

Building trust back into computing

By Alan Pedersen

The IT industry has started to see a shift in priorities, placing more emphasis on the privacy and security of products. Speaking at PL&B's Annual International Conference in July, Richard Noakes, of Microsoft UK, outlined his organisation's vision of 'trustworthy computing'.

Web-based services have been hailed as the future for information technology, fundamentally changing the way in which organisations do business online. In a nutshell, web services are applications (customer/enterprise relationship management packages or human resources systems) delivered over a platform (the World Wide Web).

According to the marketing hype, web services allow companies to break down applications into bite-sized chunks and choose which parts they want to use, decide how little or how often they want to use them, and save themselves a fortune into the bargain. According to John Noakes, we are headed towards the "drag and drop, plug and play world of switching on and switching off application services that [we] may only need to consume for a few minutes, a few hours, or a few weeks."

These web-based applications have also been developed for public consumption, allowing Internet users to access web e-mail, personal organisers, and online gaming - as and when they want.

WHAT IS THE COST?

As is often the case with new technology, the emerging world of web services comes with a sting in its tail, which, according to Noakes, brings with it a "new emphasis of privacy, security and availability of information." This emphasis has created a new industry buzzword - "trust". But the idea of trustworthy comput-

ing is a phrase that Noakes feels is little understood in business today. Certainly, when it comes to issues of trust, Microsoft has had its fair share of publicity. Only recently, it settled with the US Federal Trade Commission after allegations that the IT giant misrepresented the security of its Passport authentication service (see p.15). "We know we've got a big job to do," said Noakes. "Trustworthy computing and Microsoft - they are not happy bedfellows, you might say."

"It's not something we can fix tomorrow, next week, next month, not even next year. It's a 10-15 year effort."

Achieving trust is no easy task, said Noakes, but a vital one nonetheless. "We have a duty to make our software as secure as possible." However, he accepted that it is nearly impossible to achieve 100 per cent success. "A perfectly secure piece of software code has never been written and quite frankly will never be written...Bugs will always exist. But what we can do, is try and minimise the amount of bugs."

DEFINING ONLINE TRUST

Trust is a difficult concept to define accurately, said Noakes. Consumers' definition of trust will vary according to the software or programmes they use and their priorities or preferences. Some may not trust a company because of security flaws in its services. Some may not trust their information to be used correctly. Others may simply lose trust in applications that do not function properly.

Microsoft's vision of 'trustworthy computing' is broken down into three components: security, privacy, and availability. Noakes used the ubiquitous rise of the ATM machine as an example of how these three components work to create trust. An ATM machine, he explained, has to ensure transactions are made secure and private, but it is also important to make the service available. If customers cannot access their money, or read their bank statements, they will not use the service.

MISCONCEPTIONS OVER NET PASSPORT

Noakes said that Net Passport, Microsoft's online user identification and authentication service, has been misunderstood. One of the main misconceptions, he explained, was that it collects an excessive amount of personal information that is then passed onto third parties. The idea behind the project, he said, was to offer

Internet users access to a range of Passport participating websites without requiring them to remember multiple usernames and passwords. This in itself, he argued, helps protect information since poor control of passwords is recognised as one of the weakest links in the security chain.

Rather than collecting too much data, Noakes argued, Passport only requires a username and password for customers to access sites. The service also places the user in control of their personal information, he said. If any additional information is provided, users have to pro-actively opt-in should they want to receive marketing information. Customers can choose the sites with which they will allow their information to be shared.

TRUST IS A LONG TERM GOAL

Gaining trust in online services is an area in which the whole of the IT industry needs to sit up and take notice, warned Noakes: "It's not just about Microsoft, it's an industry-wide challenge...It's not going to be quick and it's certainly not going to be easy. It's not something we can fix tomorrow, next week, next month, not even next year. It's a 10-15 year effort."

Microsoft has already started the ball rolling. In January of this year, Microsoft unveiled its "trustworthy computing" initiative. In a memo to 50,000 staff, Bill Gates spelled out the organisation's new priority: "We've made our software and services more compelling for users by adding new features and functionality...but all those great features won't matter unless customers trust our software," said Gates.

PRIVACY INITIATIVES

On the privacy front, Noakes cited a number of existing initiatives. They include the creation of a corporate privacy department, signing up to the US Safe Harbor programme, and implementing privacy features in Microsoft's latest web browser. He stressed Microsoft's ongoing commitment to allowing customers greater control over access to their information. The organisation is also in the

process of rolling out corporate privacy guidelines for its subsidiary operations, and is developing an online privacy statement generator for businesses.

Noakes said that Microsoft has already taken 9,000 developers out of their jobs to provide them with training in security. This, he said, is an unprecedented commitment to addressing security issues. "No other company of our size and structure has made anywhere near that level of commitment."

Future projects, said Noakes, will take some time to develop. For example, the recently announced Palladium project (Microsoft's plan to fuse software and hardware security to provide greater protection) will not hit the market for at least another seven years, he said.

In summing up his speech Noakes reinforced Microsoft's commitment to trustworthy computing. "We know we've got more work to do," he said. "But we're an open company, we listen to ideas. There are multiple examples of us doing what the market requires...Without trust we can't really go any further as an industry."



Richard Noakes is Net Policy and Regulatory Affairs Manager for Microsoft UK.

For more information on Net Passport, see: www.passport.com

For Microsoft's Palladium project: www.microsoft.com/PressPass/features/2002/jul02/0724palladiumwp.asp

Bill Gates memo on trustworthy computing can be found at: www.wired.com/news/print/0,1294,49826,00.html

Microsoft – A privacy timeline for 2002

January 15th – Microsoft Chairman, Bill Gates, announces the organisation's new 'trustworthy computing' initiative. Software developers are instructed to make security, privacy and availability a priority, taking precedence over features and functionality.

May 7th – Fritz Bolkestein, Director of Internal Markets at the European Commission, confirms that the Commission is to look into claims that Net Passport, Microsoft's online authentication service, violates EU data protection laws.

June – Plans to develop a new security architecture are announced. The Palladium project aims to fuse encryption-facilitating hardware with security and authentication software. The goal of the project, according to Microsoft, is to create a kind of virtual vault providing users with "greater data security, personal privacy, and system integrity."

July – Privacy advocate Caspar Bowden joins Microsoft as its Senior Privacy and Security Officer for Europe, Middle East and Africa.

July 2nd – The Internet Task Force, a subcommittee of the EU Data Protection Working Party, concludes that a number of elements of Net Passport raise legal data protection issues. Following an initial probe into the service, the task force confirms that it will carry out further analysis.

August 8th – Following a year-long investigation by the US Federal Trade Commission, Microsoft announces a commitment to improving security of its Net Passport service. As part of a 20-year settlement the organisation also agrees to be subject to a third party compliance audit every two years (see p.15 for full story).