

available at [www.sciencedirect.com](http://www.sciencedirect.com)journal homepage: [www.elsevier.com/locate/cose](http://www.elsevier.com/locate/cose)


---



---

**Computers  
&  
Security**


---



---



## Microsoft's new window on security

Danny Bradbury

---

### ARTICLE INFO

#### Article history:

Received 14 July 2006

Revised 18 July 2006

Accepted 18 July 2006

---

#### Keywords:

Vista

Operating system

Security

Kernel

Legacy

---

### ABSTRACT

Microsoft may be trying to escape from its past by building new security features into its next operating system, but it has been forced into some compromises.

© 2006 Published by Elsevier Ltd.

Few operating systems have been as widely anticipated as Microsoft's next major version of windows. Vista, originally supposed to ship this year, will now ship to consumers in 2007, with a corporate version shipping in November 2006. It will be the most heavily marketed system since Windows 95, which is fitting, given that it was the introduction of that system that heralded the start of Microsoft's security woes.

Prior to Windows 95, Windows was essentially a stand-alone operating system. It did not even include its own TCP/IP stack. Instead, customers had to buy them off the shelf. Windows 95, with its bundled browser, was Microsoft's response to the evolution of the Internet and the Web, which it had largely ignored until that point.

Trying to build an Internet-capable operating system on the foundations of one not designed for it had severe implications for security. The company's huge market share led to a monoculture on the desktop which malware writers, suddenly faced with the convenience of Internet-based distribution, were happy to exploit. These factors, along with vulnerable code and inadequate software patching mechanisms, created the conditions for a perfect storm, and the image of the operating system has corroded badly over the past decade.

Vista is supposed to stop the rot. Microsoft is marketing the operating system as the first version of windows to be fully

developed under its Secure Development Lifecycle. The SDL is a secure software development process introduced in 2002 after Bill Gates, piqued by increasing security problems, instigated a three-month code freeze while the company sent its developers back into training.

The tension over Vista has been showing. The firm first began shipping Vista 'bits' to developers in October 2003, and promptly began changing them removing key elements such as the WinFS object-oriented filing system. Almost three years on, it has been delayed multiple times and still is not ready. "We will never have a gap between Windows releases as long as the one between XP and Windows Vista; count on it," soothed CEO Steve Ballmer publicly in July, on the same day as outgoing chief software architecture Bill Gates stoically predicted a 20% chance that the new operating system would be delayed past January.

The biggest delay in Vista has been caused by its security requirements, and the fact that the development team had to work with a large established code base. Changing the operating system while retaining compatibility with existing applications has been one of the toughest challenges, and that is why Microsoft implemented User Account Control (UAC).

Previous versions of Windows offered user accounts with different privileges. Ideally, users would log in using the

---

E-mail address: [danny@itjournalist.com](mailto:danny@itjournalist.com)

standard account, which restricted their ability to carry out certain tasks. Most of the time, however, they logged in using administrator-class accounts, which gave them full access to the system, because otherwise much software would not work. "A lot of developers have written code while running in administrator mode themselves, so the software doesn't cope very well," explains Steve Lamb, technical security evangelist at Microsoft.

Just as applications running in administrator mode have more access to system resources, so does malware running under the same account. Consequently, accounts running in administrator mode have been vulnerable to attack by worms and viruses. This has been partly responsible for the rise in botnet activity in the past five years.

UAC, turned on by default, attempts to get around the problem by enabling standard user accounts to perform tasks traditionally restricted to administrator accounts, requesting an administrator password at the point of execution. Users of administrator accounts running in a new 'approval mode' are also required to confirm execution when they attempt actions requiring greater privileges.

UAC has angered analysts, who argue that simply throwing dialogue boxes at users will desensitize them rather than providing any real security. They will become an irritation that people click through without even reading. Microsoft has taken steps to improve things in Vista beta two, but Andy Walker, author of 'Windows Vista Helpdesk', remains unconvinced.

"In beta 2 they haven't done a good job at solving that problem," he warns. "It's not crashing and asking you for approval when you're doing simple tasks like changing the time, but if they ship beta two with UAC the way it is, it will be a disaster."

Even Microsoft admits that some steps taken to fix legacy application support in Vista are a kludge. It uses file system and registry virtualization, so that when a legacy application attempts to write to the system registry, for example, it creates a copy of the file in the user's profile. "Although virtualization allows the majority of legacy applications to run, it is a short-term measure—not a long-term solution," says the TechNet documentation. "Not only can a lack of compliance with User Account Control affect the security of an application, but it can also reduce the application's performance, require additional end-user training, and cause application conflicts."

The same could be said for the anti-phishing features in Internet Explorer 7, which will be an integral part of Vista. The site checks URLs that the user attempts to visit against a centrally-maintained list of known phishing URLs. It also uses behavioural analysis to look for suspicious activities, such as collecting user information without an SSL certificate. If it finds a phishing site, it alerts the user.

However, *Why Phishing Works*, a study by analysts at Berkeley and Harvard University, found that 23% of users ignore browser cues designed to warn against phishing. And SSL's security is questionable – it is relatively easy to obtain an SSL certificate without being verified as a legitimate company.

Microsoft has taken some other, more effective security steps with its Bitlocker drive encryption technology. The system, which came out of the Next-Generation Secure Computing Base (NGSCB) originally announced in 2003, is designed to

stop unauthorised access to a hard drive (in the event of a laptop theft, for example). It also checks the integrity of system files during startup to ensure that the system has not been tampered with.

Computers with the Trusted Platform Module (TPM), a hardware-based anti-tampering mechanism designed to store protected information, get full volume encryption using an AES encryption key created by the hardware. The key can be either 128 or 256 bits long depending on how the option is set in Windows Group Policy.

Users also get the option to store the encryption key on a USB drive for two-factor authentication, although a recovery password (hopefully protected by the IT department) can be entered during bootup, should the USB key be lost. Bitlocker will only ship on high-end versions of Vista to avoid problems with consumers losing their passwords, says Lamb.

Talking of passwords, Microsoft has removed the Graphical Identification and Authentication (GINA) logon architecture so familiar to Windows users. The company has replaced it with a platform enabling developers to extend the logon screen to support different credential types, such as smartcards and biometric readers. Previously, companies had to rewrite the GINA interface to achieve these goals, and Microsoft hopes that the new system will push companies towards strong authentication, which is a requirement under the US Sarbanes Oxley corporate governance rules. The new credentials system has other possibilities, says the company, such as requiring the same strong authentication to access corporate resources (users could be required to scan their fingerprints or submit a smart card to access a particularly sensitive back-end database).

One of the more promising security features within the system is Address Space Layout Randomisation. Because malicious code has sometimes co-opted executable code in other areas of the system, Vista will move the code around to one of 256 random locations in an attempt to obfuscate it and prevent it being exploited. In a related move, the company also introduced better heap buffer overflow protection for the operating system. Applications will often try to stuff the system buffer with data so that it overflows into executable areas of memory. Now, when the operating system detects this, it can automatically terminate the offending application. A single API call also allows third-party developers to use this feature.

But in a sense, third-party developers are one of Microsoft's biggest problems. Badly written drivers are a major source of Windows reliability problems, for example. A mandatory driver signing feature in Vista will mean that drivers running in kernel mode (typically hardware drivers, working with resources closer to the heart of the operating system) have to be digitally signed. By forcing developers to sign the code with a digital certificate, Microsoft hopes that this will make it easier to identify and work with those driver developers whose software needs extra hardening, in a bid to increase security.

However, this does not add up; Lamb says that according to Watson, Microsoft's online system for collecting information about system crashes, the significant percentage of system errors are caused by a handful of drive vendors, which suggests that it already has a handle on the offending parties.

The real challenge seems to be teaching them to code properly.

Moreover, driver signing will only be mandatory for 64-bit systems, because Microsoft's priority was to make Vista backwards compatible with 32-bit code, and there are so many unsigned 32-bit drivers already on the market that the recompilation task would have been too disruptive. So for 32-bit system users (by far the majority of current users), little will change and anonymous system drivers will still fail.

The same is true of the Patchguard feature, which stops software from patching the system kernel (replacing parts of the core system kernel with third-party code). Kernel patch protection only works on 64-bit systems, and even then, some of this functionality only works on certain processors. For example, the operating system will prevent software from modifying certain kernel resources on all 64-bit processors, but it will only stop software from patching any part of the system kernel when running on an AMD 64-bit processor. As Lincoln might have said of Vista, you can protect some of the processors all of the time, and all of the processors some of the time, but you cannot protect all of the processors all of the time. And if you are running a 32-bit chip, all bets are off.

Imagine a developer trying to climb out of a deep hole while dragging a huge, heavy bag, and it would be an accurate picture of Microsoft's predicament. It wants to solve the security problem and it knows how to do it, but it is haunted by its mistakes because it has to support its legacy code base. The alternative for the company would have been to redevelop the operating system from the ground up without support for its legacy code base, but this would have stifled the uptake of an operating system – a dangerous move, given that the client OS business constitutes almost a third of the company's revenue.

"They could have released XP service pack 3, 4 and 5 and moved Vista forward as a new code base," argues Walker. That way, the company could have gradually eased companies away from the legacy system over a longer period, while

continuing to promote the benefits of Vista. That ship has sailed, however, and the product's security has suffered as a result.

Paradoxically, Microsoft's other security-focused activities could also place its users in jeopardy. It is attempting to build a managed services hegemony in the security area. Windows Defender, its anti-spyware service, will ship with Vista, while customers will be given the option to buy OneCare, its consumer-focused anti-virus and security scanning service, at a price lower than most competitors. It is also building a set of integrated managed security services for the enterprise with its ForeFront and Exchange Hosted Services products.

The danger there is that when a company provides a range of security products designed to protect its own operating system, it extends the monoculture that helped to create the security problem in the first place. Using different anti-virus and anti-spyware products that those provided by the operating system vendor might help to product a varied security portfolio using different engines to help capture larger numbers of malware variants and other attacks.

In spite of the compromises that it has made, Microsoft is making a valiant effort to protect the next version of Windows, and its huge existing user base. The company is nevertheless trapped; it continually promotes the virtues of change and forward mobility, but it is constrained by its history. It is fitting that the company has chosen to delay the shipment of the operating system until January 2007. In many ways, Microsoft is like the two-faced Roman God Janus, the Roman God of doorways and passages, after whom the month was named. That God, like Microsoft's developers, gazed longingly both at the future and at the past.

**Danny Bradbury** is a freelance journalist, who started out writing about computers and business in 1989. He began writing on a magazine for computer resellers before moving to *Personal Computer World*, a consumer magazine about PCs. He left in 1993 to work at *Computergram*, a daily newsletter for the computer industry, and then became technical editor on *Unix News* magazine.