Legal Issues, A Site Manager's Nightmare

Stephen E. Hansen

Stanford University

Excerpts from the Electronic Communications Privacy Act of 1986

> 2511(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.
>
> 2511(2)(h)(ii) It shall not be unlawful under this chapter record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

1. Logging For Fun and Profit

What do we mean when we talk about computer security? For most of us it means the protection against the loss of or tampering with computer based information and protection against possible denial of service. If you are a site manager, your users, clients, or employers want assurances that their files won't be read if they don't want them to be, won't be modified or deleted without their consent, and want to be able to access their files when necessary. So we take steps to provide and enforce various security mechanisms that are aimed at protecting the privacy of information and access to resources. But there are often tradeoffs between privacy and security that must be recognized and evaluated. On many systems every time you login, logout, send a mail message, print a file, or copy data to or from another system the who, what, where, and when of the transaction is logged (on some systems every command is logged). Not too long ago there was a rather spirited discussion on one of our local network bulletin boards on whether or not this logging was an invasion of privacy. If this seems silly to you, consider your reaction if you learned that the US Post Office was keeping logs of the source and destination of every piece of mail that you sent. On the other hand, the phone companies have been doing this very thing with your phone calls for years and years for billing purposes. But the fact that many systems log this information in pursuit of several admirable goals such as ensuring reliability and security is not always appreciated by the average user.

From a legal perspective this type of service-related logging is allowed under section 2511(2)(h)(ii) of the Electronic Communications Privacy Act of 1986,

> "It shall not be unlawful under this chapter... for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service."

But for the security conscious (fanatic, paranoid?) administrator the tendency is to log more and more information about more and more activities. It used to be that resource limits (i.e. limited disk space and low density tape) provided a natural governor on these activities, but for many systems these limits no longer applies. At what point does logging for the purpose of verification, fault tracing, or resource billing become service observing or random monitoring, which is prohibited under section 2511(2)(a)(i) of the Act. So here we have a federal law that provides the means to charge and prosecute people who access private data on our systems, but if we are not careful we may find ourselves in violation of the law by acting too aggressively on our own for the purpose of maintaining security.

2. Investigator or Accomplice

When a security breach is detected or suspected it may be necessary to override normal file protection controls and scan files belonging to system users. In most cases ethics, and in some cases the law, tells you to get permission from the users before looking at their files. This may not be practical, however, due to time constraints or due to the possibility of alerting a suspect

The first time I had to deal with a break-in the only legal issue we considered was did, "we have enough evidence." Our main concern was getting the law enforcement groups interested in our problem. The "bad guys" were almost certainly from outside our organization. We quickly restricted access to one account on one system, and the legitimate user of that account agreed to use a different one while the investigation was in progress. We set things up so that every time the compromised account was accessed, the bit-streams in both directions were logged, both the keystrokes coming in and what was going out to their screens. This information turned out to be invaluable in quickly notifying managers all over the country that their systems had been penetrated. It gave us names, times, and places of the machines that had been accessed by these "Crackers". It was key to tracking down the source of these break-ins.

It was only later that someone else made the comment, "What if these guys used your system to break into someone else's system: could the owners of these other systems come after you for giving the Crackers the means to do it?". Now this was a rather chilling thought. I have for some time advocated the idea that if it is possible to control and monitor a break-in, then you should do so in order to collect information and track down and arrest those responsible. There are, of course, real risks to your own system in this, but if you can stay on top of things those risks can be minimized. However, if there are need to get them out in the open and address them. Cliff Stoll's pursuit of the West German hackers is only the most well known of probably dozens of successful uses of this strategy. If we are open to civil or criminal liability by permitting the attackers to use our systems while we chase them down then we will have lost one of our most potent offensive weapons. We will be reduced to the unsatisfactory alternative of merely shutting them out and

funding the alarm, with the knowledge that not everyone will hear it or heed it. It is likely that additional legislation is needed here. I have heard some prosecutors say that new laws relating to computer crimes are not necessary, that existing law on trespass, theft, trade secrets, etc. are sufficient, but I am doubtful. The art of applying existing law to computer-related activities is still an uncertain one. I am uncomfortable with the idea that someone may make the analogy between our logging and tracking operation and someone allowing a thief to use his garage as a storage place for stolen goods while he tries to follow the bad guy around to see where he lives. Sure the police can do it but they would frown on you doing it on your own. I think the analogy is a bad one, I don't think it 'maps' very well. But would an MIS VP who's had his system trashed agree? Would Bell South agree? Would a judge or jury agree? I think it's took a close look at this one.

3. Vigilant Watchman or Peeping Tom

The next security problem I dealt with was not a break-in from the outside, but rather it was a legitimate user, a graduate student who wasn't happy with how quickly we responded to problems. ("Steve! The print spooler's stuck again!"). This guy got root access somehow (via a trojan Is command in /tmp directory I think) and booby-trapped a module that is linked into most system utilities. He added a small code fragment to this module that looked for the presence of a uniquely named copy of the csh shell in /tmp. If it found it would change its ownership to root and turn on its setuid bit, giving him root access. What got us on to him was finding a setuid root file buried in his directories during a security scan. We went and looked at that file and found that it was a setuid root copy of csh. We went looking around and found a directory containing plain text and encrypted files. The plain text files appeared to be the source for some of the encrypted files that he'd neglected to remove. The contents of some of the plain were sufficiently worrisome that we spent the time to break the encryption and read the rest of the files. It was all rather incriminating.

At this point we went to the student's advisor who was also the owner of the system and showed him what we'd found. The professor called in the student, showed him the evidence and chew him out. He was told that if he wanted to graduate he'd better behave. He did, got his PhD, left us on good terms, and is now on the staff of the research arm of a major telecommunications company. In this case, once we found the file that provided super user access to the system we felt justified in looking further. Today, we would operate a bit differently, if we found a setuid root file in a user's directory we would immediately close and archive the account and get approval from the user, or, if necessary, the system's owner before looking further. There a at least a couple of reasons for this. One is a greater sensitivity toward the privacy of user files. The other is legal, the Privacy Act in section 2701 provides penalties for anyone who "obtains, alters, or prevents authorized access to a... electronic communication while it is in electronic storage...". But while it appears to give us an out by making an exception "... with respect to conduct authorized by the person or entity providing a ... electronic communication service" the Act has only been tested with respect to telephone monitoring. To me, the key words here are "conduct authorized". What constitutes authorized conduct?

But let's take it a step further, what if you find out that someone has compromised yo just one or more user accounts, but all the way to root, to the super user. Do you scan everyone's files? Don't you have to? Let's make it real sticky and say that you found that the slimemold who in has been hiding account and password information in old mail files of what seems to b Do you go looking in everybody's mail, including your boss's, the Provost's, the Director of the Human Resources Department, Major Filbert's? Again, don't you have to? What a mess! Our ma in, and the one least satisfying in its resolution, had a number of system administrators on looking at a lot of private, and in some cases very personal, mail, just to find a few caches of important system information hidden by one or more outside intruders. This is a very distasteful thing the people

involved enjoyed it, and the anger directed at the vandals who made this necessary was considerable. But even though most of the users soon found out about the break-ins and knew we were prying intruders out of the file system I done don't think they realized just how invasive our h own private files, otherwise we may very well had a number of very outraged users on our r

The best solution to this problem would be to state in advance of issuing any account system administrators reserve the right to review a user's files in certain situations, our duct". One of these situations is when a reasonable suspicion exists that the files cont activities that are either illegal or violate the system's or organization's rules of conduct. should be in writing and signed off by each user. It should state what you will and will no conditions, and why. Especially why. This preemptive tactic of laying out the rules in advance implemented by every site. A side benefit of implementing these guidelines is that it w administrators to think about, in advance, the way in which they will or can respond to s type. In the heat of the moment it is all too easy to rush in and do something you'll regret later. Your staff will have pre-established procedures to follow, even if you're not immediately available to advise them. By setting up your procedures in advance you can get management to pre-approve your responses, something that you probably won't want to take the time for when the day comes. And if push and you have to go in and justify your actions you will want to be able to show that you were following well known procedures designed to protect the privacy and security of all users.

Having an agreed-to set of rights and rules for both users and system administrators clarifies your relationship. In many or most non-educational or commercial service sites such rights and rules are likely to be rather-one sided towards the administrators, but at least you know where you stand by writing these agreements in advance. Running such an agreement and your procedures by the legal department may be useful in showing you a few hard patches of ground in the swamp of computer law.

4. Conclusions

Our logging of the various system activities are, in general, necessary for the smooth operation of the systems, but it can be taken to extremes. You risk drowning in information and possibly violating privacy laws or regulations.

Allowing intruders to remain on your system and use it as a base of operations while you collect evidence and attempt to track them down may have some legal liability if they subsequently break into another system. The potential for liability urgently needs evaluation by legal professionals.

Your legal right to search a user's files without permission or prior agreement is uncertain. An agreed to set of rights, rules, and procedures between users and administration can be helpful in determining the legality of your actions in the event of unauthorized access. The existence of guidelines and procedures can be invaluable in responding quickly, legally, and ethically to real or suspected security problems.

I've focused on the Federal Electronic Communications Privacy Act of 1986. This is certainly not the only law that will apply in the case of unauthorized access but it does cover a number of likely situations, and unlike the Computer Fraud and Abuse Act of 1986 it is not restricted to government systems. In addition, several states have very similar statues and more are likely to follow.