19

Where Do We Go from Here?

> It is not your part to finish the task, yet
> you are not free to desist from it.
>
> עָ
>
> *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.

Here's our take on where the future is headed. We've been wrong before, and we'll likely be wrong again. (One of us, Steve, was one of the developers of NetNews. He predicted that the ultimate NetNews traffic load would be one or two messages per day, in 50 to 100 newsgroups.)

> It's hard to make predictions, especially about the future.
>
> —YOGI BERRA

19.1 IPv6

When will IPv6 be generally deployed and in use? It should be deployed shortly in the new generation of cell phones; it's also being adopted today in China and Japan. The current generation of backbone routers do not implement IPv6 forwarding in hardware, and the software implementations are not efficient enough to handle heavy traffic. In the late 1990s, ISPs were turning over their routers in 18 months, rotating core routers towards the edges. This trend has slowed of late because of the recent economic slowdown.

Most UNIX and Linux clients already support IPv6. Windows XP has developer support for IPv6; Microsoft has stated publicly that full user-level support will be in the next major release of

Windows, which ought to be around 2004 if they keep to their historic release pace. Within four years of that, it should be widely deployed. Will it be used?

It is not clear what the economic drivers are for a company to spend the time and effort needed to switch over to IPv6. True, the address space crunch would be solved, but most large intranets use private address space and NAT to deal with address space issues. They might wish to improve connectivity to the aforementioned cell phones (voice over IP?) without going through a translator.

One strong driver would be the presence on IPv6 of Internet services that are not available on IPv4. But it is hard to imagine a Web site that would limit itself to the new protocol only. Furthermore, few services, if any, are envisioned for v6 that can't be implemented on v4, assuming that enough address space were available. One possible candidate is peer-to-peer networking—*if* legal uses become popular enough.

The address space crunch is the obvious reason for switching over—it was the original motivation for designing IPv6. IPv4 space is scarce, and said to have a high "street" value. If these addresses were auctioned and a market for address space formed (definitely *not* the Internet tradition), there would be a strong economic incentive to switch. See [Rekhter *et al.*, 1997] for a discussion of the issues.

The three of us disagree about the date of general IPv6 emplacement, but we do agree that 2008 is about the earliest we could see widespread use.

19.2 DNSsec

The lack of authentication of DNS replies is one of the weakest points of the Internet. In the context of the Web, the problem is severe. We *need* something like DNSsec, and as DNS-spoofing attack tools become more widespread, use of the Web as we know it could grind to a halt if nothing is done. Thus, we predict that despite the inherent PKI problems (who is the root?), DNSsec is going to be deployed. The security it provides is too important, and the problems it solves will not go away any other way. Eventually, some public keys will be included in DNS client distributions, and DNS replies will be signed.

That's not to say that widespread deployment of DNSsec is without its challenges. Can we afford to have a signed .COM? The memory footprint of a signed top-level domain will be extremely large. However, we think that these problems can be overcome. More seriously, too many sites don't take security seriously, until the lack of it bites them on the ankle. We can go only so far by putting protection in the infrastructure.

19.3 Microsoft and Security

Recently, the media has been reporting that Microsoft is now going to focus on security. This seems to be true; it's not just public relations propaganda. They are offering widespread security training and awareness courses and are developing new security auditing tools; their corporate culture is already changing. We salute this effort, and hope that the rest of the industry will follow their lead.

Though we may start seeing some effects soon, it is going to take a long, long time to realize. Apart from the installed base and the need for backward compatibility, a huge amount of code must be reviewed, and the complexity offers many opportunities for subtle, emergent behavior.

19.4 Internet Ubiquity

Clearly, many more devices are going to be connected to intranets, if not the Internet. Hotel door locks, refrigerators, thermostats and furnaces, home intercoms, and even mailboxes have been networked. How does a light switch in a smart house know whom to trust?

One of us has experimented extensively with a wired house. The hard part isn't the electronics, the devices, or even thinking of useful things to do—it is the system administration tasks that join the other Saturday chores. Can these systems be implemented on a wide scale for the public; if so, will our homes become more useful, but less secure?

Besides the usual uses of an always connected Internet link to the home, there are interesting possibilities for new services. Automated programs can announce weather alerts and other emergencies. We've heard voice announcements of satellite passes and other astronomical events, reminders to take out the trash and recycling, and a variety of other notifications. Many of these have a time-sensitive component that could be marketed as a service if there were enough demand.

Services like TiVo can help integrate home entertainment with dynamic scheduling. Peer-to-peer networking already supplies a great deal of musical content, though on an *ad hoc* and probably illegal basis. One way or the other, entertainment access will grow.

19.5 Internet Security

Security on the Internet has been deteriorating over the last 20 years, and cyberlife is going to become more dangerous in the future. The PC virus writers may win the battle with the PC virus defenders. Imagine a world where virus-checking software simply doesn't work. Ultimately, the halting problem does not work in our favor. At the very least, virus checkers will have to spend more and more CPU time to determine if a file is infected. If we can't trust our virus-checking software, we will have to revert to better network hygiene, signed binaries, and a more reliable *Trusted Computing Base (TCB)*.

The Internet infrastructure is going to come under increasing attack. The points of greatest vulnerability are DNS name servers, the BGP protocol, and common failure modes of routers [Schneider, 1999].

There is a strong movement afoot to secure the boot process and to verify the operating system and all applications on the system. The main hardware manufacturers, including Compaq, HP, IBM, and Intel, have formed the *Trusted Computing Platform Alliance (TCPA)*. The idea is to make computers less vulnerable to Trojan horses and other malicious code. Microsoft is also part of the TCPA and is hard at work on Palladium, a software platform designed to support the TCPA. Applications include things like digital rights management, in addition to full path security.

Many of the schemes, such as TCPA/Palladium and other security efforts, pose a potential risk to privacy, as well as to the openness of platforms, and the ability of third parties to develop software. While these issues were not the focus of this book, they are important considerations that result from efforts to deal with the growing threats on the Internet. Is it worth buying a more secure computer if it gives you less privacy and fewer choices of software vendors?

There are other questions to consider. Will the next version of Red Hat Linux have its public key in the ROM of the next IBM Thinkpad? It's not out of the question. If you buy an Internet-ready DVD player on eBay, how does it get reoriented to know that you are its new master, while the previous owner's access rights are revoked? How do you secure the networked home? If the washing machine wants to send telemetry data back to the manufacturer, how do the packets get out through your firewall? Do you want to let it? (Will the washing machine's warranty limit the number of times you're allowed to use it? Will the machine tell the manufacturer that you allowed it to run when it wasn't properly leveled? Who owns that washing machine's data, and how does the owner control its use?)

19.6 Conclusion

In this book, we've covered Internet security as it pertains to today's world. While we don't know how similar problems will be solved in the future, we are certain that the same security precepts that have guided people for the last three decades and perhaps for the last five thousand years will continue to hold true.

As Karger and Schell point out, we are going backward, not forward; today's systems don't even achieve the security level Multics had in the 1970s [Karger and Schell, 2002]. We are losing ground. We can't afford to, and must do better.

> "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