DuD
Datenschutz und Datensicherheit

Single Sign In im Internet

Eine Betrachtung des Microsoft Passport Service

Holger Mack

Die Einführung des Passport Service durch die Firma Microsoft hat vor einigen Monaten kräftige Wellen geschlagen: Die Furcht vor einem allmächtigen Microsoft, das über personenbezogene Daten von Millionen von Nutzern verfügt, hat zur Gründung mehrerer „Gegeninitiativen“ geführt. Derweil forciert Microsoft die Verbreitung durch die (automatische) Integration von Hotmail- und MSN-Nutzern sowie die forcierte Erstanmeldung unter Windows XP. Holger Mack beschreibt die Funktionsweise des Dienstes und diskutiert seine Gefährdungen und Risiken.

MSc. Dipl.-Ing. Holger Mack

Security Consultant bei der Secorvo Security Consulting GmbH, Karlsruhe. Arbeitsschwerpunkt: Single Sign On, Public Key Infrastrukturen, Windows 2000/XP Security.
E-Mail: mack@secorvo.de

Einleitung

Single Sign On ist seit Jahren ein Thema in den IT-Abteilungen fast jeden Unternehmens. Mit der Anzahl an verschiedenen Anwendungen, die ein PC-Benutzer an seinem Arbeitsplatz heute durchschnittlich bedienen muss, ist auch oft die Anzahl der Passwörter oder Zugangscodes, die sich ein Benutzer merken muss, stark gestiegen. Da viele dieser Anwendungen die Authentisierung mit eigenen proprietären Implementierungen realisieren, ist es heute nicht unüblich, dass sich Benutzer bis zu zehn oder mehr Passwörter für die verschiedenen Anwendungen merken müssen. Während es allerdings einige Unternehmen in den letzten Jahren geschafft haben, wenn auch keine Single-Sign On, so doch ein „Reduced Sign On“ zu realisieren und so die Anzahl der Passwörter zu reduzieren, ist man im Internet immer noch darauf angewiesen sich eine Vielzahl von Benutzernamen und Passwörtern zu merken.

Obwohl dieses Problem nicht neu ist, hat es in letzter Zeit an Bedeutung gewonnen. Neben der verstärkten Nutzung des Internets für Dienste, die eine Authentisierung des Benutzers erfordern (z.B. Online-Banking oder -Shopping), spielen hier auch die Ideen für die Zukunft des Internets eine große Rolle. Das Internet soll verstärkt für sogenannte Web-Services eingesetzt werden. Diese sollen verteilte Anwendungen im Internet ermöglichen. In solchen Szenarien wächst die Bedeutung einer sicheren Authentisierung, da das Internet verstärkt für den Zugriff auf sicherheitskritische oder kostenpflichtige Dienste genutzt werden soll. Solche Web-Services sollen es auch ermöglichen, dass Dienste im Namen des Benutzers automatisch auf andere Dienste zugreifen können sollen. Um auch in solchen Szenarien Sicherheit zu gewähren muss ein Authentisierungsmechanismus auch Delegation unterstützen.

Derzeit bewerben sich mehrere Hersteller darum, dass ihre Technik die Grundlage solcher Web-Services sein sollte. Microsoft mit dem .NET-Framework[1] und Sun mit der J2EE-Plattform[2] sind hier sicherlich die prominentesten Kontrahenten. Als Austauschformat beruhen diese Web-Services auf XML basierten Standards wie SOAP, UUDP, WDSL.[3] Keiner dieser Standards adressiert die Sicherheitsaspekte wie Authentisierung in geeigneter Weise, sondern verlässt sich darauf, dass die Sicherheitsaspekte an anderer Stelle gelöst werden.

Zum Thema Authentisierung hat Microsoft mit dem Passport Service nun eine Lösung vorgestellt, die allerdings schon viel Kritik einstecken musste.

In diesem Beitrag wird beschrieben und analysiert, was hinter dem Passport Service steckt und wie Passport aus Sicherheitssicht zu bewerten ist. Außerdem wird kurz darauf eingegangen, welche Alternativen sich abzeichnen und in welchem Status sich diese zur Zeit befinden.

1 .NET Passport

Wenn heute ein Anbieter von Web-Seiten im Internet oder im firmeninternen Intranet eine sichere Authentisierung der zugreifenden Benutzer benötigt, sei es um den Zugriff auf sensible oder kostenpflichtige Daten zu kontrollieren oder auch nur um ein individualisiertes Angebot präsentieren zu können, liegt es in der Verantwortung des Web-Seiten Betreibers, entsprechende Mechanismen zu implementieren. Das Ergebnis ist eine Vielzahl von teilweise proprietären oder auch unsicheren Lösungen. Oft sind solche, von Entwicklern ohne Sicherheitserfahrung entworfenen Verfahren unsicher (z.B. Übertragung der Passwörter

[1] http://www.microsoft.com/net/
[2] http://java.sun.com/j2ee/
[3] Spezifikation und nähere Informationen finden sich unter http://www.w3c.org

im Klartext) oder enthalten sicherheitskritische Fehler (z.B. Buffer Overflow). In den meisten Fällen basieren solche Lösungen auf primitiven Mechanismen wie der Angabe des Benutzernamens und Passworts, in den seltensten Fällen kommen zertifikatsbasierte (z.B. SSL mit Client Authentifizierung) oder andere sichere Verfahren (z.B. SecurID) zum Einsatz.

Aus Sicht der Benutzer bedeutet diese Situation, dass für jeden Dienst eigene Benutzernamen und Passwort Kombinationen notwendig sind. Bei Benutzern, die viele Web-Angebot nutzen, kann diese Liste von Passwörtern sehr schnell unhandlich werden. Oft veranlasst dies die Nutzer überall die gleichen einfachen Passwörter auszuwählen. Die Konsequenz ist, dass man damit mglw. dem Online Gemüsehändler das Passwort für das Online-Banking gibt [KOR00].

Das Ziel des Microsoft .NET Passport Systems ist es, diese individuelle und verteilte Authentisierung durch einen zentralen Dienst zu ersetzen, der verspricht, zentral die Authentisierung von Benutzern im Internet zu ermöglichen. Die definierten Ziele sind dabei zum einen Anbietern von Web-Angeboten die Möglichkeit zu geben die Authentisierung an einen zentralen Dienst „auszulagern“ und somit sich den eigenen Implementierungsaufwand zu ersparen. Neben der Einsparung des Implementierungsaufwands, soll so auch die Sicherheit der Authentisierung erhöht werden, da der Authentisierungsdienst in entsprechend gesicherter Umgebung betrieben werden kann.

Zum anderen verspricht ein zentraler Dienst aus Sicht der Benutzer ein höheres Maß an Komfort. Der Benutzer muss sich nur noch ein Passwort für alle am Passport-System teilhabenden Web-Dienste merken. Zusätzlich ermöglicht Passport ein sogenanntes Single-Sign-In (SSI), d.h. der Benutzer muss sich im Laufe einer Internet-Sitzung nur beim ersten Zugriff auf eine Web-Seite explizit mit Benutzername und Passwort authentifizieren, beim Zugriff auf weitere Dienste erfolgt die Authentisierung dann automatisch ohne weitere Passwort-Eingabe.

2 Wie funktioniert der Service?

Das Grundprinzip des Microsoft Passport Service ist, dass ein Web-Server die Authentisierung des Zugriffs auf Web-Seiten nicht selbst übernimmt, sondern diese Aufgabe an einen zentralen Dienst „auslagert“. Hierzu wird der Benutzer beim Zugriff auf die geschützte Web-Seite per HTTP redirect an den Passport Server weitergeleitet. Der Benutzer authentifiziert sich dann mit Benutzername und Passwort gegenüber dem Passport Service.[4] Wenn diese Authentifizierung erfolgreich war werden mehrere Aktionen ausgelöst:

- Der Passportdienst legt mehrere Cookies [WICH98] im Browser des Benutzers ab. Diese Cookies dienen unter anderem dazu, den Benutzer bei späteren Anfragen automatisch zu authentifizieren. Auf diese Weise wird der Single-Sign-In Mechanismus implementiert. Außerdem legt der Server im Browser mit Hilfe von Cookies eine Liste von Web-Seiten an, gegenüber denen der Benutzer innerhalb dieser Sitzung authentisiert wurde. Diese Liste ist für den späteren Ausloggg-Vorgang von Bedeutung.
- Der Passport-Server erstellt ein Ticket für den Web-Server. Dieses Ticket enthält die innerhalb des Passport-Systems eindeutige PUID (Personal User Identification) des authentifizierten Benutzers und zusätzlich vom Benutzer explizit zur Weitergabe an den Web-Dienstleister freigegebenen Informationen wie z.B. die E-Mail Adresse (dazu später mehr). Dieses Ticket wird mit einem für den Web-Server individuellen symmetrischen Schlüssel verschlüsselt.
- Der Benutzer wird dann wieder an den originalen Web-Server zurückverwiesen. Das Ticket für den Server wird als Parameter dieser Weiterleitung an den Web-Server übergeben.
- Der Web-Server gibt das Ticket an den auf dem Server installierten Passport Manager weiter. Dieser entschlüsselt das Ticket und liefert die PUID und mögliche andere enthaltene Daten an den Web-Server zur weiteren Auswertung.
- Zum Schluss legt der Web-Server noch einige Cookies im Browser des Benutzers ab, u.a. um weitere Authentisierungsanfragen beim Passport Service zu vermeiden.

Wichtig ist hier darauf hinzuweisen, dass mit diesem Verfahren ausschließlich eine Authentifizierung des Benutzers vorgenommen wurde. Der Web-Dienstleister weiß damit, dass der Benutzer mit dieser PUID sich gegenüber dem Passport-Service authentifiziert hat. Die anschließenden Schritte, d.h. die Zuordnung zu einem Benutzerkonto bzw. Autorisierung des Zugriffs liegt weiterhin in der Verantwortung des Betreibers der Web-Seite.

Durch die Verwendung des Passport-Service entfällt auch nicht die Notwendigkeit, sich auf Webseiten registrieren zu lassen. Dieser Schritt muss auch weiterhin durchgeführt werden.

3 Registrierung

Damit der oben beschriebene Authentifikationsdienst von einem Web-Dienstleister oder einem Benutzer genutzt werden kann, müssen sich beide beim Passport Service registrieren lassen. Für den Web-Server-Betreiber bedeutet dies, dass er eine Liste von Bedingungen erfüllen muss, die Microsoft an den Anbieter stellt [MIC03]. Diese Bedingungen enthalten neben funktionalen und darstellerischen Anforderungen auch Hinweise auf Datenschutz- und Sicherheitsanforderungen. Diese sind allerdings sehr allgemein gehalten.

Technisch muss auf dem Web-Server das Passport Manager Modul installiert sein.[5] Anschließend muss ein Service Agreement mit Microsoft unterschrieben werden. Nach diesen Schritten wird dem Web-Server eine eindeutige Site ID zugewiesen. Im Rahmen dieser Prozedur muss auch der geheime Schlüssel zwischen Web-Server-Betreiber und Microsoft Passport Service ausgetauscht werden.[6]

Ein Benutzer des Passport Services muss sich vor der ersten Benutzung ebenfalls beim Passport Service registrieren lassen. Als minimale Angaben sind hierzu eine E-Mail Adresse und die Wahl eines Passworts erforderlich. Zur Prüfung der E-Mail Adresse wird eine E-Mail an den Benutzer geschickt, die bestätigt werden muss. Neben der E-Mail-Adresse können in einem Passport Profil auch noch zusätzliche Informationen hinterlegt werden. Dazu gehören Angaben wie Name, Vorname, Adressinformationen, Geschlecht und Beschäftigung. Die Eingabe dieser Daten ist freiwillig.

[4] Andere Authentisierungsverfahren sind für spätere Versionen geplant.

[5] Das Modul ist sowohl für Windows-Plattformen als auch für Linux Systeme verfügbar.

[6] Genaue Details über die Prozeduren zur Erzeugung und zum Austausch dieser Schlüssel werden in der vorhandenen Dokumentation nicht gegeben.

Als Standardeinstellung wird nur die PUID bei der Authentisierung an den Web-Server übergeben, der Benutzer kann hier allerdings noch entscheiden, welche Informationen der Passport Service zusätzlich an den Web-Server weitergeben darf. Dabei stehen neben der Möglichkeit, keine Informationen weiterzugeben, drei weitere Optionen zur Verfügung:

- Weitergabe der E-Mail Adresse
- Weitergabe von Vor- und Nachname
- Weitergabe der anderen Registrierungsinformationen.

Neben der reinen Authentisierung bietet Microsoft auch noch den sogenannten Express Purchase Service an. Hierbei kann der Benutzer optional alle Daten, die für eine Kreditkartenzahlung notwendig sind (Kreditkartennummer, Lieferadresse etc.) auf dem Passport Server hinterlegen. Wenn der Benutzer nun bei einem Händler, der beim Passport Service registriert ist, bezahlen will, kann er den Passport-Server beauftragen die Daten dem Web-Server zur Verfügung zu stellen. Auf diese Weise muss der Benutzer diese Daten nicht wiederholt eingeben. Die Übertragung erfolgt dabei verschlüsselt auf dem gleichen Weg wie bei der initialen Authentisierung.

4 Sicherheit des Passport Service

Bei der Bewertung der Sicherheit des Passport-Service spielen mehrere Aspekte eine Rolle. Zum einen ist es sowohl für den Web-Server-Betreiber als auch für den Benutzer wichtig, welches Sicherheitsniveau diese Authentisierung wirklich bieten kann. Zum zweiten ist die zentrale Datenbank aus Sicherheits- und Datenschutzsicht von Bedeutung.

4.1 Zentrale Datenbank

Eine der Hauptkritikpunkte am Passport Service ist immer wieder die potentielle Gefahr durch die zentrale Sammlung von sicherheitskritischen und personenbezogenen Daten. Dies beinhaltet die persönlichen Daten, die im Profil des Benutzers gespeichert werden. Durch die Tatsache, dass jeder Login-Versuch bei einem am Passport-System teilhabenden Web-Server über den Passport Server abläuft, ergibt sich außerdem die Möglichkeit, detaillierte Nutzungsprofile der Benutzer zu erstellen. Auch Anbietern sollte bewusst sein, dass bei der Nutzung des Passport-Service zur Benutzer-Authentisierung zumindest die Namen aller Kunden eines Angebots gesammelt werden können. In Zeiten in denen diese Kundendatenbanken teilweise das größte Kapital eines Unternehmens sind, werden viele Anbieter einem solchen Dienst sehr kritisch gegenüber stehen.

Im Privacy Statement [MIC04] wird die Art der Speicherung und Weitergabe der persönlichen Daten des Benutzers beschrieben, es wird dabei aber nicht explizit auf die mögliche Speicherung und Verarbeitung der Verbindungsdaten eingegangen.

Neben dem möglichen Missbrauch der Daten in der zentralen Datenbank durch den Betreiber des zentralen Authentisierungsdienstes, ist eine solche Datenbank fast zwangsläufig auch ein attraktives Ziel für externe Angreifer. Ein erfolgreicher Angriff auf die Datenbank hätte auch extreme Konsequenzen für die Sicherheit der angeschlossenen Web-Angebote.

Neben der Vertraulichkeit der Daten in der Datenbank spielt natürlich auch die Verfügbarkeit des Passport-Service eine wichtige Rolle. Hier bietet ein zentraler Service ein „einfache“ Möglichkeit, mit einem Angriff, z.B. durch Distributed Denial of Service Attacken [MÖKE00], auf einmal alle vom Passport Dienst abhängigen Web-Server auszuschalten.

Microsoft gibt an [MIC01], dass die Server des Passport Dienstes in einem speziellen Data-Center mit hohen technischen, organisatorischen, personellen und physikalischen Schutzmaßnahmen betrieben werden. Was das genau bedeutet, ist allerdings nicht bekannt.

4.2 Authentisierung

Die Sicherheit der Authentisierung hängt sehr stark von der Sicherheit der zentralen Datenbank ab. Ist diese und sind vor allem die darin gespeicherten Authentisierungsdaten nicht ausreichend gesichert, ist auch die Authentisierung wertlos. Aber auch unter anderen Aspekten muss die Sicherheit des gewählten Authentisierungsverfahrens bewertet werden.

Die Techniken, die bei Passport zur Sicherung der Authentisierung eingesetzt werden, ermöglichen eine Reihe von potentiellen Angriffen.

Spoofing

Eine Gefahr für alle Web-basierten Angebote sind immer wieder Angriffe durch sogenanntes Spoofing. Hierbei versucht der Angreifer, den Benutzer zu täuschen und ihn dadurch dazu zu bewegen, Benutzername und Passwort preiszugeben. Dies kann z.B. dadurch geschehen, dass dem Benutzer eine Web-Seite präsentiert wird, die aussieht wie der eigentliche Passport-Webseite, die aber Benutzername und Passwort nicht zum Microsoft-Server sondern zum Server des Angreifers weiterleitet. Solche Angriffe unter Ausnutzung von Schwächen des IP oder DNS Protokolls sind seit langem bekannt und sind auch auf den Passport Service anwendbar [KOR00]. Zur Vermeidung solcher Angriffe wird beim Passport Dienst SSL [ESMÜ97] zur Server-Authentisierung eingesetzt. Obwohl das SSL-Protokoll technisch solche Spoofing Angriffe verhindern kann, ermöglicht die Art, wie es im Internet eingesetzt wird, auch hier Spoofing Angriffe. Ein solcher Angriff kann zwar mit geschultem Auge erkannt werden, es kann aber davon ausgegangen werden, dass nur wenige Benutzer in der Lage sind bzw. sich die Mühe machen solche Angriffe aufzuspüren indem sie z.B. Zertifikate der SSL Server und der ausstellenden Zertifizierungsstellen überprüfen.

Cookie Stealing und Replay Attacken

Der Passport Mechanismus basiert auf der Verwendung von Cookies. So legt z.B. der Passport Server ein Cookie im Browser des Benutzers ab. Dieses enthält das Passwort des Benutzers und wird dazu verwendet, dem Benutzer nach der einmaligen Eingabe des Passworts weitere Passwort-Eingaben zu ersparen. Obwohl dieses Cookie verschlüsselt ist,[7] kann es von einem Angreifer dazu verwendet werden, sich gegenüber dem Passport-Dienst als legitimer Benutzer auszugeben.

Eigentlich sollten solche Cookies dadurch geschützt sein, dass sie nur von dem Server gelesen werden können, von dem sie im Browser abgelegt worden sind. Es sind aber eine Reihe von Attacken bekannt, wie in verschiedenen Browsern solche Cookies mit Hilfe anderer Web-Seiten „gestohlen“ werden können. In [SLE01] wird gezeigt wie ein solcher Angriff erfolgreich gegen den Passport-Service durchgeführt wurde.

Um die Auswirkungen von solchen Replay-Attacken einzuschränken ist sowohl in den verschlüsselten Cookies als auch in den Tickets für den Web-Server ein Zeitstempel abgelegt, der den Erstellungszeit-

[7] Als Verschlüsselungsverfahren kommt Triple-DES zum Einsatz.

punkt des Cookies/Tickets angibt. Es ist damit dem Passport Server oder dem Web-Server möglich zu prüfen, wie lange die letzte explizite Authentisierung zurückliegt und zu entscheiden, ob das Ticket/Cookie noch akzeptiert wird oder ob eine neue explizite Authentisierung angefordert wird. Diese Entscheidung unterliegt aber dem jeweiligen Service-Anbieter und wird nicht vorgegeben.

Ein weiteres Problem der Verwendung von Cookies besteht bei Computern, die mehreren Benutzern zugänglich sind. Solange die Cookies noch im Browser Verzeichnis gespeichert sind, kann sich jeder automatisch bei Passport einloggen. Dies lässt sich nur verhindern, wenn der Benutzer sich aus dem Passport System abmeldet und alle Cookies aus dem Browser löscht. Dies betrifft sowohl die Cookies, die vom Passport-Server hinterlegt werden als auch die, die vom Web-Server zu Zwecken der Authentisierung im Browser Verzeichnis des Benutzers gespeichert wurden.

Da die Cookies nur jeweils von dem Web-Server gelöscht werden können, von dem sie abgelegt wurden, muss ein „work around“ verwendet werden. Dabei kommt die Liste der besuchten Web-Seiten, die der Passport Server im Browser des Benutzers in Form von Cookies abgelegt hat zum Einsatz. Der Server nimmt diese Liste und ruft ein Script auf dem jeweiligen Server auf, welches die Löschung der Cookies durchführt. Diese Praxis ist allerdings fehleranfällig, da sie voraussetzt, dass sich ein Benutzer immer korrekt abmeldet und auch die einzelnen Web-Seiten das Löschen der Cookies richtig umgesetzt haben.

Die Verbindung zwischen Passport Server und Browser sind immer durch SSL entsprechend geschützt, so dass ein einfaches Spoofing der Web-Seiten verhindert werden kann und auch sichergestellt ist, dass Benutzername und Passwort nie im Klartext übertragen werden.[8] Für den Schutz der Verbindung zwischen Browser und Web-Server gibt es dagegen zwei verschiedene Sicherheitslevel.

- Im sogenannten Standard Sign-In [MIC01] wird das verschlüsselte Ticket für den Web-Server nicht über eine verschlüsselte SSL Verbindung übertragen. Es kann damit bei der Übertragung von einem Angreifer abgefangen und später dazu verwendet werden, sich gegenüber dem Server zu authentifizieren (Replay Attacke). Dieses Sicherheitsniveau ist daher nur für sehr niedrige Sicherheitsniveaus zu empfehlen.
- Beim sogenannten Secure-Channel Login [MIC01] dagegen wird die komplette Strecke mit SSL geschützt, was ein abfangen des Tickets erschwert.

Der Web-Seiten Betreiber entscheidet, welche Methode der Authentisierung gefordert wird. Die Cookies und Tickets, die bei einem Login erstellt werden, unterscheiden sich, je nachdem ob Standard oder Secure Channel Login verwendet wird.

Passport unterstützt außerdem noch eine dritte Sicherheitsstufe, den sogenannten Strong Credential Login. Hierbei kann vom Benutzer verlangt werden, sich zusätzlich zum normalen Login mit Hilfe einer weiteren vierstelligen PIN gegenüber Passport zu authentisieren. Dies ist für hohe Sicherheitsanforderungen gedacht. Bei dieser Variante sind die Regeln zum Umgang mit falschen Login-Versuchen schärfer als bei den anderen beiden Varianten.[9]

5 Alternativen

Neben Microsoft haben auch andere die Notwendigkeit einer verbesserten Authentisierung erkannt und versucht, andere konkurrierende Modelle zu entwerfen. Prominentestes Beispiel ist hier sicher die Liberty Alliance[10] die unter Führung des Microsoft Rivalen Sun 2001 entstanden ist. Ihr haben sich bereits eine Reihe namhafter Firmen angeschlossen. Ziel ist es, eine offene Spezifikation zu entwerfen, die eine dezentralen Authentisierung im Internet ermöglicht, und somit die Authentisierung auf mehrere Anbieter verteilt realisiert werden kann. Bis heute sind allerdings noch keine Details der geplanten Spezifikation bekannt. In den letzten Pressemitteilungen wird angekündigt, dass die erste Version der Spezifikation Mitte des Jahres verfügbar sein soll.

Weitere Aktivitäten finden im Rahmen der DotGnu Initiative[11] als Teil des Virtual Identity Projekts statt. Hier wird ebenfalls an einer Lösung des Authentisierungsproblems gearbeitet. Als erstes Ergebnis gibt es hier bereits einen ersten Internet-Draft, der einen solchen Dienst beschreibt [ZAN02].

Obwohl über keine der Alternativen Details bekannt sind, werden sich diese von der derzeitigen Version des Passport-Service hauptsächlich dadurch unterscheiden, dass sie keine rein zentralen Dienste sein werden. Vielmehr werden hier verteilte Modelle zum Einsatz kommen, bei denen die Authentisierung auf mehrere Dienstleister verteilt sein wird. Dies löst einige der Probleme des zentralen Passport Service, wirft aber auch neue Fragen auf, z.B. wie ein einheitliches Sicherheitsniveau zwischen den verschiedenen Authentisierungsdienstleistern hergestellt werden kann, oder wie die Vertrauensbeziehungen zwischen den Servern hergestellt werden.

In der Praxis könnte dies so aussehen, dass das Profil des Benutzers bei einem Betreiber liegt, dem der Benutzer sowieso vertraut, z.B. der Online-Bank. Dieser Betreiber ist dann auch für die Authentifizierung zuständig. Wenn der Benutzer sich auf einer anderen Web-Seite einloggen will, kann der neue Server die Authentisierung beim Authentifizierungsserver anfordern.

Neben den anderen Konkurrenten hat auch Microsoft angekündigt, in zukünftigen Versionen des Passport Services verteilte Authentifizierung zu unterstützen. Außerdem ist angekündigt auf Kerberos als Authentisierungsprotokoll umzusteigen. Kerberos ist ein Protokoll, das eine solche verteilte Authentifizierung ermöglichen könnte, und das immer wieder im Zusammenhang mit Authentisierungsdiensten genannt wird.

Fazit

Obwohl Microsoft angibt, dass es bereits über 200 Millionen registrierte Passport Benutzer gibt, ist die tatsächliche Nutzung dieses Dienstes noch nicht weit verbreitet. Die hohe Anzahl an registrierten Benutzern ist hauptsächlich darauf zurück zu führen, dass alle Accounts des freien E-Mail Anbieters Hotmail[12] automatisch auf Passport Accounts umgestellt wurden. In der Realität ist die Anzahl der aktiven Benutzer des Passport Dienstes, sowie der Web-Server, die Passport zur Authentisierung einsetzen, noch relativ gering. Offensichtlich ist entweder der Bedarf noch nicht vorhanden, oder Microsoft tut sich weiterhin schwer, die Internet-Welt davon zu überzeugen, dass

[8] Im Laufe der Tests war dies nicht immer der Fall, eine Systematik ließ sich allerdings noch nicht erkennen.

[9] Beim normalen Login wird zum Erschweren von Brute-Force-Attacken der Passport Account nach mehreren falschen Versuchen mehrere Minuten gesperrt. Beim Strong Credential Login wird der Zugang zum Strong Credential Login nach Fehlversuchen komplett gesperrt und muss explizit wieder freigeschaltet werden.

[10] http://www.projectliberty.org/

[11] http://www.dotgnu.org

[12] Hotmail ist ein Dienst von Microsoft

man Microsoft in Sicherheitsfragen trauen kann.

Insgesamt hat ein solcher zentraler Dienst einige gravierende Nachteile. Durch den „Single Point of Failure“ wird einer der großen Vorteile des Internets, seine verteilte und damit robuste Architektur stark beeinträchtigt. Die Erfahrung zeigt, dass die Sicherheit im Internet noch nicht ausgereift genug ist, um ein solch verlockendes Ziel, das ein solcher zentraler Dienst darstellt, adäquat gegen die verschiedenen Arten von Angriffen schützen zu können – unabhängig vom Betreiber einer solchen Dienstleistung.

In der gegenwärtigen Version des Passport Service sind auch noch eine Reihe von Kompromissen eingegangen worden, um den Benutzerkomfort zum jetzigen Zeitpunkt und ohne zusätzliche Softwareinstallationen zu realisieren. So werden Techniken zur Sicherung des Dienstes eingesetzt (z.B. Cookies) , die hierfür nicht entwickelt wurden und auch nur bedingt geeignet sind.

Außerdem leidet der Passport Service natürlich auch unter den allgemeinen Sicherheitsmängeln des Internets, mit denen auch andere Web-Server zu kämpfen haben (z.B. DNS-Spoofing). Ob das so erreichte Sicherheitsniveau den Anforderungen entspricht, sollte also kritisch geprüft werden.

Besonders kritisch ist die potentielle Datensammlung und Profilbildung, die eine solcher Dienst ermöglicht. Auch wenn versichert wird, dass dies nicht geschieht, ist die Verlockung, einen solchen Dienst in diese Richtung zu missbrauchen, sicher groß. Außerdem ist die Bewertung dieses Kriteriums auch stark vom dem Betreiber entgegen gebrachten Vertrauen abhängig. Es ist daher sehr kritisch zu hinterfragen, ob die zentrale Speicherung aller dieser Daten (unabhängig davon wer einen solchen Dienst betreibt) der richtige Weg ist.

Wie sich der Markt der Authentisierung im Web entwickeln wird ist derzeit noch nicht abzusehen. Viel wird auch davon abhängen, ob sich die von vielen Firmen angekündigten Web-Services durchsetzen werden. Eine Voraussetzung dafür ist sicherlich auch, dass das Problem der Authentifizierung zufriedenstellend gelöst werden kann, um das Vertrauen der Benutzer und Anbieter in solche Dienstleistungen zu gewinnen.

Passport ist derzeit das einzige funktionierende System und hat damit natürlich einen entscheidenden Startvorteil. Allerdings hat es Microsoft derzeit schwer, Akzeptanz bei den Anbietern zu finden. Angetrieben von dieser mangelnden Akzeptanz und der offensichtlich großen Unterstützung, die die Liberty-Alliance erfährt, könnte hier aber durchaus eine ernsthafte Alternative entstehen.

In wie weit die Datenschutzaspekte bei diesen Entwicklungen eine Rolle spielen werden ist noch nicht abzusehen. Dies ist speziell vor der sehr oft sehr unterschiedlichen Wahrnehmung und Bewertung von Datenschutzaspekten in den USA und in Europa (und speziell in Deutschland) abhängig.

Literatur

[ESMÜ97] Esslinger, Bernhard; Müller, Maik: *Secure Sockets Layer (SSL) Protokoll*. Datenschutz und Datensicherheit (DuD), 12/1997, S. 691-697.

[KOR00] Kormann, David P.; Rubin, Aviel D.: *Risks of the Passport Single Signon Protocol*, Computer Networks, Elsevier Science Press, Vol. 33, pages 51-58, 2000.

[KUWÖ02] Kuschke, Michael; Wölfel, Ludger: *Microsoft Passport und Konkurrenten*, iX 2/2002, S. 96-98.

[MIC01] Microsoft .NET Passport – *Security and Privacy Overview*, Oktober 2001, Microsoft Corporation

[MIC02] Microsoft .NET Passport – *Technical Overview*, September 2001, Microsoft Corporation

[MIC03] Microsoft .NET Passport – *SDK Documentation Version 2.1*, 2001, Microsoft Corporation

[MIC04] Microsoft .NET Passport – *Privacy Statement*, Oktober 2001, Microsoft Corporation

[MÖKE00] Möller, Klaus; Kelm, Stefan: *Distributed Denial of Service Angriffe*. DuD 5/2000, S. 292-293.

[SIE02] Siering, Peter: *Das Microsoft-Internet. .NET und was dranhängt*. c't 4/2002, S. 86 ff.

[SLE01] Slemko, Marc: *Microsoft Passport to Trouble*, Rev 1.18, November 2001

[WICH98] Wichert, Michael: *Web-Cookies – Mythos und Wirklichkeit*, DuD 5/1998, S. 273-276.

[ZAN02] Zandbelt, Hulsebosch: *IDSec: Virtual Identity on the Internet*, January 2002, Internet Draft, IETF