Московский физико-технический институт (государственный университет)

Стандарт Secure MIME.

Эссе по курсу Защита информации студента 012 группы Чугунова Николая.

Secure/Multipurpose Internet Mail Extensions (S/MIME) – это спецификация для защищенной работы с электронной почтой. S/MIME основан на известном стандарте MIME и описывает протокол для добавления сервисов защиты с помощью инкапсуляции в MIME зашифрованных объектов и объектов цифровой подписи. S/MIME может также использоваться с HTTP. Ниже описывается протокол S/MIME, различные типы и применение. Поясняется так же, как создавать тело MIME с добавление криптографических опций в соответствии с криптографическим синтаксисом сообщений(CMS-Cryptographic Message Syntax) - стандартом форматирования, выделенным из PKCS#7(Public Key Cryptographic Standard- криптографический стандарт с открытым ключом).

В 1995 году RSA Data Security, Inc. организовала консорциум производителей и поставщиков программных средств по разработке S/MIME. После разработки спецификации RSA передала её в IETF для дальнейшего совершенствования. Текущей версией являться S/MIMEv3. Рабочая группа S/MIME IETF в процессе разработки внесла в протокол ряд усовершенствований.

Сообщение S/MIME состоит из тела MIME и объектов CMS. Последнее образует структуру данных PKCS#7. После создания сущности MIME и выполнение соответствующего кодирования сущность посылается сервисам, обеспечивающим безопасность. В результате образуется объект CMS, который заворачивается в MIME и размещается вместе с исходным сообщением в соответствии с выбранным типом содержимого S/MIME.

Перед подписыванием, сущность MIME должна быть преобразована к каноническому виду.

Чтобы сформировать данные с типом конверта данных, необходимо выполнить следующие действия:

1. Создать сессионный ключ для выбранного алгоритма шифрования.
2. Зашифровать ключ, используя один из следующих методов:
   Транспорт ключей RSA. Ключ зашифровывается открытым ключом получателя.
   Согласование ключей Диффи-Хелмана. Открытый ключ получателя и секретный ключ отправителя используется для создания совместного симметричного ключа.
   *Известный секретный ключ***.** Ключ шифрования содержимого предварительно зашифровывается с использованием предварительно распространенного секретного ключа.
3. Для каждого получателя создается блок данных использующий информацию о получателе. Эта информация включает зашифрованный ключ шифрования и другую специфичную информацию о получателе.
4. Сообщение зашифровываться с помощью ключа шифрования.
5. К зашифрованному содержимому добавляется информация о получателе и осуществляется кодирование base64.

Подпись данных.
Спецификация S/MIME определяет два метода подписи данных:

1. Application/pkcs7-mime. Данный тип используется для передачи подписи совместно с подписываемыми данными.
2. Multipart/singed-Сообщение состоящие из нескольких частей с подписью. Данный тип известен как открытая подпись.

S/MIMEv3 не обязывает использовать тот или иной алгоритм, но предпочтительнее использовать Multipart/singed, т.к. он может быть прочитано любой программой для работы с электронной почтой.

Подписанные данные. Сообщение S/MIME с типом данных содержимого Application/pkcs7-mime с подписанными данными может состоять из данных с любым типом содержимого MIME, любое количество подписывающих могут параллельно подписывать данные с любым типом содержимого.
Для формирования подписанных данных следует выполнить следующие действия:

1. Выбрать алгоритм вычисления дайджеста.
2. Вычисляется дайджест сообщения или значения хеша для всего подлежащего подписи содержимого.
3. Для каждого подписывающего создается цифровая подпись дайджеста сообщения (т.е. дайджест зашифровывается с использованием секретного ключа подписавшего).
4. Для каждого подписывающего создается блок информации об авторе подписи,
5. Подписанное содержимое предваряется информацией о подписывающем, которое затем кодируется с помощью base64.

Открыто подписываемые данные. Возможно, что подписанные данные будут приняты пользователем, который не поддерживает S/MIME, и не сможет восстановить исходно сообщение. Чтобы разрешить эту проблему, используется Multipart/singed. Письмо состоит из двух частей. Первая часть, которая имеет любой тип содержимого MIME остается открытой. Содержимое второй части представляет собой особую разновидность подписанных данных, известная как выделенная подпись.
Тип содержимого второй части письма может быть application/pkcs7-signature.
В этом случае вторая часть письма состоит из подписи и сертификата, с помощью которого эту подпись можно проверить.

Подпись и шифрование.
Чтобы предоставить этот сервис, следует осуществить либо вложение данных или только с конвертом или только с подписью. Другими словами, нужно либо сначала подписать сообщение, либо сначала поместить сообщение в конверт. Решение, какой процесс выполнять первым зависит от пользователя и от реализации. Спецификация S/MIMEм3(rfc 2633) указывает на потенциальные угрозы безопасности, свойственные каждому методу.

Запрос на регистрацию.
В дополнение к безопасности S/MIME определяет формат для передачи запроса на выпуск сертификата открытого ключа. Для запроса сертификата в удостоверяющем центре используется тип содержимого MIME application/x-pkcs10.

Сообщение только с сертификатом.
Сообщение только с сертификатом имеет тип application/pkcs7 и подготавливается таким же образом, как и сообщение с подписанными данными. Необходимость в этом сообщении, которое используется для транспортировки сертификатов к совместимой с S/MIME сущности, возникает после того, как удостоверяющий центр получил запрос на сертификат. Сообщение только с сертификатом может также использовать для транспортировки *списков отмены сертификатов.*

Расширенные сервисы обеспечения безопасности.

Я рассмотрю три расширенных сервиса по обеспечению безопасности, которые могу использоваться с наращиванием имеющихся средств безопасности S/MIME и сервисов обработки сертификатов.

Подписанное уведомление о получении. Уведомление о доставки предоставляет автору сообщения продемонстрировать третей стороне, что получатель не только принял сообщение, но и проверил его подпись. В конечно счете, получатель подписывает все сообщение и соответствующую ему подпись, чтобы подтвердить получение. Замечу, что этот сервис используется только для подписанных данных.

Метрика безопасности. Метрики безопасности используется двумя способами. Первое и, вероятно наиболее очевидное в описании важности данных. Для этого используется ранжированный список меток (конфиденциально, секретно, для ограниченного круга лиц). Другой подход состоит в исполь-

зовании меток для управления доступом. При этом описывается, какого рода получатели имеют доступ к данным (например, личный врач).

Защищенные списки рассылки. При использовании сервисов S/MIME передающие агенты должны создавать специфичные для каждого получателя структуры данных. По мере роста числа получателей данного сообщения эти действия могут привести к снижению производительности при отправке сообщений. *Агенты списков рассылки*(MLA –mail list agent) могут принимать одно сообщение и выполнять все специфичные для получателя действия по зашифрованию сообщений для каждого получателей.

Поддрержка расширенных сервисов обеспечения безопасности реализована фирмой phaos на java. В программе the bat разработчики пишут, что они сделали поддержку, но найти опцию, где они сделали я не смог.

Совместимость

После того как стандарт S/MIME впервые стал доступным ряд поставщиков предприняли усилия по встраиванию его в свои продукты. Однако отсутствие совместимости является важной проблемой. Например, многие поставщики сохраняют совместимость с S/MIMEv2, тогда как другие перешли на S/MIMEv3 без поддержки обратной совместимости. К другим проблемам относиться ограничения на обработку сертификатов, имеющихся в различных продуктах.

Анализ

Шифрование и подписывание данных сделано в популярных программах the bat, outlook, mozilla.

Отправитель, шифрующий сообщение открытым ключом, должен быть уверен, что ключ действительно принадлежит адресату, а не подменен злоумышленником, выступающим от имени адресата. Для этого открытые ключи заверяться цифровой подписью, но подписью не адресата, а доверенного лица – центра сертификации. Это является самым узким местом в S/MIME.Поскольку сертификат подписывается доверенной третьей стороной, третья сторона должна убедиться, что она подписывает public key именно получателя.

Можно сделать самоподписывающийся сертификат. Но тогда надо доставить этот сертификат отправителю и добавить его в доверенные корневые центры сертификации. Это требует от отправителя понимая, что происходит.

Ниже приведены примеры подписанного и зашифрованного сообщений.

Return-Path: <nickmipt@mail.ru>
Delivered-To: evklid@birulevo.net
Received: (qmail 26483 invoked from network); 13 May 2004 15:15:19 +0400
Received: from mx9.mail.ru (194.67.23.29)
  by kunnilinux.birulevo.net with SMTP; 13 May 2004 15:15:19 +0400
Received: from mail by mx9.mail.ru with local
      id 1BOECq-000GSc-00
      for evklid@birulevo.net; Thu, 13 May 2004 15:16:52 +0400
X-ResentFrom: <nickmipt@mail.ru>
Received: from [195.54.208.3] (port=25 helo=kunnilinux.birulevo.net)
      by mx9.mail.ru with esmtp

id 1BOECq-000GSM-00
for nickmipt@mail.ru; Thu, 13 May 2004 15:16:52 +0400
Received: (qmail 26451 invoked from network); 13 May 2004 15:15:07 +0400
Received: from unknown (HELO EVKLID) (10.4.20.77)
by fosgen.binet.lan with SMTP; 13 May 2004 15:15:07 +0400
Date: Thu, 13 May 2004 15:16:45 +0400
From: nick <nickmipt@mail.ru>
X-Mailer: The Bat! (v2.10.01) Personal
Reply-To: nick <nickmipt@mail.ru>
X-Priority: 3 (Normal)
Message-ID: <296337898.20040513151645@mail.ru>
X-Confirm-Reading-To: nickmipt@mail.ru
Disposition-Notification-To: nickmipt@mail.ru
To: nickmipt@mail.ru
MIME-Version: 1.0
Content-Type: multipart/signed; protocol="application/pkcs7-signature"; micalg=sha1; boundary="----------116FA373DA4EC61"
X-Spam: Not detected

This is a cryptographically signed message in MIME format.

----------116FA373DA4EC61
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: quoted-printable

Hello nickmipt,

=20

--=20
Best regards,
nick mailto:nickmipt@mail.ru

----------116FA373DA4EC61
Content-Type: application/pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: S/MIME Cryptographic Signature

MIIDtQYJKoZIhvcNAQcCoIIDpjCCA6ICAQMxCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCC
AiQwggIgMIIBiaADAgE-
CAghRb2wCBmqkFzANBgkqhkiG9w0BAQUFADBIMUYwCwYDVQQpEwRu
aWNrMAsGA1UEKhMEbmljazAdBgkqhkiG9w0BCQEWEG5pY2ttaXB0QG1haWwucnUwCwYDVQQD
EwRuaWNrMB4XDTA0MDUwNTAwMDAwMFoXDTA1MDUxNTAwMDAwMFowSDFGMAsGA1U
EKRMEbmlj
azALBgNVBCoTBG5pY2swHQYJKoZIhvcNAQkBFhBuaWNrbWlwdEBtYWlsLnJ1MAsGA1UEAxME
bmljazCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA6eqlI94PR2ju/rvp6f568czKla9n
MzMYmcNS04+Z/lm52dXH6PlqlgOUh6wcvR8Z6I+ypL9StYPuRrPn57E1tHhTEdZLRt2mKJ6u
DNX6rkhV/D88g8Jj8IZKtqA+Dm908FLioGYVS3xHzt/XtwH8KNf4/Hya/2CogtMaF/8/WMcC
AwEAAaMTMBEwD-
wYDVR0TBAgwBgEB/wIBADANBgkqhkiG9w0BAQUFAAOBgQDlYGuCB47FxzhX

fHvZNaZHTuEcUpXoGnB2CAw7cThZyFCLnEKmDN5afcMaSZfL4xC6HvNs40zPlZxGFDzoD1r7
ukpmp4lpEZBvRLGsnsICBAvHxS6hTigsYx8Wq5GvXkInrzW3oy5J/chZBzpMjU9UdaP44dlq
tuB65AAZUcpZTDGCAVkwggFVAgEBMFQwSDFGMAsGA1UEKRMEbmljazALBgNVBCoTBG5pY2sw
HQYJKoZIhvcNAQkBFhBuaWNrbWlwdEBtYWlsLnJ1MAsGA1UEAxMEbmljawIIUW9sAgZqpBcw
CQYFKw4DAhoFAKBdMBgGCSqGSIb3DQEJAzELBgkqhkiG9w0BBwEwIwYJKoZIhvcNAQkEMRYE
FJrLhGhwc4QPCNqU1nCoXAFi4a1GMBwGCSqGSIb3DQEJBTEPFw0wNDA1MTMxMTE2NDVaMA0G
CSqGSIb3DQEBAQUABIGAixlVryUrl+NCDzahU8P4CCTZefAS8hyHL+e6Oel3NU2eTa5ujgaH
BDwQvlneceli5liILP2rb00p1MiJheXOOl/PJL1fC4MtAZC3q1/FgA/Bkzi27c4qN56wqSyT
yV3w2tUS864mlbeFRlJZu7IOQW3Bhs5You85O0x1u+mWkOk=
----------116FA373DA4EC61—

Return-Path: <nickmipt@mail.ru>
Delivered-To: evklid@birulevo.net
Received: (qmail 19240 invoked from network); 13 May 2004 13:04:28 +0400
Received: from mx17.mail.ru (194.67.23.5)
  by kunnilinux.birulevo.net with SMTP; 13 May 2004 13:04:28 +0400
Received: from mail by mx17.mail.ru with local
	id 1BOC9m-0004TP-00
	for evklid@birulevo.net; Thu, 13 May 2004 13:05:34 +0400
X-ResentFrom: <nickmipt@mail.ru>
Received: from [195.54.208.3] (port=25 helo=kunnilinux.birulevo.net)
	by mx17.mail.ru with esmtp
	id 1BOC9h-0004Pz-00
	for nickmipt@mail.ru; Thu, 13 May 2004 13:05:29 +0400
Received: (qmail 19143 invoked from network); 13 May 2004 13:04:07 +0400
Received: from unknown (HELO EVKLID) (10.4.20.77)
  by fosgen.binet.lan with SMTP; 13 May 2004 13:04:07 +0400
Date: Thu, 13 May 2004 13:05:48 +0400
From: nick <nickmipt@mail.ru>
X-Mailer: The Bat! (v2.10.01) Personal
Reply-To: nick <nickmipt@mail.ru>
X-Priority: 3 (Normal)
Message-ID: <456782856.20040513130548@mail.ru>
To: nickmipt@mail.ru
MIME-Version: 1.0
Content-Type: application/pkcs7-mime; name="smime.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7m"
Content-Description: S/MIME Encrypted Message

X-Spam: Not detected

MIIB+wYJKoZIhvcNAQcDoIIB7DCCAegCAQAxge4wgesCAQAwVDBIMUYwCwYDVQQpEwRuaWNr
MAsGA1UEKhMEbmljazAdBgkqhkiG9w0BCQEWEG5pY2ttaXB0QG1haWwucnUwCwYDVQQDEwRu
aWNrAghRb2wCBmqkFzANBgkqhkiG9w0BAQEFAASBgIyD82Ofa/VaXl4dDH6zYZky407mt1Mk
djfeLpATpiwJLFfZJQBsC1dTuuMuujMr9MUxnVRu4e1PjrEuMmKE2ogeCkO+pln/NWqY+/iG
WmeX9xXmq97qClEW3zHBRZAcrWuXwiAxXel9uFaIvQ7FfLd4EzOH9bNKp6o/JQqe0za0MIHx
BgkqhkiG9w0BBwEwGQYIKoZIhvcNAwIwDQIBOgQI36TMl7HhTG2AgcgTVGnITY7X1fLzu7J9
Q6ckrEKXDMHHg+NcD6Do+qi+UdaJpSERBKlGAJrt2HwkpZYehfsDwqDBXZM4N+kRt6bwuu7I
ceeCDZg16c4P5gQ9czZKtFym1xXGvprpG5Sl0M7Gqza1uD8gvOEEK1sFPHw59U8NSzYZFwwV
E5gYS3w16octNP81PppNLjBXVVgMnHxT4KMXHHcR1SLZlNeg6SVUnL8AHqFLsjOw2QqrZpmu
AvjukqiUnhar9FkKLTx/s1tPlduBi7fwbw==

Список использованной литературы:

1. RFC2632 S/MIME Version 3 Certificate Handling http://ietf.org/rfc/rfc2632.txt
2. RFC2633 S/MIME Version 3 Message Specification http://ietf.org/rfc/rfc2633.txt
3. RFC2634 Enhanced Security Services for S/MIME http://ietf.org/rfc/rfc2634.txt
4. Help of “The Bat!” program