

# FINANCIAL TIMES

www.ft.com

USA \$1.00 Canada C\$2.00 Bermuda \$2.25

**SECURITY AND AUTHENTICATION ISSUES** by Mark Vernon

**P2P SECURITY ISSUES**

## Network risks may emerge from within the business

## New rules needed

**From Page 4**

particular problem with P2P is that there are some hacker tools specifically developed to sniff-out types of P2P technology.

"The answer is to educate the employees to understand the problem, check for any unauthorised technology regularly and then make sure you make an example of those flaunting the rules."

However, part of the perceived security threat is false. As suggested above, the confusion arises from conflating the Napster P2P model with those more properly used as business applications. "The Napster model concentrated upon linking desktops together and replicating files, whereas P2P vendors in the business space focus upon linking servers together leaving the information where it resides while making it appear as if it is centralised," says Todd Mickelsen, vice-president EMEA at NextPage, a US-based P2P vendor.

"By its very nature, P2P encourages an open and distributed approach to data, but when P2P is transposed to businesses it is premature to assume that all approaches to P2P encouraged wild and uncontrolled access to users and data."

NextPage removes the concern by making the "peers" servers, rather than desktops, so that usual security measures can be applied.

Richard Barber, future technology architect at the specialist security consultancy Integralis, adds a further point: it actually applies to all new applications on the network though perhaps particularly to P2P since that application market is less mature. "Business-

focused applications do address security, but caution must be raised since the designer of software is the least likely to discover its weaknesses," he says. "Code reviews by external security-aware professionals is a must."

However, putting the point more positively, Alex Goodall, a technology specialist at Andersen, points out that P2P allows new kinds of security devices to be developed. "P2P changes the rules of the game, but in a neutral way," he says. "As with the internet, P2P allows more dangerous attacks on a computer system, but it also provides the capacity to create more powerful and sophisticated defences."

He foresees the deployment of intelligent agents running around networks rooting out suspicious files and viruses and informing all the computers on a network to be watchful in real time. "There will always be a competition between hackers and security experts. But P2P, if correctly deployed, should be neutral on this score," he says.

The fact that P2P operates internally within the corporate network brings advantages, too, for the very reason that it does not have to rely on firewalls.

Because the technology works within the network, businesses can keep all information and traffic within the security of their network systems without ever having to reach out to third party servers in order to connect people, says Charlie White, chief executive of US vendor eZmeeting.

Further, by exploiting P2P, solutions such as eZmeeting do not have to distribute copies of data in order to facilitate collaboration.

P2P encourages an open and distributed approach to data, but it potentially exposes the organisation to viruses and hackers when the system sidesteps security safeguards

On one level, the P2P security threat is like any other. It simply poses an additional risk as a new means of data transfer. So if you implement P2P, you add to the complexity of authenticating who is online and authorising their online activities.

But establishing authentication and authorisation is a different kind of problem in the P2P scenario since, by definition, it bypasses the server-based systems that typically perform these tasks.

"First, a business can no longer assume that other entities are who they say they are. This is the authentication problem, which can be solved with stronger forms of identification such as digital IDs," explains Colin Wyatt, senior vice president and managing director, Entrust EMEA, an internet security software vendor.

Second, businesses "can no longer simply allow other entities indiscriminate access to the applications they use and the information they manage", he adds.

"This is the authorisation problem, which can be solved with a security policy and an entitlements-based system."

In short, P2P applications designed for business use contain authentication and authorisation functionality that is robust enough for unexceptional daily use.

But the P2P threat has a pernicious dimension, too. P2P potentially exposes the organisation afresh to viruses and hackers because it sidesteps network security systems, notably firewalls. Butler Group analyst Mike Davis explains: "P2P communications protocols remove the need for the enterprise server to be involved, but this also means that the

security systems on the servers are by-passed, including virus checkers."

In other words, the use of P2P networks provides an opportunity not only for malicious software to propagate, but also for the exploitation of communication protocols by malicious software.

The immediate security response is to use a scanning solution that constantly monitors what is travelling into the PC, a facility that most anti-virus programmes include.

However, desktop protection may not prove to be the best method in the future, and network scanning may become more desirable, says Andre Post, researcher at Symantec Security. The

point here is technical. Scanning may be fine inside the firewall, but most network security assumes the threat stems from outside of the organisation.

"The P2P risk is when the threat is inside the organisation and, say, opens a port through the firewall to another machine outside, leaving an unmanaged gateway to the organisation's network," says Mr Davis. Thus, network monitoring as a whole is advisable.

Another source of risk comes from the purely human. Because of its association with Napster, P2P looks "cool" to some, though they may not realise how their enthusiasm for a P2P device can compromise corporate networks, if installed on office systems.

"The fear is very real," says Matthew Norris, technology underwriter at Hiscox insurers. "Unauthorised P2P is another unauthorised technology which could well introduce as large a security hole as an employee setting up their own modem. The

**Turn to Page 6**

### There's more on the web

Expanded, interactive coverage of peer-to-peer computing – plus other main themes in this issue of the FT-IT Review – is available at our website, [www.ft.com/ftit](http://www.ft.com/ftit)