Базовые технологии безопасности операционных систем.

К базовым технологиям безопасности относятся аутентификация, авторизация, аудит и технология защищенного канала. Шифрование - это краеугольный камень всех служб информационной безопасности, будь то система аутентификации или авторизации, средства создания защищенного канала или способ безопасного хранения данных. В современных алгоритмах шифрования предусматривается наличие параметра - секретного ключа. В криптографии принято правило Керкоффа: "Стойкость шифра должна определяться только секретностью ключа". Аутентификация предотвращает доступ к сети нежелательных лиц и разрешает вход легальным пользователям. Термин "аутентификация" в переводе с латинского означает "установление подлинности". Аутентификация - это процедура доказательства пользователем того, что он есть тот, за кого себя выдает. Средства авторизации контролируют доступ легальных пользователей к ресурсам системы, предоставляя каждому из них именно те права, которые ему были определены администратором.

Аудит - фиксация в системном журнале событий, связанных с доступом к защищаемым системным ресурсам. Технология защищенного канала призвана обеспечить безопасную передачу данных по открытой сети. Защищенный канал подразумевает наличие трех основных функций: Взаимную аутентификацию абонентов при установлении соединения Защиту передаваемых по каналу сообщений от несанкционированного доступа Подтверждение целостности поступающих по каналу данных

Технологии шифрования.

Для того чтобы защитить информацию от несанкционированного доступа, применяются технологии шифрования. Однако у пользователей, не обладающих надлежащими знаниями о методах шифрования, может возникнуть ложное ощущение, будто все чувствительные данные надежно защищены. Рассмотрим основные технологии шифрования данных. Пофайловое шифрование. Пользователь сам выбирает файлы, которые следует зашифровать. Такой подход не требует глубокой интеграции средства шифрования в систему, а, следовательно, позволяет производителям криптографических средств реализовать мультиплатформенное решение для Windows, Linux, MAC OS X и т. д. Шифрование каталогов. Пользователь создает папки, все данные в которых шифруются автоматически. В отличие от предыдущего подхода шифрование происходит на лету, а не по требованию пользователя. В целом шифрование каталогов довольно удобно и прозрачно, хотя в его основе лежит все то же пофайловое шифрование. Такой подход требует глубокого взаимодействия с операционной системой, поэтому зависит от используемой платформы. Шифрование виртуальных дисков. Шифрование виртуальных дисков подразумевает создание файла на жестком диске. Этот файл в дальнейшем доступен пользователю как отдельный диск (операционная система «видит» его как новый логический диск). Например, диск X:\. Все сведения, хранящиеся на виртуальном диске, находятся в зашифрованном виде. Главное отличие от предыдущих подходов в том, что криптографическому программному обеспечению не требуется шифровать каждый файл по отдельности. Здесь данные

шифруются автоматически только тогда, когда они записываются на виртуальный диск или считываются с него. Шифрование всего диска. В этом случае шифруется абсолютно все: загрузочный сектор Windows, все системные файлы и любая другая информация на диске. Защита процесса загрузки. Если зашифрован весь диск целиком, то операционная система не сможет запуститься, пока какой-либо механизм не расшифрует файлы загрузки. Поэтому шифрование всего диска обязательно подразумевает и защиту процесса загрузки. Обычно пользователю требуется ввести пароль, чтобы операционная система могла стартовать. Если пользователь введет пароль правильно, программа шифрования получит доступ к ключам шифрования, что позволит читать дальнейшие данные с диска.

Основные средства защиты, встроенные в ОС

Средства защиты, встроенные в ОС, занимают особое место в системе безопасности. Их основной задачей является защита информации, определяющей конфигурацию системы, и затем – пользовательских данных. Такой подход представляется естественным, поскольку возможность изменять конфигурацию делает механизмы защиты бессмысленными.

Проблема защиты информации в компьютерных системах напрямую связана с решением двух главных вопросов:

- обеспечение сохранности информации,
- контроль доступа к информации (обеспечение конфиденциальности).

Эти вопросы тесно взаимосвязаны и не могут решаться в отдельности. Сохранность информации означает защиту ее от разрушения и сохранение структуры хранимых данных. Система контроля доступа к информации должна обеспечивать надежную идентификацию пользователей и блокировать любые попытки несанкционированного чтения и записи данных. В то же время система контроля не должна снижать производительность работы информационных систем и сужать круг решаемых задач.

Системные средства аутентификации пользователей. Первое, что должна проверить операционная система в том случае, если она обладает хотя бы минимальными средствами защиты, – это следует ли ей взаимодействовать с субъектом, который пытается получить доступ к каким-либо информационным ресурсам. Для этого существует список именованных пользователей, в соответствии с которым может быть построена система разграничения доступа.

Под идентификацией понимается определение тождественности пользователя или пользовательского процесса, необходимое для управления доступом. После идентификации обычно производится аутентификация. Под аутентификацией пользователя (субъекта) понимается установление его подлинности. При входе в систему пользователь должен предъявить идентифицирующую информацию, определяющую законность входа и права на доступ. Эта информация проверяется, определяются полномочия пользователя (аутентификация), и пользователю разрешается доступ к различным объектам системы (авторизация). Под авторизацией (санкционированием) подразумевается предоставление разрешения доступа к ресурсу системы.

В данной ситуации существенной оказывается политика управления пользовательскими паролями, определяющая правила их назначения, хранения, изменения и другие связанные с этим вопросы. Чем большие возможности по проведению подобной политики предоставляет администратору операционная система, тем больше шансов на то, что парольная аутентификация будет действенным инструментом защиты.

Пароли с течением времени становятся известными. Это вынуждает периодически проводить их замену. Считается, что в информационных системах с низкими требованиями к обеспечению безопасности пароль должен меняться каждые три месяца, а по мере увеличения значимости вопросов, связанных с несанкционированным доступом, указанный срок сокращается до шести недель.

Не менее важно и минимально допустимое время между двумя последовательными изменениями паролей, поскольку такое изменение – типичное действие в случае получения кем-либо несанкционированного доступа к системе либо ресурсам пользователя.

Одной из распространенных угроз безопасности информационной системы является терминал, оставленный пользователем без присмотра во время работы. В качестве контрмеры можно автоматически блокировать доступ либо прерывать сеанс работы в системе спустя некоторое время после прекращения активности пользователя.

Существуют утилиты, позволяющие проводить закрытие экрана автоматически, однако применять их не рекомендуется, поскольку при этом возникают условия для установки программы, эмулирующей закрытие экрана и считывающей пользовательский пароль.

Особую опасность представляет удаленный вход в систему через телефонную сеть. Поскольку контролировать эту сеть невозможно, то необходима установка дополнительных паролей на последовательные порты.

Разграничение доступа пользователей к ресурсам.

Управление доступом может быть достигнуто при использовании дискреционного или мандатного управления доступом

Дискреционное управление доступом – наиболее общий тип управления доступом. Основной принцип этого вида защиты состоит в том, что индивидуальный пользователь или программа, работающая от имени пользователя, имеет возможность явно определить типы доступа, которые могут осуществить другие пользователи (или программы, выполняемые от их имени) к информации, находящейся в ведении данного пользователя. Дискреционное управление доступом отличается от мандатной защиты тем, что оно реализует решения по управлению доступом, принятые пользователем.

Мандатное управление доступом реализуется на основе результатов сравнения уровня допуска пользователя и степени конфиденциальности информации.

Существуют механизмы управления доступом, поддерживающие степень детализации управления доступом на уровне следующих категорий:

- владелец информации;
- заданная группа пользователей;

- все другие авторизованные пользователи.

Это позволяет владельцу файла (или каталога) иметь права доступа, отличающиеся от прав всех других пользователей и определять особые права доступа для указанной группы людей или всех остальных пользователей.

В общем случае существуют следующие права доступа:

- доступ по чтению;
- доступ по записи;
- дополнительные права доступа (только модификацию или только добавление);
- доступ для выполнения всех операций.

Управление доступом пользователя может осуществляться на уровне каталогов или на уровне файлов. Управление доступом на уровне каталога приводит к тому, что права доступа для всех файлов в каталоге становятся одинаковыми. Например, пользователь, имеющий доступ по чтению к каталогу, может читать (и, возможно, копировать) любой файл в этом каталоге. Права доступа к каталогу могут также обеспечить явный запрет доступа, который предотвращает любой доступ пользователя к файлам в каталоге.

В некоторых ОС можно управлять типами обращений к файлу помимо контроля за тем, кто может иметь доступ к файлу. Реализации могут предоставлять опцию управления доступом, которая позволяет владельцу помечать файл как разделяемый или заблокированный (монопольно используемый).

Разделяемые файлы позволяют осуществлять параллельный доступ к файлу нескольких пользователей одновременно. Блокированный файл будет разрешать доступ к себе только одному пользователю в данный момент. Если файл доступен только для чтения, назначение его разделяемым позволяет группе пользователей параллельно читать его.

Механизмы привилегий позволяют авторизованным пользователям игнорировать ограничения на доступ или, другими словами, легально обходить управление доступом, чтобы выполнить какую-либо функцию, получить доступ к файлу, и т.д. Механизм привилегий должен включать концепцию минимальных привилегий (принцип, согласно которому каждому субъекту в системе предоставляется наиболее ограниченное множество привилегий, необходимых для выполнения задачи).

Принцип минимальных привилегий должен применяться, например, при выполнении функции резервного копирования. Пользователь, который авторизован выполнять функцию резервного копирования, должен иметь доступ по чтению ко всем файлам, что-бы копировать их на резервные носители информации. Однако пользователю нельзя предоставлять доступ по чтению ко всем файлам через механизм управления доступом.

Наличие нескольких путей получения повышенных привилегий является потенциально уязвимым местом в защите операционной системы. Особенно опасно, когда переустановка идентификатора пользователя производится не бинарным файлом, а программой командного интерпретатора, что объясняется легкостью ее модификации.

Указанное обстоятельство заставляет администратора системы контролировать штатные пользовательские командные интерпретаторы. Поскольку большинство пользователей обходится ограниченным набором приложений, в ряде случаев можно зафиксировать круг доступных программ, что особенно актуально при проведении нормативной политики безопасности. Свобода пользователя ограничивается пределами его каталога и возможностью использовать программы только из разрешенных каталогов.

Иногда пользователь вообще не нуждается в непосредственном взаимодействии с операционной системой, работая постоянно с каким-либо приложением, например клиентом базы данных. В этом случае целесообразно использовать возможности разграничения доступа, предоставляемые СУБД.

Средство проверки корректности конфигурации ОС.

Операционная система имеет большое количество настроек и конфигурационных файлов, что позволяет адаптировать ОС для нужд конкретных пользователей информационной системы. Однако это создает опасность появления слабых мест, поэтому для проверки целостности и корректности текущей конфигурации в ОС должна быть предусмотрена специальная утилита.

При запуске утилита сначала проводит верификацию прав доступа к системным файлам, затем проверяет системные файлы и сравнивает их с описанием в мастер-файле, который содержит установки, соответствующие избранному уровню безопасности. В ходе выполнения задачи для системных файлов проверяются владелец и группа, права доступа, размер и контрольная сумма, количество ссылок и время последней модификации.

Результаты выполнения программы записываются в текстовом виде в специальных файлах. Все корректировки, проводимые программой, протоколируются, и систему можно в любой момент вернуть к прежнему состоянию, что страхует администратора от необратимых действий.

Инструмент системного аудита.

Вопросы информационной безопасности не могут успешно решаться, если нет средств контроля за происходящими событиями, поскольку, только имея хронологическую запись всех производимых пользователями действий, можно оперативно выявлять случаи нарушения режима информационной безопасности, определять причины нарушения, а также находить и устранять потенциально слабые места в системе безопасности. Кроме того, наличие аудита в системе играет роль сдерживающего фактора: зная, что действия фиксируются, многие злоумышленники не рискуют совершать заведомо наказуемых действий.

Программные средства, осуществляющие такой контроль, называются средствами аудита. Поскольку в информационной системе предприятия имеется несколько функциональных уровней, на каждом из них желательны средства мониторинга событий. Сегодня наличие механизмов аудита является обязательным требованием к крупным программным продуктам, работающим на любом из уровней.

Аудит невозможен без идентификации и аутентификации пользователей. С этой целью при входе в систему программой аудита пользователю присваивается уникальный идентификатор. Регистрационные действия выполняются

специализированным аудит-демоном, который проводит запись событий в регистрационный журнал в соответствии с текущей конфигурацией. Аудит-демон стартует в процессе загрузки системы.

Каждое событие принадлежит какому-либо классу аудита. Такое деление упрощает анализ большого количества событий. Принадлежность событий к классам и набор классов могут быть сконфигурированы системным администратором.

Существует около двадцати классов отслеживаемых событий. Каждый класс имеет два имени – полное и сокращенное. Для любого класса устанавливается один из трех флагов аудита: аудит в случае успешного выполнения действия, аудит неудачных попыток, безусловный аудит.

Сетевые средства защиты.

Защита информации на сетевом уровне имеет определенную специфику. Если на системном уровне проникнуть в систему можно было лишь в результате раскрытия пользовательского пароля, то в случае распределенной конфигурации становится возможен перехват пользовательских имен и пароля техническими средствами. Например, стандартный сетевой сервис telnet пересылает пользовательское имя и пароль в открытом виде. Это заставляет вновь рассматривать задачу аутентификации пользователей, но уже в распределенном случае, включая и аутентификацию машин-клиентов. Высокая степень защиты достигается путем замены стандартных открытых сервисов на сервисы, шифрующие параметры пользователя/машины-клиента, чтобы даже перехват пакетов не позволял раскрыть эти данные. Наконец, немаловажное значение имеет аудит событий, происходящих в распределенной информационной среде, поскольку в этих условиях злоумышленник не столь заметен и имеет достаточно времени и ресурсов для выполнения своих задач.

Стандартные средства защиты, существующие в ОС, не являются столь же объемлющими, что и на системном уровне. Дело в том, что если на системном уровне однородность гарантирована, и любые изменения могут вводиться достаточно эффективно, то в условиях локальной сети применяется, как правило, набор разнородного оборудования, функционирующего под управлением различных ОС, производители которых априорно не заинтересованы в соответствии средств этих систем концепции безопасности.

Ядро безопасности ОС

Ядро безопасности (ЯБ) ОС– набор программ, управляющих частями системы, ответственными за безопасность. ЯБ реализует политику обеспечения безопасности системы. Данная политика состоит из множества правил надзора и охраны взаимодействий между субъектами (процессы) и объектами (файлы, устройства, ресурсы межпроцессорного взаимодействия).

Действие в ОС подотчетно, если его можно проследить для конкретного пользователя. ЯБ повышает подотчетность путем установления соответствия между всеми входами в систему и реальными пользователями.

Полномочия ядра ассоциируются с процессами. Они позволяют процессу выполнить определенные действия, если процесс обладает необходимой привилегией.

Полномочия подсистем ассоциируются с пользователями. Они позволяют пользователю выполнять определенное действие посредством команд, отнесенных к подсистеме.

Подсистема – набор файлов, устройств и команд, служащих определенной цели. Полномочия ядра заносятся в “множество полномочий”, ассоциированное с каждым процессом. Полномочия устанавливаются по умолчанию, пользователь может их и переустановить.

Когда пользователь входит в защищенную ОС, имеет место ограниченная идентификация и проверка подлинности. Система по входному имени проверяет пароль в базе данных паролей. Если имя найдено, система опознает пользователя путем зашифрованного пароля с содержимым соответствующего поля в базе данных паролей.

ЯБ расширяет стандартный механизм. Существуют определенные правила, ограничивающие допустимые пароли, новые процедуры для генерации и изменения паролей. Расположение и защита определенных частей базы данных паролей изменены. Администратор имеет больший контроль над процессом входа. Этот аспект системы поддерживает отдельный пользователь – администратор опознавания.

Кроме того, ЯБ предоставляет полный “след” действий – журнал учета. Журнал содержит записи о каждой попытке доступа субъекта к субъекту (успешные и неудачные), о каждом изменении субъекта, объекта, характеристик системы. Подсистема учета управляется специальным администратором учета. Администратор учета управляет собранной информацией, которая помогает администратору выяснить, что случилось с системой, когда и кто в этом участвовал.

Одна из важных функций ЯБ – локализация потенциальных проблем, связанных с безопасностью. Ограничительный механизм состоит из:

- парольных ограничений;
- ограничений на использование терминалов;
- входных ограничений.

Администратор опознавания может позволять пользователям самостоятельно вводить пароли или использовать сгенерированные пароли. Пароль может подвергаться проверке на очевидность.

Определяются следующие состояния паролей:

- пароль корректен;
- пароль просрочен (пользователь может войти в систему и изменить пароль, если у него есть на это полномочие);
- пароль закрыт (пользователь заблокирован, необходима помощь администратора).

Пользователи часто не подчиняются принудительной периодической смене паролей, восстанавливая предыдущее значение. Чтобы препятствовать этому, кроме максимального, устанавливается еще и минимальное время действия паролей.

Поддерживается возможность генерировать отчеты о различных аспектах функционирования системы: пароли, терминалы, входы.

Ни одна ОС не является абсолютно безопасной. Возможны следующие пути вторжения:

- некто (кто-то) может узнать пароль другого пользователя или получить доступ к терминалу, с которого в систему вошел другой пользователь;
- пользователь с полномочиями злоупотребляет своими привилегиями;
- хорошо осведомленный пользователь получил неконтролируемый доступ непосредственно к компьютеру.

Опасно предоставлять оборудование для открытого доступа пользователям. Любые средства защиты системы будут бесполезны, если оборудование, носители сохраненных версий и дистрибутивы не защищены.

Подсистема учета ОС регистрирует происходящие в системе события, важные с точки зрения безопасности, в журнале учета, который впоследствии можно анализировать. Учет позволяет анализировать собранную информацию, выявляя способы доступа к объектам и действия конкретных пользователей. Подсистема учета с большой степенью надежности гарантирует, что попытки обойти механизм защиты и контроля полномочий будут учтены.

Сетевые серверы – это ворота, через которые внешний мир получает доступ к информации на компьютере. Поэтому ЯБ должно:

- определить, какую информацию/действие запрашивает клиент;
- решить, имеет ли клиент право на информацию, которую запрашивает сервис;
- передать требуемую информацию/выполнить действие.

Ошибки в сервере и “черные ходы” могут подвергнуть опасности защиту всего компьютера, открывая систему любому пользователю в сети, осведомленному об изъяне. Даже относительно безобидная программа может привести к разрушению всей системы.