Summary: The release of Windows XP brought with it a startling alert that predicted the end of the Internet. This prediction was based on one of the newest additions to the Window operating system: Raw Sockets. According to the warning, this feature was going to turn Windows XP into a tool of mass destruction. Now, here we are about one year after the release of Windows XP Beta 1 and there have been no global data meltdowns. This article revisits the Raw Sockets debate and takes a close look at what really happened.

Raw Sockets Revisited: The day the Internet died.

May 2001 brought with it an alarming warning of a potential Internet nightmare that the world has never before seen. As a result of this warning, the media, security professionals, and computer geeks throughout the Internet immediately started contemplating this new threat and what it could mean for the future of digital communications. Could this warning be real? Was it valid? Could a hacker really crash the Internet? These questions and more became the centerpieces of an online debate that continued to sweep through almost every online publication site and tech talk show. What we are talking about is *Raw Sockets*.

In May 2001, a well-known CEO of a security and consulting company, Steve Gibson, released the Raw Socket's warning. According to his Web site, Raw Sockets was a "seriously dumb idea[el]from Microsoft" that "[el]spells catastrophe for the integrity of the Internet." As a result of this bold statement, Steve Gibson and his Web site instantly made headlines.

In short, Steve Gibson expressed a serious and heartfelt concern about the implementation of Raw Sockets into Windows' latest operating system, Windows XP. He felt that by incorporating Raw Sockets into its software, Microsoft was inviting every script kiddie and malicious hacker to use its operating system as a platform to launch denial of service (DoS) attacks. In addition to basic DoS attacks, the GRC Web site appears to closely link the integration of Raw Sockets with an increased used of distributed DoS attacks, which are much more damaging to an online presence. Although he did contact Microsoft, the results of his warnings weren't to his liking. In fact, he told Microsoft that he would "[el]go off and make a big bunch of noise and draw the world's attention to this impending threat to the operation and security of the global Internet." This is exactly how this story became news.

Because this whole debate has been fueled by one man and his comments, we will dissect *his* concerns with Raw Sockets and see what value they hold. After these points are

validated or invalidated, we will take a look at the impact that Windows XP has had thus far on the world of computing[md]and more specifically on the Internet.

What Is a Raw Socket?

A *Raw Socket* is simply a reference to the capability of a computer program to *directly* access the communications aspect of computer hardware. Normally, a program must interface with a mediator program called an Application Programming Interface (API) to send and receive data from the computer's hardware. This ensures data integrity and reduces the chance of error.

This power can be understood by looking at how a mailing system works. In a business environment, most letters and mailers are sent out on company letterhead in a prestamped envelope. This increases productivity and reduces the risk of addressing errors. In addition, it legitimizes the message. This is because any message on company letterhead is assumed to be the real deal. The same applies to the normal way data is sent from one computer to another. By using an API, a program must use the prepackaged digital "envelopes" to pass data on to the Internet. This makes the API responsible for ensuring that the required information, such as the destination and return address, are present in each packet.

Raw Sockets, on the other hand, allows a computer program to directly access all aspects of the data in the packet. In other words, this would be the same as using a custom stamp to create company letterhead on-the-fly. Although this power would allow the sender to have more control over what information is stamped on the envelope, such as the return address, it also would increase the potential risk of error. Likewise, Raw Sockets allows its users to customize various aspects of a data packet, which increases the chance of error, be it accidental or intentional. For example, Raw Sockets gives a hacker the ability to create a packet with a fake return address.

One of the most prevalent threats Raw Sockets helps to facilitate is the infamous SYN DoS attack. Typically, a client computer initiates a conversation with another computer by sending it a packet with a SYN (Synchronous Idle Character) flag set. This tells the host computer that someone is about to send data, to which it replies with a SYN ACK (Acknowledge) packet. The client computer receives the SYN ACK packet, which tells it that the host exists and that the host is ready to receive data. The client sends one final ACK packet, informing the host computer that is received the SYN ACK, and that it is about to send data (see Figure 1).

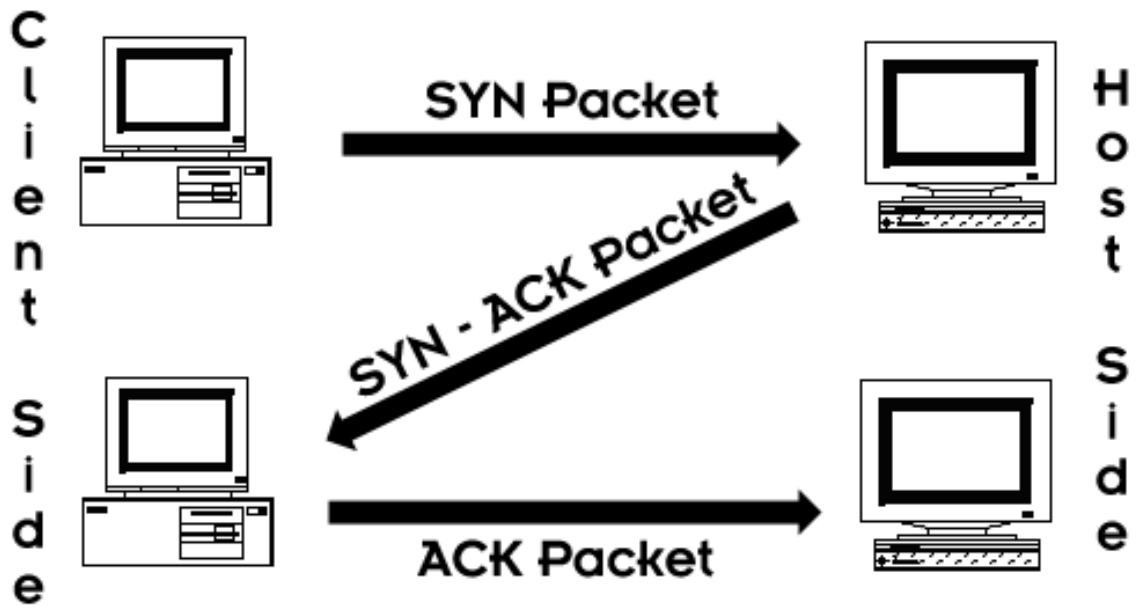

Figure 1

Normal session setup.

If a hacker had the ability to forge a packet's information, he or she could create a SYN packet with a fake, or spoofed, return address. In this case, the host computer would receive the SYN packet from the client computer (hacker), read the return address, and send the SYN-ACK packet to a fake return address. If there were no computer at the spoofed address, the host computer would sit and wait for several minutes before realizing that no one was connecting to it. However, during that time, the host computer would have a port open, waiting for a returning ACK. Because there are only so many ports available for connecting client computers, a hacker could quickly use up all of the host computer's resources (see Figure 2).

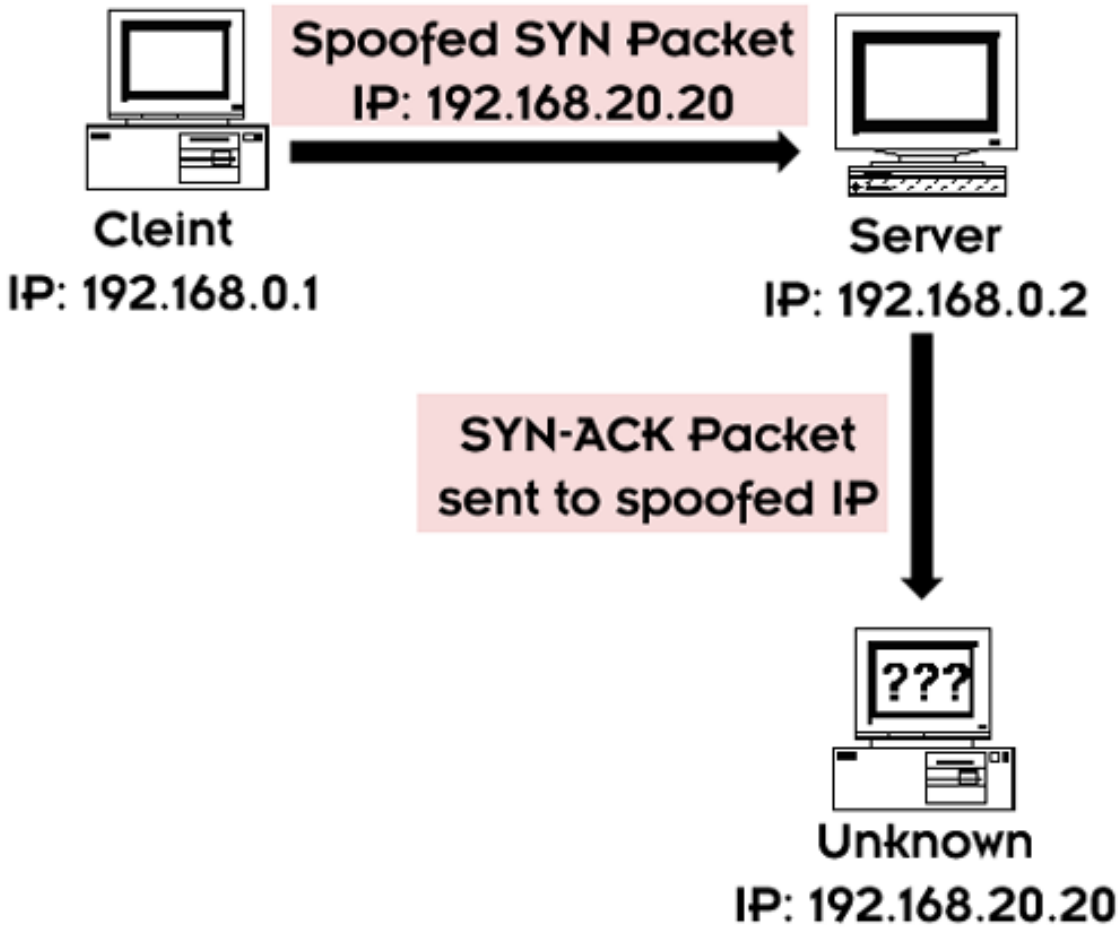

Figure 2

Spoofed SYN DoS attack.

This is the threat that Steve Gibson fears from the release of Raw Sockets in Windows XP/.NET. Ironically, soon after the release of his warning, his Web site was attacked and forced offline by another type of DoS attack that did not use any form of Raw Sockets.

The Threats

In short, there are several reasons why including Raw Sockets in Windows XP is thought to be a bad idea. This section takes a look at these concerns, and what they really mean for you. These are the summarized points made at www.grc.com:

- Raw Sockets have never been included by default with an operating system before Windows XP.

This isn't true. Windows 2000 includes Raw Socket support. In addition (and GRC finally recognized this), *every* version of Windows supported Raw Sockets with the use of a third-party program or driver. This basically means that even if Windows XP didn't include Raw Socket support, a hacker could simply incorporate this feature into a DoS program and install it into an "owned" computer. Therefore, this point is null and void.

- All other operating systems that support Raw Sockets do so only under administrator or root level access. Windows XP Home Edition is run with everyone setup as an administrator.

This is true! The Web site is 100% correct on this point, and I am *glad* it is. Basically, Microsoft is providing a piece of software that gives each and every user the full potential of what its software is capable of. In other words, is it right to restrict and control access to users of the Internet just because some people may abuse it? NO! Not even if you live in some location under governmental oppression. Now, there are some situations in which more control is necessary, and it is rightly justified. For example, the workplace has the right to control every aspect of its computing environment because the company that owns the computer is responsible for what is done on it. However, if this is needed, Windows provides other versions of XP that include the capability to lock out Raw Sockets and other less-desirable features of the operating system.

- "For the first time ever, applications running under the Home Edition of Windows XP[md]whether deliberately executed or running as hidden 'Trojan' programs[md]will be easily able, without modifying the operating system in any way, to generate the most damaging forms of Internet attacks."

I copied this as it exists verbatim on the GRC Web site simply because it illustrates the type of hype and propaganda that got this whole Raw Sockets debate going. This statement is an exaggerated and wordy way of saying a simple fact. It basically says that Windows XP Home Edition will allow a program to generate spoofed packets. Of course, so will Windows .NET, Windows 2000, Linux, AIX, SCO, Unix, Mac OS-X, and almost any other operating system out there. I wonder why this isn't mentioned.

- Windows-based, Internet attacks are common; and with the release of Raw Sockets, the attacks will be even more threatening.

At the time of the XP warning, this statement was unprovable, so it could not be verified either way. However, we are now six months after the public release of Windows XP (and more than a year since the release of Windows XP beta 1), and there has not been a single whisper of an attack taking advantage of Windows XP Raw Sockets' capability. There is no time limit for when this more threatening attack will take place, so once again no one can dispute this statement. Is this more smartly crafted propaganda?

- No previous versions of Windows had Raw Socket support, and they worked fine. Therefore, the addition of this feature is unjustified.

This is a very interesting point, and it is one of my favorites. One of the most restricting aspects of Windows was its limited power with regards to networking. Almost every other operating system supported the use of Raw Sockets. In fact, Microsoft added this feature as "[el]a response to customer demand for Winsock standard compliance." Again, isn't the point of a free market to please the customer? Do we need to be regulated and controlled based on every possible threat that exists? If that is the case, you may as well pull the plug on the Internet right now!

- Windows XP security supports legacy software that requires a limited set of restrictions. As a result, this operating system "[el]will be used to attack and damage any chosen Internet user or site."

  Again, this is a bold and prophetic statement. It also is a clever way of rewording an unprovable statement. One could say that *any* operating system will be used to attack and damage a user or site, and be technically correct. The fact that Windows XP includes Raw Socket support has no relevance to this statement. With or without Raw Socket support, Windows XP will be used to attack and damage users and Web sites.

Summary

The point of this discussion on Raw Sockets is to debunk any myth that Microsoft's choice to include Raw Sockets capability with Windows XP will result in a total crash of the Internet. To date, there have been no major DoS attacks that can be attributed to this additional feature.

When this warning was released, most of the security community disregarded it as a method of getting attention (for example, http://grcsucks.com). GRC (and Steve Gibson in particular) has been in the news before with his prophetic statements. In a 1992 article in *InfoWorld*, he predicted the end of the pattern-matching virus scanners. However, it is

now 10 years later, and pattern-matching remains the most commonly used method of virus protection programs.

For those of you are who are still concerned about Windows XP and Raw Sockets, I suggest you enable the Windows XP firewall, which was also included as a new feature to Windows XP. After the firewall is enabled, why not let Mr. Gibson test your computer using his own ShieldsUp© program? You will most likely find that the operating system he predicts as the beginning of the end for all Internet users scores a "Full Stealth!", which means that it passes his own tests with flying colors.