September, 2001

Editor's View

The Computer as a Tool

Developers are critical in providing a safe, efficient tool for users.

By Tamar E. Granor

Early this summer, the online world was abuzz with discussion about the distributed denial of service (DDoS) attacks documented by Internet security expert Steve Gibson. He posted a detailed description of the attacks on his Web site (www.grc.com).

Gibson had bitter words for some major ISPs who, he said, could cut down on such attacks with a minor configuration change.

He also criticized Microsoft's plans to include raw socket support in Windows XP. Gibson believes this will make Windows XP systems a major target of hacker activity. As he explains it, raw sockets make it significantly easier for hackers to "spoof" (forge) the source IP address of the packets used to flood a server and bring it down. Packets with forged IP addresses can't be traced back to their source. Thus, fighting such an attack is extremely difficult. (For Gibson's detailed explanation of the threat, see www.grc.com/dos/winxp.htm. Microsoft's response is at www.microsoft.com/technet/security/raw_sockets.asp.)

The reaction: blaming users

Since I'm not a networking or Internet expert, I can't evaluate Gibson's and Microsoft's arguments. I'm more interested in the reaction from operating system experts and developers. Many are holding users responsible for letting their systems be taken over by hackers. One even suggested that some people shouldn't be allowed to have computers. This group blames users for not having firewalls installed and for inadequate virus protection.

I'm disturbed by this attitude. To me, it indicates that too many of the people responsible for creating and maintaining systems have forgotten why we're all doing this.

If drivers had to install seatbelts…

Today, the prevailing view of the computer is as an appliance, or a tool. Clearly, a computer is a far more complex tool than, say, a hammer or a screwdriver, but it's nowhere near as technically sophisticated as a car. Yet, using a computer safely is much more difficult than driving a car safely.

We expect computer users to understand why they're at risk and to take preventive actions. We want them to evaluate and install anti-virus software, and keep it updated; we want them to evaluate and install firewall software; and, we want them to be alert to new security issues and take appropriate measures when they arise.

By contrast, cars come with essential safety equipment (seat belts, air bags, steel frames) installed and properly configured. When a serious issue is discovered, every owner of an affected car is notified by mail.

Imagine if cars didn't come that way and we were told to choose from among the seat belts on the market, and then install them ourselves. How many cars would have seat belts? If you think everyone would take care of this, consider how many people still don't wear a seat belt, despite decades of evidence that seat belts save lives.

If people won't perform such a simple task to protect their lives, how can we possibly believe they're going to do what's needed to secure their computers? More importantly, why should they have to?

I believe personal computers should come with anti-virus software installed and properly configured. If the user's input is needed to handle things such as scheduling updates, that should be part of the initial configuration of the machine.

The same argument applies to firewalls. If experts agree every computer should have one, why don't new computers include a properly configured firewall? We shouldn't assume the average user has the knowledge necessary to figure out which firewall is appropriate, and then install and properly configure it.

Windows XP includes an inbound firewall. That is, the operating system will have the ability to filter incoming traffic to keep uninvited packets out. But, my understanding is that the firewall will not be turned on by default. The user will have to turn it on in the Internet Connection Wizard.

It's great that Microsoft is adding this capability to Windows. But why wouldn't an important setting like this be turned on by default? Also, why inbound only? Microsoft appears to be saying that if you keep invaders out, you don't need to worry about your outbound traffic. But there are other ways for hostile programs to get onto a computer besides unexpected inbound traffic.

Like any other tool

Computer and software producers should stop expecting computer users to become computer experts, and instead, take the steps needed to let them use computers as a tool. Those of us in the industry enjoy knowing what's "under the hood," but we shouldn't expect average users to have this knowledge. People aren't expected to know the internal workings of the other tools in their lives. Most of us haven't a clue how our cars and washers and dryers and dishwashers do their thing. We just know how to use them. We'll know our industry is approaching maturity when the same thing can be said about computers.

What does this mean for us?

As application developers, we need to let this same concept guide us in our approach to application design. We need to design our applications with transparency of the interface in mind. By transparency, I mean the user shouldn't be aware of the interface—it should just make it easy for him to accomplish his ultimate goals. The user interface should hide the internal structure and let the user work in an environment that corresponds to the task at hand. This is the best approach for providing the user with an efficient and sophisticated *tool*.