ЗАЩИТА ЭЛЕКТРОННОЙ ПОЧТЫ

О. А. Сукач[1], В. С. Оскерко[2]

[1]-студентка 1 курса, факультета МЭО, группы УВЭД-5, Белорусского государственного экономического университета.
[2]-научный руководитель, доцент кафедры информационных технологий, Белорусского государственного экономического университета, Минск, 220672, Партизанский пр., 26, тел. (8017) 249-19-81, e-mail oskerko:@bseu.minsk.by.

***Аннотация*:** Электронная почта на сегодняшний день является одной из наиболее применяемых технологий обмена данными между пользователями. В настоящее время это способ повсеместного общения пользователей в INTERNET.В корпоративных системах подобный метод находит свое применение в качестве средства обеспечения электронного документоборота.

Ключевые слова: электронная почта, клиент-серверные приложения, почтовые сообщения, защита информации.

1. Введение

Системы электронной почты функционируют на различном оборудовании и основываются на различных концепциях, однако главные причины их построения и работы аналогичны. Система электронной почты является одним из примеров сетей, построенных по принципу клиент-серверных приложений. Здесь, как и в других подобных распределенных механизмах, пользователь взаимодействует с клиентским программным обеспечением, а администратор-с серверным. Серверы различаются уровнями производительности и надежности, совместимостью с различными стандартами электронной почты, устойчивостью к ошибкам,

возможностью расширения.

Говоря об архитектуре посроения серверного программного обеспечения, следует отметить, что обычно она состоит из трех основных частей:

подсистема хранения сообщений, транспортная подсистема и служба каталогов. Подсистема хранения сообщений отвечает за получение сообщений и хранения до момента прочтения их пользователем. Хранящиеся в подсистеме сообщения могут также содержать присоединенные к ним файлы. Они обычно занимают много места, поэтому часто их количество или размер ограничиваются. Транспортная подсистема, называемая также системой маршрузации сообщений, осуществляет пересылку сообщений от одного почтового ящика к другому. Сообщение электронной почты бесполезно, если оно не поступит в нужный почтовый ящик. Служба каталогов распологает списком имен всех пользователей в системе и обеспечивает пересылку почты адресатам. Каталоги могут содержать списки сетевых имен или более развернутую информацию, с помощью которой можно обьеденить пользователей по фирмам, рабочим группам или по географическому признаку. Для того чтобы найти пользователя в системе электронной почты, нужно знать только его адрес.

2. Принцип защиты электронной почты

Основными угрозами в системах электронной почты являются следующие: Несанкционированный доступ к почтовым сообщениям (ПС), т.е. нарушение конфиденциальности;

Преднамеренное изменение получателем ПС с целью нарушения его достоверности или целостности;

Выдача себя за другого пользователя, чтоб снять с себя ответственность

Или же использовать его полномочия среднее целью формирования ложного ПС; изменения законного ПС; санкционирование ложных обменов ПС

Или же их подтверждение;

Отказ от факта передачи ПС;

Утверждение о том, что ПС получено от некоторого пользователя, хотя на самом деле оно сформулировано самим злоумышленником;

Несанкционированные изменения полномочий других пользователей на

отправку и получение ПС (ложная запись других лиц, ограничение или расширение установленных полномочий и т. п.);

Набор статистики обмена ПС (отслеживание: кто, когда и каким ПС получает доступ);

Заявление о сомнительности протокола обеспечения безопасности доставки ПС из-за раскрытия некоторой конфиденциальной информации;

Заявление о ложном времени получения ПС.

Одним из основополагающих документов в части требований защиты информации являются Рекомендации ISO 7498-2-89 и Стандарты МККТТ/

ISO для безопасной обработки ПС (Рекомендации серий X.400,X.500 МККТТ).

Стандарты и рекомендации для безопасной передачи , приема и обработки сообщений в системе определяют следующие принципы защиты информации:

Конфиденциальность содержания;

Конфиденциальность последовательности сообщений;

Целостность содержания;

Целостность последовательности содержания;

Аутентификация источника ПС;

Доказательство доставки;

Доказательство передачи;

Безотказность поступления;

Безотказность доставки;

Управление контролем доступа;

Защита от попыток расширения своих законных полномочий, а также изменения полномочий других пользователей;

Разметка по уровню защиты ПС;

Защита от модификации программного обеспечения путем добавления новых функций.

Надежная защита при передаче, обработке и хранении конфиденциальной информации базируется на применении современных криптографических программных и аппаратно-программных средств, реализующих механизмы шифрования информации, а также подтверждения ее целостности и подлинности среднее использованием электронной цифровой подписи. Защита информации в почтовых системах должна состоять из комплексных организационно-технических мероприятий по применению программных и аппаратно-программных криптографических методов и средств защиты среднее целью предотвращения несанкционированного доступа к конфиденциальной информации, обрабатываемой и хранимой абонентами системы и передаваемой по коммуникационной сети среднее использованием незащищенных линий связи.

3.Средства защиты электронной почты

Почта Privacy-Enhanced Mail.

Почта среднее повышенной секретностью (Privacy-Enhanced MAIL,PEM) представляет собой стандарт INTERNET, одобренный Советом по архитектуре сети, для обеспечения безопасности электронной почты в INTERNET. Первоначальный вариант был создан группой секретности и безопасности (Privacy and Security Research Group) Internet Resources Task Force (IRTF), а затем разработка была передана в рабочую группу PEM(PEM working Group)при IETF.Протоколы PEM предназначены для шифрования, проверки подлинности и целостности сообщения и управления ключами.

PEM является расширяемым стандартом. Процедуры и протоколы PEM разработаны так, чтоб быть совместимыми со множеством подходов к управлению ключами, включая симметричную схему и использование открытых ключей для шифрования ключей шифрования данных. Симметричная криптография применяется для шифрования текста сообщений. Для контроля целостности сообщения используются криптографические способы хэмирования. Другие документы поддерживают механизмы управления ключами с помощью сертификатов открытых ключей, алгоритмов, режимов и связанных идентификаторов, а также электронные подробности, инфраструктуру и процедуры управления ключами.

PEM поддерживает только определенные алгоритмы, но и позволяет добавлять алгоритмы более поздних версий. Сообщения шифруются алгоритмом PEM в режиме CBC. Проверка подлинности, обеспечиваемые средством проверки целостности сообщения(Message Integrity Check, MIC), использует MD2 или MD5. Симметричное управление ключами может применять либо DES, либо тройной DES с двумя ключами(так

называемый режим EDE). Для управления ключами PEM так же поддерживает сертификат открытых ключей, используя RSA(длина ключа до 1024 бит) и стандарт X.509 для структуры сертификатов.

PEM обеспечивает три сервиса повышения секретности: конфиденциальность, проверку подлинности и контроль целостности сообщений. К электронной почтовой системе не предъявляется никаких специальных требований. PEM может быть встроена выборочно, в определённые узлы или у конкретных пользователей, при этом её установка не влияет на работу остальной сети.

Длина ключей RSA, используемых в PEM, может меняться в диапазоне от 508 до 1024 бит. Этого достаточно практически для любого уровня безопасности. Более вероятно, что вскрытие будет направлено против протоколов управления ключами. Для обеспечения конфиденциальности никогда не записывайте на бумажный носитель свой закрытый ключ! Процедуры сертификации ключей в PEM, если все пользователи строго следуют соответствующим указаниям, делают это невозможным но, как известно, люди часто неаккуратны. Нарушитель может поступить хитрее и модифицировать реализацию PEM, работающую в вашей системе. Эта измененная версия может тайком пересылать нарушителю всю вашу почту, зашифровав ее открытым ключом; ему может быть послана даже копия вашего закрытого ключа. Если измененная реализация будет работать хорошо, то вы никогда не узнаете, что случилось.

Реального способа предотвратить такое вскрытие не существует. Вы можете использовать однонаправленную хэш-функцию и получить контрольную сумму исполняемого кода PEM. Затем, при каждом запуске программного обеспечения, можно проверять контрольную сумму, чтобы вовремя обнаружить изменения. Но нарушитель точно так же может изменить и код контрольной суммы при изменении кода PEM. Если у атакующего есть доступ к вашему компьютеру, он может разрушить безопасность PEM.

Вывод заключается в том, что нельзя доверять никакому элементу ПО, если вы не доверяете всей аппаратуре, на которой оно работает. Для многих такие опасения покажутся необоснованными, но для некоторых пользователей эта угроза вполне реальна.

4.Разновидности PEM

Средство TIS/PEM

Доверенные информационные системы (Trusted Information Systems, TIS), частично поддерживаемые Управлением по передовым научным проектам правительства Соединенных Штатов, являются особой, весьма специфической реализацией PEM (TIS/PEM). Они были разработаны для платформ UNIX, затем их также перенесли на VMS, DOS и Windows.

Хотя спецификации почты с повышенной секретностью определяются для Internet одним главным сертификационным центром, TIS/PEM поддерживает существование нескольких иерархий сертификации. Для того чтобы пользоваться услугами TIS/PEM, узлу не нужно присоединяться к иерархии Internet.

Программа RIPEM

RIPEM - это программа Марка Риордана (Mark Riordan), реализующая протоколы PEM. Свободный доступ к этой программе закрыт, однако для частного, некоммерческого применения ей можно воспользоваться бесплатно. Лицензия на право работать с этой программой входит в документацию.

Код не может быть экспортирован. Конечно, законы правительства США не действуют за пределами Соединенных Штатов, и кое-кто из пользователей игнорирует экспортные ограничения. Код RIPEM доступен по всему миру на электронных досках объявлений. Для экспорта разрешена версия, называемая RIPEM/SIC, реализующая только цифровые подписи.

Протокол MSP

Протокол безопасности сообщений (Message Security Protocol, MSP) - это военный аналог PEM. Он был создан NSA в конце 80-х годов во время работы над программой создания безопасной системы передачи данных по сети (Secure Data Network System, SDNS-program). Это совместимый с X.400 протокол уровня приложения для закрытия электронной почты. MSP планируется использовать в разрабатываемой сети оборонных сообщений (Defense Message System, DMS).

Предварительный протокол безопасности сообщений (Preliminary Message Security Protocol, PMSP), который предполагается использовать для «несекретных, но важных» сообщений, представляет собой адаптированную для применения с X.400 и TCP/IP версию MSP. Этот протокол также называют Mosaic.

Как и PEM, программные реализации MSP и PMSP достаточно гибки, их конструкция позволяет подстроиться под использование различных алгоритмов для осуществления функций безопасности, таких как подпись, хэширование и шифрование.

5. Обеспечение информационной безопасности X.400

Существуют два аспекта защиты при передаче и обработке ПС X.400: а) управление и администрирование системы защиты; б) защита обмена ПС. Обеспечение защиты в архитектуре X.400 включает в себя защиту ПС, непосредственно предоставленных MTS UA, MS и AU. В общем случае многие элементы службы защиты ПС обеспечивают возможность защиты в направлении отправитель-получателю и требуют использования UA. При этом они не требуют использования MTS, обладающей возможностями защиты (например, секретность содержимого может обеспечиваться путем шифрования содержимого ПС отправителем и его расшифрования получателем с различными параметрами защиты, передаваемыми внутри конверта ПС). Такое сообщение может передаваться MTS, которая будет обрабатывать формат содержимого (неформатированные октеты) и поля защиты в конверте. Некоторые из элементов службы защиты ПС взаимодействуют с MTS и требуют применения MTA с возможностями защиты.

Защиту почтовой системы X.400 целесообразнее осуществлять, используя разработанную в МОПНИЭИ почтовую систему. Преимущество подобного подхода заключается в использовании защищенной электронной почты, соответствующей стандарту X.400, основным достоинством которого является защита почтового сервера от несанкционированного доступа. Для предоставления абонентам услуг защищенной электронной почты в МО ПНИЭИ разработан электронный почтамт на базе программного продукта Messenger 400. У каждого пользователя электронной почты устанавливается ПО *абонентского пункта* (АП) защищенной электронной почты X.400, в котором криптографическая защита информации и процедура аутентификации выполнены на встроенном в АП ПО «Верба-О». Особенностью данного метода является обязательное наличие криптосервера и АП центра управления ключевой системой (ЦУКС), присоединяемых к электронному почтамту. Но для конкретной реализации данного метода требуется дополнительная проработка вопросов, связанных с согласованием перехода И С ТКП на защищенную почту X.400. В данной книге рассмотрены типовые решения по построению защиты почтовых систем на базе X.400.

Архитектура построения защищенной почтовой системы с использованием разработки МО ПНИЭИ представлена на рис. 3.29.

Основными компонентами защищенной почтовой системы являются:

- защищенный абонентский пункт или защищенный АП. На нем как раз и реализуются все функции криптографической защиты информации, серверная часть использует только аутентификацию пользователей почтовой системы. Таким образом, защита реализована на уровне пользователей, то есть почтовые сообщения (ПС) на серверную часть приходят уже зашифрованными и подписанными, почтовый сервер обеспечивает лишь транспортные функции по доставке ПС;
- криптосервер, на который вынесены с UNIX-платформы электронного почтамта средства криптографической защиты информации, используемые для аутентификации;
- шлюз ELINK, используемый АП для связи с системой передачи сообщений Messenger 400. Шлюз ELINK обеспечивает передачу сообщений с абонентского пункта на почтовый сервер Messenger 400 по протоколам LAPS и ELINK и строгую аутентификацию абонентов на основе системы криптографической защиты информации. При подсоединении абонента к почтовому серверу производится аутентификация пользователя с помощью криптосервера. Может производится как односторонняя, так и двусторонняя

аутентификация. Шлюз ELINK реализован в составе почтового сервера и представляет с одной стороны интерфейс обращения к криптосерверу, а с другой - к Messenger 400 (рис. 3.30).

Защищенный АП обеспечивает:

• обмен защищенной информацией через систему электронной почты Messenger 400 с использованием процедур абонентского шифрования электронной подписи сообщений;

• аутентификацию абонентов на почтовом сервере с целью предотвращения попыток НСД;

• обмен данными с почтамтом по протоколам SPX/IPX, TCP/IP, X.28/X.25, а также по специализированному помехоустойчивому протоколу LAPS;

• обмен частными сообщениями от абонента к абоненту с обеспечением сохранности частной почты;

• многоадресную доставку сообщений;

• передачу «электронных посылок», то есть присоединение документированного (текстового, бинарного) файла к сообщению. Файл затем будет отправлен вместе с сообщением получателю;

• выдачу извещений о доставке или невозможности доставки сообщений;

• прямой обмен защищенными сообщениями между двумя АП по коммутируемым телефонным линиям и аутентификацию абонентов при установлении соединения;

• защиту от НСД с регистрацией попыток НСД, реализованной на базе системы «Аккорд»;

• регистрацию протокола сеанса связи и ведение журналов входящих и исходящих сообщений на НЖМД с возможностью вывода данной;

• шлюз ELINK, используемый АП для связи с системой передачи сообщений Messenger 400. Шлюз ELINK обеспечивает передачу сообщений с абонентского пункта на почтовый сервер Messenger 400 по протоколам LAPS и ELINK и строгую аутентификацию абонентов на основе системы криптографической защиты информации. При подсоединении абонента к почтовому серверу производится аутентификация пользователя с помощью криптосервера. Может производится как односторонняя, так и двусторонняя аутентификация. Шлюз ELINK реализован в составе почтового сервера и представляет с одной стороны интерфейс обращения к криптосерверу, а с другой - к Messenger 400 (рис. 3.30).

6.E-commerce.

Огромные потенциальные преимущества, которые обеспечивает электронная коммерция (e- commerce), сводятся на нет повышенными рисками, возникающими, когда начинается практическая эксплуатация этого потенциала. • 8) с использованием асинхронных обмен факсимильными, голосовыми и видеосообщениями (в СООТВСТ ствующей

Поэтому защищенность е-коммерции становится первостепенной задачей, особенно для организаций, предполагающих большое присутствие в Сети on-line. В сети Internet общение между людьми, а также контакты организаций между собой происходят в основном через электронную почту. Незащищенная электронная почта может быть легко перехвачена, и ее содержимое может быть изменено. Поэтому обеспечение защиты электронной почты стало важной частью общей защиты инфраструктуры предприятия. Организация может защитить свою электронную почту, предлагая пользователям одну из следующих возможностей, либо используя их обе:

- Цифровые подписи электронной почты
- Шифрование электронной почты

7.Цифровая подпись электронной почты

Первая стадия защиты электронной почты вашей организации для пользователей заключается в том, чтобы в цифровом виде подписать их сообщения, используя сертификат. Цифровые сигнатуры включают в себя три важных принципа защиты:

- Проверка: Когда пользователь посылает электронную почту, которая подписана цифровой подписью, получатель может немедленно подтвердить личность отправителя

- Защита от отказа: Отправитель не сможет отрицать, что он или она отправляли данное письмо.

- Целостность содержания: Добавление цифрового представления к электронному письму гарантирует, что любые последующие изменения содержимого сообщения будут немедленно обнаружены. Цифровая подпись электронного письма не изменяет фактическое содержание тела письма в любом виде. Netscape Messenger, Microsoft Outlook и Outlook Express, а также коммерческие продукты, такие как MailSecure (Baltimore Technologies), дают пользователям возможность подписывать личные сообщения. Настроив опции безопасности электронной почты, пользователь сможет автоматически подписывать исходящие сообщения. Каждый сертификат связан с ключевой парой, состоящей из открытого ключа, доступного любому, и личного ключа, доступного только владельцу сертификата. С помощью eToken Enterprise, сертификат и оба ключа надежно хранятся в пользовательском eToken, обеспечивая мобильность и защищенность.

Пользовательский сертификат и связанный с ним личный ключ требуются для подписи электронной почты. Когда электронное письмо посылается получателю, копия сертификата отправителя и его соответствующий открытый ключ посылается вместе с ним. Например, когда Наталия посылает Олегу подписанную электронную почту, Олег также получает сертификат Наталии и ее открытый ключ.

8.Шифрование и дешифрование электронной почты

Вторая стадия в обеспечении защиты корпоративной электронной почты должна гарантировать защиту содержимого сообщений, шифруя их, а также подписывая. Зашифрованное сообщение не читаемо до тех пор, пока оно не расшифровано.

Чтобы зашифровать сообщение, отправитель должен иметь копию открытого ключа получателя. Зашифрованное сообщение может быть расшифровано и прочитано только владельцем соответствующего личного ключа. Теперь, когда Наталия послала Олегу подписанное сообщение, Олег имеет ее открытый ключ и может использовать его для зашифровки сообщений, которые он пошлет обратно Наталии. Наталия может расшифровать сообщение, используя соответствующий личный ключ, и сможет прочесть содержимое письма, как проиллюстрировано ниже:

Всякий раз, когда пользователи принимают письмо с цифровой подписью, они могут сохранять сертификат отправителя и его общий ключ в их адресной книге для электронной почты. Также пользователи могут просматривать список каталогов в сети, содержащих открытые ключи и сертификаты, и использовать их для отправки зашифрованной электронной почты.

9.Token Enterprise

eToken Enterprise поддерживает хранение в безопасности множества сертификатов и ключей в пользовательском eToken. Сохраняя сертификаты и ключи, eToken обеспечивает высший уровень безопасности, мобильности и удобства. Когда пользователь вставляет eToken и вводит правильный пароль, все сертификаты и ключи, хранимые в eToken, становятся легко доступными для использования.

Комплекс средств защиты информации, передаваемой по электронной . почте PostCrypt-Mail

Комплекс PostCrypt-Mail v2.03 предназначен для обеспечения защиты сообщений, передаваемых по электронной почте, от несанкционированного доступа с использованием механизмов криптографической защиты (электронная цифровая подпись (ЭЦП), шифрование, выработка кодов аутентификации сообщений имитовставок).

Идентификация и аутентификация пользователей комплекса осуществляется на основе предъявляемого электронного идентификатора (записанного на устройстве хранения) и введенного псевдонима и пароля доступа. В качестве устройств хранения

электронных идентификаторов и секретных ключей ЭЦП пользователей в данной версии PostCrypt-Mail могут применяться:

- жесткий диск персонального компьютера (ПК);
- дискета;
- электронный брелок eToken.

Комплекс PostCrypt-Mail допускает работу на одном компьютере нескольких пользователей с различными электронными идентификаторами. Для нескольких электронных идентификаторов пользователей может использоваться одно и тоже устройство хранения.

Максимальное количество пользователей комплекса, зарегистрированных на одном ПК -1024.

В состав комплекса PostCrypt-Mail входят:

- АРМ управления комплексом;
- исполняемый модуль защиты информации PostCrypt-Mail;
- подключаемый модуль (plug-in) защиты информации PostCrypt-Mail для Microsoft Outlook 97/98/2000, позволяющий автоматически обрабатывать входящие/исходящие сообщения электронной почты вместе с вложениями;
- подключаемый модуль (plug-in) для командной оболочки Microsoft Windows, позволяющий вызывать исполняемый модуль защиты информации PostCryp t-Mail непосредственно из всплывающего меню Проводника Microsoft Windows..

Для восстановления работоспособности комплекса после возможных сбоев предусмотрена возможность создания/восстановления служебных баз комплекса из архивных копий. В комплексе также реализована возможность создания мобильной (носимой) копии на дискете, что позволяет готовить, отправлять и принимать защищенные сообщения на любом компьютере, имеющем доступ к электронной почты. Комплекс функционирует на IBM-совместимых компьютерах под управлением операционных систем Windows 95/ 98/ Me/ NT/ 2000. Подключаемый модуль защиты информации PostCrypt-Mail для Microsoft Outlook предназначен для работы с Microsoft Outlook версий 97/98/2000.

В стандартный комплект поставки комплекса PostCrypt-Mail входят:

- программа инсталляции INSTALL.EXE для Windows 95/ 98/ Me/ NT/ 2000;
- руководство пользователя PostCrypt-Mail в формате .pdf;
- лицензионный файл PLICENCE.DAT;
- файл README.TXT, содержащий краткое руководство по инсталляции и описание особенностей конкретной версии и редакции системы.

ЛИТЕРАТУРА

Петров. А. А. Компьютерная безопасность. Криптографические методы защиты./ Издательство “ЛАЙТ Лтд. », Москва , 2000.