Examples of data protection best practice in your organisation: In practical terms, we're talking about the length of time you say you keep (and you actually do keep) information from your clients, employees or volunteers. Application forms, booking forms and basic contact details.

Information security (Infosec for short or otherwise known as cyber security) refers to the technical and operational measures that any organisation must take to ensure that the data they hold is safe and secure. Information security is about people, products, processes and all working aspects of a company or organisations. It's about the way you store the information, and what happens if it gets lost or stolen.

Examples of Information Security in your organisation: This involves business practices like creating strong passwords, changing your password every 3 months, whether to encrypt your data or, actually, whether you'd pick up a flash drive from the floor and put into your computer to see what's on it (don't do this).

References

1. Smith, Elementary Information Security (2011, Jones & Bartlett Learning).
2. Stamp, Information Security: Principles and Practice, 2/e (2011, Wiley).

Ш. Абдуллаев, Ж. Хакимов, Д. Абдурасулова

SSL И S-HTTP - ЗАЩИТА WEB-ПРИЛОЖЕНИЙ

(Ферганский филиал Ташкентского университета
информационных технологии)

Под протоколом в электронной коммерции понимается алгоритм, определяющий порядок взаимодействия участников транзакции и форматы сообщений, которыми участники транзакции электронной коммерции обмениваются друг с другом с целью обеспечения процессов авторизации и расчетов.

В данный момент наиболее распространенным протоколом, при построении систем электронной коммерции является протокол SSL. Широкое распространение протокола SSL объясняется в первую очередь тем, что она является составной частью всех известных браузеров и Web -северов. Это, означает, что фактически любой владелец карты, пользуется стандартными средствами доступа к Интернету, получает возможность провести транзакцию с использованием SSL.

Стандарт SSL был разработан фирмой Netscape Communications. В его основе лежит шифрование с открытым ключом. Основная идея заключается в том, что при использовании стандартных протоколов обмена вся информация передается по сети Интернет в незащищенном виде. Таким образом, при прослушивании трафика одним из промежуточных узлов, Ваши пароли, номера кредитных карт и иная конфиденциальная информация могут стать достоянием общественности. Протокол SSL оговаривает методы шифрования всей передаваемой информации прозрачно для пользователя. В данный момент протокол

SSL является наиболее распространенным и используемым при построении систем электронной коммерции. Широкое распространение протокола SSL объясняется в первую очередь тем, что протокол SSL поддерживается любыми современными браузерами. Также достоинством протокола SSL является простота для понимания всех участников транзакции и хорошая скорость реализации транзакции, что связанно с использованием симметричных алгоритмов шифрования, которые на 2-4 порядка быстрее асимметричных при том же уровне крипто стойкости.

Существенным недостатком SSL является то, что протоколы, основанные на использовании SSL, не поддерживают аутентификацию клиента Интернет - магазином, происходящей на уровне документов или приложения, поскольку сертификаты клиента в таких протоколах почти не используются. Использование «классических» сертификатов клиентами в схемах SSL является делом практически бесполезным. Такой «классический» сертификат, полученный клиентом в одном из известных центров сертификации, содержит только имя клиента и, что крайне редко, его сетевой адрес (большинство клиентов имеют динамический IP-адрес). В таком виде такой сертификат более полезен торговой точке для проведения транзакции, поскольку может быть без большого труда получен мошенником. Для того, чтобы сертификат клиента что -то значил для торговой точки, необходимо, чтобы он устанавливал связь между номером карты клиента и его банком- эмитентом. Причем любой Интернет-магазин, в который обращается за покупкой владелец карты с сертификатом, должен иметь возможность проверить эту связь (возможно с помощью своего обслуживающего банка).

Отсутствие аутентификации клиента в схемах SSL является самым серьезным недостатком протокола, который позволяет мошеннику успешно провести транзакцию, зная только реквизиты карты. Тем более, протокол SSL не позволяет аутентифицировать клиента обслуживающим банком (аутентификация клиента обслуживающим банком является важным элементом защиты последнего от недобросовестных действий торговой точки и обеспечивается, например, протоколом SET)

При реализации протокола SSL вместо обычного http адреса пользователь видит https (буква s на конце обозначает secure - защищенный). Таким образом, устанавливая защищенное соединение через специальный сервер - Netscape Commerce WebServer, являющийся единственной SSL совместимой разработкой и необходимый для реализации защищенного режима. Программный продукт Netscape Commerce WebServer стоит несколько тысяч долларов, плюс плата за обслуживание.

Задолго до появления SSL компанией Enterprise Integration Technologies (EIT) была создана схема защиты информации специально для Internet - S-HTTP (secure hypertext transport protocol). Стандарт S -HTTP предназначенный, в первую очередь, для поддержки протокола передачи данных HTTP, обеспечивает авторизацию и защиту документов. В общем S - HTTP позволяет пользователям обговорить практически любой аспект шифрования - от механизмов, с

помощью которых можно получить ключи шифрования, до способа шифрования. Кроме того, можно обговорить режим взаимодействия. Другими словами клиент и сервер договариваются подписывать цифровой подписью запросы, шифровать или и то и другое. Тогда как SSL гарантирует, что соединение между программой просмотра и клиентом устанавливается с сервером и ни с кем иным, то S -HTTP предоставляет широкий спектр инструментов шифрования и делает это на уровне отдельного документа. Значительным преимуществом S -HTTP над SSL можно считать использование цифровой подписи. Так же, в отличие от SSL, протокол S-HTTP полностью совместим с отличными от S-HTTP серверами Web, хотя, в этом случае, информация не будет защищена, если хотя бы один из игроков не озабочен защитой.

Подводя итоги, SSL в настоящее время является де-факто стандартом, обеспечивающим конфиденциальность информации. Он поддерживается всеми известными браузерами, однако алгоритм шифрования SSL недостаточно надежен.

Протокол S-HTTP предназначен только для HTTP-серверов и не работает на других платформах Internet, распространенность S -HTTP только среди производителей Web-серверов. Общей чертой SSL и S -HTTP является то, что разрабатывающие их компании делают ставку на защиту денежных расчетов.

Литература

1. Арипов М. Англо-русско-узбекский словарь сокрашенных слов по информатике. Т., Университет, 2001 г.
2. Евсеев Г. Специальная информатика. Учебное пособие. М., 2002 г.
3. Молдовян К. Безопасность глобальных сетевых технологии. М., 2002 г.

Р.Р. Абраров, М.Е. Бурлаков

ОРГАНИЗАЦИЯ ДЕЦЕНТРАЛИЗОВАННОЙ, БЕЗОПАСНОЙ И АНОНИМНОЙ MESH-СЕТИ

(Самарский университет)

Достижение надежных и эффективных сетей передачи данных является сложной задачей. Беспроводные Mesh-сети (Wireless Mesh Network) – это один из примеров обеспечения широкополосной, надежной и масштабируемой сети передачи данных. Беспроводные ячеистые сети могут объединять в единую сеть различные устройства. WMN обеспечивает лучшую мобильность, более низкую стоимость развертывания, простое расширение сети, а также надежные соединения [1].

На рисунке 1 представлены возможности протоколов Mesh-сетей. Существующие протоколы Mesh-сетей могут организовать сеть только при наличии маршрутизатора. Однако, с развитием технологий, внедряемых в мобильные