ABE SINGER

conference password sniffing

LEGAL AND ETHICAL ISSUES

Abe Singer has been a computer security researcher with the Security Technologies Group at the San Diego Supercomputer Center for the past five years. His work has involved developing SDSC logging infrastructure and analysis capabilities, participating in incident response and investigation, and working with the TeraGrid Security Working Group. Mr. Singer, with Tina Bird, is the author of *Building a Logging Infrastructure,* SAGE Short Topics booklet #12.

abe@oyvay.nu

AN INCIDENT OCCURRED AT THE 2004 USENIX Security Symposium (see Letters to the Editor, *;login:,* December 2004). Both parties involved are friends of mine, and I was invited to participate in the private argument they were having about the incident. I had already been thinking about the issues involved, and the situation got me thinking more about it. I do not intend in this article to go into the details of that incident or to explain the actions of either party (they are quite capable of doing that themselves). But I want to discuss the general issues that were highlighted by it.

It has become commonplace at some computer conferences, especially security conferences, for someone to go sniffing the network (both wired and wireless) for cleartext transmissions of passwords. Sometimes the person doing this activity is affiliated with the conference, and the activity is "official." But more often the activity is done informally, and while not approved by the conference organizers, it is usually condoned.

This activity is often meant to be used for a "wall of shame," so named because the passwords would be posted publicly for the purpose of embarassing the user—showing that they are being "stupid" for not using an enrypted protocol. In a few cases, the sniffing is done for "research" purposes, to see how many cleartext protocols are still in use.

So, the questions are, is such activity legal, and under what circumstances? If permission can be granted, who has the ability to give it? And even if the activity is legal, is it ethical? Is it okay to allow some people but not others to sniff the network? What sort of example or precedent is set when we says it's okay for the "good guys" to do it?

This article will explore these legal and ethical issues. As is often the case, there may not be clear-cut answers, but hopefully the reader, and especially those involved with running conferences, will have a better understanding of what they may or may not be allowed to do, and consider whether or not such activity is the "right" thing to do.

I have to provide the usual caveat that I Am Not a Lawyer. However, in preparing for this article I consulted a great deal with an attorney who specializes in federal wiretap law, and the legal points presented are based on his input.

The Law

Is it illegal to sniff passwords and other communications from a network at a conference? Yes, it is very likely a violation of U.S. federal law, and possibly some state laws (I'll limit the discussion here to federal law). Packet sniffing can sometimes break the same law that federal prosecutors use to prosecute telephone wiretappers. This law can be used to punish any person "who intentionally intercepts . . . any wire, oral, or electronic communication" (18 USC § 2511(1)(a)). Convicted violators are felons who face up to five years in prison.

Some will say, "But as a system administrator I'm allowed to monitor my own network! People do that every day! Are you saying that's illegal?" There are exceptions in the law, some of which may cover system administrators. But even sysadmins can't sniff packets on their own network for no reason and in all situations. The real question is whether any of these exceptions apply to sniffing for passwords on a conference network. I think the answer is that they usually do not.

There is an exception to the wiretap law (the Electronic Communications Privacy Act, or ECPA) for network providers: It is not illegal to intercept communications "while engaged in any activity which is a necessary incident to . . . the protection of the rights or property of the provider" (18 USC § 2511(2)(a)(i)). In plain English, you can sniff packets to protect your rights or your property. But this exception applies only to the acts of the "officer, employee, or agent" of the provider. The average conference attendee, sitting in the audience or hallway, running dsniff on his or her laptop probably does not fall into any of these categories.

Now, it's certainly possible for the person sniffing to secure the permission of the conference organizers. But are they the providers of the network? At many conferences I have attended, the network is provided by the hotel or by a local ISP. In those cases, does the conference have standing to grant permission to sniff the network? The answer may very well be "no." And if the answer is "no," by authorizing the activity, the organizers may also be liable for breaking the law.

(USENIX does run its own conference network these days, including using their own address space. So, in that particular case, USENIX would be considered the service provider. But I'm trying to keep this argument generic.)

Furthermore, it is difficult to argue that sniffing *my* password to systems on *my network* furthers the protection of the *conference network*. So while some sniffing activities may be legitimate under the provider exception, sniffing user passwords is probably not one of them. Not even the provider of the network can grant permission for that activity, at least not without the risk of being complicit in breaking the law.

Gray Areas

Others may argue that the people who use plaintext protocols over a conference network are asking for it. The implication is that something about the conference setting alters the playing field. For example, at Blackhat Las Vegas last year, some people were cautioned not to power up their WiFi cards.

Does "should have known" justify conference sniffing? The closest exception in the federal law is consent. It is not illegal to intercept communications if "one of the parties to the communication has given prior consent" (18 USC § 2511(2)(c)). Courts examining this exception have been reluctant to hold those accountable who did not actually consent, just because "they should have known better." The question is, under the circumstances, did this person actually consent to the interception? Maybe the facts of the conference setting's particular situation (and they will be unclear at best) amount to consent, but more likely they do not. It is a gray area, so for a moment let's discuss gray areas and the law.

If you are deciding whether your conduct breaks a law, do what you can to avoid gray areas. Gray areas can be a lawyer's best friend (especially when they are paid by the hour) and a client's worst nightmare, because they get resolved only after lengthy, expensive litigation. Perhaps the courts will vindicate you at the end of the day (and perhaps not), but that proverbial day is sure to be a day of uncertainty, anxiousness, and expense. And if the law you may have broken is a criminal law, it all gets magnified. Gray areas about criminal violations sometimes get resolved only after a potentially invasive investigation into your private life.

Does this mean that the FBI is about to begin arresting people at the next USENIX conference? No. Law enforcement has many other potential crimes worth investigating, and doesn't have enough resources to look at every accusation of conference packet sniffing. But get this: The law provides for civil penalties in addition to criminal (18 USC § 2520(1)); the "victim" of sniffing can sue the person sniffing in civil court for damages (real or statutory), possible punitive damages, and legal fees. The statutory damages may be a *minimum* of $10,000.

So, *if* the conference organizers approve sniffing passwords *and* that particular activity is found to be ille-

gal, the victim might be able to sue the conference for damages.

And the potential illegality of the act may have some bearing on the ethics of the situation.

Avoiding Gray Areas

What is a conscientious conference organizing committee to do? What if they *want* to encourage packet sniffing, as a lesson to attendees in the importance of using encrypted protocols?

There is one way; it's called "consent." Ask attendees or users for permission to sniff their communications and you do not have to worry about wiretap law. If you provide computers, such as in a terminal room, use system banners that are visible and meaningful. These days, most conferences are mostly wireless, so it's a little more difficult to banner. The best way to make it clear that the user has consented is to have them sign a form. If signed forms are not feasible, posting signs around the conference and having session moderators make regular announcements *may* be acceptable.

The wording of banners/signs can make a difference (e.g., "You consent to be monitored" is better than "You have no privacy," although either is better than no banner at all). Be careful not to inadvertently limit the scope of consent (e.g., "Your email messages may be monitored" does not give authority to monitor instant messages).

To avoid gray areas, then, have banners on your network; get consent from your users; if you're protecting the network, get permission from the provider (be an agent) and stick to proper motives.

Ethics

In addition to the question of the legality of sniffing at conference networks, there are also ethical issues. Ethics are not defined by what is legal (although the law often follows ethical standards) but by what is *right*. Just because something can be done doesn't mean that it *should* be done, and doesn't mean that it is right to do so.

Of course, because ethics aren't defined as clearly as the law is, they are often open to debate. In many fields, ethical standards are developed and codified, and define generally accepted practices and behavior. For instance, doctors, lawyers, engineers, CPAs all have ethical standards to live up to. In those fields, violations of ethical standards can result in revocation of the violator's license to practice. In the research community, there are ethical guidelines about accuracy and attribution of source data. Altering data to fit one's hypothesis is generally considered unacceptable, and plagiarism is a firing offense in many universities. I read about a case a few years ago where a renowned scientist was found guilty of forging data; as a result, the institution that had granted his Ph.D. years earlier revoked it. The CISSP certification has a code of ethics to be followed, but I have not heard of a credential being revoked.

Ethics change over time (as does the law). What was once acceptable may no longer be, or vice versa. The notion that it's wrong to alter data when it doesn't fit has only been established for about the past 100 years. While conference password sniffing may have been considered harmless in the past, I'm starting to think maybe it no longer is.

There was a time when people would break into other people's systems just to show them that they were insecure. It was often tolerated, almost as a friendly competition. These days, most people would not think of doing such a thing without explicit permission from their target. Aside from the fear of being drawn into a protracted legal defense of their actions, it's just not considered appropriate anymore. And, as a result, we quickly dismiss the hacker's defense of "I was just trying to show them they had a security problem."

So the first ethical argument might be, "Who cares? It's none of the conference's business!" Well, I think it *is* the business of an honest conference. Organizations such as USENIX, and the conferences that it produces, are about educating professionals, and I think that should include promoting responsible behavior. And the best way to promote that behavior is by example, especially at a security conference.

Waiving Privacy

Suppose a conference could create a situation where the activity were legal, for instance by having all attendees give consent by signing a form or (horrors) a click-through agreement. Or they construct an argument that supports the provider-protection exception. Is it ethical to ask users to waive protection (and privacy) under the law in order to use the network at a conference, just so that some people can run a wall of shame?

I think there are enough USENIX attendees who are privacy advocates who would balk at having to sign such an agreement (although many would be taking their own measures to protect their their privacy, regardless). I think they would have the same reaction if their ISP tried to do the same. I certainly would not consider it right for my ISP to insist that I waive my privacy in order to get service; why should I expect less of a conference network?

In fact, much of the existing wiretap law exists to *enforce* privacy. The Electronic Communications Privacy Act's purpose was to limit what ISPs were allowed to do in terms of monitoring customer communications, in addition to spelling out how and when law enforcement is allowed to monitor (see Daniel Appleman, "Primer on Cybercrime Laws," in this issue). As a service provider, a conference that requires user consent for monitoring undermines the privacy protections that the law intended. Many in the security and privacy communities fought for those laws in the first place; should we really be sidestepping them for our own convenience?

Some might say, "Well, the law is wrong. I should be able to do this to educate people or to conduct research." That's a fine opinion. Get the law changed. I think there are ethical dilemmas in ignoring the law because you disagree with it (although the U.S. certainly has a tradition of rebelling against laws perceived to be unjust).

Shaming

And then there are the arguments that the purpose of a wall of shame is to educate the user by "shaming" him into using more secure protocols. I think educating people is a very good thing and, as I said above, a noble goal for a conference. But is "shaming" the right way to do it?

Public humiliation is certainly one method of education. But I think most professional educators would agree that it is not the most effective method. For anyone reading this who has children: Would you find it acceptable for their school teacher to embarrass them in front of the class, in order to "teach" them?

And who is actually being "shamed" here? Some, possibly most, of the attendees using plaintext protocols are doing it because that's what their employer provides, and they have no alternative (other than to seek other employment). The attendee is not the person who needs educating, and they really have no choice other than not to use the conference network. In these cases, we should be finding a way to educate their *employer*—the sysadmin, IT executive, whoever makes the decisions and controls the technology. And the wall of shame isn't going to have much of an effect on those people.

To be honest, I find things like a wall of shame to be immature and more about geeks having pissing contests: "Ha ha, look at what I did to that luser" is pretty damned immature. (The 2004 incident I referred to above is not a case of this. In that situation, the goal was to collect statistics about protocols used, without the intent of providing any way to identify the individuals involved.)

Can't we find a more constructive way to educate people than by "shaming" them?

Blaming the Victim

When someone is compromised due to something like a sniffed password, a common justification is "he should have known better" and "he was asking for it." Those are just absurd excuses. The same justification used to be applied (and sometimes still is) to blame a rape victim. "She was wearing a short skirt and low-cut blouse—she was asking for it." These days, at least in the U.S., this defense would offend most reasonable people.

Would anyone honestly excuse a thief who said, "They left their door unlocked, so I stole their TV to teach them a lesson"? In the same vein, should we excuse password gathering or other malicious activity because the victim "deserved it"? (Yes, if you leave all of your doors unlocked, you may find it difficult to prove to the police that your TV was stolen, but it's still theft, and in no way mitigated by the fact that you were stupid.)

Now, I'm not saying people shouldn't take measures to protect themselves—they certainly should. But lack of knowledge, imprudence, or simple human error should not be used to justify behavior that is wrong or malicious.

Recommendations

Now that I've had a good, healthy rant about what's wrong, I have some constructive suggestions.

First, organizers should certainly consider their liability if they approve, condone, or knowingly ignore people committing illegal activities on their network.

I think conference organizers should think long and hard about whether to permit such activity in a legal manner, and how to do so. It's pretty clear that the only way sniffing can be done legally is by requiring all users of the network to give consent, or at least for the conference to proclaim loudly and frequently that the network is being monitored. And the organizers should think about whether it's right to promote that loss of privacy.

And they should think about whether they want to promote ethical behavior by attendees, and take action against those who don't follow the rules. A conference can decide (as DefCon certainly has) that they don't care how their attendees behave. But I think that an organization such as USENIX (I'm not

trying to single out USENIX here, but this *is* a USENIX publication) can only gain respect by such promotion, and has very little to lose. I'm not saying that they should actively police the network; rather, they should declare that certain behavior is unacceptable and take action against violators if there is a complaint, or if violators are otherwise detected.

Both organizers and attendees should think about how to better educate those who may still be using plaintext protocols and/or their employers or service providers. Making the world a better place is a good goal to strive for. Perhaps a kiosk could be provided, which attendees could plug their laptops into and sniff themselves to see if they are using plaintext protocols, without anyone else being privy to the information. Or demonstrations could be given using conference-provided systems (and passwords).

And somebody should educate the programmers who continue to write software that requires or enables cleartext transmission of credentials. But that's for another article.

Conclusion

Sniffing passwords at conferences is probably illegal as currently done. While there may be legal ways to do so, I think sniffing sends the wrong message and that there are better ways to educate people. Conferences that promote security should also promote responsible behavior in word and deed. Some may disagree: such is the nature of ethical debate. I think it's time we had a good debate on ethics, and I welcome the arguments.

Editor's Note
USENIX does have a policy regarding sniffing at conferences. Complaints about sniffing the network will be handled first by warning the perpetrator, then by asking that person to leave if a warning is not sufficient incentive to cease the behavior. See the draft minutes of the April 2005 meeting of the Board of Directors at www.usenix.org/about/minutes/Apr05_draft.pdf.