Система электронного перевода денежных средств в сети фирмы Дженерал Электрик

Курсовая работа по курсу «Защита Информации» Студента 014 гр. Юркуса А.А.

В последние годы значительно возросла необходимость повышенной защиты банковской информации. Требуется обеспечить целостность данных, которыми обмениваются стороны, и проверку аутентичности отправителя. Ниже будут описаны криптографические методы, которые используются компанией GE Information Services в глобальной сети для защиты банковской информации.

1. Введение и обзор.

1.1. Глобальная передача данных.

GE Information Services (GEIS) - это подразделение американской компании General Electric. Оно управляет самой широкой в мире коммерчески доступной сетью телеобработки. Доступ к глобальной сети передачи данных GEIS возможен в 750 городах в 30 странах; благодаря соединению с сетями передачи данных общественного пользования число стран увеличивается до 70. Доступ к сети возможен с 90% деловых телефонов во всем мире. Сеть позволяет обслуживать одновременно до 4000 пользователей в часы пиковой нагрузки и передавать до 400 миллионов символов в час по пяти спутниковым каналам, подводным кабельным линиям и наземным линиям, протяженностью 500 000 миль. В обслуживании участвуют более 500 компьютеров, используемых для обработки и связи.

Сеть GEIS.

GEIS имеет двадцатилетний опыт работы в международном банковском деле, обеспечивая управление денежными средствами, электронную передачу платежной информации, аккредитивов, займов, ревизионных отчетов и уведомлений об окончании платежей.

1.2. Проблема безопасности при передаче банковской информации

1.2.1. Задача.

В последние годы значительно возросла необходимость повышенной защиты банковской информации. Требуется обеспечить целостность данных, которыми обмениваются стороны, и проверку аутентичности отправителя. Проблема безопасности остро стояла перед лицами, подписывающими документы, ревизорами и банковскими инспекторами. Требовалось решение, отвечающее международным стандартам, не вносящее задержек в обработку данных, недорогое, обеспечивающее высокую степень защиты.

1.2.2. Решение.

Система перевода денежных средств GEIS, используемая для передачи банковской информации, была изменена путем включения новых интерфейсов. Интерфейсы содержат модули защиты, выполняющие криптографическую обработку сообщений и персональную аутентификацию автоматически. Решение, разработанное фирмой Racal-Guardata, представляет собой двухуровневую криптографическую систему, реализующую алгоритм шифрования данных DEA, во-первых, при аутентификации сообщений

(ANSI X9.19) и, во-вторых, при совместной персональной аутентификации и аутентификации сообщений. Совместное использование обоих методов обеспечивает аутентификацию сообщений и авторизацию. В качестве среды для выполнения этих функций выступает физически защищенное устройство, известное как модуль защиты. В зависимости от предъявляемых требований модуль защиты может выполняться в виде карточки безопасности или отказоустойчивой универсальной ЭВМ. Для процесса авторизации используется устройство Watchword.

2. Система перевода денежных средств GEIS.

Система перевода денежных средств (СПДС) позволяет законным клиентам банка (казначею корпорации или секретарю большой компании) вырабатывать команды по платежам. Эти команды вырабатываются при помощи персонального компьютера пользователя или универсальной ЭВМ для передачи в пункты доставки банка в соответствии с условиями, определяемыми банком. СПДС также используется дилерами ценных бумаг для выполнения платежных операций. СПДС - это услуга, предоставляемая GEIS банкам, которые в свою очередь продают услуги своим корпоративным клиентам. Для казначеев корпорации основное требование - быстро, безопасно и точно оперировать денежными средствами. В частности, это помогает казначею получить преимущества на основных финансовых рынках мира при инвестировании и использовании фондов. Административный центр клиентуры (АЦК) банка отвечает за создание шаблонов, используемых клиентами для различных видов платежей, определяемых банком. Эти шаблоны являются электронным эквивалентом платежных форм. Обычно это формы для переводов внутри банка или на счета других банков внутри страны или за его пределами.

Система перевода денежных средств GEIS.

Клиент выбирает шаблон, заполняет его необходимой информацией, тем самым формируя команду. Информация, добавляемая клиентом, носит переменный характер и контролируется банком. Обычно это сумма, дата и (до внедрения криптографической аутентификации) проверочный ключ. Система поддерживает два уровня работы - работа банка и работа клиента. Эти уровни взаимоисключающие: персонал банка не может выполнять функций клиентов, клиенты не могут выполнять функций персонала. АЦК несет полную ответственность за управление ключами и создание шаблонов. Клиент отвечает за создание команды, а пункт доставки обязан проверять шаблоны и команды и санкционировать их оплату.

3. Стандарты по безопасности.

При разработке системы договорились о применении существующих стандартов, в частности, стандарта ANSI DEA (X3.92) и стандартов по аутентификации: оптовые сделки - ANSI X9.9, розничные – ANSI X9.19. Основное внимание было уделено стандарту X9.19, так как стандарты аутентификации аналогичны, но X9.9 был более старым и находился в переработке. Для создания ключевой системы за основу взят стандарт ANSI X9.17 (система главного и сеансных ключей).

4. Оборудование, обеспечивающее защиту СПДС.

Для выполнения требований по аутентификации сообщений и пользователей для пользователей ПК и универсальных машин предлагается использование трех продуктов:

1) генератор и контроллер Watchword для аутентификации пользователей и контроля доступа;

2) карточка безопасности для персонального компьютера для выработки и проверки кода аутентификации сообщения (КАС);

3) периферийный модуль защиты на базе универсальной ЭВМ для выработки и проверки КАС большого объема.

4.1. Watchword.

Устройство Watchword фирмы Racal-Guardata использует метод одноразового пароля, требующий правильного ответа на различные запросы при каждом использовании системы. Система состоит из генератора и контроллера. Генератор представляет собой небольшой блок, хранимый у законного пользователя. В устройстве хранится секретный ключ, известный только контроллеру, и персональный идентификатор (ПИН) пользователя, защищенные самой конструкцией устройства. Для входа в главную систему пользователь должен аутентифицировать себя при помощи генератора. При этом генерируется семизначный ответ на семизначный неповторяющийся запрос контроллера. В качестве контроллера может выступать выделенный компьютер PC-AT или программа, выполняемая в главной ЭВМ во взаимосвязи с модулем защиты (см.раздел 4.3). Для предотвращения незаконного использования генератора правильный ответ формируется только при вводе пользователем ПИН. Система Watchword зависит от того, что пользователь имеет (генератор), и от того, что он знает (ПИН). Знание одного из компонентов не даст возможности незаконного входа в систему. Генератор использует алгоритм DES для выработки семизначного ответа (**R**) из семизначного запроса (**C**). Контроллер, имеющий копию секретного ключа, способен опознать пользователя, расшифровав **R** для получения **C**. В зависимости от использования Watchword может вырабатывать цифровую подпись в дополнение к функции разграничения доступа. $\mathbf{E_{KU}(C)=R}$. Аутентификация пользователя происходит при помощи Watchword. Контроллер создаст запрос **C**. Ответ **R** посылается по сети контроллеру для проверки.

4.2. Карточка безопасности для персонального компьютера.

Карточка безопасности фирмы Racal-Guardata выполняется в защищенном корпусе и подключается к шине расширения ПК PC-AT,XT и других IBM-совместимых. Она обеспечивает широкий диапазон функций, связанных с аутентификацией, шифрованием и управлением ключами. Карточка использует DEA (ANSI X3.92). Криптографические ключи, используемые карточкой, можно хранить в ПК после их шифрования на главном ключе двойной длины (**LMK**). Встроенный микропроцессор управляет использованием и защитой ключей карточки. Таким образом, после шифрования ключа на местном главном ключе, он не подвергается расшифровке, в том числе и противником, использующим функции дешифрования карточки. Этот метод позволяет программное восстановление часто используемых ключей и, следовательно, восстановление аппаратуры после отказов и т.д. Число хранимых ключей не ограничено. $\mathbf{E_{LMK}(SK)}$. Аутентификация сообщений происходит с помощью карточки безопасности персонального компьютера. Для выработки КАС карточка восстанавливает сеансный ключ **SK**, зашифрованный на местном главном ключе (**LMK**). КАС вычисляется в соответствии с ANSI X9.19 и добавляется к платежной команде. Высокая скорость работы достигается использованием прямого доступа к памяти. Канал прямого доступа к памяти в главном ПК используется для быстрого обмена данными с буфером данных карточки (6 кбайт), а встроенный канал - для быстрых DES-преобразований под правлением микропроцессора. Карточка может использоваться для шифрования данных, хранимых в ПК, для передачи информации в аналогичные ПК или универсальные ЭВМ, оборудованные главным модулем защиты (см. раздел 4.3). Если не требуется секретность, карточка может использоваться для выработки и проверки КАС; при этом сообщения не зашифрованы, но защищены от злоумышленного искажения, уничтожения или подстановки. Криптозащита требует регулярного обновления ключей, и карточка предоставляет несколько вариантов управления ключами. Большие сети можно разбить на взаимно безопасные зоны. Новые сеансные ключи можно передавать зашифрованными на зональном главном ключе. При совместном использовании с Watchword карточка позволяет проводить проверку динамического пароля и вырабатывать цифровую подпись, уникальную для пользователя.

4.3. Главный модуль защиты.

Этот модуль представляет собой защищенное устройство, периферийное по отношению к универсальной ЭВМ. Выполнен в виде трех одинаковых блоков в одном корпусе, благодаря чему обеспечивается тройная отказоустойчивость. Модуль выполняет криптографические функции, необходимые для защиты системы и среды, в которой эти функции могли бы безопасно выполняться. Модуль обеспечивает высокую пропускную способность ввиду аппаратной реализации DES. Предусмотрена физическая защита блока в виде замков и переключателей, подключенных к специальной схеме защиты. Модуль обеспечивает аутентификацию сообщений на базе DES, проверку ПИН и ряд функций DES, в том числе шифрование и управление ключами. Для подписания платежной команды КАС вводится в Watchword как запрос, а ответ считается подписью и добавляется к платежной команде и КАС. $\mathbf{E_{LMK}(SK)}$. Главный модуль защиты используется для проверки КАС или в качестве контроллера для аутентификации пользователя. Центральный процессор и программно-аппаратные средства DES поддерживаются внутренней энергонезависимой памятью. Память используется для хранения главных ключей, которые управляют работой и обменом модуля с системой главной ЭВМ. При установке главные ключи загружаются из нескольких ПЗУ, которые могут храниться у разных лиц (это уменьшает степень риска). Структура управления ключами в модуле защиты иерархическая; главные ключи никогда не передаются за пределы модуля; рабочие ключи надежно шифруются на главных ключах. Зашифрованные рабочие ключи могут храниться на любой главной ЭВМ, поскольку они могут использоваться только модулем защиты.

5. Аутентификация и авторизация в СПДС.

5.1. Создание шаблонов.

Шаблон создается в АЦК (административный центр клиентуры). К шаблону добавляется КАС (**MAC1**) и "подпись" создателя шаблона, формируемая следующим образом: 32 бита КАС преобразуются в семизначное число и при помощи прикладной программы выдаются создателю шаблона как запрос. При помощи генератора Watchword создатель вырабатывает семизначный ответ (SIG1), который добавляется к шаблону и играет роль подписи. Подпись гарантирует целостность сообщения и однозначное определение создателя шаблона. Затем шаблон помещается в сеть.

5.2. Создание команды.

Пользователь получает шаблон из сети и проверяет его достоверность при помощи КАС шаблона. Он не может проверить подпись создателя шаблона. Затем он заполняет шаблон, формируя команду. Команда защищается при помощи собственного КАС (**MAC2**). На этом этапе команда может быть помещена в сеть, но она не будет доставлена клиенту (банку), пока пользователь не введет свой идентификатор (**ID**). После этого КАС преобразуется в запрос, предоставляемый пользователю. Пользователь при помощи генератора Watchword вырабатывает ответ, который становится его подписью SIG2, добавляется (становится частью) к команде, которая после этого передается.

5.3. Проверка команды.

При получении команды пункт доставки способен:

а) проверить КАС шаблона;

б) проверить подпись создателя шаблона;

в) проверить КАС команды;

г) проверить подпись создателя команды;

д) обновить контрольный журнал.

6. Управление ключами в СПДС

6.1. Ключевая структура.

Как упоминалось, АЦК отвечает за создание шаблонов совместно с КАС, подписью и сеансным ключом шифрования. При получении пользователем проверяется КАС, заполняется шаблон, т.е. формируется команда для отправки на пункт доставки. КАС, формируемые АЦК и пользователем (**MAC1** и **MAC2**), вырабатываются при помощи сеансного ключа (**SK**). Этот ключ вырабатывается модулем защиты в АЦК при создании шаблона и добавляется к нему в зашифрованном виде в соответствии с двухуровневой структурой ANSI X9.17.

Формат шаблона-платежа в СПДС.

Описание полей: PN - номер платежа, UN - номер пользователя, PT - тип платежа, DD - назначенная дата, 1-61 - текущие поля, 62 - порядковый номер, 63 - $\mathbf{E_{UCWK}(SK)}$, 64 - $\mathbf{E_{DPCWK}(SK)}$, 65 -поразрядная карта отображения информации, 66 - КАС шаблона, 67 - подпись шаблона, 68 - КАС платежа, 69 - идентификатор пользователя, 70 - подпись платежа. Поля 63 и 64 содержат сеансный ключ, зашифрованный разными зональными ключами. Поля 66 и 68 будут содержать КАС, сформированные при помощи сеансного ключа. Создание ключевой системы начинается с генерации зональных главных ключей. Зоной называется группа, состоящая из двух или более абонентов. Зональный главный ключ имеет длину 112 битов; он не передается по каналам связи, а доставляется каждому абоненту в соответствии с процедурами, описанными в стандарте ANSI X 9.17. Зональный главный ключ хранится у каждого абонента в зашифрованном виде (на ключе **LMK**). Зональный главный ключ для связи между АЦП и клиентом обозначается через **UCMK**, а для связи между АЦП и пунктом доставки – через **DPCMK**. Следующий шаг - генерация зональных рабочих ключей **UCWK** и **DPCWK**. Они пересылаются по каналам связи, зашифрованные на ключах **UCMK** и **DPCMK** соответственно. Зональный рабочий ключ дешифруется в карте секретности или модуле секретности получателя и зашифровывается на ключе **LMK**. При создании бланка АЦП генерирует сеансовый ключ **SK**. Затем АЦП шифрует его в виде $\mathbf{E_{UCWK}(SK)}$ - для клиента и $\mathbf{E_{DPCWK}(SK)}$ - для пункта доставки и помещает оба эти значения в некоторые фиксированные поля шаблона 63 и 64.

6.2. Обработка шаблонов и платежей.

После создания шаблона имеются поля для номера платежа, номера пользователя, типа платежа, текущих записей (поля 1-61); поля 63 и 64 заполняются модулем защиты. Поле 65, поразрядная карта отображения информации, устанавливается автоматически и используется модулем защиты для выработки КАС шаблона (поле 66). Создатель шаблона получает запрос, сформированный на основе КАС, и формирует ответ при помощи генератора (поле 67). Затем шаблон может помещаться в GEIS, и копия посылается в пункт доставки в качестве эталона. Когда пользователь производит платеж, то формируются свои КАС и подпись. Платеж поступает в сеть для доставки по назначению. КАС платежа охватывает все сообщение, включая поле 62, являющееся порядковым номером. Это предотвращает повторную передачу сообщений. При получении платежа подписи и КАС платежа и шаблона проверяются. Для проверки КАС шаблона извлекается поле 64. $\mathbf{E_{LMK}(DPCWK)}$ извлекается из базы. Это позволяет в модуле защиты при помощи $\mathbf{E_{DPCWK}(SK)}$ восстановить сеансный ключ. Затем вырабатывается КАС шаблона и сравнивается с полем 66; если они совпадают, вырабатывается соответствующий запрос. При помощи номеров платежа и пользователя можно установить подписавшего. Информация, идентифицирующая пользователя, и запрос вводятся в контроллер, который формирует ответ. Ответ сравнивается с полем 67. После успешной проверки шаблона проверяется платежное сообщение. В модуле защиты при помощи сеансного ключа вырабатывается КАС и сравнивается с полем 68. При их совпадении вырабатывается запрос. С помощью поля 69, идентифицирующего

пользователя, контроллер формирует ответ, который сравнивается с полем 70. При любом несовпадении или неудачном поиске в базе процесс прерывается.

7. Заключение.

Были исследованы управление ключами и криптографические процессы, используемые для защиты передачи банковской информации. Ставилась цель показать, как безопасно управлять ключами в сети GEIS. Пользователь должен использовать только генератор Watchword для идентификации и авторизации, а остальные процессы автоматизированы и скрыты от него.

Список использованных материалов:

1. Безопасность в сетях передачи банковской информации.

http://www.myportal.ru/sec/doc6.html

2. Система электронного перевода денежных средств в сети фирмы Дженерал Электрик.

http://www.cryptography.ru/db/msg.html?mid=1169307&uri=node88.html

3. Компьютеры и безопасность, 1989, том 8, №3, стр.209-221. М. Шейн. Безопасность электронного перевода денежных средств.

Computers & Security, 1989, vol.8, N3, pp.209-221. M.Shain. Security in Electronic Funds Transfer.