Эссе по курсу "Защита информации", кафедра радиотехники, Московский физико-технический институт (ГУ МФТИ), http://www.re.mipt.ru/infsec

Цыганова Анна Михайловна.
111гр.

PGP –Довольно хорошая секретность. Обзор.

2005г.

Введение:

Наверное, каждый из нас, за исключением разве что законченных параноиков и специалистов в области криптографии, сталкивался с явлением, называемым перлюстрацией. Даже если вы не находитесь в местах не столь отдаленных и не работаете в закрытом учреждении с обязательной цензурой входящей и исходящей почты, ваши сообщения могут быть прочитаны третьей стороной. Смс-ки в телефоне, электронные письма, разговоры в ICQ со случайными друзьями и подругами в Интернете, подсмотренные вашей второй половиной—в настоящий момент имеют восходящий тренд в статистике причин разводов в нашей стране. Переговоры с партнерами о выгодном контракте наверняка заинтересуют ваших конкурентов. Мы начинаем задумываться о защите наших секретов, достаточно надежной и в то же время простой в применении системе.

Конечно, при определенных обстоятельствах заинтересованным лицам всегда может оказаться выгоднее применить силовой криптоанализ и получить открытый текст без ключа. Поэтому, выбранная криптосистема должна быть, прежде всего, экономически обоснована. Вероятно не стоит выбирать криптосистемы с закрытым кодом, так как они не могут быть проверены на бэкдоры и уж тем более новые системы, которые не получили оценку криптографической стойкости со стороны видных аналитиков. Многие в настоящее время делают выбор в пользу PGP для защиты личной переписки, информации, хранящейся на дисках.

Что же такое PGP?

PGP-Pretty Good Privacy или Довольно Хорошая Секретность это протокол и программа для обеспечения индивидуального шифрования. Она разработана и опубликована в 1991 году Филлипом Циммерманом и была пионером среди систем подобного уровня, опубликованных для общего доступа, в силу законодательных ограничений на распространение криптографических технологий.

PGP-это система, сочетающая преимущества симметричных и ассиметричных криптосистем.

Как это работает?

Для начала PGP сжимает пользовательские данные, тем самым уменьшая избыточность и повышая стойкость к криптоанализу. При этом маленькие, либо уже сжатые файлы не сжимаются.

После этого создается сеансовый ключ--одноразовый симметричный ключ, который применяется только для одной операции. Он генерируется псевдослучайным образом в зависимости от движений мыши, системных таймеров и задержек нажатий клавиш. Используется генератор псевдослучайных чисел, создающий непредсказуемые сеансовые ключи. Его более подробное описание можно найти в RFC 1750. В результате создается файл, который перемешивается до и после каждого использования, и дополняется новыми данными , зависящими от времени суток и иных показателей. Файл содержит как случайные данные выхода генератора, так и случайные данные ключа, используемого для задания исходного внутреннего состояния генератора. С помощью сеансового ключа шифруется уже сжатое сообщение. После каждого использования файла данные перемешиваются, дабы исключить возможность восстановления по нему предыдущих или будущих сеансовых ключей.

Сеансовый ключ так же шифруется открытым ключом получателя, затем прикрепляется к шифротексту и передается получателю.

Расшифрование происходит соответственно в обратном порядке. Получатель, используя свой закрытый ключ, получает сеансовый ключ и восстанавливает открытый текст. Так, шифрованием ассиметричным образом сеансового ключа, решается проблема его передачи, и пользователь получает преимущества работы более скоростных симметричных алгоритмов.

PGP располагает набором поддерживаемых симметричных алгоритмов (с тайным ключом): *CAST, Triple-DES, IDEA, Twofish*, а также *AES.*

Открытые же ключи PGP несут в себе информацию о том, какие блочные симметричные шифры поддерживаются программой получателя, чтобы программа отправителя знала, какие шифры может применять для шифрования сообщений.
Для быстрой проверки файлов на несанкционированные изменения, а так же как средство защиты от ошибок PGP использует так называемые «дайджесты» или «отпечатки» сообщений. Это отображение файла в более короткий образ, сродни контрольной сумме, используемой в сетевых протоколах транспортного уровня. Дайджест вычисляется при помощи криптографической хэш-функции. При малейшем изменении исходной информации изменится и отпечаток сообщения. При этом по отпечатку невозможно восстановить исходное сообщение. Для получения дайджеста в PGP используется алгоритм SHA-1 (Secure Hash Algorithm)-160-битовый хэш-алгоритм.
В вычислительном плане практически невозможно создать подставное сообщение, имеющее тот же отпечаток. Для этого потребовалось бы перебрать 2^160 вариантов, однако, учитывая парадокс о днях рождения, два сообщения с идентичным отпечатком можно создать за 2^80 итераций. Однако, в недавнее время появилась атака со сложностью 2^70. Видимо алгоритм односторонней хэш-функции для PGP скоро будет снова изменен. Эта атака подробно описана в статье Collision Search Attacks on SHA1 [9]

К сожалению, ассиметричные криптосистемы подвержены атаке человек-по-середине. Поэтому, несмотря на то, что открытый ключ может распространяться беспрепятственно, однако нельзя полностью быть уверенным, что открытый ключ действительно принадлежит человеку, чье имя указано в сертификате. В целях защиты от подделки ключа в PGP применяется децентрализованная схема поручительства.
Конечно, лучший способ избежать подмены открытых ключей—это передача ключа при лично встрече. Но если вы находитесь далеко от вашего партнера, то организация встречи будет проблематичной. Однако вы можете воспользоваться помощью вашего общего знакомого, владеющего подлинной копией ваших ключей. Он подписывает их собственных закрытым, поручаясь в их достоверности. Затем уже подписанные сертификаты загружаются на сервер-депозитарий с тем, чтобы вы могли их скачивать, и сверять подпись посредника его открытым ключом. Вы так же можете быть чьим-то поручителем. Однако при подписании чьего-то ключа, вы должны быть гораздо более уверены в его подлинности, чем если собираетесь его использовать лично. Хотя при этом вы ни чем не рискуете, подписывая чужой ключ, вы всего лишь удостоверяете, что он принадлежит человеку, чье имя указано на нем.

В соответствии с распределенной схемой выгодно иметь как можно больше удостоверяющих подписей своего ключа—тогда шанс, что ваш собеседник доверяет хотя бы одной из этих подписей выше.

Такая схема распространения ключей во многом выгоднее централизованной, которая мало того что просто дороже, но и выписываемое удостоверение ограничено во времени, что заставляет вас вносить плату снова и снова при продлении его действия. Так же вы не сможете проверить, насколько аккуратна эта организация при хранении ваших данных.

PGP различает три разные степени доверия поручителям: отсутствия доверия, частичного доверия или полного доверия. Информация о степени доверия хранится вместе с ключами на вашей связке. При этом ваш собственный ключ должен быть безусловно доверяемым. Так же по умолчанию вы безусловно доверяете собственным подписям. В результате вы оказываетесь на вершине своей доверительной пирамиды и можете решать, кому доверять, вместо того чтобы пользоваться мнением посторонней организации--централизованного центра сертификации.

Кроме того, PGP использует так называемую концепцию мета-поручителей, из которой следует, что вы можете доверять с разной степенью доверия. Например(1):

Уровень 0 Вы верите, что располагаете подлинной копией ключа A.
Уровень 1 Вы верите, что располагаете подлинной копией ключа A, и что A подписывает только достоверные ключи. Иными словами, A – человек, заслуживающий доверия.
Уровень 2 Вы верите, что располагаете подлинной копией ключа A, и что A подписывает только достоверные ключи людей, заслуживающих доверия.
. . .
Уровень n Вы верите, что ключ A используется только для подписания ключей, принадлежащих людям из категории n-1 (а также, что располагаете подлинным ключом A).

Формат файлов и пакеты PGP

Формат файлов--это набор правил, которые позволяют определить, как построить файл, разрешено ли то или иное и если разрешено, то что же это значит. Все форматы используемых и создаваемых PGP файлов описываются документом OpenPGP Message Format.
Данный документ описывает следующие форматы файлов:
.pgp –зашифрованные сообщения PGP
.sig—автономные подписи
.asc—экспортируемые ключи
.pkr—открытые ключи
.skr—закрытые ключи
Последние два типа файлов создаются при установке PGP и по умолчанию называются pubring.pkr и secring.pkr (собственно связка открытых и закрытых ключей).

PGP Имеет собственный стандарт пакетов, на которые разбиваются данные. Каждый пакет оснащается заголовком, определяющим его тип, и длину пакета. Пакеты бывают следующих типов:
1 Public-Key Encrypted Session Key Packet
2 Signature Packet
3 Symmetric-Key Encrypted Session Key Packet
4 One-Pass Signature Packet
5 Secret Key Packet
6 Public Key Packet
7 Secret Subkey Packet

8 Compressed Data Packet
9 Symmetrically Encrypted Data Packet
10 Marker Packet
11 Literal Data Packet
12 Trust Packet
13 User ID Packet
14 Public Subkey Packet
60-64 Private or Experimental Values

Возможные атаки на PGP и уязвимости.

Прежде всего, одним из недостатков PGP является слабый механизм оповещения заинтересованных лиц о компрометации вашего закрытого ключа. В ограничении его действия вы теперь не можете полагаться на список аннулированных сертификатов. Единственное, что вы можете предпринять, это издать сертификат об аннулировании (Key Revocation Certificate-- KRC) самостоятельно, либо попросить об этом вашего доверенного отменителя. В случае если вы утратили закрытый ключ либо ключевую фразу то вам придется воспользоваться только доверенным отменителем, либо попросить чтобы все кто заверил ваш открытый ключ, отозвали свои подписи.

Кроме того, существуют уязвимости, относящиеся скорее к особенностям операционных систем—файлы подкачки и неполное удаление файлов.

Когда при удалении файла операционная система вовсе не удаляет их физически—начало файла помечается особым образом, давая системе понять, что это место может быть использовано для перезаписи. PGP при этом предлагает воспользоваться утилитой-шредером.

Так же все современные ОС используют метод, называемый виртуальной памятью. Если для выполнения программы требуются ресурсы, превышающие емкость ОЗУ, на диске выделяется пространство, которое ОС использует для хранения не используемых в данный момент программой данных. Однако PGP старается не держать важные данные долго в памяти, чтобы предотвратить запись их на диск.

Другая, и, возможно наиболее актуальная уязвимость, которую PGP проконтролировать не в состоянии, это вирусы и трояны. Вредоносная программа может внедриться в ваш компьютер и, например, считывать нажатия клавиш. Для защиты необходимо использовать антивирусные программы.

Следующая атака более дорогостоящая из-за сложного оборудования, тем не менее, не стоит сбрасывать ее со счетов. Это так называемый Ван-Эйковский перехват или TEMPEST. Аппаратура фиксирует всплески электромагнитного излучения, исходящего от электронных устройств, от электронно-лучевой трубки вашего монитора. PGP содержит защитную функцию—отображение символов специальным нечетким сглаженным шрифтом, затрудняющим перехват.

В 2002 г. на конференции Information Security Conference криптологи Брюс Шнайер, Кахил Джеллад и Джонатан Катц предложили методику проведения криптоаналитической атаки на основе подобранного шифротекста и "дешифрующего оракула". Одна из сторон при этом должна способствовать взломщику.

В общих чертах она выглядит следующим образом:

1. Взломщик, прослушивая канал связи, перехватывает зашифрованное письмо. Он определённым образом модифицирует OpenPGP-пакет, добавляя произвольный открытый текст внутрь тэга шифротекста, а затем отсылает модифицированное сообщение адресату.
2. Адресат получает и расшифровывает письмо: сначала своим закрытым ключом расшифровывает симметричный сеансовый ключ, затем PGP (или иная реализация OpenPGP) этим симметричным ключом расшифровывает шифротекст послания. Однако, поскольку открытый текст был добавлен взломщиком внутрь тэга шифротекста, PGP криптографирует и этот открытый текст, зашифровывая его сеансовым ключом. В итоге адресат видит "мусор" в тексте полученного сообщения и возвращает всё сообщение отправителю, дабы выяснить, что это такое.
3. Взломщик вновь перехватывает письмо. Теперь он располагает и своим открытым текстом, добавленным на этапе 1, и его симметрично зашифрованным вариантом. Произведя некоторые элементарные вычисления (простой XOR) над полученными данными он восстанавливает сеансовый ключ и дешифрует исходное сообщение, перехваченное на этапе 1.

При этом требуется совпадение ряда допущений, и, конечно же, ничего не получится в том случае, если: а) получатель не заинтересуется происхождением «мусора» в полученном сообщении б) не вернет эту часть сообщения отправителю в) вернет, зашифровав его открытым ключом отправителя (и новым сеансовым), при условии что имеет заверенную копию этого ключа г) взломщик не сможет перехватить сообщение еще раз.

Данная атака представляла потенциальную угрозу, и стандарт был изменен в соответствии с рекомендациями криптологов, описанная уязвимость была устранена.

В 2005 году была опубликована еще одна потенциальная атака, еще более труднореализуемая, чем предыдущая, на основании адаптивно подобранного шифротекста, взломщику содействует дешифрующий оракул, обладающий верным ключом дешифрования и сообщающий взломщику о правильности расшифрования сообщения. Взломщик при этом должен иметь в своем распоряжении сообщение, симметрично зашифрованное ключевой фразой. Он вносит некоторые изменения в сообщение и справляется у оракула о результатах быстрой проверки (сообщения снабжены специальным тэгом quick check, повторяющие последние два байта вектора инициализации). Процесс повторяется до возвращения положительного ответа. Теперь взломщик знает последние два байта вектора инициализации, сдвигает его на эти два байта и повторяет процесс. Однако не существует реализаций PGP, попадающей под все допущения данного метода.

Подробное описание этих атак находится здесь [2] и здесь [3] .

Бесплатные альтернативы PGP.

На настоящий момент существует две наиболее известные бесплатные альтернативы PGP. Это GPG и OpenPGP. GnuPG (GNU Privacy Guard, Страж приватности GNU) --

некоммерческий продукт, использующий IETF стандарт. Изначально эта программа разрабатывалась для Linux, позже вышли версии, совместимые с Windows, однако ни о каком графическом интерфейсе речь не идет, все действия выполняются из программной строки.
OpenPGP разрабатывающийся на основе стандарта RFC 2440bis, который описывает стандартные функции PGP, форматы пакетов, форматирование и стандартные алгоритмы.

Развитие PGP

Первая версия PGP использовала RSA в качестве алгоритма с открытым ключом, Bass-o-Matic – для симметричного шифрования, MD4 – для выработки хэшей, и LZHUF – для сжатия данных. Bass-o-Matic это алгоритм придуманный лично Филлипом Циммерманом, однако позже была доказана его уязвимость. Последующие версии PGP разрабатывались группой энтузиастов со всего света, и Bass-o-Matic был заменен на IDEA.
Благодаря открытости программного кода, сторонние группы разработчиков получили возможность создавать собственные версии PGP.

На первых порах PGP не имел официального статуса, во многом из-за проблем с лицензированием внедряемых технологий и запретом правительства США на экспорт криптографических технологий. Однако после разрешения всех юридических проблем, программа стала полноценной. Она была переписана с нуля и дополнена графическим интерфейсом. В программе было реализовано множество новых функций и алгоритмов, таких как блочные шифры CAST и 3DES и хэш-функция SHA-1. Наиболее важным нововведением стал формат ключей Diffie-Hellman.

Дальнейшие версии PGP пополнились такими полезными утилитами и приложениями, как PGPdisk, позволяющий создавать и использовать полностью зашифрованные виртуальные диски. PGPfone для защиты телефонных переговоров (для IP-телефонии), плагины для ICQ и встраиваемые модули для почтовых программ. Так же появились самораспаковывающиеся архивы SDA. Получателю такого архива (он был исполняемым файлом) вовсе не требуется иметь установленную PGP. Он должен лишь ввести ключевую фразу.

В настоящее время вышла девятая версия PGP, находящаяся в стадии бета-тестирования, у которой пока отмечаются сложности со взаимодействием с некоторыми антивирусами. Однако в основном отзывы положительные, новая версия во многом автоматизирована и самостоятельна, реализовывает концепцию click –to-encrypt.

В целом, PGP завоевывает новые позиции. Однако пока мечта его автора не осуществилась—PGP не имеет массового распространения, большинству пользователей кажется слишком сложным использовать шифрование. Но, думается, что с дальнейшей автоматизацией и развитие концепции click-to-encrypt привлечет новые потоки пользователей. PGP подкупает открытостью, надежностью шифрования, и прогрессирующей простотой использования, заинтересовывая нуждающихся в секретности людей.

Список литературы.

1. A security Analysis of PGP. Sieuwert van Otterloo.2001г. (Стюарт Ван Отерлоо) http://www.bluering.nl/pgp/

2. Bruce Schneier. *Applied Cryptography*. John Wiley and Sons, вторая редакция, 1996г.

3. Serge Mister & Robert Zuccherato. An Attack on CFB Mode Encryption As Used By OpenPGP . http://eprint.iacr.org/2005/033.pdf
4. Kahil Jallad; Jonathan Katz; Bruce Schneier Implementation of Chosen-Ciphertext Attacks against PGP and GnuPG. http://www.schneier.com/paper-pgp.pdf

5. The Internet Engineering Task Force. RFC 2440 bis. http://www.ietf.org/proceedings/04mar/I-D/draft-ietf-openpgp-rfc2440bis-09.txt

6. Форумы pgpru.com

7. 1991–2004 PGP Corporation. Phil Zimmermann, "An Introduction To Cryptography".

8. The Internet Engineering Task Force. RFC 1750. http://www.ietf.org/rfc/rfc1750.txt

9. Collision Search Attacks on SHA1. Xiaoyun Wang. Yiqun Lisa Yin. Hongbo Yu. 2005г. http://theory.csail.mit.edu/~yiqun/shanote.pdf