МОСКОВСКИЙ ФИЗИКО - ТЕХНИЧЕСКИЙ ИНСТИТУТ

(ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ)

Microsoft .NET Passport.

Эссе по курсу “Теория защиты информации ” студента

912 группы ФРТК Щербинина С.П.

МОСКВА 2003

Учетная информация о потребителях, в частности регистрационные имена пользователей, пароли и номера кредитных карт, хранится в собственных базах данных многих Web-узлов электронной коммерции. В результате пользователю приходится помнить несколько наборов учетной информации - нередко отдельный набор для каждого сайта, где он что-либо заказывал. Пользователи, забывшие свое имя или пароль для регистрации на одном из сайтов, часто предпочитают отказаться от посещений, чтобы избежать хлопот, связанных с получением новой учетной записи. Кроме того, многие потребители из соображений конфиденциальности и безопасности нередко отказываются от регистрации и получения учетной записи, чтобы не открывать личную информацию (например, дату рождения или пол).

Очевидно, что проблемы есть, и их надо решать. Это можно сделать с помощью систем единого входа, когда пользователь может использовать единые идентификационные данные на разных ресурсах. Одной из таких систем является Microsoft Passport.

Процесс проверки прав пользователя на доступ к ресурсам состоит из двух частей – аутентификации (идентификации) и авторизации. Аутентификация только идентифицирует пользователя, проверяет тот ли он, за кого себя выдает. Авторизация – это проверка для уже идентифицированного пользователя, имеет ли он доступ к определенному ресурсу или право на выполнение определенной операции. Причем первая составляющая присутствует во всех системах, а вторая – только в системах, где нужно предоставлять разный доступ разным пользователям

Microsoft .NET Passport - система аутентификации пользователей, позволяющая клиентам Internet-магазинов завести одно имя и один пароль для регистрации, доступа к Web-службам и совершения покупок на всех Web-узлах, которые являются членами системы. Пользователи могут контролировать личную информацию, которая попадает в учетные записи и сообщается на посещаемые ими сайты (группа компаний Liberty Alliance Project, организованная по инициативе Sun Microsystems, работает над аналогичной системой и предлагает Microsoft объединить усилия). .NET Passport поможет администраторам и разработчикам Web-сайтов сэкономить время, затрачиваемое на управление процедурами идентификации пользователей. Поняв сущность и принципы работы .NET Passport, можно построить удобный в управлении сайт электронной коммерции с высоким уровнем обслуживания потребителей.

Службы и системная конфигурация

.NET Passport предлагает три службы: единый вход (sign-in, SSI), экспресс-покупка (express purchase, EP) и детский паспорт (Kids Passport). Благодаря службе SSI пользователи могут создать одну учетную запись для доступа к .NET Passport-совместимым службам, таким, как персонализированные страницы в .NET My Services (в прошлом эта служба была известна под названием HailStorm). Служба EP позволяет хранить информацию о кредитных картах, адресах платежей и доставки в электронном бумажнике .NET Passport, чтобы не вводить информацию повторно для оплаты каждого заказа. Служба Kids Passport полностью отвечает требованиям закона о защите детей в сети (Children?s Online Privacy Protection Act, COPPA), в соответствии с которым владельцы Web-узлов должны получить согласие родителей на использование и публикацию личных данных детей.

Система .NET Passport организует центральное хранилище учетных записей и выполняет аутентификацию пользователей для сайтов-участников, поэтому Web-узлам не нужны собственные базы учетных записей. Система состоит из базы учетных записей .NET Passport, нескольких сетевых серверов, называемых компанией Microsoft регистрационными

(Registration) серверами, сервера Member Service, серверов Update, Login, Wallet и Kids. Серверы Registration, Member Service и Update позволяют создавать и изменять учетные записи пользователей. Сайты, которые являются членами системы .NET Passport, применяют сервер Login для аутентификации пользователей через службу SSI, сервер Wallet выдает информацию о кредитных картах через службу EP, а сервер Kids обеспечивает соответствие требованиям COPPA через службу Kids Passport. Компания Microsoft размещает хранилище учетных записей .NET Passport и сетевые серверы в защищенном информационном центре.

Что такое учетная запись?

Учетная запись пользователя .NET Passport состоит из четырех элементов: идентификатора .NET Passport Unique Identifier (PUID), являющегося 64-разрядным двоичным числом,

учетных данных (credential), пользовательского профиля и бумажника. Когда пользователь создает учетную запись, система .NET Passport генерирует PUID, идентифицирующий учетную запись в базе данных. Учетные данные .NET 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 .NET Passport. Лица, желающие пользоваться службой EP, должны сохранить номера кредитных карт, адреса платежей и доставки товаров в бумажнике .NET Passport.

Учетные записи .NET Passport предоставляются пользователям бесплатно. Учетная запись .NET Passport автоматически создается при регистрации в службе MSN Hotmail, персональных страниц MSN или регистрации Windows XP с помощью мастера Registration Wizard. Пользователи, не получившие учетной записи одним из этих методов, могут создать ее на специальном Web-узле регистрации. Для защиты информации, пересылаемой в процессе регистрации, используется протокол Secure Sockets Layer (SSL); в базе данных конфиденциальная информация о пользователях шифруется с применением алгоритма Triple DES (3DES) (в том числе пароль и сведения о кредитной карте). Сразу же после того, как пользователь получает учетную запись, .NET Passport посылает ему по электронной почте сообщение для проверки адреса.

Служба SSI

Пользователь, получивший учет-ную запись .NET Passport, может обратиться к службам Web-сайта - участника системы .NET Passport. На сайтах-участниках отображается официальная ссылка на .NET Passport Sign In. Когда пользователь щелкает по ссылке, Web-узел использует метод переадресации HTTP, чтобы направить браузер пользователя на сервер .NET Passport Login. В строке переадресации указывается URL сервера, например http://login.passport.com/login.srf, за которым следует строка запроса. Строка запроса начинается с вопросительного знака (?) и содержит код языка Web-узла, ID, URL возврата и другие данные, необходимые серверу Login. Используя ID и URL возврата, сервер Login проверяет, зарегистрирован ли Web-узел в системе .NET Passport, а затем выдает стандартную страницу входа .NET Passport. Эта страница может быть выведена в соответствии с дизайном зарегистрированного Web-сайта. В этом случае на странице присутствует логотип сайта-участника, его оформление и другая информация. Диалоговое окно регистрации может быть интегрировано с Web-узлом; компания Microsoft называет этот метод встроенным входом - inline sign-in.

После ввода учетных данных пользователь щелкает на кнопке Sign In в диалоговом окне Sign-in. В результате генерируется запрос на аутентификацию пользователя, в который методом HTTP POST вносятся учетные данные, и устанавливается соединение SSL с сервером .NET Passport Login. Затем запрос на аутентификацию пользователя и его данные поступают на сервер Login. Страница входа всегда связывается с сервером Login через SSL, и сайт-участник не принимает учетных данных; это делает только сервер Login.

Сервер Login сравнивает учетные данные с информацией в базе учетных записей .NET Passport. Если пользователь пять раз подряд вводит неверный пароль, то сервер Login на 5 мин блокирует учетную запись. После успешной аутентификации сервер Login извлекает PUID и соответствующую информацию из профиля пользователя (которую тот согласился предоставить сайтам-участникам). Сервер Login генерирует и записывает в браузер пользователя пять cookies .NET Passport, 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. Сервер Login шифрует PUID, время последнего обращения и информацию из профиля пользователя в cookies. Затем сервер Login направляет браузер пользователя по старому URL. Сервер Login шифрует PUID и общую информацию профиля с помощью ключа шифрования сайта, назначенного службой .NET 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 .NET 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.

После того как пользователь успешно выполнит процедуру входа, сайт-участник отображает официальную ссылку .NET Passport Sign Out. Сайт-участник, а не система .NET Passport, проводит авторизацию и обеспечивает доступ пользователя к конкретным ресурсам и службам сайта. В целях безопасности, срок действия авторизации на сайте-участнике ограничен (по умолчанию - 4 ч). По истечении этого срока пользователь должен повторить процедуру входа.

После того как пользователь выполнил процедуру входа с помощью .NET Passport на сайте-участнике, ему не нужно повторно вводить данные на других сайтах-участниках, посещаемых им в текущем сеансе работы в Internet, за исключением тех случаев, когда Web-узел требует повторного ввода информации в качестве дополнительной меры безопасности. Сервер Login скрыто проверяет другие сайты, просматривая cookies в браузере, выясняет, что пользователь уже зарегистрировался, обновляет cookies и пересылает шифрованный PUID и общую информацию из профиля пользователя на другие сайты, в соответствии с описанной выше процедурой. . Сессия действует не в рамках одного сайта, а в рамках всех сайтов системы паспорт.

Для завершения сеанса пользователь щелкает на ссылке Sign Out. Процедура выхода передает в сервер Login команду удалить cookies .NET Passport и запускает сценарий, который удаляет с каждого сайта специфические cookies. Все cookies .NET Passport - временные. Поэтому, даже если процедура выхода не выполнена, браузер удалит cookies, когда пользователь закроет его. Однако если пользователь активизировал процедуру автоматического входа, то для удаления cookies необходимо щелкнуть на ссылке Sign Out.

Между сайтом-участником и сервером Login не устанавливается прямого соединения. Весь обмен информацией происходит через браузер (т. е. через процедуры перенаправления HTTP, строки запросов и HTTP POST).

Безопасность процедуры регистрации

Описанная выше базовая процедура входа .NET Passport называется стандартной. Стандартный вход связан с риском для информационной безопасности: cookies передаются простым текстом, а не через протокол HTTP over Secure Sockets Layer (HTTPS), поэтому взломщик может перехватить cookies .NET Passport, пересылаемые от сервера Login или Web-узла в браузер. Затем взломщик может выдать себя за пользователя во временном окне аутентификации сайта, повторив от его имени процедуру регистрации. Чтобы избежать подобной ситуации, в .NET Passport 2.0 (последняя на данный момент версия) предусмотрено два метода безопасного входа: вход через защищенный канал и вход с расширенным набором учетных данных (strong credential).

Для входа через защищенный канал необходимо использовать SSL для защиты передаваемой информации в процессе аутентификации между браузером и сайтом и между браузером и сервером Login. Взломщик не может извлечь cookies из перехваченных им зашифрованных данных. Помимо cookies стандартного входа сервер Login и Web-узел генерируют защищенные HTTPS-cookies, которые нельзя изменить, и сравнивают PUID в защищенных cookies с PUID в обычных cookies. Если на компьютере пользователя нет защищенных cookies или два PUID не совпадают (это произойдет, если взломщик изменит одну из стандартных cookies), то процедуру входа придется повторить.

Для входа с расширенным набором учетных данных пользователь должен ввести четырехзначный ключ безопасности после того, как будет успешно завершена процедура входа через защищенный канал. Пользователь генерирует ключ безопасности в своей учетной записи .NET Passport во время первого посещения сайта-участника, требующего расширенного набора учетных данных; ключ становится частью учетных данных пользователя. В процессе создания ключа пользователь должен ответить на три из десяти “секретных” вопросов (не связанных с учетными данными или профилем пользователя) и подтвердить свои ответы на отдельной странице регистрации. Только после этого система .NET Passport активизирует ключ безопасности. .NET Passport использует ответы на вопросы, чтобы идентифицировать пользователя, если он забудет ключ.

Служба EP

На сайтах-участниках, пользователям которых предоставляются услуги EP, имеется официальная ссылка на экспресс-покупку в .NET Passport с информацией о виртуальной корзине покупок на данном сайте. Поместив товары в корзину, пользователь щелкает на ссылке, чтобы активизировать службу EP. Для доступа к бумажнику .NET Passport пользователю необходимо повторно ввести пароль. После завершения процедуры обращения к бумажнику Web-узел перенаправляет браузер пользователя на сервер .NET Passport Wallet. Сервер Wallet отображает информацию о бумажнике в браузере, и пользователь может выбрать номер кредитной карты, адреса платежа и доставки заказа. Сервер Wallet может встроить эту информацию в страницу оформления платежей сайта, но не выполняет авторизацию кредитных карт.

В завершение процедуры покупки пользователь щелкает на кнопке Continue или Buy Now в нижней части страницы платежа. Затем сервер Wallet составляет форму HTTP POST, которая содержит информацию о кредитной карте в формате Electronic Commerce Modeling Language (ECML - язык моделирования для электронной коммерции). ECML, признанный

отраслевым стандартом, был разработан специалистами Microsoft, Visa, American Express, MasterCard и других компаний. Сервер Wallet использует ключ шифрования сайта, чтобы зашифровать информацию, отправляет информацию по обратному адресу URL и перенаправляет браузер на страницу корзины для покупок. Web-узел извлекает зашифрованную информацию о кредитной карте из формы HTTP POST и восстанавливает ее с помощью ключа шифрования сайта, а затем выполняет необходимые процедуры авторизации платежа и пересылки товара. Для защиты передаваемой информации в службе EP используется протокол SSL.

Сайты-участники могут использовать службу EP без службы SSI. Но сайты, на которых активизирована служба SSI, могут использовать PUID в качестве индекса баз данных статуса корзины для покупок и отслеживания заказов. Также Web-узлы, на которых не реализована служба SSI, должны предоставить ссылку Sign Out, чтобы защитить информацию о бумажнике пользователя.

Удобство и эффективность

.NET Passport - отличный образец системы централизованного управления информацией о пользователях Web-узла, и одновременно простой и эффективный способ для доступа пользователей к службам сайтов. Для взаимодействия с другими системами разработчики Microsoft реализовали процедуру аутентификации пользователей .NET Passport на базе стандарта Kerberos. В отрасли продолжаются споры о конфиденциальности и безопасности .NET Passport, но потребители, похоже, уже сделали выбор: ко времени подготовки данной статьи в системе .NET Passport зарегистрировались несколько сотен миллионов пользователей. Одновременно число сайтов-участников в производственном режиме достигло 100, и примерно 200 Web-узлов функционируют в режиме PREP. По-видимому, поставщики начинают понимать, что они могут с выгодой применить инструмент централизованной идентификации пользователей и сосредоточить усилия на проектировании приложений для электронной коммерции

Список использованной литературы:

- www.osp.ru/win2000/2002/04/018_1_print.htm
- www.microsoft.com/technet/security/bulletin/ms01-055.asp.
- www.passport.net