4. Лекция: Службы информационной безопасности.
Рассмотрены основные службы безопасности, проблемы конфиденциальности информации, ее целостности и доступности в компьютерных системах.

Службы информационной безопасности являются службами базового уровня, которые используются для противостояния атакам. Каждая из этих служб направлена на борьбу с определенным типом атак (см. табл. 4.1). Службы, о которых мы расскажем в данной лекции, не следует путать с фактическими механизмами безопасности, реализованными в них.

Особенности использования служб информационной безопасности в рамках отдельной организации зависят от уровня оценки риска в этой организации и планирования системы безопасности. Знание базовых требований к безопасности позволяет грамотно использовать соответствующие службы для противостояния атакам.

Таблица 4.1. Службы информационной безопасности и типы атак

Атаки	**Службы безопасности**			
	Конфиденциальность	Целостность	Доступность	Идентифицируемость
Доступа	X			X
Модификации		X		X
Отказ в обслуживании			X	
Отказ от обязательств		X		X

Конфиденциальность

Служба конфиденциальности обеспечивает секретность информации. Правильно сконфигурированная, эта служба открывает доступ к информации только аутентифицированным пользователям. Ее надежная работа зависит от службы обеспечения идентификации и однозначного определения подлинности лиц. Выполняя эту функцию, служба конфиденциальности ограждает системы от атак доступа. Служба конфиденциальности должна учитывать различные способы представления информации - в виде распечаток, файлов или пакетов, передающихся по сетям.

Примечание

В процессе обсуждения вы часто будете сталкиваться с рекомендациями по должному определению подлинности лиц. Как ничто другое, это служит иллюстрацией того, что все системы безопасности находятся в тесной взаимосвязи друг с другом. Ни одна из служб не может работать автономно.

Поэтому при реализации готовых программных продуктов возможно возникновение сбоев в работе систем информационной безопасности.

Обеспечение конфиденциальности файлов

Существуют различные способы обеспечения секретности документов в зависимости от их вида. Бумажные документы нужно защищать физически, т. е. хранить в отдельном месте, доступ к которому контролируется службой конфиденциальности. Не следует забывать о таких вещах, как запирание картотек и ящиков столов, ограничение доступа в кабинеты внутри офиса или в сам офис.

В работе с электронными документами имеются свои тонкости. Во-первых, файлы могут храниться одновременно в нескольких местах: на внешних запоминающих устройствах большой емкости (жестких дисках или магнитных лентах), на гибких дисках, zip-дисках или компакт-дисках. Во вторых, физический доступ к месту хранения файлов не обязателен. Сохранение конфиденциальности магнитных лент и дисков аналогично защите бумажных документов и связано с ограничением физического доступа. Контроль над файлами в компьютерных системах осуществляют системы управления доступом (это может быть шифрование файла). Работа этих систем зависит от надежной идентификации и аутентификации пользователя и правильной конфигурации, исключающей обход защитных механизмов через уязвимые места системы. В табл. 4.2 показаны механизмы обеспечения конфиденциальности файлов и требования к ним.

Таблица 4.2. Механизмы обеспечения конфиденциальности файлов и требования к ним

Механизмы обеспечения конфиденциальности	Контроль физической безопасности.
	Контроль доступа к файлам на компьютере.
	Шифрование файлов.
Требования к конфиденциальности файлов	Идентификация и аутентификация.
	Правильная настройка компьютерной системы.
	Правильное управление ключами при использовании шифрования.

Обеспечение конфиденциальности при передаче данных по сети

Недостаточно защитить только ту информацию, которая хранится в виде файлов, ведь злоумышленники могут перехватить ее в процессе передачи по сетевому соединению. Следовательно, требуется обеспечить конфиденциальность информации, передаваемой по каналам связи (см. рис. 4.1). Это делается с помощью технологий шифрования.

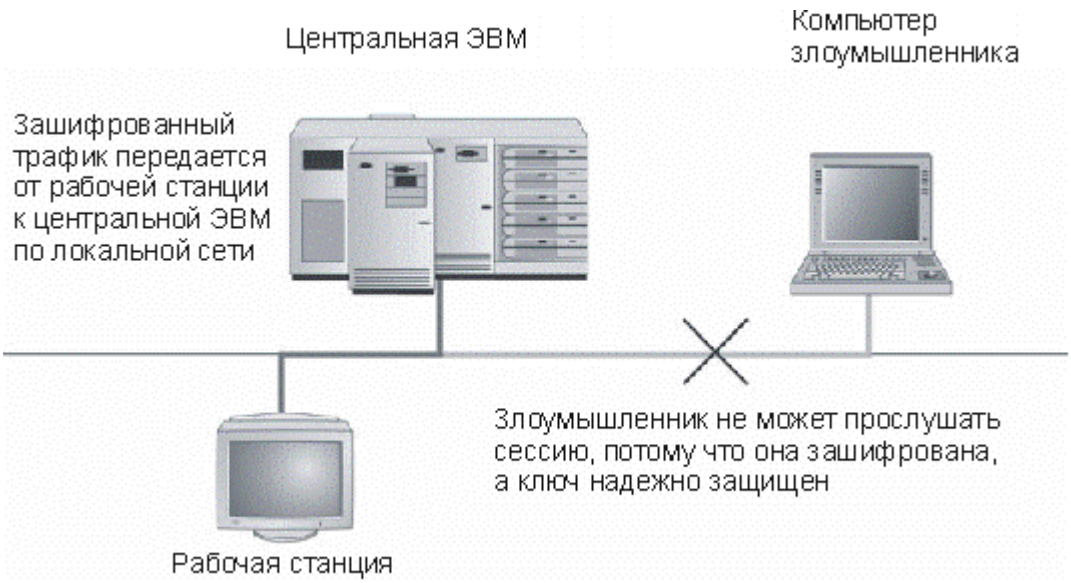

Рис. 4.1. Шифрование обеспечивает защиту информации при передаче по сетям

Механизмы защиты можно применить как для отдельного сообщения, так и для всего трафика соединения. Шифрование позволит предотвратить атаки подслушивания, но не сможет защитить от перехвата информации. В последнем случае требуется надежная система идентификации и аутентификации для определения подлинности удаленного получателя (см. рис. 4.2).

Рис. 4.2. Шифрование в сочетании с надежной идентификацией позволяет предотвратить перехват трафика

Конфиденциальность потока данных

Служба обеспечения конфиденциальности потока данных весьма обеспокоена самим фактом передачи информации между двумя конечными

пунктами (см. рис. 4.3). Конфиденциальность потока данных не касается сохранности передаваемой информации. Наличие потока данных позволяет анализатору трафика выявить организации, между которыми установлена связь. Количество трафика, передающегося от узла к узлу, также представляет собой ценную информацию. Например, многие службы новостей наблюдают за поставками пиццы в Белый дом и Пентагон. Главная идея состоит в том, что увеличение количества пицц указывает на возникновение какой-то неординарной ситуации. Для описания такого типа деятельности существует специальный термин - анализ движения и событий (traffic and pattern analysis).

Конфиденциальность потока данных обеспечивается за счет скрытия информации, передаваемой между двумя конечными пунктами, внутри гораздо большего трафика данных. В Вооруженных Силах используется такой прием: две воинских части сначала устанавливают связь, а затем передают постоянный объем данных, независимо от числа фактически отправляемых сообщений (свободное место заполняется информационным "мусором"). Таким образом, количество трафика остается постоянным, и какие-то изменения в интенсивности передачи сообщений обнаружить нельзя.

Рис. 4.3. Анализ потоков информации позволяет выявить совместно работающие организации

Примечание

Большинство коммерческих организаций не задумывается о конфиденциальности потока данных. Однако в некоторых случаях сам факт установки соединения является секретной информацией. Предположим, происходит слияние двух компаний. В этом случае возникновение между

ними новых информационных потоков является секретной информацией до тех пор, пока не будет объявлено об этом событии.

Предотвращение атак

Служба обеспечения конфиденциальности позволяет предотвратить атаки доступа. Впрочем, сама по себе она полностью не решает эту проблему. Эта служба должна работать совместно со службой идентификации для определения подлинности лиц, предпринимающих попытки доступа к информации. В этом случае значительно уменьшается риск получения злоумышленником несанкционированного доступа.

Вопрос к эксперту

Вопрос. Уточните, как использовать службы безопасности для защиты моей системы?

Ответ. Службы безопасности, которые мы обсудили в этой лекции, представляют собой базовый блок в концепции построения защиты. Фактическая же ее реализация зависит от множества различных механизмов, которые мы рассмотрим далее. Пока удовлетворитесь этим ответом, поскольку понимание того, как эти службы помогают защитить вашу информацию, позволит выбрать нужные средства для использования в вашем окружении.

Целостность

Служба обеспечения целостности следит за правильностью информации. При должном уровне организации эта служба дает пользователям уверенность в том, что информация является верной, и ее не изменил никто из посторонних. Подобно службе конфиденциальности, служба обеспечения целостности должна работать совместно со службой идентификации, чтобы осуществлять надежную проверку подлинности. Данная служба является "щитом" от атак модификации. Информация, которую она защищает, может быть представлена в виде бумажных распечаток, в виде файлов либо в виде данных, передаваемых по сети.

Целостность файлов

Как уже говорилось выше, информация может быть представлена в виде бумажных распечаток или в виде файлов. Конечно, легче обеспечить защиту бумажных документов, да и установить факт изменения содержимого такого документа гораздо проще. Ведь злоумышленнику требуется определенный навык, чтобы поддельный документ выглядел достоверно. А компьютерный файл может изменить любой, кто имеет к нему доступ. Существует несколько способов защиты бумажных документов от подделки. Можно

ставить подпись на каждой странице, сшивать документы в папки, изготавливать несколько копий документа. Механизмы обеспечения целостности затрудняют подделку документов. Хотя злоумышленники научились копировать подписи, сделать это все же непросто, требуется серьезный навык. Достаточно сложно добавить или удалить документ из общей подшивки. А если копии документов разосланы всем заинтересованным сторонам, то подменить сразу все документы практически невозможно.

Ну и конечно, основной способ предотвращения подделки документов - полное исключение неправомочного доступа. Для этого используются те же самые механизмы, что и для обеспечения конфиденциальности - физические меры безопасности.

Чтобы изменить электронный файл, злоумышленнику всего-навсего нужно открыть документ в текстовом редакторе и впечатать соответствующую информацию. При сохранении новый файл запишется поверх старого. Основным способом защиты целостности в этом случае является контроль над доступом к файлам на компьютере. С помощью механизма управления доступом можно установить для файла разрешение "только для чтения" и запретить запись изменений. В этом случае важно правильно идентифицировать пользователя, который хочет внести изменения. Тут поможет служба установления подлинности. Контроль доступа к файлам на компьютере надежно работает, если файлы хранятся в отдельной компьютерной системе или сети, контролируемой организацией. А если файл нужно скопировать в другие подразделения? В этом случае на помощь приходит другой механизм для выявления неправомочного изменения файла - цифровая подпись. Цифровая подпись файла позволяет определить, что файл изменился с момента создания подписи. Цифровая подпись должна быть сопоставлена с конкретным пользователем; таким образом, служба обеспечения целостности должна включать в себя также функции идентификации и аутентификации.

Обеспечение целостности информации при передаче

Данные можно изменить в процессе их передачи по сетевым соединениям, но для этого должна быть выполнена атаки перехвата. При наличии механизмов сильной идентификации и аутентификации атакам перехвата можно противостоять (см. рис. 4.2), а технологии шифрования позволяют предотвратить большинство типов атак на модификацию.

Предотвращение атак

Служба обеспечения целостности позволяет предотвращать атаки на модификацию и атаки на отказ от обязательств. При должном уровне ее организации любое неправомочное изменение будет немедленно

обнаружено. Взаимодействие со службой идентификации и аутентификации позволит противостоять атакам, направленным на организацию извне. А цифровая подпись позволит обнаружить атаки на отказ от обязательств.

Вопросы для самопроверки

1. Для документов, хранящихся в виде бумажных распечаток, самым эффективным методом соблюдения конфиденциальности является _____.
2. Служба обеспечения целостности информации обеспечивает защиту от атак _____.

Доступность

Служба обеспечения доступности информации поддерживает ее готовность к работе, позволяет обращаться к компьютерным системам, хранящимся в этих системах данным и приложениям. Эта служба обеспечивает передачу информации между двумя конечными пунктами или компьютерными системами. В данном случае речь идет в основном об информации, представленной в электронной форме (но подходит и для обычных документов).

Резервные копии

Для сохранения важной информации самым простым способом является создание ее резервных копий и размещение их в безопасном месте. Это могут быть копии на бумаге либо на электронных носителях (например, на магнитных лентах). Резервные копии предотвращают полную потерю информации при случайном или преднамеренном уничтожении файлов.

Внимание!

Даже наличие резервных копий не гарантирует стопроцентную сохранность информации. Вы можете обнаружить, что случайно уничтожена магнитная лента с важным файлом. Важно вовремя отслеживать создание резервных копий ценных файлов.

Безопасным местом для хранения резервных копий являются сейфы или изолированные помещения, в которые ограничен физический доступ лиц. Резервные копии действительно помогают восстановить важную информацию, но не всегда позволяют делать это быстро. Ведь резервные копии нужно сначала забрать из специального хранилища, доставить в нужное место, а затем загрузить в систему. Кроме того, потребуется какое-то время для восстановления каждого приложения или всей системы.

Переключение по отказу

Переключение по отказу (fail-over) обеспечивает восстановление информации и сохранение производительности. Системы, настроенные подобным образом, способны обнаруживать неисправности и восстанавливать рабочее состояние (выполнение процессов, доступ к информации или соединениям) автоматически с помощью резервных аппаратных средств.

Переключение по отказу еще называется прямым восстановлением, поскольку не требует настройки. Резервная система располагается на том же рабочем месте, что и основная, чтобы незамедлительно включиться в работу при возникновении сбоя в исходной системе. Это наименее дорогостоящий вариант для большинства систем переключения по отказу.

Примечание

Механизмы обеспечения доступности являются самыми дорогими средствами безопасности в организации. Чтобы определить состав необходимых аппаратных средств, важно учесть требования соответствующих процедур управлением риском.

Восстановление в аварийной ситуации

Восстановление в аварийной ситуации защищает системы, информацию и производственные мощности от стихийных бедствий типа пожара и наводнения. Это сложный процесс, позволяющий вернуть организацию в рабочее состояние в то время, когда становится невозможно попасть к основному оборудованию или в помещения.

Предотвращение атак

Механизмы обеспечения доступности используются для восстановления систем после атак на отказ в обслуживании. Надежных и эффективных способов предотвращения атак DoS мало, но данная служба позволит уменьшить последствия атак и вернуть системы и аппаратуру в рабочее состояние.

Идентифицируемость

Про службу идентификации часто забывают, когда речь идет о безопасности. Главная причина в том, что сама по себе эта служба не позволяет предотвратить атаки. Она должна работать совместно с другими службами, чтобы увеличивать их эффективность. Если рассматривать эту службу отдельно, то мы увидим, что она усложняет систему безопасности и повышает ее стоимость. Однако без работы службы идентификации и служба обеспечения целостности, и служба обеспечения конфиденциальности обречены на неудачу.

Идентификация и аутентификация

Идентификация и аутентификация выполняют следующие функции. Во-первых, устанавливают личность индивидуума, во-вторых, доказывают, что индивидуум является именно тем, за кого себя выдает. Аутентификация использует любую комбинацию трех вещей:

- то, что вы знаете (пароль или PIN-код);
- то, что вы имеете (смарт-карта или бейдж);
- то, чем вы являетесь (отпечаток пальца или снимок сетчатки глаза).

Можно выбрать один элемент из этого списка, но лучше использовать их комбинацию, например, пароль и смарт-карту. Это называется двухфакторной аутентификацией. Двухфакторная аутентификация гораздо сильнее, чем однофакторная, поскольку каждый фактор имеет свои слабые места. Например, пароль можно угадать, а смарт-карту украсть. Биометрическую аутентификацию тяжелее фальсифицировать, однако человека могут насильно заставить поместить руку в сканер.

В реальной жизни для аутентификации используется пропуск, предъявляемый охране. Это считается достаточным для того, чтобы служащий мог войти в здание. Для установления подлинности лиц, желающих попасть в секретные охраняемые помещения, используются сканеры геометрии руки. Опознавательный механизм напрямую связан с физическим наличием индивидуума.

В компьютерном мире физические опознавательные механизмы не работают. Здесь для аутентификации пользователя традиционно используется пароль. Подлинность связана с идентификатором пользователя, который назначается администратором системы. Считается, что у администратора есть определенное доказательство, что лицо, получающее идентификатор, на самом деле является тем, за кого себя выдает. Пароли - единственный фактор установления подлинности пользователя и, как следствие, являются "слабым звеном". В отличие от реальной жизни здесь нет никакой гарантии физического присутствия индивидуума. Именно поэтому рекомендуется использование двухфакторной аутентификации, которая обеспечивает более сильный опознавательный механизм.

Идентификация и аутентификация применяются в системе управления доступом к файлам в компьютерных системах, обеспечивающей конфиденциальность и целостность этих файлов. Идентификация и аутентификация очень важна для работы механизмов шифрования и цифровых подписей. В этом случае идентификационные данные передаются удаленному пользователю, который подтверждает свою подлинность на локальном уровне, а затем эти сведения доставляются в нужное место. На рис. 4.4 показан процесс идентификации с помощью цифровой подписи при

отправке сообщения. Пользователь сначала подтверждает свою подлинность, используя механизм защиты подписи на своем локальном компьютере. Затем локальный компьютер отправляет сообщение, подписанное этой цифровой подписью. Пользователь, принимающий сообщение, использует цифровую подпись как доказательство того, что отправитель является автором сообщения.

Механизм идентификации и аутентификации - это ключ к другим службам безопасности. Если он дает сбой, то их надежная работа оказывается под угрозой.

Рис. 4.4. Работа механизма идентификации и аутентификации в соединении удаленного доступа

Аудит

Аудит позволяет фиксировать происходящие события. Записи аудита связывают пользователя с действиями, которые он выполняет в системе. Без надежной службы идентификации и аутентификации аудит становится бесполезным, поскольку нет гарантии, что зафиксированные действия на самом деле выполнены указанным лицом.

Аудит в реальной жизни осуществляется с помощью журналов регистрации, ведомостей пропусков на выход, видеозаписей. Его задачей является отчет о выполненных действиях. Служба целостности должна гарантировать, что информация в журнале аудита не изменялась, иначе ее достоверность ставится под сомнение.

В компьютерных системах аудит ведется с помощью журналов, в которые записываются действия пользователя. Если служба идентификации и аутентификации работает должным образом, то эти события можно

отождествить с определенным пользователем. Электронные журналы аудита тоже необходимо защищать от любых изменений.

Предотвращение атак

Служба идентификации сама по себе не может противостоять атакам, поскольку работает вместе с другими службами. Она ведет запись действий, выполняемых зарегистрированным пользователем и таким образом позволяет восстановить картину событий в случае атаки.

Защитите свою информацию

Сначала освежите в памяти проект 2. В нем были выявлены способы, которые могут использоваться при атаке на вашу систему. В этом проекте вы определите способы защиты информации в своей системе и в организации.

Шаг за шагом

1. Начните со списка атак и стратегий осуществления этих атак, разработанного в проекте
2. Для каждого метода атаки определите наиболее походящую службу безопасности, которая позволить предотвратить или обнаружить эту атаку.
3. Для каждой выявленной службы примите решение о том, требуется ли ей для надежного функционирования служба идентификации. Если это так, то добавьте и эту службу к списку.
4. Расположите список по приоритетам, начиная от самой важной (с вашей точки зрения).
5. Если будут реализованы все службы безопасности, удастся ли вам обнаружить или предотвратить атаки, выявленные в проекте 2?

Выводы

Для защиты секретной информации самой важной является служба конфиденциальности. Однако не забудьте, что для одной информации требуется исключить возможность ее модификации, а для другой - возможность доступа. В обоих случаях нужна надежная служба идентификации и аутентификации. Если имеются системы или информация, от работы которых зависит деятельность организации, то потребуется также служба обеспечения доступности. Для ее работы не нужна служба идентификации и аутентификации.

Контрольные вопросы

1. Перечислите основные службы безопасности.

2. Какая служба полагается на службу конфиденциальности для обеспечения полной защиты информации?
3. Какие службы используются для противостояния атакам на модификацию?
4. В работе каких служб используется система контроля доступа?
5. Должны ли коммерческие организации соблюдать конфиденциальность потока данных?
6. Какой основной механизм обеспечивает конфиденциальность и целостность информации при передаче?
7. Для предотвращения перехвата должно использоваться шифрование - вместе с какой службой безопасности?
8. Может ли служба обеспечения доступности предотвратить атаки на отказ в обслуживании?
9. Назовите три типа аутентификационных факторов.
10. Почему двухфакторная аутентификация сильнее, чем однофакторная?
11. Зачем нужен аудит?
12. Какие службы позволяют предотвратить атаки на отказ от обязательств?
13. Какие службы позволяют предотвратить атаки доступа?
14. На какие три службы безопасности должен опираться аудит?
15. Примером работы какой службы безопасности является развертывание плана аварийного восстановления?