**Задание на 03.02.2022**

МДК 03.02 Программно-аппаратные средства защиты информации

1. **Сделать конспект лекции**
2. **Сделать практическую работу №11 Работа с антивирусной программой «Касперский»**
3. **Сделать практическую работу №12 Работа с антивирусной программой «Dr. Web»**
4. **Отчет отправить на почту svebalch@mail.ru**

**Лекция 11**

**Ключи. Организация хранения ключей (с примерами реализации). Распределение ключей. Использование комбинированной криптосистемы. Метод распределения ключей Диффи-Хеллмана. Протокол вычисления ключа парной связи ЕСКЕР.**

Любая криптографическая система основана на использовании криптографичес­ких ключей. Под ключевой информацией понимают совокупность всех действую­щих в информационной сети или системе ключей. Если не обеспечено достаточно надежное управление ключевой информацией, то, завладев ею, злоумышленник получает неограниченный доступ ко всей информации в сети или системе. Управ­ление ключами включает реализацию таких функций, как генерация, хранение и распределение ключей. Распределение ключей - самый ответственный процесс в управлении ключами.

**1. Ключи. Организация хранения ключей**

При работе с открытыми КС необходимо обеспечить защиту аутентифицирующей информации, хранимой в КС. В открытых КС часто отсутствуют внешние максимально защищенные от НСД устройства, хранящие аутентифицирующую информацию, и данную информацию, используемую для аутентификации, приходится хранить в реальном объекте файловой системы (БД аутентификации).

Эту информацию необходимо защищать от 2 основных видов угроз:

 - угроза непосредственного доступа злоумышленника к БД аутентификации с целью ее копирования, модификации, удаления;

 - угроза несанкционированного изучения БД аутентификации.

Защита от первого вида угрозы реализуется, как правило, на уровне ядра ОС путем ограничения доступа к той БД аутентификации всех субъектов, за исключением привилегированных. Либо защита от данного вида угроз реализуется путем определения дискреционной политики безопасности. Однако, как правило, способы защиты от угроз первого вида не работают корректно и их можно обойти, используя существующие уязвимости.

Поэтому при защите БДА большее внимание уделяется защите от несанкционированного исследования их содержимого.

Методы:

1). Шифрование

Такой подход к закрытию содержимого БД аутентификации не является стойким, так как:

1. Шифрование должно быть на ключах, которые необходимо хранить. Хранение в операционной системе недопустимо.
2. При аутентификации пользователя необходимо расшифровать пароль, тем самым нарушить его секретность. Такой способ также уязвим к атакам, например, к атакам, заключенным в пошаговом исследовании процесса аутентификации с помощью известных отладчиков.

2). Хэширование

Для защиты от исследования БДА используется две типовых схемы хранения ключевой информации:

Схема 1

Пусть пользователь с N i имеет идентификатор $ID\_{i}$и ключ идентификации $K\_{i}$, тогда первая типовая схема предполагает наличие в БД аутентификации двух основных полей:

|  |  |  |
| --- | --- | --- |
| № | Информация для идентификации | Информация для аутентификации |
| 1 | ID1 | E1 |
| 2 | ID2 | E2 |
| … |  |  |
| n | IDn | En |

$Ei = F\left(IDi, Ki\right), F$ – функция хэширования. Функция $F$ должна удовлетворять следующим свойствам:

1). Необратимостью: восстановить$ Ki$ возможно было бы только полным перебором

2). Вероятность совпадения хэшей 2 произвольно взятых сообщений должна быть чрезмерно мала, если длина сообщения меньше длины хэша, то вероятность должна быть равна нулю.

3) Рассеивание – при малейшем изменении сообщения его хэш должен существенным образом изменяться.

При использовании такой схемы хранения ключевой информации, ОС в явном виде не знает те ключи, пароли, которые используются пользователем для входа в систему.

Алгоритм аутентификации пользователя будет выглядеть следующем образом:

 Пользователь вводит идентификатор при входе в систему. Подсистема аутентификации ищет наличие данного идентификатора в БД аутентификации. Если данный идентификатор не найден, то идентификация отклоняется. Если же введенный идентификатор равен некому $IDi$, то подсистема аутентификации извлекает $Ei$, соответствующий ему. Далее пользователь вводит пароль k. Подсистема аутентификации вычисляет $y = F(IDi, ki)$. Если $y=Ei$ , то аутентификация принимается.

Недостатком данной схемы является то, что достаточно часто закрытые образы паролей формируются как $Ei = F(ki)$. Тогда пользователи, имеющие одинаковые пароли, будут иметь одни и те же хэши. Злоумышленник, обнаружив подобную ситуацию, может сделать вывод, что пользователи используют одинаковые пароли.

Для устранения этого вводится вторая схема аутентификации.

Схема 2

Вторая типовая схема предполагает хранение вместе с идентификатором $ID\_{i}$случайной информации $S\_{i}$, формирующейся при создании учетной записи.$ S\_{i}$ называется символом привязки.

$$Ei = F(S\_{i},ki)$$

|  |  |  |
| --- | --- | --- |
| **№** | **Информация для идентификации** | **Информация для аутентификации** |
| 1 | ID1 , S1 | E1 |
| 2 | ID2, S2 | E2 |
| … |  |  |
| n | IDn, Sn | En |

В этом случае хэши будут различны. Данная схема используется в системах класса Unix.

**Утверждение о подмене эталона**

Если злоумышленник имеет доступ на запись в БД аутентификации, то он может пройти аутентификацию как любой пользователь КС, отраженный в ней, в том числе и как администратор. Следовательно, доступ на запись в БД аутентификации должны иметь только привилегированные субъекты.

**Защита баз данных аутентификации операционных систем класса Windows NT.**

В данных ОС БД аутентификации хранится в каталоге: winnt\system32\config

БДА носит название SAM, а файл System, в котором хранится ключ шифрования БД аутентификации.

В данной БД аутентификации хранится 2 вида хэшей:

 - LANMAN, используемый для удаленной сетевой аутентификации с ранних версий Windows;

 - NTLM, используется для локальной аутентификации.

**Алгоритм вычисления хэша LANMAN**



Например, если пароль будет состоять из заглавных букв английского алфавита (26), прописных букв английского алфавита (26), цифр (10), специальных символов (13), то

$$A=26+26+10+13=75$$

$$S=75^{10}$$

Тогда время подбора $T=\frac{75^{10}}{10^{7}}$ сек

Используя хэш LANMAN, получим, что

$$A=49$$

$$S=49^{7}$$

Время подбора пароля $T=\frac{49^{7}}{10^{7}}≈5^{7}$

Минусы:

 - все символы пароля преобразуются в заглавные, что уменьшает энтропию паролей, сокращает пространство их перебора;

 - пароль разбивается на две части, которые образуются независимо друг от друга;

При выборе паролей больше 14 символов хэши LANMAN из БД исчезают, следовательно, необходимо выбирать пароли из 15-16 символов.

**Хэш NTLM**



Хэш NTLM имеет длину 16 байт. Каждому из паролей длины меньшей или равной 16 символов соответствует единственный хэш NTLM, по которому ОС будет определять корректность его ввода пользователем. Однако если выбрать пароли больше 17 символов, то для них найдутся другие с длинной меньше или равной 16 символам, которые будут иметь тот же самый хэш. В этом случае ОС будет пускать пользователя на пароле меньшей длины. Есть вероятность, что длина таких паролей будет очень мала. Поэтому в целях безопасности использование паролей длиной больше или равной 17 символов необходимо запретить. Для ОС, построенных на технологии NT, следует выбирать пароли 15-16 символов.

**2. Распределение ключей**

При использовании симметричной криптосистемы две вступающие в инфор­мационный обмен стороны должны сначала согласовать секретный сессионный ключ, то есть ключ для шифрования всех сообщений, передаваемых в процессе обмена. Этот ключ должен быть неизвестен всем остальным, и его необходимо периодически обновлять одновременно у отправителя и получателя. Процесс со­гласования сессионного ключа называют также обменом или распределением ключей.

Асимметричная криптосистема предполагает использование двух ключей -открытого и закрытого (секретного). Открытый ключ можно разглашать, а за­крытый надо хранить в тайне. При обмене сообщениями необходимо пересылать только открытый ключ, обеспечив его подлинность.

К распределению ключей предъявляются следующие требования:

* оперативность и точность распределения;
* конфиденциальность и целостность распределяемых ключей.

Для распределения ключей между пользователями компьютерной сети исполь­зуются следующие основные способы [95]:

1. Использование одного или нескольких центров распределения ключей.

2. Прямой обмен ключами между пользователями сети.

Проблемой первого подхода является то, что центру распределения ключей известно, кому и какие ключи распределены, и это позволяет читать все сообще­ния, передаваемые по сети. Возможные злоупотребления могут существенно на­рушить безопасность сети. При втором подходе проблема состоит в том, чтобы надежно удостовериться в подлинности субъектов сети.

Задача распределения ключей сводится к построению такого протокола распре­деления ключей, который обеспечивает:

* взаимное подтверждение подлинности участников сеанса;
* подтверждение достоверности сеанса;
* использование минимального числа сообщений при обмене ключами.

Характерным примером реализации первого подхода является система аутен­тификации и распределения ключей Kerberos.

Остановимся подробнее на втором подходе - прямом обмене ключами между пользователями сети.

При использовании для защищенного информационного обмена криптосисте­мы с симметричным секретным ключом два пользователя, желающие обменяться криптографически защищенной информацией, должны обладать общим секрет­ным ключом. Эти пользователи должны обменяться общим ключом по каналу связи безопасным образом. Если пользователи меняют ключ достаточно часто, то доставка ключа превращается в серьезную проблему.

Для решения этой проблемы можно применить два основных способа:

1. Использование асимметричной криптосистемы с открытым ключом для за­щиты секретного ключа симметричной криптосистемы.

2. Использование системы открытого распределения ключей Диффи-Хеллмана.

Реализация первого способа осуществляется в рамках комбинированной крип­тосистемы с симметричными и асимметричными ключами. При таком подходе симметричная криптосистема применяется для шифрования и передачи исходно­го открытого текста, а асимметричная криптосистема с открытым ключом - для шифрования, передачи и последующего расшифрования только секретного клю­ча симметричной криптосистемы.

Второй способ безопасного распространения секретных ключей основан на применении алгоритма открытого распределения ключей Диффи-Хеллмана. Этот алгоритм позволяет пользователям обмениваться ключами по незащищен­ным каналам связи.

**Лекция 12**

**Использование комбинированной криптосистемы**

Главным достоинством асимметричных криптосистем с открытым ключом явля­ется их потенциально высокая безопасность: нет необходимости ни передавать, ни сообщать кому бы то ни было значения секретных ключей, ни убеждаться в их подлинности. Однако быстродействие асимметричных криптосистем с открытым ключом обычно в сотни и более раз меньше быстродействия симметричных крип­тосистем с секретным ключом.

В свою очередь, быстродействующие симметричные криптосистемы страдают существенным недостатком: обновляемый секретный ключ симметричной крип­тосистемы должен регулярно передаваться партнерам по информационному об­мену, и во время этих передач возникает опасность раскрытия секретного ключа.

Существует эффективный метод комбинированного использования симмет­ричного и асимметричного шифрования.

Комбинированное применение симметричного и асимметричного шифрования позволяет устранить основные недостатки, присущие обоим методам. Комбини­рованный (гибридный) метод шифрования позволяет сочетать преимущества высокой секретности, предоставляемые асимметричными криптосистемами с от­крытым ключом, с преимуществами высокой скорости работы, присущими сим­метричным криптосистемам с секретным ключом.

При таком подходе симметричную криптосистему применяют для шифрования исходного открытого текста, а асимметричную криптосистему с открытым клю­чом - только для шифрования секретного ключа симметричной криптосистемы. В результате асимметричная криптосистема с открытым ключом не заменяет, а лишь дополняет симметричную криптосистему с секретным ключом, позволяя повысить в целом защищенность передаваемой информации. Такой подход ино­гда называют схемой *электронного цифрового конверта.*

Пусть пользователь А хочет применить комбинированный метод шифрования для защищенной передачи сообщения М пользователю В.

Тогда последовательность действий пользователей А и В будет следующей.

Действия пользователя А:

1. Создает (например, генерирует случайным образом) симметричный сеансо­вый секретный ключ Ks.

2. Шифрует сообщение М на симметричном сеансовом секретном ключе Ks.

3. Шифрует секретный сеансовый ключ Ks на открытом ключе Кв пользовате­ля В (получателя сообщения).

4. Передает по открытому каналу связи в адрес пользователя В зашифрован­ное сообщение М вместе с зашифрованным сеансовым ключом Ks.

Действия пользователя А иллюстрируются схемой шифрования сообщения комбинированным методом (рис. 3.9).



*Рис. 3.9. Схема шифрования сообщения комбинированным методом*

Действия пользователя В (при получении электронного цифрового конвер­та - зашифрованного сообщения М и зашифрованного сеансового ключа Ks):

5. Расшифровывает на своем секретном ключе kв сеансовый ключ Ks.

6. С помощью полученного сеансового ключа Ks расшифровывает принятое сообщение М.

Действия пользователя В иллюстрируются схемой расшифрования сообщения комбинированным методом (рис. 3.10).



*Рис.**3.10. Схема расшифрования сообщения комбинированным методом*

Полученный электронный цифровой конверт может раскрыть только законный получатель - пользователь В. Только пользователь В, владеющий личным секрет­ным ключом кв, сможет правильно расшифровать секретный сеансовый ключ Ks и затем с помощью этого ключа расшифровать и прочитать полученное сообще­ние М.

При методе цифрового конверта недостатки симметричного и асимметричного криптоалгоритмов компенсируются следующим образом:

* проблема распространения ключей симметричного криптоалгоритма устра­няется тем, что сеансовый ключ Ks, на котором шифруются собственно со­общения, передается по открытым каналам связи в зашифрованном виде; для зашифрования ключа Ks используется асимметричный криптоалгоритм;
* проблемы медленной скорости асимметричного шифрования в данном слу­чае практически не возникает, поскольку асимметричным криптоалгорит­мом шифруется только короткий ключ Ks, а все данные шифруются быст­рым симметричным криптоалгоритмом.

В результате получают быстрое шифрование в сочетании с удобным распреде­лением ключей.

При комбинированном методе шифрования применяются криптографические ключи как симметричных, так и асимметричных криптосистем. Очевидно, выбор длин ключей для криптосистемы каждого типа следует осуществлять таким об­разом, чтобы злоумышленнику было одинаково трудно атаковать любой меха­низм защиты комбинированной криптосистемы.

В табл. 3.1 приведены распространенные длины ключей симметричных и асим­метричных криптосистем, для которых трудность атаки полного перебора при­мерно равна трудности факторизации соответствующих модулей асимметричных криптосистем [95, 157].



Если используется короткий сеансовый ключ (например, 40-битовый DES), то не имеет значения, насколько велики асимметричные ключи. Хакеры будут ата­ковать не их, а сеансовые ключи.

**Метод распределения ключей Диффи-Хеллмана**

*Метод открытого распределения ключей,* изобретенный У. Диффи и М. Хеллманом, позволяет пользователям обмениваться ключами по незащищенным каналам | связи. Его безопасность обусловлена трудностью вычисления дискретных лога­рифмов в конечном поле, в отличие от легкости решения прямой задачи дискрет­ного возведения в степень в том же конечном поле. Суть метода Диффи-Хеллмана заключается в следующем (рис. 3.11).



Пользователи А и В, участвующие в обмене информации, генерируют независи­мо друг от друга свои случайные секретные ключи kА и kв (ключи kА и kв - случай­ные большие целые числа, которые хранятся пользователями А и В в секрете).

Затем пользователь А вычисляет на основании своего секретного ключа kА от­крытый ключ:

KA=gkA(mod N).

Одновременно "пользователь В вычисляет на основании своего секретного клю­ча kв открытый ключ:

KB=gkB(mod N).

Здесь N и g - большие целые простые числа. Арифметические действия вы­полняются с приведением по модулю N [95]. Числа N и g могут не храниться в секрете. Как правило, эти значения являются общими для всех пользователей сети или системы.

Затем пользователи А и В обмениваются своими открытыми ключами КА и Кв по незащищенному каналу и используют их для вычисления общего сессионного ключа К (разделяемого секрета):

пользователь А: К = (Кв )kA (mod N) = (gkB ) kA (mod N),

пользователь B: K' = (KA)kB(mod N) = (gkA )кв (mod N),

при этом К = К', так как (gkB)kA =(gkA)kB(mod N).

Таким образом, результатом этих действий оказывается общий сессионный ключ, который является функцией обоих секретных ключей kА и kв.

Злоумышленник, перехвативший значения открытых ключей КА и Кв, не может вычислить сессионный ключ К, потому что он не имеет соответствую­щих значений секретных ключей kА и kв. Благодаря использованию однонап­равленной функции операция вычисления открытого ключа необратима, то есть невозможно по значению открытого ключа абонента вычислить его сек­ретный ключ.

Уникальность метода Диффи-Хеллмана заключается в том, что пара абонен­тов имеет возможность получить известное только им секретное число, передавая по открытой сети открытые ключи. После этого абоненты могут приступить к защите передаваемой информации уже известным проверенным способом -применяя симметричное шифрование с использованием полученного разделяемо­го секрета.

Схема Диффи-Хеллмана дает возможность шифровать данные при каждом сеансе связи на новых ключах. Это позволяет не хранить секреты на дискетах или других носителях. Не следует забывать, что подобное хранение секретов повыша­ет вероятность попадания их в руки конкурентов или злоумышленников.

Схема Диффи-Хеллмана позволяет также реализовать *метод комплексной за­щиты конфиденциальности и аутентичности передаваемых данных.* Алгоритм предоставляет пользователю возможность сформировать и использовать одни и те же ключи для выполнения цифровой подписи и симметричного шифрования передаваемых данных.

Для одновременной защиты целостности и конфиденциальности данных целе­сообразно применять шифрование и электронную цифровую подпись в комплек­се. Промежуточные результаты работы схемы Диффи-Хеллмана могут быть ис­пользованы в качестве исходных данных для реализации метода комплексной защиты целостности и конфиденциальности передаваемых данных [53]. Действи­тельно, согласно данному алгоритму пользователи А и В сначала генерируют свои секретные ключи kА и kв и вычисляют свои открытые ключи КА и Кв. Затем або­ненты А и В используют эти промежуточные результаты для одновременного вычисления общего разделяемого секретного ключа К, который может использо­ваться для симметричного шифрования данных.

Метод комплексной защиты конфиденциальности и аутентичности передавае­мых данных работает по следующей схеме:

* абонент А подписывает сообщение М с помощью своего секретного ключа kА, используя стандартный алгоритм цифровой подписи;
* абонент А вычисляет совместно разделяемый секретный ключ К по алгорит­му Диффи-Хеллмана из своего секретного ключа kА и открытого ключа Кв абонента В;
* абонент А зашифровывает сообщение М на полученном совместно разделя­емом секретном ключе К, используя согласованный с партнером по обмену алгоритм симметричного шифрования;
* абонент В при получении зашифрованного сообщения М вычисляет по ал­горитму Диффи-Хеллмана совместно разделяемый секретный ключ К из своего секретного ключа kв и открытого ключа КА абонента А;
* абонент В расшифровывает полученное сообщение М на ключе К;
* абонент В проверяет подпись расшифрованного сообщения М с помощью открытого ключа абонента КА.

На основе схемы Диффи-Хеллмана функционируют протоколы управления криптоключами SKIP (Simple Key management for Internet Protocols) и IKE (Internet Key Exchange), применяемые при построении защищенных виртуаль­ных сетей VPN на сетевом уровне.

**Протокол вычисления ключа парной связи ЕСКЕР**

В *протоколе вычисления ключа эллиптической кривой ЕСКЕР* (Elliptic Curve Key Establishment Protocol) определение параметров системы и генерация ключей аналогичны алгоритму асимметричного шифрования ECES.

Предположим, что общий ключ вычисляется пользователями А и В.

Пользователь А имеет секретный ключ а и открытый ключ QA = аР = (хА, уА). Аналогично пользователь В имеет секретный ключ b и открытый ключ QB = bР = = (хB, уB).

Вычисление ключа парной связи проводится в четыре этапа:

*Этап 1.* Действия пользователя А:

* выбирается случайное целое число kА, 1  kА  n - 1;
* вычисляется точка RA = kAP;
* вычисляется точка (х1, у1)= kAQB;
* вычисляется sA = kA + ахАх1 mod n;
* RA отправляется пользователю В.

*Этап 2.* Действия пользователя В:

* выбирается случайное целое число kв, 1  kв  n - 1;
* вычисляется точка RB = kBP;
* вычисляется точка (х2, у2) = kвQА;
* вычисляется sB = kв + bxBx2 mod n;
* RB отправляется пользователю А.

*Этап 3.* Действия пользователя А:

* вычисляется (х2, у2) = aRB;
* вычисляется ключ парной связи К = sA(RB + xBx2QB).

*Этап 4.* Действия пользователя В:

* вычисляется (х1, у1) = bRA;
* вычисляется ключ парной связи К = sB(RA + xAx1QA) значению sA(RB + xBx2QB).

Важным достоинствами схемы распределения ключей Диффи-Хеллмана и про­токола вычисления ключа парной связи ЕСКЕР является то, что они позволяют обойтись без защищенного канала для передачи ключей. Однако необходимо иметь гарантию того, что пользователь А получил открытый ключ именно от пользовате­ля В, и наоборот. Эта проблема решается с помощью сертификатов открытых клю­чей, создаваемых и распространяемых центрами сертификации СA (Certification Authority) в рамках инфраструктуры управления открытыми ключами PKI (Public Key Infrastructure).