

TUNNELING Under

Napster and other peer-to-peer clients are giving network users a reason to violate security policies. BY AL BERG

NEWS

Napster, and services like it, has raised the ire of the music industry because it infringes on copyright restrictions. Network administrators are none too pleased with it, either, because of the bandwidth it consumes and potential security holes it opens in the network. Some companies have taken steps to block their network users from accessing peer-to-peer (P2P) clients, but it hasn't resolved the problem. Users are now finding ways to circumvent the blocks on outbound 'Net traffic through HTTP tunnels. This practice potentially creates huge security problems.

VIEWS

What harm can a Britney Spears song cause your network? After all, they say a little music is good for your soul. True enough. But when the tunes are consuming a significant amount of bandwidth, it's enough to make a network admin feel tormented for an eternity. And, as if that wasn't enough, these file-sharing clients open security holes that turn desktops into windows to your network.

Napster, Gnutella and other popular P2P programs have made MP3 music files and other entertainment packets easy to find and download off the Internet. Not surprisingly, Napster's largest audience falls in the 18- to 34-year-old bracket. It should then come as no surprise that many of these young adults are turning to their office computers, connected to the Internet via T1, T3 or DSL lines, for quick and efficient music downloading.

A network admin probably wouldn't notice if one employee was downloading a Metallica single, or even if a second staffer was grabbing the latest Faith Hill release. But it starts to become a problem when dozens of people are downloading MP3s, logging on to Real Audio or receiving live video feeds from CNN. And while employees are jamming to the Backstreet Boys or watching clips of Monday Night Football, some hacker could be using that open line to snoop through the network and steal proprietary information.

Some may say Napster is a people problem and not a technical problem. In theory, a simple policy restricting downloading MP3 and visiting certain Web sites should take care of the problem. Unfortunately, people don't always follow usage policies, which necessitates the closing of ports used by P2P clients.

But even blocking the ports used by the offending applications doesn't always do the trick. As many network admins are finding, the attraction of Napster and other such services is so powerful that users are finding ways to circumvent network defenses to get to their music. One popular way is HTTP tunneling.

HTTP tunneling defeats the restrictions by disguising forbidden traffic—telnet, POP3, SMTP and Napster—as ordinary Web browsing material. The method works because most companies allow HTTP to travel unmolested through their firewalls.

For example, let's say a network admin is blocking outgoing POP3 traffic, which in turn prevents users from accessing their outside e-mail accounts. Using the GNU HTTP Tunnel software, an industrious user could set up a tunnel on his home computer that listens to the network on port 7654 with the command "hts -F mypc:110 7654." The user would then set up the tunneling client on his office computer with the command "hts -F 110 -P PROXY:80 REMOTE:7654."

Through this tunnel, the network user could encapsulate all his POP3 traffic as HTTP and forward it to his home computer via the network's default gateway over port 80. Incoming traffic would take the reverse path and appear as a legal Web request. It's sinisterly ingenious.

The same technique could allow users to establish a proxy link to a browser outside the network, giving them an unrestricted ability to surf the Web and collect prohibited materials.

So what's the problem besides some unauthorized bandwidth pilfering? Companies implement security policies for a reason. For example, keeping users from accessing external POP3 mail servers or telnet-based applications prevents sensitive information from leaving the protection of the corporate network without a protective cloak of encryption.

The attraction of Napster and other such services is so powerful that users are finding ways to circumvent network defenses to get to their music.

Tunnels also can provide attackers with a clear channel for planting sniffers or Trojan horse programs that could eavesdrop on network activities. The tunnel is a near perfect backdoor since most firewalls allow HTTP traffic to pass through, both ways, unhindered. The attacker's traffic can also escape IDS detection because it's buried in a deluge of HTTP logging data.

Right now, there's no effective tool for detecting an HTTP tunnel or the software used to create them. However, it's possible to monitor the contents of HTTP packets, which contain clues of an HTTP tunnel. All outgoing tunnel data is placed in HTTP packets, which will contain one of seven headers. These headers

are described in the package's README file and the source code. As you can probably tell, this cumbersome and time intensive process isn't much of a solution.

The news doesn't get any better for network admins. The tunnel diggers are hard at work improving their products. Future releases are slated to include SSL encryption to foil sniffer-based detection of tunneled packets, data compression for better performance and the extension of the program to allow tunneling of connections over other protocols, including telnet and FTP.

HTTP tunnels are just another example of the continuous arms race between security professionals and attackers. A technique such as tunneling only gives credence to the need for comprehensive security solutions that include firewalls, screening, strong policies and procedures, as well as a sophisticated network monitoring system. Until then, Britney Spears fans and network admins will continue to compete for bandwidth and spar over security. ▶

AL BERG (al@al-berg.com) is a security consultant with Mentor Technologies.

Watermarks Won't Soak Napster, Yet

Could a coalition of music and technology companies thwart Napster outside of court? Not likely, at least in the short run. Although denied by the Secure Digital Music Initiative (SDMI), published reports indicate that hundreds of hackers successfully broke the half-dozen watermarks developed by the group to prevent online music piracy.

Headed up by Leonardo Chiariglione, the inventor of MP3 technology, SDMI in September challenged amateur hackers and security professionals to try to break its six security methods for protecting online copyrighted material.

SDMI placed on its Web site six songs, each containing an embedded digital serial number that acts much like a watermark does on paper money and bank checks. The group promised \$10,000 to anyone who could remove the watermark without degrading the quality of the music, and then prove the compromised file could be easily duplicated.

Despite widespread criticism among security professionals and a boycott among open-source users, the SDMI challenge drew hundreds of entries. Three days after the contest ended Oct. 8, nearly 450 breaches of all six of the watermarks were turned over to SDMI for analysis.

Chiariglione said in published reports that it's too early to say how many of the digital serial numbers were compromised, if any. SDMI is now analyzing the data supplied by the contestants to see what vulnerabilities and technical problems were uncovered. Information collected from the contest will be used to improve the watermark technology.

In the meantime, the music industry is continuing to press its court case for shutting down Napster. ▶

—Lawrence M. Walsh