Global Information Assurance Certification Paper

Should You Use Microsoft Passport, .NET, and .Net My Services?
By Richard Zurlnick

This report details certain security risks and potential defects of the Microsoft Passport Service, .NET, and .NET My Services and considers the conduct of the Microsoft Corporation This is a particular technology that has legal and regulatory ramifications. A proposal addressing these issues is included.
Passport and .NET are being promoted heavily at the time if this writing. Passport is a single sign-in authentication service for .NET, designed for consumers and Web merchants. A user can authenticate once through Passport and for the remainder of that session, the user will be automatically be permitted access to other secure .NET Web sites. Consumer information can be stored by Passport so that credit card numbers and shipping addresses will automatically be transferred to the Web merchant when a user makes a purchase. Currently, users of Hotmail, MSN Messenger and Microsoft Certified Partners are required to use Passport. Other services such as My Calendar, My Wallet, My Address, My Profile My Contacts, and My Notifications, will be tied to Passport. At this time, Passport is available at no charge to users.
In the future, Passport will be the single sign-in for .NET My Services (formerly named Hailstorm) that will launch in 2002. All users and companies will pay a fee to use .NET My Services. It will permit users from any company or to communicate with users from any other participating company regardless of the applications or systems native to each. In this way, business can be conducted without forming custom templates for invoices, databases etc. The information and services will be available from a range of devices including hand held devices and cellular phones.
Passport and .NET use the following nonproprietary programming standards: [i] [ii]

1. XML: Extensible Markup Language
   XML uses symbols to describe the contents of a page or file, as does HTML. However, XML describes the content according to the data being presented, not just how it is displayed. XML can be used to by disparate systems across the web to interchange data.

2. UDDI: Universal Description, Discovery, and Integration
   UDDI is a registry service designed to act as a sort of telephone book for the Internet. Any business can list themselves by name, product, location, or the Web services they offer. The goal is to allow businesses to find each other easily on the Web and interact with each other without incompatibilities.

3. SOAP: Simple Object Access Protocol
   SOAP provides an avenue for different operating systems to communicate with a common program by standardizing how HTTP headers and XML files are encoded. Thus, a Windows computer can call a program in a Linux computer over the Internet and then pass and retrieve data.

4. WDSL: Web Services Description Language

WDSL is an XML-based language that specifies the services available at a business and provides a method for others to access to those services over the Internet. It supports UDDI.

The security aspect of .NET is founded on the Microsoft Passport authentication service. On September 21, 2000, Microsoft announced that Passport authentication will be handled by the Kerberos system. Kerberos was invented at the MIT Institute, and is freely available with copyright provisos similar to that of the BSD operating system. Kerberos issues time limited, encrypted tickets to users who can then move from service to service without reauthenticating. Each time a user switches to a new service, Kerberos issues a new ticket based on encrypted information from the client.

Kerberos is well maintained and is likely the best choice for .NET, but it is vulnerable. A visit to the Kerberos home page security section reveals a litany of vulnerabilities that affect it.[iii] The bugs range from buffer overflows to root vulnerability to denial of service attacks. The CERT/CC (Carnegie Mellon Emergency Response Team Coordination Center) states in Advisory 2000-06 "If vulnerable services are enabled on the Key Distribution Center (KDC) system, the entire Kerberos domain may be compromised."[iv] When corporations and ordinary users trust it in the .NET paradigm, the attacks on Kerberos and its integrity will increase in number and severity.

Microsoft has altered Kerberos with its own proprietary extensions that can potentially cause compatibility issues with non-Windows servers. At issue is a digitally signed PAC (Privilege Attribute Certificate) added to Kerberos by Microsoft that is not compatible with the DCE (Digital Computing Environment), an agreed upon standard by which computers can exchange data and use applications through networks.[v] Microsoft itself states, "UNIX systems using MIT's Kerberos implementation need some special configurations to be able to participate in a Windows 2000 domain using Kerberos authentication"[vi]

There is a potential Denial of Service to Windows clients attempting to receive authorization to use services from a non-Windows server because not every company or organization will install a Widows proxy server or perform the configuring and mapping necessary to become compatible with the Microsoft version of Kerberos.[vii] Such companies and organizations may be denied a certificate to be in the "federation of trust" by Microsoft and therefore not eligible to participate in the Passport system.

Microsoft has subverted a freely available and widely used authentication protocol by requiring proprietary modifications in any non-Windows server.[viii] This becomes a serious issue when, as Microsoft plans, Passport becomes the dominant authentication service on the Internet. Windows XP makes no fewer than 5 attempts to convince a new user to sign up for Passport.

During the final editing of this report, Microsoft announced that it would use an industry standard version of Kerberos. The point can still be made though, that the first inclination of Microsoft is to use its monopoly position to exclude competitors.

It is still true, however, that while Passport will have no trouble authenticating users, the PAC can prevent users from receiving authorization to services offered by non-Windows servers.[ix]

Passport itself has several known vulnerabilities. Dave Thomas of Bugtoaster, the software quality assurance company inadvertently discovered a security hole when using

Passport with Windows 95/98 machines. The client DUN (dial-up networking) uses a shared API (Application Program Interface) to summon the Passport credentials from an encrypted file. When the user logs into the Passport Data center, the API passes the username and password in clear text from one process to another in a known memory area specified by the API for Windows. An attacker can easily write a worm designed to retrieve and transmit the credentials thereby compromising the user's data and possibly their finances.

Windows 2000 and NT do not pass unencrypted login information through memory but are still vulnerable. Steve Gibson, who heads the computer security firm of Gibson Research (**http://.grc.com**,) states that an attacker can write a worm that records keystrokes from any version of Windows and transmit the results which include the username and password.[x]

Microsoft has an infamous reputation for deficient security. The following incidents illustrate its inadequate enforcement of its own security policies:

On March 22, 2001, an individual who falsely claimed to be a Microsoft employee used social engineering techniques to convince Verisign Inc. to issue official digital certificates with the common name "Microsoft Corporation". An attacker can use these certificates to distribute malicious code that professionals and ordinary users would trust as genuine Microsoft code. In particular, the Class 3 certificates convey the ability to sign executable content including ActiveX controls, Office macros, and other software. Potentially, the greatest harm can come from ActiveX and Office macros because both can be sent as either web pages or HTML mail.[xi]

Was Verisign at fault? Yes, but Microsoft hired Verisign to ensure the security and integrity of its certificates. Microsoft must have procedures in place to test the security of not just its products, but also the agents assigned to distribute them.

On April 25, 2001, Microsoft Product Support Services (PPS) issued an advisory bulletin concerning certain security hotfixes available only to its Premier Customers and Gold Partners. From April 6, 2001 to April 23, 2001, Microsoft hotfixes downloaded to these specific customers had been infected with the Funlove virus.[xii]

This is a similar situation to the Verisign incident as it was a third party who distributed the hotfix.[xiii] Microsoft must accept responsibility for damage done to its customers by the missteps of its officially sanctioned agents. Third party vendors must obtain a certificate from Microsoft in order to deliver .NET compatible services. Potential .NET customers must consider Microsoft's track record before deciding if .NET will be as secure as possible.

On June 22, 2001, Microsoft failed to renew its Digital Certificate for **secure.microsoft.co.uk**, an e-commerce site for developers that wish to purchase software before its official release. Visitors to the site could not be sure that it was the official Microsoft entity.[xiv]

On January 4, 2001, Several Microsoft Websites experienced a blackout. Microsoft.com, MSN, Hotmail, Expedia.com and MSNBC were all unavailable to users for a day. The cause of this Denial of Service was, as Microsoft stated: "A Microsoft technician made a configuration change to the routers on the edge of Microsoft's Domain Name Server network." Knowledgeable Microsoft watchers say that one reason so many sites were inaccessible is that all four of its Domain Name Servers were on the same subnet, a vulnerable arrangement uncharacteristic of a sophisticated provider.[xv]

On October 16, 2001 Zdnet reported that a member of the Certified Partners area of Microsoft.com was shown a VBS error message that led to detailed information about the names and addresses of Microsoft's Web and database servers in addition to usernames and passwords provided in clear text. This area of Microsoft.com is gated by Passport. Microsoft and third parties are capable of security holes that Passport does not guard against.[xvi]

Microsoft has a less than stellar record in developing its own security products.

On April 16, 2001 Microsoft issued Security Bulletin MS01-021, which contained a patch for a Denial of Service vulnerability in the default configuration of its ISA (Internet Security and Acceleration) server, an enterprise firewall and Web cache server. If an external attacker can induce a network user to open an HTML e-mail containing a request of excessive length, the server will see it as access violation and will cease to pass traffic. This is significant because the ISA was touted by Microsoft as security product, specifically a firewall.[xvii]

Microsoft products are frequent victims of exploits and virus and worm attacks. The company issues patches on a regular basis, sometimes before a major attack takes place. This was the case when the Code Red and Nimda worms caused the recent wave of Microsoft server infestations. However, this serves to reinforce the argument that the products are not introduced to the market in a secure state.

John Pescatore of the well-respected Gartner Group issued an advisory on September 19, 2001 stating in part that:

> Gartner remains concerned that viruses and worms will continue to attack IIS until Microsoft has released a completely rewritten, thoroughly and publicly tested, new release of IIS. Sufficient operational testing should follow to ensure that the initial wave of security vulnerabilities every software product experiences has been uncovered and fixed. This move should include any Microsoft .NET Web services, which requires the use of IIS. Gartner believes that this rewriting will not occur before year-end 2002 (0.8 probability)[xviii]

There are a number of privacy and security issues to consider before agreeing to use .NET and Passport. The Passport login consists of the user's e-mail and password. It is a relatively easy matter to obtain someone's e-mail address and then use standard password guessing or cracking techniques to gain access to their account. An attacker would be authenticated to the Web sites holding the user's bank accounts, credit cards, e-mail, personal files, calendar, etc. In the case of .NET My Services, an unknown hacker or a competitor could access business applications, financial accounts, and sensitive files and e-mail.

There are privacy concerns based on the constant collecting and storing of personal data. As the Passport grows and matures, the network will contain considerable information about the personal habits, choices, and relationships of its viewers. Details about one's personal health and employment can be stored on .NET. The temptation to capitalize on this valuable consumer/employee information will be powerful.

The Passport Whitepaper states: "Microsoft Web sites or services are not allowed to mine the .NET Passport database and do not have access to it. Microsoft will not share .NET Passport information with any Microsoft or third-party service operator." The same Whitepaper leaves a loophole: "This document is for informational purposes only.

MICROSOFT MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, IN THIS DOCUMENT."[xix]

Microsoft has shown itself to be a vigorous legal advocate for itself. Its Attorneys threatened Slashdot.com for discussing the Kerberos implementation that Microsoft had published on the Internet, claiming such discussions were violations of the Digital Media Copyright Act.[xx] A company attorney warned a former Microsoft contract employee, Jason Bishop, who worked on the development of SOAP, just before he was to give a speech at Java-XML SIG. Mr. Bishop had done nothing to indicate that he would violate any agreement between himself and Microsoft. Three Microsoft SOAP people, including one attorney came to the meeting, ostensibly to intimidate Bishop.[xxi]

In its Passport Whitepaper, Microsoft emphasizes the security measures built into Passport such as redundancy, SSL (Secure Socket Layer), and Triple DES (Data Encryption Standard). However, just in the past ten months, Micrososft has spread a virus to its favored customers through a hotfix, handed out an official Microsoft digital certificate to an imposter, experienced a blackout by its own hand, neglected to renew a digital certificate for one of its Web sites, released a flawed firewall, attempted to interfere with a discussion on a Web site, revealed confidential information about its servers and users, and issued 51 Security Bulletins.

Consumers, businesses, and governments will be investing a great deal of faith in Microsoft and its "federation of trust" (third parties). What liability will Microsoft have if it or one of the third parties neglects to follow security procedures as has happened in the past? Microsoft tends to use tunnel vision when it pursues a goal. There is little regard for antitrust concerns or consumer protection. Its softly worded Security Bulletins do not assuage the professional computer security community.

On April 3, 2000,U.S. District Court Judge Thomas Penfield Jackson ruled "…Microsoft used its monopoly power by anticompetitive means and attempted to monopolize the Web browser market, both in violation of §2. Microsoft also violated § 1 of the Sherman Act by unlawfully tying its Web browser to its operating systems." (An appeal is pending).[xxii] In September 2001, The Consumer Federation of America, Consumers Union, Media Access Project and U.S. Public Interest Research Group, joined together to write a letter to federal and state prosecutors that expressed their belief that Microsoft is flaunting the ruling of the federal appeals court by integrating its Internet services into Windows XP.[xxiii]

Microsoft has recently used the image of a padlock to demonstrate its new emphasis on security but there is no clear or prominent warning on the Passport sign-up page that discloses the possibility of lost or stolen data, compromised user ID's and passwords, disclosure of private information, or service blackouts. Microsoft simply offers a disclaimer of responsibility within its Passport "Terms of Use" document.[xxiv]

A vendor can never promise total security for data or 100 % uptime. However, when a vendor seeks and is likely to become the dominant authenticator of the Internet for consumers, business and governments, then a mandatory disclosure of the risks involved seems reasonable.

Before it is permitted collect fees to direct the majority of Internet commerce through its servers, consumers and businesses must be shielded from Microsoft's legal might and must be granted inexpensive avenues of recourse for damage that exceeds that legal

threshold. This will require a sort of "Internet Bill of Rights" piece of legislation passed by Congress and regulated by the Federal Communications Commission.
It will contain these elements:

1. A statement indicating the thresholds of damages, losses, and blackouts caused by a Web entity that has not followed its own procedures or neglected to act reasonably to prevent a damaging failure.
2. A disclosure of risks associated with the use of the particular Internet service.
3. An uncomplicated specific procedure that allows consumers to contact the vendor and make a claim for losses and damages beyond the legal threshold.
4. The appropriate state and federal agencies to contact if the vendor disallows the consumer's claim.
5. Certain restrictions against predatory lawsuits brought by monopolies against consumers or public interest groups.

Any Web entity that accepts payment for goods and services would be required to post this Bill of Rights with a link from the home page. The page that collects the payment would contain the full text of the Bill of Rights. When services are provided for no charge, the Web entity would be required to post only a disclosure of risks in the same way.
Should you use Microsoft Passport .NET and .NET My Services? Consider the record of the Microsoft Corporation regarding its privacy and security foibles, its anticompetitive tendencies and anti-consumerism, and its powerful and intimidating legal tactics. The degree of personal risk is difficult to quantify, but you should use Passport and .NET only if it fills very important needs in your personal or professional life.

[i] Eisenberg, Robert. "What is HailStorm?" DevX.com. April-June 2001. URL: **http://www.enterprise-zone.com/articles/hailstorm/reisenberg/reisenberg-01.asp**
[ii] **http://whatis.techtarget.com/**
[iii] **http://web.mit.edu/kerberos/www/advisories/index.html**
[iv] **http://www.cert.org/advisories/CA-2000-06.html** 17 May 2000
[v] Ts'o, Theodore. "Microsoft 'embraces and extends' Kerberos V5." Usenix.org. 3 Dec. 1997. URL: **http://www.usenix.org/publications/login/1997-11/embraces.html**
[vi] **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/ssssprodtechnol/ windows2000serv/ maintain/featusability/rsvpker.asp**
[vii] Orlowski, Andrew. "Why Microsoft's Open HailStorm promises flatter to deceive." The Register. 21 September 2001. URL: **http://www.theregister.co.uk/content/archive/21792.html**
[viii] Babcock, Charles. "Kerberos Made To Heel To Windows 2000." zdnet.com. 28 February 2000. URL: **http://www.zdnet.com/zdnn/stories/news/0,4586,2449668,00.html**
[ix] Orlowski, Andrew. "Why Microsoft's Open HailStorm promises flatter to deceive." The Register. 21 September 2001. URL: **http://www.theregister.co.uk/content/archive/21792.html**
[x] Rush, Wayne. "Your Stolen Passport." zdnet.com 26 Sept 2001. URL: **http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2814881,00.html**

[xi] Poulsen, Kevin "Microsoft vexed by falsified certs." Security Focus. 22 May 2001
URL: **http://www.securityfocus.com/news/178**
[xii] Weiss, Todd R. "Missing Antivirus Software Left Microsoft Clients Vulnerable." 26 April 2001
http://www.computerworld.com/storyba/0,4125,NAV47_STO59982,00.html
[xiii] Leyden, John. "Microsoft Hotfixes Infected With Funlove Virus." The Register. 25 April 2001.
URL: **http://www.theregister.co.uk/content/archive/18516.html**
[xiv] Leyden, John. "Microsoft Fails to Renew its Digital Certificate." The Register. 29 June 2001.
URL: **http://www.theregister.co.uk/content/archive/20082.html**
[xv] Leyden, John. "Microsoft Blames Lowly Techie For Web Blackout." 25 January 2001.
URL: **http://www.theregister.co.uk/content/archive/16354.html**
[xvi] Berlind, David "Microsoft.com error reveals IDs, passwords." 16 Oct 2001 URL:
http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2818129,00.html
[xvii]**http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-021.asp** 25 April, 2001
[xviii] Pescatore, John. "Nimda worm Shows you can't always patch fast enough" 19 Sept. 2001
http://www3.gartner.com/DisplayDocument?doc_cd=101034 19 Sept. 2001
[xix] **http://www.microsoft.com/myservices/passport/technical.doc** Sept. 2001
[xx] Kermath, Annie. "Slashdot Gives Microsoft Lawyers The Bum's Rush." 19 May 2000.
URL: **http://www.theregister.co.uk/content/archive/10934.html**
[xxi] Lettice, John. "Microsoft Sends in Lawyers to Stop 'Open' SOAP From Getting Out" 25 May 2000.
URL: **http://www.theregister.co.uk/content/archive/10986.html**
[xxii] BBCNews. "Excerpts from the Guilty Verdict." 3 April 2000 URL:
http://news.bbc.co.uk/hi/english/in_depth/business/2000/microsoft/newsid_700000/700702.stm
[xxiii] Ricuitti, Mike. "Strategy: Blueprint Shrouded in Mystery." 18 Oct. 2001
URL: **http://news.cnet.com/news/0-1003-201-7502765-0.html**
[xxiv] **http://www.passport.com/consumer/termsofuse.asp?lc=1033&id=950&cb=0&cbid**=