by MICHAEL O'BRIEN

"If it logs in, shoot it."– Harried Internet service provider

"Never look back. Someone might be gainin' on ya."– Leroy Robert "Satchel" Paige

"The vulnerability exists in versions of EvilAliens' Alien/OS 34762.12.1 or later, and all versions of Microsoft's Windows/95."– CERT Advisory CA-96.13

Mr. Protocol Mans the Barricades

Q: *Help! Help! Help! Help! Hackers! Terrorists! Nazis! Martians!*

A: Geez, the first quiet afternoon we've had around here in weeks and now *you* start off. It's bad enough that Mr. Protocol's tenuous grasp of reality sends him off at full tilt chasing raw random rumors. Now you're acting worse than he does. You're hired to ask the leading questions about Mr. Protocol's latest panic, not to start generating hysteria on your own. Hysteria generation should be left to qualified professionals like Mr. P. Don't try it at home. Especially, don't try it at *my* home. I get enough of it!

Here, hold this tuning fork. Mmmm, you're vibrating at a nice, 440 A, just like an old-time orchestra before everyone decided to go brighten up their sound by declaring A to be 760 or something. That means it must be a nice, old-time problem, like hackers. Except you run Doorframes 95, which is too damn dumb to be hacked, so what's your problem? Oh, quit tearing at Mr. Protocol's pants cuff like that. You're not a trained supplicant and amateurs unnerve him. Must be something to do with your service provider, eh? I thought so.

Flying by the Seat of their Pants

Someone's done a rough head count of Internet service providers, and the rumored number was in the thousands. I believe it. If telephone cable had been as cheap and easy to lay as Pentium computers are to buy, there would have been the same number of telephone companies two years after Alex Bell spilled acid on himself. It stands to reason that you're not going to get that many total Internet experts trained up in the same amount of time, so some of these folks–in fact, most of them–are doubtless flying by the seat of their pants.

TOM BARRETT

This doesn't prove too bad for the customer–except for the usual woefully inadequate capacity planning–until disaster strikes. Disaster can take many forms. Lots of people give lots of seminars in disaster planning and recovery. Serious people wearing suits attend them, too, so that the first guy to decide to visit your bank driving a truck loaded by the Diesel Fuel, Fertilizer and Orbital Insertion Society (Motto: "If it doesn't fly now, it soon will.") doesn't delay your monthly statement.

Does your ISP attend these seminars? Chances are he doesn't; he's too busy trying to understand why the phone company can't install another 25 lines by tomorrow. He's got enough stuff biting him right now to worry about something that might bite him tomorrow...or might not. This is a basic, survivalist attitude, which works in most places. When it doesn't work it's spectacular.

In fact this may or may not bother you. If you never use a shell account it *may* not bother you at all, or at least, not very much.

Most ISPs offer two kinds of individual-use accounts: shell accounts and PPP (or SLIP) accounts. The larger providers support a third service, whose name is often a trademark that varies from provider to provider.

Shell accounts are just that: a dial-in account that gives access to a shell on

some sort of UNIX system. These were the first kinds of accounts offered when the ISP business started, because they're the easiest to provide. You buy a box, put some sort of UNIX on it, lay in some phone lines and modems, plus some sort of Internet connection, and hang out your shingle.

Market pressures resulted in amazing usage of these accounts. By nature, they support only a text-based form of access to services such as Telnet, FTP, archie, gopher and the like. Pretty quickly, someone came up with software that transferred IP over the dial-up connection from an application run at the shell level. This enabled dial-up shell users to make use of a wider variety of programs; in particular, graphical Web browsers.

Of course, there is no reason why providers couldn't support IP connections directly, and today, almost all of them do. The only additional resource required to support an IP connection, as opposed to a shell connection, is a pool of IP addresses to assign to the customers on an as-needed basis.

Software to handle the IP-level connection is also required at each end, of course, as well as application software at the customer's end, but IP address space is the only unique, consumable resource. Each simultaneous dial-up IP customer needs his or her own IP address. On a machine supporting shell accounts, however, the machine's own IP address is shared by all the customers who are, after all, using the machine jointly, just like the old dial-up time-sharing customers on services like Tymnet.

IP dial-up accounts use one of two special protocols, the Point-to-Point Protocol (PPP), or the Serial Line IP Protocol (SLIP), to encapsulate the IP packets for transmission over the dial-up line. PPP is the designated replacement for SLIP and handles some situations with considerably more grace. It can also be set up to be much more secure.

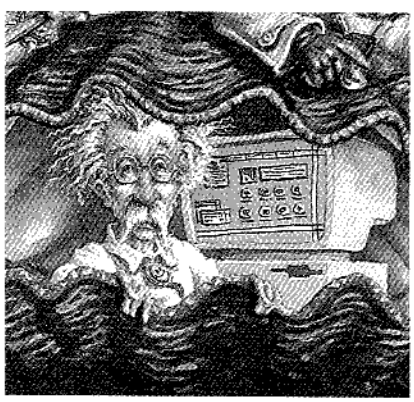
The third type of service is generally similar to the IP dial-up customer, but uses (generally) a single application, unique to the provider, as an interface to various Internet services, such as email, Web browsing and the like. The notion is to make the Internet easier for a novice to use, by providing a uniform graphical interface to all the services. One could view this as the "Disney" approach. For security purposes, it's largely equivalent to dial-up IP.

Now, what happens when the pirates come aboard?

Mr. Protocol is glad you asked.

Seeking Out the Dangers

Mr. Protocol did not poke me to write this column to inform you of the existence of bad guys on the Internet. Mr. Protocol poked me because there are a large number of Internet providers who do not make intelligent responses to certain challenges they face. Where the provider falls short, the customer shares the scrapes and bruises. Let's look at some likely scenarios.



Shell accounts are the most dangerous because the bad guys get on the system by buying their way on. It's that simple. Most UNIX systems come with a configuration that allows files owned by one person to be read by everyone else on the system. Thus if the provider is either ignorant or egalitarian, everyone gets to read everyone else's files, except for whatever files and directories have been explicitly protected by their owners. Because a DOS/ Windows or a Mac world leaves users generally foggy on this whole "protection" issue, many users leave the most astonishing things readable.

Luckily, the assumption is made by software systems in general that personal mail is *not* to be readable by everyone in the world, so your mail is usually protected from outside access, even if your files are not. Yes, users of shell accounts *can* protect their files, it's just that many don't realize it's possible. You can always tell who had UNIX around when they were in college: Their shell accounts will be full of all kinds of file modes.

So, you protect your files so that only you can read them. Are you safe? You wish.

It may be possible to run a dial-up system that gives access to a UNIX shell in such a way that it is secure. Schools do this sort of thing all the time. But at school, a) it is a constant war, and b) once you catch the bad guys you get to do unpleasant things to them without any of the bother of a trial. This does tend to keep a lid on things. At a commercial provider, all bets are off. And there are a lot of things you have to do to the average UNIX system to make it really secure for dial-up use.

First of all, everything must be buttoned down tightly by people who know what they're doing. Privileged programs have to be configured absolutely correctly. One standard thing to do is to calculate a checksum for every privileged binary file in the system, and periodically recalculate the checksum to see if anything has changed. This will detect Trojan horses. There are many other things like this that a newly fledged provider may not know.

Second, the provider must be able to detect when an attack is in progress. Failed login attempts and failed attempts to use the `su` command all have to be logged, and the logs have to be read and understood.

Third, the provider needs to know what to do when an attack is detected, and what to do if the attack was successful. And what to do when a CERT advisory comes out. And who to call if someone finds a new hole on their system. And what to do to clean up afterward.

Let's face it, systems with open shell accounts are messy.

Life improves dramatically if you use the Net exclusively through a PPP account. There are, generally speaking, only a few things that can go wrong, mostly because most PPP client machines are as dumb as a box of rocks–or, in the words of the noted

systems analyst Prof. Foghorn Leghorn, "About as sharp as a bag of wet mice." Yes, when you run PPP, you're on the Internet. But you aren't running any servers, and your machine will ignore just about any packet that's addressed to you, if it isn't part of the particular application you're running at that moment. The greatest hacker in the world can't hack what isn't there, and Lord knows, on most consumer Internet machines there's not much there. This leaves two possibilities.

First, a bad guy can break into your provider's machine. It's probably some sort of UNIX box that just doesn't happen to offer shell accounts, after all. Having done that, he gets to snoop on all your packets in both directions, basically watching everything you do over your shoulder. You thought that nice steamy session in a locked Internet Relay Chat channel was private, didn't you? Hoo hah. Or an America OnLine chat room. No one can crack AOL, after all, can they? Hoo hah on several counts. In the first place, they don't have to. In the second place, who says?

We'll get to that later.

The second thing that can go wrong with a PPP account involves your mail. Mail is the one thing that does not run on your machine, even though you are actually on the Internet via PPP. That's because your machine is not connected to the Internet all the time. Your provider's machine is, and mail is set up so that the mail is delivered to you at your provider's mail host. When your mail is being delivered, a host needs to be there to take delivery. When you come along and run PPP, your machine talks to the mail host, generally via an application running Post Office Protocol, or POP, and sucks up the waiting mail, bringing it over to your machine where you can read it.

You identify yourself to the POP mail server via a username and password combination, as you would to access a shell account. In fact, it is often the same password. So, if anyone cracks your password, they get to read all your mail.

The problem is, you identify yourself to the POP mail server via a username and password combination, as you would to access a shell account. In fact, it is often the *same* password. So, if anyone cracks your password, they get to read all your mail. And if they use the right kind of program, they can read it without deleting it, leaving you with no clue that someone has been reading over your shoulder.

Now, here's a scenario: You try to log on to your ISP, using the usual means but you can't. With some software you're left in the dark as to what went wrong, unfortunately. But pretend for the moment that you figure out that your password has been changed. If you've been spamming the Net with advertisements, shame on you, you're hosed, time to move on to the next provider. If you've been a good citizen, though, you call your provider. "Oh," they say, "we've been under attack and there's some evidence your account was compromised, so we changed your password. Your new password is '2ab=3G.'"

Well, fair enough. Or is it? Look what just happened. You called up, claiming to be you and with no further supporting evidence, *they told you your password.* Double plus ungood, with oak leaf clusters. Mr. P. awards them the Gilded Big Stuf Ding-Dong Wrapper. This scenario actually occurred, and as another noted columnist often remarks, I swear I am not making this up.

Now, most providers, if called on the telephone, will not give out passwords–mostly because if it's a UNIX system they don't know them, but hey. Most providers, if called, would probably not change a "forgotten" password without some identification. But invasion flusters people. Beware. Even if

the bad guys didn't invade your account by hacking your password, it looks like all they'd have to do is call up and ask for the `#*$#@` thing.

Separating Good from Bad

So, your provider has been attacked. Maybe they got through, maybe they didn't. Let's look at some more possibilities:

1) Your provider sends you email, or even a typed letter, saying, "We were attacked. Several accounts were compromised. All passwords have been changed, including yours, to a password that cannot be easily determined via most known methods of attack. Please check your files and notify us of any damaged or missing files."

Prognosis: These guys are honest. Stick with them, unless it happens again. Then, reevaluate. Might not be their fault. Change your password to something equally difficult. Do not change it back to what it was, ever.

2) Your provider makes an announcement: "Our system was attacked. The attackers failed to damage our system. We've changed all the passwords on general principles."

Prognosis: This may or may not be true. Change your password, as in case (1). Keep the bloodshot eye of suspicion on the provider until you can figure out if they're weenies or just very, very good. If the latter, don't ever change providers. You've found dry ground in a swamp and you should stay there.

3) You see users named "Mega-GodZilla" running `sendmail-debug`. "Root" is logged on five times. Strange things happen to your mail. Life on-line becomes a twilight zone. Your provider says nothing, or says that all is peachy.

Prognosis: Elvis has left the building. Evacuate immediately. Run, don't walk, to the nearest alternate provider. These guys are into some heavy denial. Eventually, they will find the BIOS passwords changed on their Pentium servers. They don't know it yet, but this entire ISP has just changed hands, all except the check-cashing part. And even that might provide a few surprises, if they did their accounting on-line. If you did *your* accounting on-line, change everything, up to and including your children's social security numbers. You might want to consider changing their middle names. If you don't, somebody else just might.

Internet service providers are a strange breed. There is nothing quite like this situation. The only general public utility that is the regular target of hacking attacks is the phone company, and we more or less expect barefaced lies from all of the major telephone companies because they're very large, and what they say has a big effect on public morale. Besides, we all know they're very good at chasing the bad guys, once they manage to get off the dime.

But there are a lot of Internet service providers, with widely varying degrees of competence, and it's very tough even for an experienced Internaut to predict the behavior of an ISP under fire. Add to that the fact that there is very little the average customer can do to ameliorate his or her vulnerability to an attack on or through an ISP, and suddenly the Internet becomes a more worrisome place.

There are only two really good things one can do, Mr. Protocol feels. First, when the first real attack comes, and it *will* come, watch your provider like a hawk. Second, don't pick dumb passwords. And don't give your password out. And for heaven's sake don't let your provider give it out! ➸

Mike O'Brien has been noodling around the UNIX world for far too long a time. He knows he started out with UNIX Research Version 5 (not System V, he hastens to point out), but forgets the year. He thinks it was around 1975 or so.

He founded and ran the first nationwide UNIX Users Group Software Distribution Center. He worked at Rand during the glory days of the Rand editor and the MH mail system, helped build CSNET (first at Rand and later at BBN Labs Inc.) and is now working at an aerospace research corporation.

Mr. Protocol refuses to divulge his qualifications and may, in fact, have none whatsoever. His email address is `amp@cpg.com`.