МЕТОДОЛОГИЯ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В АС

1.Защита от угрозы нарушения конфиденциальности

Защита машинных носителей информации (МНИ).

Особенности:

- последовательный либо прямой метод доступа;
- различные физические принципы реализации;
- различие объемов хранимой информации;
- многообразие вариантов реализации фирмами.

Задача злоумышленника:

1) выбор соответствующего данному носителю привода;

2) запуск соответствующего комплекта программ (операционных средств, драйверов и т.п.);

3) осуществление (организация) считывания в память КС содержимого носителей.

Отсюда тактика защиты. Существуют носители (накопители) со встроенными средствами защиты, требующими специальных паролей.

Парольные системы для защиты от НСД.

Под НСД в руководящих документах понимают доступ к информации, нарушающий установленные правила разграничения доступа и осуществляемый с использованием **штатных** средств. НСД может быть случайным либо преднамеренным.

Категории методов защиты от НСД:

- организационные (мероприятия и регламентирующие инструкции);

- технологические (программно-аппаратные средства идентификации, аутентификации и охранной сигнализации);

- правовые (меры контроля за исполнением нормативных актов).

Идентификация - присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных.

Аутентификация - проверка принадлежности пользователю предъявленного им идентификатора.

Безопасность (стойкость) системы идентификации и аутентификации это степень обеспечиваемых ею гарантий того, что злоумышленник не способен пройти аутентификацию от имени другого пользователя.

Методы **аутентификации** основаны на наличии у каждого пользователя:

- индивидуального объекта заданного типа (пропуск, магнитная карта и т.п.);
- знаний некоторой информации (пароля), известного только ему и проверяющей стороне;
- индивидуальных биометрических характеристик (тембра голоса, рисунка папилярных линий, структуры радужной оболочки глаза и т.п.).

Если в процедуре аутентификации участвуют только две стороны, то это **непосредственная аутентификация** (direct password authentication).

Если в этой процедуре участвует третья *доверенная* сторона, то ее называют **сервером аутентификации,** а метод называют с *участием доверенной стороны* (trusted third party authentication).

Общие подходы к построению парольных систем.

Наиболее распространенные методы аутентификации основаны на применении многоразовых и одноразовых паролей. Из-за своего широкого распространения и простоты реализации парольные системы часто становятся мишенью атак злоумышленников. Эти методы включают следующие разновидности способов аутентификации:

- по хранимой копии пароля или его свёртке **(plaintext- equivalent)**;
- по некоторому проверочному значению **(verifier-based) ;**

- Без непосредственной передачи информации о пароле проверяющей стороне (zero-knowledge);
- С использованием пароля для получения криптографического ключа (cryptographic).

Для более детального рассмотрения принципов построения парольных систем сформулируем несколько основных определений.

Идентификатор пользователя – некоторое уникальное количество информации позволяющее различать индивидуальных пользователей парольной системы(проводить их идентификацию). Часто идентификаторы также наз. именем пользователя или именем учетной записи пользователя .

Пароль пользователя – некоторое секретное кол-во информации известное только пользователю и парольной системе, которое может быть запомнена пользователем и предъявлена для прохождения процедуры

аутентификации. Одноразовый пароль дает возможность пользователю однократно пройти аутентификацию. Многоразовый пароль может быть использован для проверки подлинности повторно.

Учетная запись пользователя – совокупность его идентификатора и его пароля.

База данных пользователей парольной системы содержит учетные записи всех пользователей данной парольной системы.

Под парольной системой будем понимать программно-аппаратный комплекс реализующий системы идентификации и аутентификации пользователей АС на основе одноразовых или многоразовых паролей. Как правило такой комплекс функционирует совместно с подсистемами разграничения доступа и регистрации событий. В отдельных случаях парольная система может выполнять ряд дополнительных функций, в частности генерацию и распределение кратковременных (сеансов) криптографических ключей.

Основными компонентами парольной системы являются:

- интерфейс пользователя;
- интерфейс администратора;
- модуль сопряжения с другими подсистемами безопасности;
- база данных учетных записей.

Парольная система представляет собой “передний край обороны” всей системы безопасности. Некоторые ее элементы(в частности реализующие интерфейс пользователя) могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику.

Поэтому парольная система становиться одним из первых объектов атаки при вторжении злоумышленника в защищенную систему.

Перечислим типы угроз безопасности парольных систем.

1.Разглашение параметров учетной записи через :

- Подбор в интерактивном режиме
- Подсматривание
- Преднамеренную передачу пароля ее владельцем другому лицу
- Захват базы данных парольной системы с дальнейшей дешифрацией

- Перехват переданной по сети информации о пароле
- Хранение пароля в доступном месте

2. Вмешательство в функционирование компонентов парольной системы через

- Внедрение программных закладок
- Обнаружение и использование ошибок, допущенных на стадии разработки
- Выведение из строя парольной системы

Некоторые из перечисленных типов угроз связанны с наличием так называемого человеческого фактора, проявляющегося в том, что пользователь может:

- Выбрать пароль, который легко запомнить и также легко подобрать
- Записать пароль который сложно запомнить и положить запись в доступном месте
- Ввести пароль так что его смогут увидеть посторонние
- Передать пароль другому лицу намеренно или под влиянием заблуждения

Выбор паролей

Для уменьшения влияния человеческого фактора при выборе и использовании паролей необходимо выполнить ряд требований:

- установить оптимальную длину пароля;
- использовать в паролях различных групп символов;
- проверка и отбраковка паролей по словарю;
- установить максимальный и минимальный срок действия пароля;
- ведение журнала истории паролей
- применять алгоритмы, бракующие пароли на основании данных журнала историй;

- ограничение числа попыток ввода пароля;
- поддержка режима принудительной смены пароля пользователя;
- использование вопросо-ответного диалога при вводе неправильного пароля (для замедления цикла подбора);
- запрет на выбор пароля самим пользователем и автоматическая генерация паролей;
- принудительная смена пароля при первой регистрации пользователя в системе (для защиты от неправомерных действий системного администратора, имеющего доступ к паролю в момент создания учетной записи).

Оценка стойкости парольных систем осуществляется по формуле:

1) P = V*T/S, где $S=A^L$

Здесь A - мощность алфавита паролей;

L - длина пароля;

S - мощность пространства паролей;

V - скорость подбора паролей;

T - срок действия пароля;

P - вероятность подбора пароля в течение его срока действия.

ПРИМЕР:

Пусть задано P = 0.000001. Найти минимальную длину пароля, обеспечивающую его стойкость в течение одной недели непрерывных попыток подобрать пароль. Пусть скорость интерактивного подбора паролей V = 10паролей/мин. Тогда в течение недели можно подобрать:

10*60*24*7=100800 паролей.

Тогда из формулы 1 имеем:

S = 100800/0.000001 = 1.008*E+11

Полученному значению S соответствуют пары:

A = 26, L = 8 и A = 36, L = 6.

Хранение паролей

Важным аспектом стойкости парольной системы, является способ хранения паролей в базе данных учетных записей. Варианты хранения паролей:

1) в открытом виде;

2) в виде сверток (хеширование);

3) зашифрованными в некотором ключе.

Особенности второго и третьего вариантов.

Хеширование не обеспечивает защиту от подбора паролей по словарю в случае получения базы данных злоумышленником.

При выборе алгоритма хеширования необходимо: - гарантировать несовпадение значений сверток, полученных на основе различных паролей пользователей;

- предусмотреть механизм, обеспечивающий уникальность сверток в том случае, если два пользователя выбирают одинаковые пароли, предусмотрев некоторое количество “случайной” информации.

Варианты шифрования базы данных учетных записей:

1) ключ генерируется программно и хранится в системе, обеспечивая возможность ее автоматической перезагрузки;

2) ключ генерируется программно и хранится на внешнем носителе с которого считывается при каждом запуске;

3) ключ генерируется на основе выбранного администратором пароля, который вводится в систему при каждом запуске.

Наиболее безопасное хранение паролей обеспечивается при комбинации второго и третьего способов.

Стойкость парольной системы определяет ее способность противостоять атаке противника, а также зависит от криптографических свойств алгоритма шифрования или хеширования.

Передача пароля по сети.

Если передаваемая по сети в процессе аутентификации информация не защищена надлежащим образом, возникает угроза ее перехвата и использования для нарушения защиты парольной системы.

Многие компьютерные системы позволяют переключать сетевой адаптер в режим прослушивания адресованного другим получателям сетевого трафика.

Основные виды защиты сетевого трафика:

1) физическая защита сети;

2) оконечное шифрование;

3) шифрование пакетов.

Способы передачи паролей по сети :

1) в открытом виде; (TELNET, FTP и других)

2) зашифрованными;

3) в виде сверток;

4) без непосредственной передачи информации о пароле (“доказательство с нулевым разглашением”).

При передаче паролей в зашифрованном виде или в виде сверток по сети с открытым физическим доступом возможна реализация следующих угроз безопасности парольной системы.

- перехват и повторное использование информации;

- перехват и восстановление паролей;

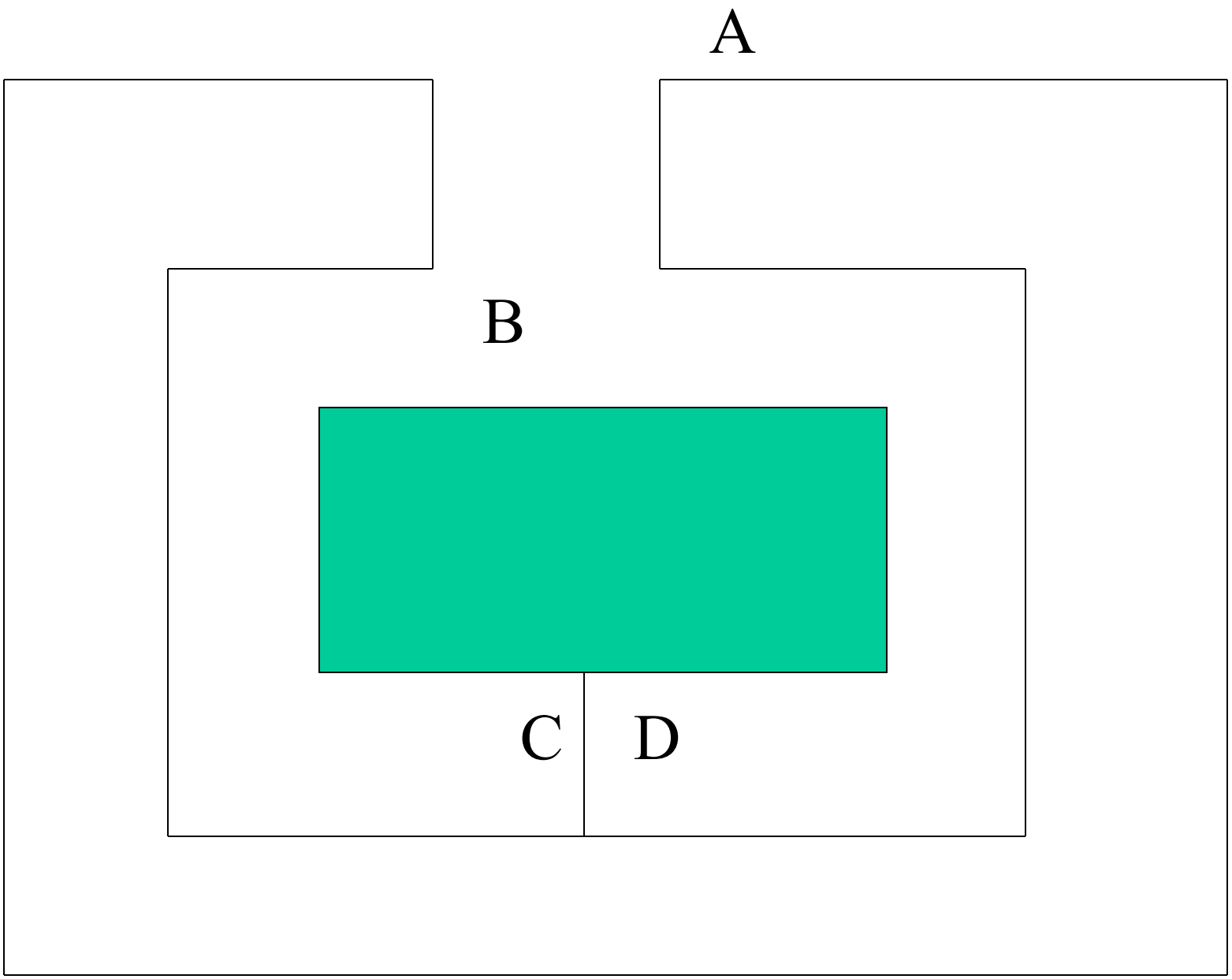
- модификация информации с целью введения в заблуждение проверяющей стороны;

- имитация злоумышленником действий проверяющей стороны для введения в заблуждение пользователя.

Схемы с **нулевым разглашением** впервые появились в на рубеже 80-90-х годов. **Идея**: обеспечить возможность одному из пары субъектов доказать истинность некоторого утверждения второму, умалчивая при этом о содержании самого утверждения.

Общая схема процедуры **аутентификации с нулевым разглашением** состоит из последовательности информационных обменов (итераций) между двумя участниками процедуры, по завершению которой проверяющий **с заданной вероятностью** делает правильный вывод об истинности проверяемого утверждения. С увеличением числа итераций возрастает вероятность правильного распознавания истинности (или ложности) утверждения.

Классическим примером неформального описания системы аутентификации с нулевым разглашением служит так называемая пещера АЛИ-БАБЫ.


A
B
C
D

Пещера имеет один вход, путь от которого разветвляется в глубине пещеры на два коридора, сходящихся затем в одной точке, где установлена дверь с замком. Каждый, кто имеет ключ от замка, может переходить из од- ного коридора в другой в любом направлении. Одна итерация алгоритма состоит из последо- вательности шагов:

1. Проверяющий становится в точку A.

2. Доказывающий проходит пещеру и добира- ется до двери (оказывается в точке C или D). Проверяющий не видит, в какой из двух кори- доров тот свернул.

3. Проверяющий приходит в точку B и в соответствии со своим выбором просит доказывающего выйти из определенного коридора.

4.Доказывающий, если нужно, открывает дверь ключом и выходит из названного проверяющим коридора.

Итерация повторяется столько раз, сколько требуется для распознания истинности утверждения «доказывающий владеет ключом от двери» с заданной вероятностью. После i-той итерации вероятность того, что проверяющий попросит доказывающего выйти из того же коридора, в который вошел доказывающий, равна $(1\backslash 2)^i$.

Еще один способ повышения стойкости парольных систем в сети - применение одноразовых **(one-time)** паролей. Общий подход к их применению основан на последовательном использовании **хеш-функции** для вычисления **одноразового пароля на основе предыдущего:**

Вначале пользователь получает упорядоченный список одноразовых паролей, последний из которых также сохраняется в системе аутентификации. При каждой регистрации пользователь вводит очередной пароль, а система вычисляет его свойства и сравнивает с хранимым у себя эталоном.

Криптографические методы защиты

К средствам криптографической защиты информации (СКЗИ) относятся аппаратные, программно-аппаратные и программные средства, реализующие криптографические алгоритмы преобразования информации с целью:

- защиты информации при ее обработке, хранении и передаче по транспортной среде АС;

- обеспечения достоверности и целостности информации (в том числе с использованием алгоритмов цифровой подписи) при ее обработке, хранении и передачи по транспортной среде АС;

- выработки информации, используемой для идентификации и аутентификации субъектов, пользователей и устройств;

- выработки информации, используемой для защиты аутентифицирующих элементов защищенной АС при их выработке, хранении, обработке и передаче.

Предполагается, что СКЗИ используется в некоторой АС (или иной информационно-коммуникационной системе или сети связи), совместно с механизмами реализации и гарантированной политики безопасности.

Особенности криптографического преобразования :

- в СКЗИ реализован некоторый алгоритм преобразования информации (шифрование, элек. подп….);

- входные и выходные аргументы криптографического преобразования присутствуют в АС в некоторой материальной форме (объекты АС);

-СКЗИ для работы использует некоторую конфидециальную информацию (ключи);

- алгоритм криптографического преобразования реализован в виде некоторого материального объекта, взаимодействующего с окружающей средой

Т.о, **роль СКЗИ в защищенной АС - преобразование объектов**. В каждом конкретном случае указанное преобразование имеет особенности:

- процедура шифрования использует как входные параметры **объект - открытый текст** и **объект - ключ**, результатом преобразований является **объект - шифрованный текст**;

-процедура расшифровывания использует как входные параметры **шифрованный текст и ключ;**

- процедура простановки цифровой подписи использует как входные параметры **объект - сообщение и объект - секретный ключ подписи**, результатом работы цифровой подписи является **объект - подпись**, как правило, интегрированный в **объект - сообщение**.

Итак, СКЗИ в составе защищенных АС имеет конкретную реализацию - это может быть отдельное специализированное устройство, встраиваемое в компьютер, либо специализированная программа.

Важными являются следующие моменты:

- СКЗИ обменивается информацией с внешней средой: а именно в нее вводятся ключи и открытый текст при шифровании;
- СКЗИ в случае аппаратной реализации использует элементную базу ограниченной надежности (в деталях возможны неисправности);
- СКЗИ в случае программной реализации выполняется на процессоре ограниченной надежности и в программной среде, содержащий посторонние программы, которые могут повлиять на различные этапы его работы;

- СКЗИ хранится на материальном носителе (в случае программной реализации) и может быть при хранении преднамеренно или случайно искажено;

- СКЗИ взаимодействует с внешней средой косвенным образом (питается от электросети, излучает электромагнитные поля и т.д.);

- СКЗИ изготавливает или/и использует человек, могущий допустить ошибки (преднамеренные или случайные) при разработке и эксплуатации.

Способы и особенности реализации криптографических подсистем.

Возможны два подхода к процессу криптографической защиты (в основном к шифрованию) объектов АС:

предварительное и динамическое («прозрачное») шифрование.

Без существенного ограничения общности можно выводы, касающиеся шифрования, распространить и на алгоритмы цифровой подписи.

Предварительное шифрование состоит в зашифровании файла некой программой (субъектом), а затем в расшифровании тем же или иным субъектом (для расшифрования может быть применена та же или другая (специально для расшифрования) программа). Далее расшифрованный массив непосредственно используется прикладной программой пользователя.

Данный подход имеет ряд **недостатков**, хотя и применяется достаточно широко.

Принципиальные недостатки метода предварительного шифрования:

-необходимость дополнительного ресурса для работы с зашифрованным объектом (дискового пространства - в случае расшифрования в файл с другим именем, или времени);

-потенциальная возможность доступа со стороны активных субъектов АС к расшифрованному файлу (во время его существования);

-необходимость задачи гарантированного уничтожения расшифрованного файла после его использования

Динамическое шифрование. Сущность: Происходит зашифрование всего файла (аналогично предварительному шифрованию). Затем с использованием специальных механизмов, обеспечивающих модификацию функций ПО АС, выполняющего обращения к объектам, ведется работа с зашифрованным объектом. При этом расшифрованию подвергается только та часть объекта, которая в текущий момент времени используется прикладной программой.

При записи со стороны прикладной программы происходит зашифрование записываемой части объекта.

Данный подход позволяет максимально экономично использовать вычислительные ресурсы АС, поскольку расшифровывается только та часть объекта, которая непосредственно нужна прикладной программе. Кроме того, на внешних носителях информация всегда хранится в зашифрованном виде, что исключительно ценно с точки зрения невозможности доступа к ней.

Динамическое шифрование целесообразно, таким образом, применять для защиты разделяемых удаленных или распределенных объектов АС.

Динамическое шифрование файлов необходимо рассматривать в контексте защиты группового массива файлов - каталога или логического диска.

При необходимости обращения к удаленным файлам АС на рабочей станции активизируется сетевое программное обеспечение, которое переопределяет функции работы с файловой системой ОС и тем самым с точки зрения

Рабочей станции создает единое файловое пространство рабочей станции и файла-сервера.

Поскольку работа с файлами происходит через функции установленной на рабочей станции ОС, сетевое программное обеспечение модифицирует эти функции так, что обращение к ним со стороны прикладного уровня АС происходит так же, как и обычным образом. Это позволяет обеспечить нормальную работу прикладного и пользовательского уровня программного обеспечения рабочей станции АС.

Функции работы с файлами встраиваются в цепочку обработки файловых операций.

Необходимо заметить, что модули 1-4 физически локализованы в оперативной памяти рабочей станции АС.

1.прикладная программа

2.криптомодуль

3.сетевой клиент рабочей станции

4.локальная ОС

5.транспортный уровень

6.сетевая ОС

Детализируемый перечень обрабатываемых криптомодулем основных функций работы с файлами:

- создание файла;
- открытие файла;
- закрытие файла;
- чтение из открытого файла;
- запись в открытый файл.

Рассмотрим два основных потенциальных злоумышленных действия:

1)обращение к файлу на файл-сервере с

рабочего места, не имеющего ключа расшифрования;

2)перехват информации в канале связи «рабочая станция-сервер».

Первое действие блокируется, поскольку шифрование информации происходит только в оперативной памяти рабочей станции АС и запись- считывание информации с диска файл-сервера или рабочей станции ведется только в шифрованном виде. По той же причине блокируется второе действие -- обмен по транспортной системе «рабочая станция-сервер» проходит на уровнях 3-5, когда

зашифрование уже закончено или расшифрование еще не произведено.

Можно показать, что метод динамического шифрования при условии инвариантности прикладному программному обеспечению рабочей станции является оптимальным (обеспечивает минимальную вероятность доступа к незашифрованной информации) по сравнению с другими методами применения криптографических механизмов.

Проходит на уровнях