Эссе на тему:

PGP/MIME vs. S/MIME.

Выполнил: студент 914 группы Литвинов Дмитрий Михайлович.

Проблема обеспечения конфиденциальности при обмене электронными сообщениями стояла уже давно, можно сказать, с тех пор, как люди вообще стали пользоваться электронной почтой. Ведь электронное письмо отличается от обычного тем, что его очень легко прочитать постороннему (не надо вскрывать, а потом заклеивать конверт), подделать или изменить сообщение, а то и вовсе подсунуть от имени другого какую-нибудь гадость, здесь даже не надо стараться подделывать чужой почерк.

Для обеспечения конфиденциальности почтового обмена необходимо решить следующие задачи:

1. Отправитель А, подготовив сообщение для получателя Б может пожелать зашифровать сообщение. То есть преобразовать исходное сообщение таким образом, чтобы его смог прочитать только получатель Б. Для этого сейчас используются алгоритмы с открытым ключом;

2. Отправитель А, может пожелать подписать свое сообщение. То есть добавить к нему кодовую последовательность, которая однозначно удостоверяет, что сообщение написал именно отправитель и именно в том виде, в каком оно попало к получателю;

3. Отправитель А, может пожелать зашифровать и подписать свое сообщение;

4. Отправитель А, может пожелать управлять ключами (импортировать / экспортировать открытые ключи, сертифицировать и проверять сертификацию открытых ключей других пользователей).

Ранеше сообщения, передаваемые по e-mail использующие стандарт RFC-822, защитить было довольно трудно. Основная проблема состояла в том, что с его помощью можно передавать только 7-битные текстовые сообщения. Для передачи 8-битного текста и двоичных файлов необходимо их перекодировать. На этом этапе пользователь, если хотел зашифровать сообщение, должен был подготовить его в виде отдельного файла, обработать внешней криптографической программой и лишь затем передать в программу почтовую. Если для отправителя это было еще относительно просто, то от получателя требовало определенных усилий, и правильная расшифровка из-за малейшей несовместимости могла стать невозможной.

Однако после принятия стандарта MIME (Multi-purpose Internet Mail Extensions). ситуация изменилась. Этот стандарт позволяет единое сообщение собирать из отдельных кусков

данных (текста, присоединненых файлов и служебной информации). Появляется возможность разделить в письме открытый текст, зашифрованный текст, подпись и т.д.

Разработанный RSA в 1996 году, S/MIME стал весьма распространенным и широко признанным стандартом обмена сообщениями. Технология опирается на стандарт шифрования с открытыми ключами, и, таким образом, ее реализациям гарантирована совместимость на криптографическом уровне.

Двумя основными отличительными чертами S/MIME являются цифровая подпись и цифровой конверт. Цифровая подпись гарантирует, что сообщение не было изменено в процессе передачи. Кроме того, ее наличие не позволит отправителю отказаться от своего авторства.

Подпись представляет собой зашифрованное с помощью личного ключа отправителя резюме сообщения (само резюме вычисляется с использованием алгоритма хэширования). Для проверки целостности сообщения получатель расшифровывает подпись с помощью открытого ключа отправителя. Если получившееся резюме не совпадает с вычисленным, это означает, что сообщение было изменено в процессе передачи.

Однако цифровая подпись не гарантирует конфиденциальность сообщения. В S/MIME эту функцию выполняет цифровой конверт. Для шифрования рекомендуется использовать симметричные алгоритмы типа DES, Triple DES или RS2. Симметричный ключ шифруется с помощью открытого ключа получателя, а зашифрованное сообщение и ключ передаются вместе.

Помимо обеспечения защиты сообщения и гарантии его неизменения во время передачи S/MIME идентифицирует обладателя конкретного открытого ключа с помощью цифровых сертификатов X.509. Цифровой сертификат удостоверяет, что открытый ключ действительно принадлежит тому, от чьего имени он публикуется.

Работая с S/MIME, пользователи могут выпускать свои собственные сертификаты, но, по словам Мэтью из RSA (который принимал участие в разработке S/MIME с самого начала), при отсутствии подтверждения от независимой стороны их полезность весьма ограничена. Цифровые сертификаты могут выпускать все, кто захочет, поэтому без посредничества независимой стороны для проверки и подтверждения вы не можете быть уверены, что эти сертификаты заслуживают доверия. Независимая сторона, например Verisign или GTE, может поручиться за достоверность сертификата.

Несмотря на более широкую поддержку S/MIME по сравнению с PGP, протокол столкнулся с рядом трудностей. В октябре 1997 года IETF заявила, что она не будет публиковать S/MIME в качестве RFC, потому что 40-разрядный ключ RC2, определенный в S/MIME, используется в закрытой технологии RSA Data Security. (IETF известна тем, что она сторонится всего, что уходит корнями в закрытые технологии.)

В ноябре 1997 г. RSA повторно представила S/MIME в IETF, заявив, что она отказывается от торговой марки и других прав на протокол. Кроме того, RSA согласилась опубликовать алгоритм шифрования RC2. На данный момент S/MIME-2 принят в качестве официального стандарта. И идет работа над третьей версией спецификации.

PGP, или Pretty Good Privacy, — один из тех примеров успеха, что у всех на устах. В 1991 году Фил Зиммерман, один из лучших умов в области криптографии, разработал программное обеспечение шифрования. Оказавшись в Internet, оно было загружено тысячами людей по всему миру. В течение многих лет сообразительные пользователи применяли PGP в своих целях

В 1994 году появилась первая коммерческая версия PGP (фирма PGP inc.). В 1997 году все права на PGP были купленны компанией Network Associates.

В феврале 2001 года компанию Network Associates покинул создатель алгоритма PGP Фил Циммерманн, мотивируя свое решение тем, что у руководства Network Associates имеется принципиально иное представление о будущем PGP. И в мае 2001 года при его непосредственном участии был создан Альянс OpenPGP, объединивший 11 компаний и организаций, занимающихся разработкой программ на основе спецификации OpenPGP с открытым кодом. Компания Network Associates, владеющая торговой маркой и правами на исходный код PGP, не присоединилась к этому Альянсу. Более того, она прекратила распространение бесплатной версии PGP, предназначенной для шифрования электронной почты.

Open PGP предусматривает несколько способов обеспечения целостности данных в сообщениях. Он поддерживает шифрование как с открытыми, так и с симметричными (секретными) ключами.

В модели с открытыми ключами данные шифруются с помощью однократного симметричного алгоритма, генерируемого отправителем. Этот однократный ключ тесно связан с сообщением, так как он используется только однажды. Затем он шифруется с помощью открытого ключа получателя и передается вместе с сообщением.

При получении сообщения Open PGP дешифрует однократный ключ, вложенный в сообщение, с помощью личного ключа получателя, имеющегося только у него. Затем Open PGP применяет дешифрованный однократный ключ для воссоздания полученного сообщения в первоначальном виде.

В модели с симметричными ключами пользователь может выбрать один из двух вариантов. Во-первых, сообщение можно зашифровать с помощью симметричного ключа, выводимого из пароля или другого общего секрета. Во-вторых, сообщение можно зашифровать по методу, напоминающему используемый в модели с открытыми ключами, когда однократный ключ шифруется с помощью симметричного алгоритма, выводимого из общего секрета.

Open PGP поддерживает также цифровые подписи, которые можно генерировать и вкладывать в сообщения. Сообщение и подпись шифруются затем с помощью однократного симметричного ключа, после чего однократный ключ шифруется с помощью открытого ключа и помещается перед всем зашифрованным блоком данных.

Характеристики S/MIME и PGP

	S/MIME-3	Open PGP
Формат сообщения	Двоичный на базе Cryptographic Message	Двоичный на базе предыдущей спецификации PGP Syntax (CMS)
Формат сертификата	Двоичный на базе X.509 v3	Двоичный на базе предыдущей спецификации PGP
Симметричный алгоритм шифрования	Triple DES	Triple DES
Алгоритм подписи	Диффи-Хелмана с Digital Signature	ELGamal с DSS Standard (DSS)
Алгоритм хэширования	Secure Hash Algorithm (SHA-1)	SHA-1
MIME-инкапсуляция подписанных данных	Выбор между многочастной/подписанной и ASCII-защитой	Многочастная/подписанная с форматом CMS
MIME-инкапсуляция зашифрованных данных	Прикладной/с открытыми ключами	Многочастная/шифруемая стандарт шифрования 7-mime

И S/MIME, и Open PGP служат решению задач шифрования и идентификации при обмене сообщениями, но они имеют несколько фундаментальных отличий. В настоящее время эти две технологии не совместимы между собой, однако их сторонники соглашаются, что ликвидация различий была бы выгодна для пользователей

Сегодня S/MIME пользуется наибольшей популярностью среди разработчиков систем обмена сообщениями. Многие специализированные продукты имеют встроенную поддержку S/MIME, что упрощает построение защищенных систем обмена сообщениями. Несмотря на то что RSA самостоятельно не разрабатывает пакетов для электронной почты, она имеет комплект инструментов, с помощью которого разработчики систем электронной почты могут встроить поддержку S/MIME в свои программные пакеты. Набор

интерфейсов прикладного программирования RSA BSAFE S/MIME (формально известный как S/MAIL) позволяет включить алгоритмы шифрования и управления цифровыми сертификатами и ключами.

Встроенную поддержку S/MIME имеют Outlook Express компании Microsoft, и Messenger в Communicator от Netscape. Кроме того, S/MIME поддерживается и клиентским программным обеспечением Express Mail компании OpenSoft. Продукт обеспечивает шифрование с ключом длиной до 2048 бит и совместим с цифровыми идентификаторами Verisign. К лагерю сторонников S/MIME принадлежит и ирландская компания Baltimore Technologies, чей клиент MailSecure поддерживает защищенные вложения файлов и уполномоченного по выдаче сертификатов UniCert той же компании; кроме того, он интегрируется с Exchange, Outlook и другими почтовыми клиентами.

Продукты со встроенной поддержкой PGP не столь разнообразны, но тем не менее эта технология поддерживается некоторыми известными разработчиками. Так, Qualcomm включила PGP в четвертую версию популярного почтового клиента Internet Eudora Pro.

В текущей версии популярного пакета для коллективной работы GroupWise 5.5 Novell предпочла поддерживать как S/MIME, так и PGP. Пользователи GroupWise могут шифровать/дешифровать сообщения, ставить цифровые подписи, идентифицировать и фиксировать авторство с использованием S/MIME и инфраструктуры с открытыми ключами от Entrust. Аналогичные возможности они получают и используя PGP.

Выпустив PGP Desktop Security 6.0 в составе E-mail and Files 6.0 и PGP Desk 2.0 компания Network Associates упростила поддержку PGP. Являясь компонентом PGP Enterprise Security 3.0, PGP Desktop Security 6.0 содержит подключаемые почтовые модули для GroupWise, Outlook и других приложений электронной почты.

Итак: S/MIME и Open PGP — несовместимые спецификации. Большая часть пакетов электронной почты поддерживают либо один, либо другой протокол, но тенденция поддержки обоих все более набирает силу.

В России, как известно согластно указу от 3 апреля 1995 г. N 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации.» любая разработка, экспорт, импорт и даже использование криптографических устройств требует лицензии Федерального агентства правительства связи и информации (ФАПСИ). В соответствии с требованиями ФАПСИ в отечественные почтовые системы должны встраиваться только сертифицированные средства криптографической защиты информации, реализующие алгоритмы шифрования по ГОСТ 28147-89, ЭЦП - ГОСТ Р 34.10-01 и хэш-функции - ГОСТ Р 34.11-94.

В связи с этим выбор криптографических систем защиты электронной почты для российского потребителя несколько ограничен. Вот некоторые из них:

1.Криптографическое программное расширение MS Outlook "Курьер", разработаннное компанией "Валидата" поддерживает отечественную реализацию инфраструктуры открытых ключей "Vcert PKI" на основе сертификатов X.509 v.3. В качестве криптоядра могут использоваться "Верба-OW" (разработка МО ПНИЭИ) и "КриптоПро CSP". Алгоритм шифрования - ГОСТ 28147-89, алгоритм ЭЦП – ГОСТ Р 34.10-94. Формат защищенного с помощью криптографического расширения "Курьер" почтового сообщения полностью соответствует международному стандарту S/MIME.

2. Криптопровайдер "КриптоПро CSP" разработан компанией "Крипто-Про" в соответствии с криптографическим интерфейсом корпорации Microsoft "Cryptographic Service Provider - CSP". "КриптоПро CSP" встраивается в ядро Windows с использованием функций Microsoft Cryptographic Application Programming Interface (MS Crypto API). Функции, описанные в нем, поддерживаются Windows95/98, Windows NT и Windows 2000. "КриптоПро CSP" обеспечивает использование в почтовых клиентах Microsoft Outlook и Microsoft Exchange российских криптографических алгоритмов шифрования ГОСТ 28147-89 и ЭЦП - ГОСТ Р 34.10-94 и поддерживает инфраструктуру открытых ключей в соответствии с рекомендациями X.509, RFC-2459.

Список использованной литературы:

1. http://www.rsasecurity.com/standards/smime/faq.html
2. RFC 2311
3. RFC 2312
4. http://www.openpgp.org/resources/faqs.shtml
5. RFC 2440
6. **В. Лукоянов**. Криптографическое расширение систем электронной почты.