МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
(ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ)

Вопросы безопасности и конфиденциальности Microsoft Passport

Эссе по курсу “Теория защиты информации ” студента
011 группы ФРТК Белешко А.С.

МОСКВА 2004

Предисловие

Microsoft Passport – это протокол, который позволяет пользователям подписываться на многих коммерческих веб страницах, аутентифицируя себя только на один раз на общем сервере. Microsoft Passport привлекателен тем, что он очень широко распространен. Со времени его запуска, он стал одной из самых больших онлайновых систем аутентификации в мире, с более чем 200 миллионов учетных записей выполняющей более3.5 миллиардов аутентификаций каждый месяц. Microsoft Passport используется на таких сайтах, как Nasdaq, McAfee, Expedia.com, eBay, Cannon, Groove, Starbucks, MSN® Hotmail, MSN Messenger, и другие. В этой статье обсуждаются протоколы Microsoft Passport и рассмотрены некоторые возможные атаки на систему.

Введение

Многие банки, торговые предприятия и др. стали предоставлять покупателям онлайновые сервисы, используя веб технологии. Для того чтобы быть уверенным в безопасности частных данных покупателей, онлайновые системы обычно требуют имя пользователя и пароль. При этом пользователь ставятся перед дилеммой, когда приходится создавать очередную учетную запись. Использовать ли они одинаковые имена пользователей и пароли для всей ученых записей? Если так, то это значит, что, например, онлайновый магазин продуктов будет иметь доступ к пользовательским ученым записям в онлайновой финансовой бирже. Альтернативой является создание списка, содержащего имена пользователей и пароли. Однако использование подобного списка содержит потенциальную опасность, если злоумышленник украдет его, то получит возможность аутентифицировать себе вместо вас во всех, используемых вами системах .

“Single signon”– термин, который используется для описания систем, где от пользователя требуется запомнить только одно имя пользователя и один пароль, и в дальнейшем аутентификацию можно будет проводить в различных системах. Система Kerberos – пример системы, где пользователь сообщает пароль и получает мандат взамен. Мандат может быть использован для аутентификации пользователей в различных сетевых системах. Kerberos - это “single signon” система, так как в ней, все сервисы находятся под одним административным управлением. В ее рамках существует централизованная БД, где содержатся ключи, доступные конкретному сервису, причем мандаты могут создаваться зашифрованными с помощью ключей данного сервиса.

Система single signon в приложении к веб намного более сложна. Различные веб сайты находятся под разным административным управлением. Т.о., странно представлять возможность подписаться один раз и получать аутентификацию в различных независимых веб сервисах. Microsoft Passport – это попытка Microsoft обеспечить такой сервис. В целом возможности системы ограничены возможностями использующихся веб технологий (тех технологий, которые поддерживаются большинством браузеров), мы ограничимся лишь обзором нескольких возможных проблем в безопасности при использовании этой системы.

Как мы только упомянули, одно из ограничений Microsoft Passport – это то, что он был создан на основе существующих веб технологий, чтобы клиент и сервер не нужно было модифицировать. Microsoft Passport использует HTTP redirects, JavaScript, cookies и SSL. JavaScript не обязателен, но его желательно использовать.

Как работает Microsoft Passport

Мы рассмотрим протоколы Microsoft Passport single signon и wallet. В модели Microsoft Passport, существуют 3 стороны: клиент с веб браузером (обычно это пользователь, который уже зарегистрировался в службе Microsoft Passport), коммерческая служба

(магазин или набор магазинов, в которых пользователей собирается совершить покупку) и регистрационный сервер Microsoft Passport (Password login server). Регистрационный сервер обслуживает аутентификацию, управляет информацией содержащейся в профиле пользователя и дает коммерческой службе доступ к этой информации, когда это разрешено пользователем.
Учетная запись пользователя Microsoft Passport состоит из четырех элементов: идентификатора Microsoft Passport Unique Identifier (PUID), учетных данных (credential), пользовательского профиля и бумажника. Когда пользователь создает учетную запись, система Microsoft Passport генерирует PUID, идентифицирующий учетную запись в базе данных. Учетные данные Microsoft Passport состоят из адреса электронной почты, который применяется в качестве регистрационного имени, и пароля, содержащего не менее шести символов. При желании пользователь может указать имя, фамилию, страну проживания, штат, пол, дату рождения в своем профиле. Через профиль пользователь может сообщить адрес электронной почты, имя и другую личную информацию сайтам, которые входят в систему Microsoft Passport. Лица, желающие пользоваться службой электронных платежей должны сохранить номера кредитных карт, адреса платежей и доставки товаров в бумажнике Microsoft Passport.
Протокол Microsoft Passport создан для обеспечения безопасного обмена информации пользователя из профиля и бумажника между сервером Microsoft Passport и коммерческой службой.

Протокол single signon

Взаимодействие Microsoft Passport с пользователем начинается, когда клиент, посещающий коммерческий сайт, нуждается в аутентификации (для ввода некоторой персональной информации или совершения покупки). Коммерческий веб сервер перенаправляет браузер к серверу Microsoft Passport. Сервер открывает пользователю страницу регистрации через SSL соединение. После успешной аутентификации сервер Microsoft Passport извлекает PUID и соответствующую информацию из профиля пользователя (которую тот согласился предоставить сайтам-участникам). Сервер Microsoft Passport генерирует и записывает в браузер пользователя пять cookies, поэтому во время Internet-сеанса сервер может определить PUID пользователя, дату последнего обращения, список сайтов, на которых зарегистрирован пользователь, информацию из профиля пользователя и другие предоставленные сведения. Далее сервер Microsoft Passport шифрует PUID, время последнего обращения и информацию из профиля пользователя в cookies. Затем сервер Microsoft Passport направляет браузер пользователя по старому URL. Сервер Microsoft Passport шифрует PUID с использованием triple DES и общую информацию профиля с помощью ключа шифрования сайта, назначенного службой Microsoft Passport, затем вводит зашифрованный PUID и информацию в строку запроса, посылаемую по старому адресу URL.
Web-узел извлекает зашифрованный PUID и информацию профиля из строки запроса и восстанавливает данные с помощью ключа шифрования сайта. Затем сайт создает и шифрует две уникальные для данного сайта cookies Microsoft Passport, которые содержат PUID, время обращения и информацию из профиля, и записывает cookies в браузер пользователя. Web-узел использует эти две cookies в текущем сеансе связи.
Этот процесс показан на рисунке 1.

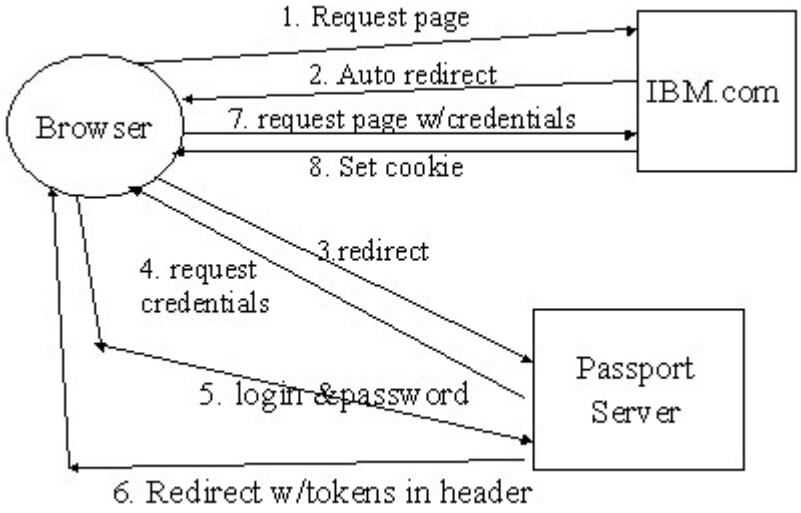

Рисунок 1. Архитектура Microsoft Passport

Идея в том, что когда пользователь возвращается, например, на сайт IBM, зашифрованное cookie, как правило, сохраняется. Сайт может дешифровать cookie, и убедиться, что пользователь уже аутентифицирован. Сервер Microsoft Passport также устанавливает cookie. Таким образом, если пользователь посещает другой сайт, например dell.com, когда браузер перенаправляет на сервер Microsoft Passport, пользователю уже не показывается регистрационная страница, а используется предыдущий cookie Microsoft Passport. Если это cookie содержит подходящие разрешения, клиент перенаправляется обратно на коммерческий сайт без его участия.

Протокол Wallet

Протокол Wallet очень похож в своей основе на single signon. В замену просто информации для аутентификации, пользователь может разместить на сервере Microsoft Passport информацию о своих кредитных картах. Т.о., когда он делает покупку на сервере, он может выбирать какую информацию открывать для этого магазина. Пользователь при этом освобождается от необходимости каждый раз вводить платежную информацию для совершения покупки на сайтах магазинов и т.п.

Безопасность Microsoft Passport

В этих пунктах мы рассмотрим некоторые проблемы безопасности протокола Microsoft Passport и некоторые специфические атаки.

Центральные места для атаки.

Как и все single-signon системы, Microsoft Passport обеспечивает сервис, которому доверяют произвести решение об аутентификации пользователя. Соглашение о такой центральной службе может быть чрезвычайно пагубно. Кроме данных об аутентификации, регистрационная служба Microsoft Passport содержит информацию из профилей всех зарегистрированных пользователей. Сохранение подобной информации в одном месте, хотя и удобно, делает сервер чрезвычайно привлекательной целью, как для DoS атак, так и для атак, с целью получения неавторизованного доступа.
Эффект Dos атак на регистрационный сервер особенно ощутим. Очевидно, использование таких систем, как Microsoft Passport возрастает в прямой пропорции от количества коммерческих служб на него подписанных. Но, так как количество коммерческих сайтов поддерживающих сервис растет, возможность выхода из строя возрастает. Оператор большого онлайнового магазина, не использующего службу Microsoft Passport должен

наблюдать значительное увеличение трафика (следовательно, и прибыли) из-за невозможности (или даже сложности) для пользователей сайта Microsoft Passport получить доступ к их цифровым бумажникам (wallet) и данным из профиля. Недобросовестный конкурент может просто загружать сайт Microsoft Passport поддельными регистрационными профилями или входами в систему.
Обычным решение проблем доступности сервера является дублирование сервисов, чтобы уменьшать возможность катастрофичных отказов. К сожалению, нет никакой информации о том, как Microsoft решает эту проблему.

Cookies и JavaScript

В стандарте Microsoft Passport описывается использование двух веб технологий. Cookies используются для хранения удостоверяющей информации в зашифрованном виде в браузерах. А JavaScript используется, чтобы сделать некоторые транзакции более эффективными (меньше использование HTTP redirects) и также, чтобы создавать более централизованного вида веб страницы. Согласно спецификации Microsoft Passport пользователь может отключить использование JavaScript в браузере, это не приведет к существенному уменьшению функциональности. Но система не работает без использования cookie.
Обычно, опасность cookie связана с возможность открытия его содержания неуполномоченному получателю. Так как cookie Microsoft Passport содержат важные данные, система зашифровывает данные, используя 3DES. Время жизни cookie Microsoft Passport на машине клиента определяются только временем открытия веб браузера и временем, указанным в cookie. Т.о. на общедоступной машине пользователь, кто забыл выйти из системы, может оставить действительную аутентификационную метку (authentication token) на машине, где ее может использовать злоумышленник.

Надежные cookies

Microsoft Passport оставляет аутентификаторы в форме cookies в браузере клиентского компьютера. Как говорит спецификация системы, “эта возможность сохраняет пользователя аутентифицированным в системе Microsoft Passport все время, даже если пользователь отсоединен от Интернета, закрыл браузер или выключил компьютер”. Идея в том, чтобы иметь надежного аутентификатора, т.о. пользователю не нужно будет заново вводить пароль. Сервер Microsoft Passport не сможет пересмотреть статус пользователя, если время жизни cookie еще не истекло. Это похоже на single signon в Kerberos.

Kerberos использует мандаты, которые представляют собой зашифрованные имя пользователя и пароль. Они обеспечивают аутентификацию на определенное количество времени, при этом, не требуя повторную регистрацию в системе. Однако, Microsoft Passport не содержит одного из фундаментальных свойств single signon. А именно, там нет понятия аутентификатор. В Kerberos клиент должен посылать аутентификатор, чтобы доказать знание ключа в мандате. Чтобы сделать это, клиент просто шифрует временную метку (timestamp). Если временную метку можно расшифровать, то клиент использует правильный ключ. Это предотвращает воровство мандатов оставленных на компьютерах. В Microsoft Passport роль мандата выполняют cookie. Обладание конкретным cookie – это все, что нужно для установления конкретного пользователя. А, учитывая некоторые современные вирусы, способные похитить этот cookie, делает использование Microsoft Passport очень небезопасным. Чтобы избежать подобной ситуации, в Microsoft Passport 2.0 (последняя на данный момент версия), помимо cookies стандартного входа, регистрационный сервер Microsoft Passport и Web-узел генерируют защищенные HTTPS-cookies, которые нельзя изменить.

Используемые форматы cookies описаны в Microsoft's Passport SDK. Рассмотрим наиболее важные из них.
MSPSec cookie аутентифицирует вас в Microsoft Passport, реализовывая возможности single signon. Т.е оно позволяет вам быть прозрачно аутентифицированными на всех сайтах, которые поддерживают Microsoft Passport. Т.е., если кому то необходимо аутентифицировать себя, как вас, то ему необходимо получить это cookie.
Другое важное cookie – это MSPAuth cookie. Оно идентифицирует вас веб серверу, с использованием 64-битного Уникального ID Microsoft Passport (PUID), которое присваивается вашей ученого записи. Оно также содержит две временные метки: время последнего "обновления" cookie, и время последнего "ручного" входа в систему Microsoft Passport.

Сайты, которые требуют более жестких мер по авторизации, чем "вы вошли (sign in) однажды по учетной записи Microsoft Passport и не вышли (sign out) до сих пор", могут требовать, что время последнего "ручного" входа в систему не превышает заданного значения. Например, Цифровой бумажник Microsoft Passport (Passport Wallet) требует, чтобы это время не превышало 15 минут.

Когда вы регистрируетесь в Microsoft Passport, вы можете выбрать опцию "оставаться зарегистрированным". При этом cookie, установятся с бесконечным временем жизни. Если вы не выбрали эту опцию, то все cookie истекают, когда вы закрываете ваш браузер. В том и другом случае, большинство cookies остаются действительными, несмотря на то, что они истекли в вашем браузере, но с некоторыми ограничениями:

- MSPAuth cookie содержит временные метки, указанные выше; это позволяет сайту требовать, что ваш билет на старше какого то времени, но это делают не все сайты.
- MSPSec cookie содержит ваш Microsoft Passport, т.е. при смене пароля, оно не будет действительным
- MSPProf cookie содержит информацию о профиле, т.о. оно становится не обновленным (но все еще действительным), после обновления профиля.

Т.о. если у вас есть cookie, для аутентификации на конкретном домене, тогда те сайты, которые не беспокоятся о свежести cookie, будут принимать эту информацию.

Атаки на Microsoft Passport

Фиктивный коммерческий сервер

Возможный фиктивный коммерческий сервер – это одно из слабых мест Microsoft Passport. Представьте, что пользователи привыкли использовать Microsoft Passport. Им нравится удобство single singon и служб цифрового бумажника. Возможно первый раз, когда они и использовали этот сервис и аутентификацию на сервере Microsoft Passport они действительно проверили сертификат SSL соединения. Вряд ли, они действительно сделали это. Еще невероятней, что они продолжают проверять сертификат каждый раз, когда они возвращаются на этот сайт.
Теперь, сам механизм атаки. Некий злоумышленник устанавливает фиктивный веб-магазин, продающий, что-нибудь привлекательное. Кроме того, он получает сертификат для домена, который он установил, например pasport.com. Злоумышленник должен убедить некоторую легитимную Сертификационную Службу сертифицировать его использование этого доменного имени. Затем пользователь посещает фиктивный веб магазин, сервер симулирует перенаправление не passport.net, и пользователю показывают страницу для входа, которая точно такая же, что и на официальном сервере Microsoft Passport. Пользователь обычно заполняет ее, не обращая внимание на URL с

орфографической ошибкой и не просматривая сертификаты SSL. Даже если он и проверит сертификат, он может не заметить неправильно написанное слово “passport”.

После того, как пользователь заполнил всю эту информацию и отправил ее, фиктивный веб сайт может далее делать с данными пользователя все, что ему захочется. Важно, что злоумышленник получил действительную для аутентификации информацию, и теперь он может аутентифицировать себя, как данный пользователь, использовать его цифровой бумажник, продавать личные сведения, и т.д.

Активная атака.

Злоумышленник с доступом к сети между клиентским веб браузером и коммерческим сервером (и способностью переписывать пакеты, проходящие между этими двумя хостами) может получить те же результаты, что, и описано выше оставляя нормальным взаимодействие клиента с коммерческим сайтом. Такой доступ не сильно сложно осуществить. Большие Интернет провайдеры концентрируют трафик тысячи пользователей через сравнительно малое количество маршрутизаторов и серверов. Получение не авторизованного доступа к одному из этих хостов ставит атакующих между пользователями и всеми службами, куда они хотят получить доступ. Любой трафик, проходящий через такой “захваченный” хост может быть прочитан и переписан. Злоумышленник использует тот факт, что пользователь вряд ли проверяет содержание URL или сертификаты, исключая, может быть, некоторые экстраординарные случаи (когда веб браузер находит несоответствие между сертификатом и URL сервера). Атака также полагается на возможность атакующего идентифицировать процесс начала аутентификации. Это просто. Предположим, что клиент соединяется с коммерческим сервером, используя регистрационный сервис www.passport.net. Атакующий, ждет между клиентом и коммерческим сайтом, ожидает HTTP redirect на www.password.net. От коммерческий сайта требуется произвести redirect в начале сессии Microsoft Passport, при этом redirect не защищен SSL. Видя redirect, взломщик перехватывает пакеты и переписывает URL в HTTP redirect на ранее установленный поддельный сервер Microsoft Passport, здесь можно воспользоваться похожими доменными именами и легитимными сертификатами, чтобы этот сервис казался подлинным. Сервер теперь работает, как прокси между клиентом и www.passport.net, и между клиентом и коммерческим сайтом, изображая сервис Microsoft Passport для клиента и обратно, переписывая все URLы и HTTP перенаправления, чтобы направлять трафик через прокси. Использование Microsoft Passport SSL не может на этом этапе предотвратить возможность прокси читать и переписывать пакеты, так как все SSL соединения завершаются на прокси, и пользователь вряд ли заметит прокси от его имени.
Хотя взломщик, не сможет прочитать содержание зашифрованных cookies (извлечь номера кредитных карт и персональную информацию), будет довольно легко сохранить пароль пользователя и использовать его, чтобы получить информацию из сохраненного профиля пользователя
Рисунок 1 показывает процесс переписывания пакетов взломщиком и прокси сервис, как компонент архитектуры Microsoft Passport показан на рисунке 1. Злоумышленник обеспечивает поддельный аутентификационный сервис на www.psport.com и компрометирует хост на пути между браузером клиента и коммерческим сайтом, на www.ibm.com

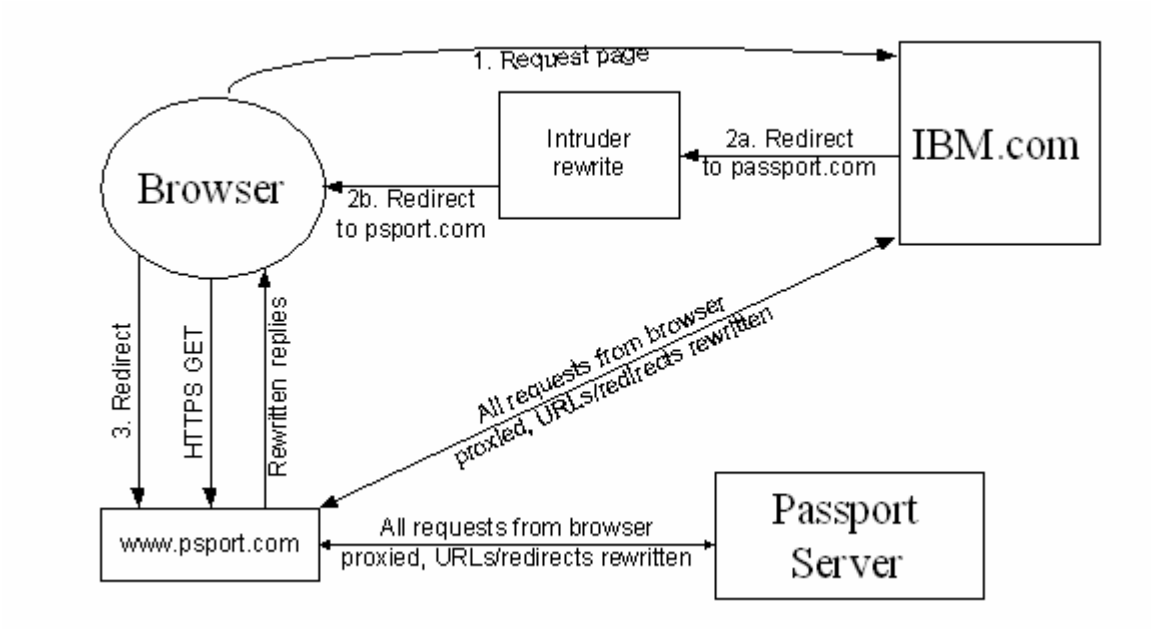

Рисунок 2.

Заключение

С распространением систем электронной коммерции, просто необходимы инструменты для управления аутентификацией пользователя. Microsoft Passport – это попытка создать подобную службу, не требуя изменений в существующих браузерах и серверах. В отрасли продолжаются споры о конфиденциальности и безопасности Microsoft Passport, но потребители, похоже, уже сделали выбор: к настоящему времени в системе Microsoft Passport зарегистрировались несколько сотен миллионов пользователей и более 100 веб сайтов используют ее для средств аутентификации.

Литература

1. Официальный сайт Microsoft Passport www.passport.net
2. *Microsoft .NET Passport Review Guide*
   John Spilker
   www.microsoft.com, 2004
   (http://www.microsoft.com/net/services/passport/review_guide.asp)
3. *Risks of the Passport Single Signon Protocol*,
   David P. Kormann and Aviel D. Rubin,
   Computer Networks, Elsevier Science Press, volume 33, pages 51-58, 2000.
   (http://avirubin.com/passport.html)
4. *.NET Passport в электронной коммерции*
   Тао Чжоу
   Журнал "Windows & .NET Magazine/RE", #04, 2002