Global Information Assurance Certification Paper

Arthur Hermann
September 29, 2001
GSEC Practical Assignment
Version 1.2e

Passport to Nowhere?

An investigation of Microsoft's Passport protocol and issues regarding its security, privacy standards and utilization in the XP and .Net initiatives

Overview

Recently, a great deal of attention has been focused on Microsoft's Passport authentication service. Microsoft refers to Passport as a single sign-on solution, which allows users to sign on to one e-commerce website (or to Microsoft's Hotmail website), and retain their authentication when moving to other Passport enabled websites.

The current interest has centered around a number of issues including recent security flaws found within Passport, privacy concerns relating to use of the service, and Microsoft's incorporation of the Passport Service into it's .Net initiative ("Hailstorm") products.

No other commonly used single sign-on solution currently exists for public web sites. There are now 165 million registered Passport users and over 200 different commerce websites the use the Passport service. Therefore, it is important to look at both the benefits and the failings of the Passport service. Indeed, since millions of users worldwide have Hotmail accounts that utilize Passport authentication and millions more will most likely use .Net products, the security and privacy concerns of this product bear great scrutiny.

New interest in Passport Security

Two researchers at the AT&T research labs in New Jersey, David P. Kormann and Aviel Rubin, published an article about risks of the Passport protocol in the July 2000 issue of the journal: IEEE Computer Networks, but it was given little attention by either their computer colleagues or the press. However, more than a year after it was published, an anonymous posting on slashdot.org with a link to the paper brought the it to the computer world's attention and began intensive interest in the subject. Rubin told "Newsbytes" : "I don't think Passport's flaws were on people's radar screens. But right now, there are a lot of people who are really aware of it." [1] In their article, Kormann and Rubin explain that the rules of normal single sign-on solutions don't apply to the web since different administrators control each web site. They go on to state that many of the shortcomings of Passport are due to the fact that it is constructed from basic web tools (HTTP redirects, JavaScript, Cookies, SSL) and that these tools just don't support the type of security one would want and expect from an authorization service. Unfortunately, these tools allow hackers to perform the same

type of attacks against Passport, as those performed against any other web site. [2]

In their paper, Kormann and Rubin explain that SSL is an excellent and proven technology. However, they feel that browsers are delivered with so many "root" public keys – allowing the owners of the corresponding private keys to be immediately trusted – that there is significant room for abuse of the authentication process. As has recently been seen, certifying authorities can make mistakes, and if a bogus certificate from one of these default "root" keys providers were deployed, all browsers would immediately trust it.

How Passport Works

Microsoft states in its "Passport Technical White Paper," that Passport's primary capability "provides user authentication that works securely across multiple sites while preserving the user's privacy" .[3] Microsoft refers to the service as the Passport single sign-in (SSI) service. The SSI service utilizes a well-known and secure database to store user's authentication information. Simply, when a user logs on to a Passport enabled site, an HTTP redirect takes them to the secure database. The user's authentication information is then checked using triple DES with a key previously created by Microsoft Passport and the Passport enabled site. Once confirmed, the user is redirected back to the browser; taking an encrypted cookie back with him. If the user then moves to another Password enabled site, the same encrypted cookie is passed to that site and no further authentication is required. The Illustration below from the Kormann and Rubin paper depicts this process:

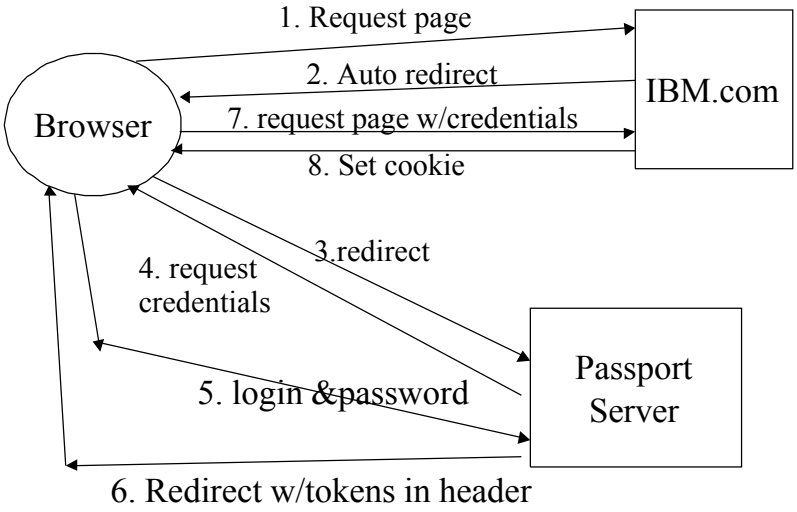

Illustration from "Risks of the Passport Single Signon Protocol." Kormann, David and Rubin, Aviel.

If the user depicted in this illustration then moved from the IBM site to the Hotmail site (which, of course, is Passport enabled), he would not have to return to the Passport Server for authentication.

Security Risks

Kormann and Rubin point out a number of security risks in the SSI service. Their key points are:

1. User Interface Issues – it is easy for a user to think that they have logged out of the Passport service when in fact they have not done so. All Passport sites display a Passport logout icon. But in Microsoft's Hotmail site there is both this icon and a link to sign out of Hotmail. A user that logs out of Hotmail without using the log out of Passport icon will continue to have authenticated credentials in his browser (Note: this has been corrected in the newest version of the Hotmail client). Any other user could then come along and use these credentials to purchase goods or view email in Hotmail. In fact, Kormann and Rubin point out that when using a Netscape browser, even after the user has signed out of Passport or Hotmail, they are actually still authenticated and can simply move back to a Passport site and immediately enter without authentication.
2. Key Management – Microsoft is not specific about how their keys are generated, but systems have been broken because their keys were not truly random when generated. More importantly, a single key is used to encrypt all of the cookies that the SSI service utilizes. This could be of grave concern, since breaking this one key would allow a hacker the ability to read cookies on any machine using the SSI service. A much better solution would be to use randomly generated keys for the encryption of cookies.
3. Allows for a Central Point of Attack – The Passport service stores authentication information in centralized databases, unlike traditional e-commerce sites which each have their own databases. This allows for a central point of attack of the Passport authentication databases. If these databases became compromised, a huge security breach would result. Additionally, such centralized databases enable the use of Denial of Service attacks, which could also cripple the SSI service.
4. Cookies – There are two major concerns relating to Passport's use of cookies. First, a concern with privacy exists, because Microsoft and vendor's using the service can store a great deal of personal information in the cookie. More importantly, the user can choose to have automatic logon to Passport sites, which requires the use of persistent cookies in their browser. Thus anyone given access to the user's browser will be authenticated into the SSI service.

Passport Attacks

A number of attacks against the Passport service have recently been published on security websites. In a letter posted on eyeonsecurity.net, a writer known as obscure^[4] outlines an attack on Passport which fools the system into sending the hijacker a session cookie. He describes an exploit using cross-site scripting in which a malicious coder can embed JavaScript in a trusted link. In the exploit described, the user only

needs to click on this link and his credentials can be sent to a remote server and then used for malicious intent.[5] Writing about this attack in eWeek, David Worthington reports that Microsoft patched the Hotmail site on August 23, 2001 (within 12 hours of being notified by the WhiteHat security group) to prohibit such an attack.[5] The ability to create such an attack was by no means specific to Hotmail. In fact this new type of attack has recently been used in many exploits including the Nimda virus. However, such an attack illustrates the particular dangers of utilizing basic browser tools to perform authentication services until such new standards such as IPSec are available.

On the New Order Website, a contributor knows as hx, posted the following "Man in the Middle Attack" against Hotmail and MSN[6]. The post included the following summary:

> The following is an exploit code that employs a 'Man In the Middle' attack against Messenger and its Hotmail module. The exploit code allows to:
> 1) Use the messenger scrambler bug to get passwords hashes.
> 2) Spoof a Hotmail site to retrieve plaintext passwords (since the protocol can be caused to transfer passwords in a non-encrypted form).
> 3) Remotely crash the client.
> 4) Upload a malicious program of your choice masqueraded as an update."

The writer then lists the code that will enable such an attack.

It is certain that additional successful attack strategies will be developed and exposed in the near future. Having had to use existing browser and web tools to build Passport, Microsoft has unfortunately opened up the service to the same type of attacks which can be launched at most websites.

Privacy Concerns and Incorporation into Microsoft XP and .Net

For a long time, critics of Microsoft and the Passport authentication service have been concerned about personal privacy with regard to the storage of information by the Passport service. Once Microsoft announced that Passport would be the key authentication feature of their new XP products and their .Net initiative, these concerns exploded onto the national scene. Critics accused Microsoft of possible monopoly infringements (the case before the U.S. Justice department was still under review) by driving away competition for any other single sign-on service, and requiring all users of Hotmail, XP, or .Net products to have Passport accounts.

In early June of this year, Microsoft released one of the last test versions of the XP operating system and it included a requirement for users to create a Passport account to use many of the .Net features including instant messaging. This immediately led to renewed calls of monopoly building against Microsoft. But others understood Microsoft's need to embed the authorization service in the operating system. In an article published soon after the release, Joe Wilcox of ZDnet news, stated: "The first .Net building block, HailStorm, relies heavily on Passport, which Microsoft has used for some time for its MSN Messenger and Hotmail services. Passport is supposed to be a

universal gateway to a variety of services--some free, others for a fee--delivered by Microsoft and third-party service providers. People sign in once, with immediate access available to any Passport-authenticated service or Web site."[9]

On August 8th, 2001, Microsoft announced that the Passport service would soon be utilizing a new standard endorsed by the World Wide Web Consortium: Platform for Privacy Preferences (P3P). This standard allows user's to determine what types of information they are willing to give to a web site, and whether they are willing to have that information shared with third parties. User's will receive a warning when they move to a vendor's website which exceeds the P3P levels they have authorized. At the same time, Microsoft has received a lot of heat over this announcement, since at the present time this standard will only be implemented in Internet Explorer 6. Since the authentication is executed within the browser, the P3P standard won't be supported in competing browsers. This has once again led to claims that Microsoft is using monopoly power to force vendors and users to utilize Microsoft's newest browser.

The Larger View

While there are certainly concerns about Passport security and privacy, it is important to also see the larger picture. There are many benefits that such a service can provide and Microsoft has had many roadblocks to overcome in developing the service. The largest of these roadblocks has been the need to use current browser and web technologies, which were not built for secure authentication.

Although it is common sport to bash Microsoft's software and services, the company's history has been one of developing fairly poor software and through subsequent releases developing something that becomes a true standard in the industry. So too, the next few releases of Passport might strengthen the service until most of the present security concerns have disappeared.

To accomplish this, Microsoft needs protocol standards (such as IPSec) which are not yet in place but which they are helping to develop. Once more secure protocol standards are in place for the World Wide Web, Microsoft should be able to modify the Passport service for substantially increased security. However, this does raise the question of whether the service is secure enough at the present time to allow Microsoft to embed it in all of its key applications; given the fact that these protocols are not yet in place.

Some might say that Microsoft has done the World Wide Web and e-commerce a large service by creating a single sign-on solution. Certainly no other vendor has yet done so. Just last week Microsoft said that it would be making significant changes in the Passport service to create acceptance in the larger e-business market place. They are suggesting that the new standards will allow Passport to function like ATM networks such as Cirrus or Plus. The company also announced that the next generation of the Passport service would be based on Kerberos (which has already been integrated into the XP operating system).

Microsoft also announced that it would be making major modifications to the Passport service; both opening up the service to allow third-party vendors to manage Passport credentials and allowing individual businesses or organizations to retain control over Passport users identities, profiles, and information. Brian Abrogast, Vice President of .Net Core Services at Microsoft, said; "almost every Web site that wants to do robust personalization or secure access to data has its own authentication system… Our goal is to lay the foundation that will allow mass adoption of Web services. We don't believe that any one company will be the only authorization provider on the Internet. We will allow Passport to accept credentials from other services and allow other services to give Passport identities."[7]

On September 26, 2001, Scott McNeally, CEO of Sun Microsystems, announced that he and Sun's corporate partners will unveil an alliance for handling user's "digital identity." Sun is known to favor a neutral method of authorization, which isn't controlled by a single company. The Sun project, code named "Liberty" is undoubtedly aimed at Microsoft's Passport. Due to the terrorist attack of September 11th, there is a growing consensus for a national identity card (70% in favor in a recent poll) that could also be utilized to provide a "digital identity." McNeally said that he believes "Sun technology will play a part – specifically, Sun's Java card software, that lets credit cards with computer chips run small programs and store personal information. 'That'll be a Java card' McNeally said about the national identity card concept."[8] This is actually a bit ironic, since many privacy advocates, as well as Sun itself have been concerned about the stockpiling of any significant personal data. The U.S. armed forces are already using Java cards, and one of their uses will be authenticating computer users.

Footnotes

1. McWilliams, Brian. "Microsoft Passport Security Flaws Now on the Radar.". Infosec.com. URL: http://www.info-sec.com/internet/01/internet_080601a_j.shtml (06 August 2001).
2. Kormann, David and Rubin, Aviel. "Risks of the Passport Single Signon Protocol." Computer Networks, Vol. 33, Pages 51-58, 2000. Reprinted URL: http://avirubin.com/passport.html
3. Microsoft Passport Business Services. "Microsoft Passport Technical White Paper." Passport.com. URL: http://www.passport.com/Business/WhitePaper.asp?lc=1033 (2001).
4. Obscure^. "Microsoft Passport Account Hijack Attack (Hacking hotmail and more)." URL: http://irc.m0ss.com/eos/scripts/eos.pl?p=29&s=1&f=1 (2001)
5. Worthington, David. "New hack poses threat to popular Web services." eWeek URL: http://www.zdnet.com/eweek/stories/general/0,11011,2808729,00.html (28 August 2001)
6. hx. "Messenger and Hotmail MITM Exploit (Arptool and Neaky).", New Order. URL: http://neworder.box.sk/showme.php3?id=5291 (19 July 2001)
7. Kanellos, Michael and Wong, Wylie. "Microsoft opens up Passport service". c/net news.com. http://news.cnet.com/news/0-1003-200-7231441.html (20

September 2001)
8. Shankland, Stephen. “Sun alliance targets Microsoft’s Passport”. c/net news.com. http://news.cnet.com/news/0-1003-200-7302671.html (20 September 2001)
9. Wilcox, Joe. “Win XP needs Passport to travel”. ZDNET.com. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,5093082,00.html (21 June 2001)

References

1. Kormann, David and Rubin, Aviel. "Risks of the Passport Single Signon Protocol." Computer Networks, Vol. 33, Pages 51-58, 2000. Reprinted URL: McWilliams, Brian. "Microsoft Passport Security Flaws Now on the Radar." Infosec.com. URL: http://www.info-sec.com/internet/01/internet_080601a_j.shtml (06 August 2001).
2. Kormann, David and Rubin, Aviel. "Risks of the Passport Single Signon Protocol." Computer Networks, Vol. 33, Pages 51-58, 2000. Reprinted URL: http://avirubin.com/passport.html
3. Microsoft Passport Business Services. “Microsoft Passport Technical White Paper.” Passport.com. URL:http://www.passport.com/Business/WhitePaper.asp?lc=1033 (2001).
4. Obscure^. “Microsoft Passport Account Hijack Attack (Hacking hotmail and more).” URL: http://irc.m0ss.com/eos/scripts/eos.pl?p=29&s=1&f=1 (2001)
5. Worthington, David. “New hack poses threat to popular Web services.” eWeek URL: http://www.zdnet.com/eweek/stories/general/0,11011,2808729,00.html (28 August 2001)
6. hx. “Messenger and Hotmail MITM Exploit (Arptool and Neaky).”, New Order. URL: http://neworder.box.sk/showme.php3?id=5291 (19 July 2001)
7. Kanellos, Michael and Wong, Wylie. “Microsoft opens up Passport service”. c/net news.com. URL: http://news.cnet.com/news/0-1003-200-7231441.html (20 September 2001)
8. Wong, Wiley and Wilcox, Joe.“New Passport Privacy linked to IE6”. ZDNET.com. URL:http://www.zdnet.com/zdnn/stories/news/0,4586,5095470,00.html (29 August 2001)
9. Wilcox, Joe. “Win XP needs Passport to travel”. ZDNET.com. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,5093082,00.html (21 June 2001)
10. Shankland, Stephen. “Sun alliance targets Microsoft’s Passport”. c/netnews.com. http://news.cnet.com/news/0-1003-200-7302671.html (20 September 2001)
11. Lyman, Jay. “Microsoft Renews ‘Passport’ But Privacy Issues Remain”. NewsFactor Network. URL: http://www.newsfactor.com/perl/printer/12731/ (10 August 2001)
12. Manjoo, Farhad. “MS Passport: Straight to the FTC”. Wired News.

URL:http://www.wired.com/news/privacy/0,1848,46095,00.html (16 August 2001)

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event