14

Where Do We Go from Here?

> It is not your part to finish the task, yet
> you are not free to desist from it.
>
> לֹא עָלֶיךָ הַמְּלָאכָה לִגְמוֹר וְלֹא־אַתָּה
> בֶן־חוֹרִין לְהִבָּטֵל מִמֶּנָּה.
>
> *Pirke Avoth 2:16*
> —RABBI TARFON, C. 130 C.E.

We hope that, by now, we have made two points very clear: that there is indeed a threat, but that the threat can generally be contained by proper techniques, including the use of firewalls. Firewalls are not the be-all and end-all of security, though. Much more can and should be done.

The most important point to remember is that not all threats come from the Internet. For example, is your dial-in modem pool secure? What sort of authentication does it use? For that matter, do you really know where *all* of the dial-in ports are? Even if you can control all of the official ones—and you probably cannot, if you work for an organization of any size at all—there may be unofficial ones that have been created for special purposes. Modems fit into shirt pockets these days; you probably cannot keep them out by fiat alone.

An obvious extension to the dial-in problem is the dial-in IP problem. More and more authorized users have IP-capable machines at home and want to take advantage of the full power that should give them. (Indeed, this very paragraph is being typed from home, from an IP-connected machine.) But full IP connectivity to a point inside the firewall raises some obvious risks. What does your security policy say about such links? What technical solutions are available?

Within AT&T, policies are still evolving. We recommend very strong authentication by the server (PPP's challenge/response mechanism [Lloyd and Simpson, 1992] is adequate), coupled with a packet filter to block any routing protocols or any packets with an invalid source address. (You don't want to run a real routing protocol to a home workstation; it would eat up too much bandwidth. A simple static default route pointing to the server should suffice.)

It may also be necessary to establish policies relating to home LANs, and to who can have access to the computers connected to it. We know a fair number of multiple-computer families;

some already have their own home nets. But security problems from employee families are hardly unknown; see, for example, [Hafner and Markoff, 1991, page 275]. Must the employee's machine be configured as a firewall?

All of these issues will become much more serious as ISDN is deployed. Workstations with integral ISDN ports are already being shipped, and some support PPP as a standard feature. The problem of enforcing a simple edict against modems is now much worse; people *will* connect their machines to their phone lines, because some of them will want to use the nifty phone management software. And once the jack is in place, it's so simple to start making high-speed data calls, especially when the official modem pools are still stuck at 14.4 Kbps. . . .

All of these problems, and more, can also be addressed by a thorough program of internal network security and education. Make no mistake—we do not think such ideas are a substitute for a firewall in a high-threat environment. But they can and will slow down the rate of any penetration attempts, regardless of their origin.

We have already discussed the concepts of tiger teams and network security sweeps. For education, we have two simple recommendations: *don't* treat your users as idiots, and *do* be as precise and specific as possible with respect to security practices. (The second is actually a corollary of the first.) While there are occasional stubborn cases, most people are happy to do the right thing if they understand exactly why it's important. Tell them about password-cracking, and port-scanning, and the details of the latest holes! The Bad Guys already know about these things, and the employees of a typical company are trusted with sensitive information far more critical to the success of the company.

In a totally different vein, changes in networking and computing technology will affect security architectures in the future. Consider, for example, how to construct a firewall that will accommodate gigabit-per-second data streams. Only the fastest computers will even be able to receive data at such rates, but if some of your users have such machines, and need that type of bandwidth, you will need an architecture or a policy that can keep up with them.

Some changes may be forced by the transition of the Internet to a new version of IP, the so-called "*IPng*." As of this writing, there are still several candidate protocols, but one of them *requires* a form of source-routing as an integral part of its design. If this protocol is selected, *all* address-based authentication mechanisms will become insecure; cryptographic authentication will become utterly essential. This is probably good, but the transition process will be painful. In particular, if the Internet deploys translation gateways as a conversion aid, organizations with firewalls will probably need their own translator to accommodate the internal process.

In general, we expect cryptography to become more common in the future. While this will reduce or eliminate certain classes of attacks—picking up passwords by monitoring a LAN will be impossible, as will most forms of address impersonation—new problems will arise. Key servers, for example, will need to be very secure. Password-guessing attacks may even become *easier* [Bellovin and Merritt, 1991] if the servers aren't designed properly. From an organizational perspective, name space planning needs to start now. A scheme that today suffices to identify a relative handful of users with cryptographic keys may not scale to an arena where there are millions of key-holders.

The advent of mobile computing will also stress traditional security architectures. We see this today, to some extent, with the need to pass X11 through the firewall. It will be more important in the future. How does one create a firewall that can protect a portable computer, one that talks to its home network via a public IP network? Certainly, all communication can be encrypted, but how is the portable machine itself to be protected from network-based attacks? What services *must* it offer, in order to function as a mobile host? What about interactions with local facilities, such as printers or disk space?

The face of the network security problem will certainly change over the years. But we're certain of one thing: it won't go away.

> "Well, I've made up my mind, anyway. I want to see mountains again, Gandalf—*mountains*; and then find somewhere where I can *rest*. In peace and quiet, without a lot of relatives prying around, and a string of confounded visitors hanging on the bell. I might find somewhere where I can finish my book. I have thought of a nice ending for it: *and he lived happily ever after to the end of his days*."
>
> Gandalf laughed. "I hope he will. But nobody will ever read the book, however it ends."
>
> "Oh, they may, in years to come."

Bilbo Baggins in *Lord of the Rings*
—J.R.R. TOLKIEN