# Windows 2000: A Threat to Internet Diversity and Open Standards?

**David Chadwick,** University of Salford

Recently, Microsoft launched Windows 2000 (formerly known as NT 5.0) with huge fanfare. A late arrival and significant new features and benefits don't differentiate Windows 2000 from most large software development projects or new operating system releases. The trait that sets Windows 2000 apart is its focus on the Internet.

Microsoft conceived Windows 2000 as the operating system for the Internet. This gave many people pause, what with Microsoft's less-than-sterling reputation regarding cohabitation of competitors' software on their operating system. The Internet is based on open standards and interworking between different systems from different suppliers. If Windows 2000 compromises the Internet's integrity and ubiquity—two of its primary hallmarks—will it really be the best operating system to base your Internet services on?

Some of the new additions to Windows 2000 show that, although Microsoft pays lip service to the Internet's sacred tenets of openness and support for standards, it has actually (and sometimes only subtly) removed or subverted these tenets.

## DNS DYNAMIC UPDATES

The Domain Name System (DNS), for a long time the core to the functioning of the Internet, is now also core to the functioning of Windows 2000. New Windows services announce themselves to the network by adding themselves to the DNS service via dynamic updates and SRV **(**service**)** records. Clients find the services they need by querying the DNS.

This replaces the Windows Internet Naming System service with an open standards-based service, which is a good thing, because WINS is proprietary. Both of these features (dynamic updates and SRV records) are specified in the Internet Engineering Task Force's Request for Comments (RFC) 2136 and 2782. And Microsoft claims that you can continue to use your existing (non-Microsoft) DNS service, provided it either supports SRV records and dynamic updates or you can manually add these records yourself.

## POTENTIAL SECURITY BREACHES

Microsoft, however, fails to make it sufficiently clear that dynamic updates to a DNS service leave you open to security breaches via the Internet, unless you can tightly control who can update your DNS service. This problem necessitates strong client authentication. A proposed Internet standard (RFC 2137) addresses this problem, using digital signatures for authentication.

Unfortunately, Microsoft does not support this function. Instead, Windows 2000 supports Kerberos v5 for client authentication, which also happens to be an Internet proposed standard (defined in RFC 1510). Microsoft has subtly altered Kerberos v5 so that it will not properly interoperate with other standard Kerberos v5 implementations. Microsoft Kerberos v5 servers will interoperate with non-Microsoft standard v5 clients, but Microsoft v5 clients will not interoperate with non-Microsoft standard v5 servers. So if you use Microsoft's tweaked version of Kerberos v5, you can verify non-Microsoft clients, but if you're using your own server security, you can't verify a Microsoft client. The result: You have no standard way of strongly authenticating Microsoft clients that wish to dynamically update your existing DNS servers. Consequently, you must either replace your existing DNS servers with Microsoft DNS servers, accept that you will have to manually configure your existing DNS servers with the Microsoft servers and services, or run both sets of DNS servers together.

The Windows 2000 changes appear to subtly exclude technologies from other vendors and make interworking more difficult.

And that's not all. Microsoft has added some proprietary extensions to its DNS server to allow it to delete these dynamically added SRV records once they become stale. So if you decide to use your existing DNS server instead of Microsoft's DNS server, you will have to manually delete the stale SRV records, increasing your management overheads. No wonder Micrsoft strongly suggests you use their DNS server.

## ACTIVE DIRECTORY

Active Directory is another example of incomplete support for Internet standards. AD is meant to be a directory server that conforms to the Lightweight Directory Access Protocol, competing with established LDAP directories from Netscape/Sun, Novell, IBM, and Lotus. AD is tightly integrated into Windows 2000, and no standard LDAP server can replace it. This is because many of the operating system calls to AD use proprietary dynamic link libraries (DLLs), not an open LDAP interface. RFC 1823 already specifies an open application programming interface defined for LDAP version 2 directory services. And the IETF's LDAP-Ext working group has nearly finished specifying an LDAP version 3 C API and a Java API.

But Microsoft hasn't used the IETF-specified APIs as the preferred means of open external access to AD (and vice versa). Microsoft instead created its own proprietary API: the Active Directory Service Interfaces. They advertise ADSI as "a single, consistent, open set of interfaces for managing and using multiple directories" so that "applications can be developed with no need to understand vendor-specific directory APIs." (PBS Web Team, "Microsoft Active Directory Service Interfaces: ADSI Open Interfaces for Managing and Using Directory Services," Microsoft Corp., Redmond, Wash., 1999.) Microsoft fails to mention that other directory vendors will need to build an ADSI interface to their directory service if they want newly developed ADSI directory-enabled applications to access them. This forces other directory vendors to support a Microsoft proprietary API in addition to, and perhaps in preference to, an open standards-based LDAP API.

## LDAP SERVICES

Many organizations have already spent millions of dollars installing their existing LDAP-based directory services, with Novell's NDS and eDirectory having the largest installed base. When Microsoft released Windows NT 4.0 with its internal directory and registry, Novell cleverly rewrote the DLL used to access the Microsoft registry so that it accessed NDS instead. An organization could then add its NT 4.0 servers to its Novell network and directory service, while the operating system continued working as though it was still accessing the local registry.

Microsoft put a stop to this in Windows 2000, which checks all the DLLs present. If it finds a non-Microsoft DLL, Windows 2000 deletes and replaces it with the Microsoft DLL. At a recent pre-

### Terms and Definitions

- *Domain name system:* The DNS is the way that Internet domain names are located and translated into Internet Protocol (IP) addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.
- *Windows Internet Naming Service:* Part of the Microsoft Windows NT Server, WINS manages the association of workstation names and locations with IP addresses, without the user or an administrator having to configure each change.
- *Request for comment:* An Internet formal document or standard that results from committee drafting and subsequent review by interested parties, some RFCs are only informational in nature. Of those that aim to become Internet standards, the final version of the RFC becomes the standard and the committee permits no further comments or changes. However, subsequent RFCs can supercede or elaborate on all or parts of previous RFCs.
- *Kerberos v5:* Kerberos is a secure method for authenticating a request for a service in a computer network. Kerberos lets a user request an encrypted "ticket" from an authentication process that can then request a particular service from a server.
- *Active Directory:* AD is a new directory service component in Windows 2000. A directory service is middleware that identifies all resources on a network and makes them accessible to users and applications. Resources include e-mail addresses, public key certificates, computers, and peripheral devices such as printers. Ideally, the directory service should make the physical network topology and protocols transparent so that a user on a network can access any resource without knowing where or how the resources physically connect.
- *Lightweight Directory Access Protocol:* A set of protocols that accesses information directories, LDAP is based on the standards contained within the X.500 standard, but is designed to run directly over TCP/IP. LDAPv3 is the latest version being standardised by the IETF.
- *Java Application Program Interface:* Constructed with Java, this API is a set of routines, protocols, and tools for building software applications. A good API makes it easier to develop a program by providing all the building blocks. A programmer puts the blocks together.
- *Analog Display Services Interface:* The standard protocol for enabling alternate voice and data services, such as a visual display at the phone, ADSI operates over the analog telephone network. ADSI enables devices such as special telephones with small display screens, cable TV set-top boxes, personal digital assistants (PDAs), pagers, and personal computers with telephone applications.
- *Novell Directory Services:* NDS manages access to computer resources and keeps track of the network users, such as a company's intranet, from a single point of administration. Using NDS, a network administrator can set up and control a database of users and manage them using a directory with a graphical user interface. Network administrators can add, update, and centrally manage remote users. The latest version of NDS is called eDirectory, and supports an LDAP interface.
- *Dynamic Link Library:* A DLL is a collection of small computer programs, any of which a larger program can call up when necessary.

sentation I attended, the Microsoft speaker stated that they made this change because non-Microsoft written DLLs were causing the NT 4.0 operating system to become unstable. And since Windows 2000 had to be very stable (operating 24 hours per day, 365 days a year), it could not tolerate foreign DLLs that might compromise its stability. The speaker then added that Novell was experiencing difficulty overcoming this feature as they attempted to help organizations replace AD with eDirectory.

Will Windows 2000 compromise the Internet's diversity and the ability of thousands of different suppliers' systems to interoperate?

## MORE LDAP MISCHIEF

Microsoft has also played more mischief with LDAP. LDAP directories have a standard schema—the set of rules that govern how the directory structures its data. Various RFCs and ISO/ITU-T standards (like X.520, RFC 1274, RFC 2218, RFC 2252, RFC 2256, and RFC 2587) specify standard schema definitions. However, Microsoft purposefully changed some of the standard schema definitions, and it does not support others that are currently being standardized.

For example, one of the most popular directory attributes, the Internet RFC 822 e-mail address (specified as early as 1991 in RFC 1274), boasts support from all existing LDAP- and X.500-based products. However, Microsoft used the same syntax as standard definition but gave the schema element a new Microsoft-derived object identifier. (Each schema element has a globally unique object identifier to ensure that different implementations can determine when they are referring to the same data object).

In addition, Microsoft redefined the ISO/ITU-T standard definition of object class top (from which all other object classes are derived) by adding more than 60 Microsoft-specific attribute types. Microsoft then still used the same ISO/ITU-T object identifier to uniquely identify its proprietary definition. This will clearly cause internetworking problems for replicating data between AD and other LDAP directories. I understand that Microsoft has agreed to reverse this decision in a future release of AD and to reinstate the ISO/ITU-T standard definition.

Despite these obstructions to a truly ubiquitous existence, Windows 2000 has many good features, and it is undoubtedly an improvement over NT 4.0 for many reasons I do not discuss here. However, will Windows 2000 compromise the Internet's diversity and the ability of thousands of different suppliers' systems to interoperate? Given that Windows 2000 seems to drive organizations to replace their existing DNS and LDAP servers with Microsoft products, Microsoft clearly intends to dominate the Internet server market as much as it has the desktop. However, too many systems using the same supplier's software and hardware is dangerous—witness the havoc recently wrought by the Love Bug virus exploiting features in Outlook. As an analogy, imagine what one virus could do to a human race cloned from one individual.

Diversity must be one of the Internet's main strengths, just as it is for the human race. It will be interesting to see whether the Internet becomes a Microsoft dominated network, using Microsoft controlled "open" standards, or whether diversity and consensual open standards will continue to retain the upper hand. ✷

*David Chadwick is a senior lecturer at the University of Salford and an active participant in IETF standardization activities. Contact him at D.W.Chadwick@salford.ac.uk.*

**Editor: Gary Robinson, technical director, Industry Standards, EMC Corp., PO Box 9103, Hopkinton, MA 01748-4103; g.robinson@computer.org**