrity, modify their software, etc.

Marcus asks, "What is the difference between the good guys and the bad guys if their actions are largely the same?" I think "largely the same" is neither ethically nor morally "the same." The crackers who justify their actions in court with "I wasn't abusing the information" and "it was for my own research/curiosity" aren't in court because they ran dsniff.

Even though this was an upsetting experience for me, the hallway track continues to provide deep, thoughtful discussions on the cutting-edge issues of our industry and society.

MARCUS RANUM:

Bill observes that many security practitioners are "ahead of the law," but I feel that professional conduct, and what is tolerated by an organization like USENIX, should be about "right and wrong." Hiding behind legalisms is not leadership. USENIX is an organization full of privacy advocates, an organization that cares enough about its members' privacy that it protects attendee email addresses and the like. By consistently turning a blind eye to people sniffing the conference network, USENIX has implicitly encouraged the kind of "anything goes" attitude that is more appropriate at DEFCON than at a respected conference concerned with its attendees' privacy. As an organization of thought leaders in the computing arena, I think USENIX should pay attention to the leadership shown by conferences like SANS, which will eject attendees for sniffing the conference WAN or any other hacking-type activity. If we are, indeed, "ahead of the law," then it's more important that our behavior be, literally, exemplary.

I'm a fairly open person, and I've always been interested in helping

other practitioners with their research. If Bill had wanted to know how often I change my password, he could have just asked. Instead, he stole what would have been gladly given, and was amused by the fact that he was able to. It's almost a USENIX tradition that some wiseacre posts passwords on the bulletin board with a sign saying "CHANGE THESE" at every conference. This whole issue would never have surfaced if Bill had asked for, and gotten, permission from USENIX to sniff the network before doing so. That opens the broader question of whether such permission would have been granted. I doubt it—but it would have been easy to find out. I suspect we're dealing with a case of "better to ask forgiveness than permission." I've already forgiven Bill, and I hope he's forgiven me for screaming at him in public; I think it's good that this issue has been aired before USENIX has to deal with an incident involving less forgiving people.

BILL CHESWICK:

As for asking permission, that's quite true, and I have done so at other conferences, with the explicit purpose of reporting the penetration of secure protocols into the common packet stream. Of course, I never cared about the particular passwords that were sniffable, Marcus's or any others, and I only forwarded his results to him as a friendly nudge. Some previous nudges had resulted in the discovery of a non-functioning encrypted tunnel, and I have been thanked for my efforts on those occasions. Would permission have been granted? I never thought that deeply about this in this particular venue: I skipped the step in my rush to deal with other pressing things at the conference. I should not have.

I have also let bygones be bygones. I'm glad we got this out in the open.

USENIX RESPONDS:

This has been an instructive experience for all of us. Future conference directories will indeed attempt to give a more explicit description both of acceptable behavior and of the risks inherent in use of the wireless network. We thank both Marcus and Bill for their mature and measured discussion of these issues.