БЕЗОПАСНОСТЬ ДОСТУПА: ПОДГОТОВКА К CISSP

***Марков Алексей Сергеевич**, доктор технических наук, старший научный сотрудник., CISSP, SBCI, г. Москва*
***Цирлов Валентин Леонидович**, кандидат технических наук, CISSP, CISM, AMBCI, г. Москва*

Публикация продолжает серию статей для специалистов по информационной безопасности, готовящихся сдать экзамен на получение статуса CISSP (Certified Information Systems Security Professional) [1–7]. Определено понятие управления доступом, категории и типы управления доступом. Рассмотрено свойство подотчетности и связанные с ним подсистемы идентификации, аутентификации, авторизации и аудита. Представлены классификации средств идентификации и аутентификации, методов разграничения доступом, сетевых протоколов аутентификации и авторизации. Даны рекомендации по успешной сдаче экзамена CISSP.

***Ключевые слова**: информационная безопасность, безопасность доступом, подотчетность, идентификация, аутентификация, авторизация, аудит, модель разграничения доступа, протокол аутентификации, технический доступ, биометрия, парольные системы, сертификация специалистов.*

INFORMATION SECURITY ACCESS: BECOMING A CISSP

***Alexey Markov**, Doctor of Science (Comp), CISSP, Moscow*
***Valentin Tsirlov**, Ph.D., CISSP, CISM, AMBCI, Moscow*

This publication continues our series of articles for information security specialists, preparing to take an exam for CISSP (Certified Information Systems Security Professional) certification. The concept of access control, categories and types of access control are defined. The properties of accountability and related subsystem as identification, authentication, authorization and auditing are considered. Classifications of identification and authentication means, access control methods, network authentication protocols are presented. Recommendations for successful completion of the exam CISSP are given.

***Keywords**: information security, security, access, accountability, identification, authentication, authorization, auditing, access control model, authentication protocol, logical access, biometrics, password system, certification of specialists*

1. Введение в управление доступом

В области безопасности информации взаимодействие между компонентами любой системы, в первую очередь, характеризуется понятием доступа (access) субъектов к объектам. Субъектом может выступать пользователь или процесс (задача, транзакция, запущенная программа или сервис), а объектом – логический или физический ресурс системы, такой как: файл, набор данных, программа, сервис, база данных, принтер, время процессора, регистр, канал передачи данных и т.д. Базовой характеристикой доступа является то, что в результате его создается поток информации от объекта к субъекту, путем выполнения операций, таких как: чтение, запись, модификация, поиск и др.

Следует указать, что понятие безопасного доступа в рамках CISSP-курса представлено в самом широком смысле, и не ограничивается только собственно санкционированным разграничением.

1.1. Категории и типы управления доступом

Управление доступом является ключевым механизмом системы менеджмента информационной безопасности. Механизмы управления доступом могут быть классифицированы:

- по уровням реализации механизмов безопасности;
- по целям или функциональным категориям;
- по этапам работы и подсистемам.

По уровням реализации выделяют три категории механизмов безопасности:

1. Административные меры (administrative access controls), включающие политики, планы, процедуры, мероприятия, определенные политикой безопасности (ПБ) организации. С примерами административных мер мы познакомились в предыдущем разделе.

2. Технические (логические) механизмы безопасности (logical/technical access controls) – программные или аппаратные средства, подсистемы и сервисы ИБ. Примерами технических механизмов являются: парольная система, ACL-списки, crc-суммы, системный журнал, межсетевой экран, сканер безопасности, инфраструктура открытых ключей, защищенный протокол, защищенная ОС и др.

3. Средства физической защиты (physical access controls) – физические барьеры, экраны и средства контроля доступом. Примеры: ограждения, вертушки на входе, замки, блокираторы, специальное освещение, средства пожаротушения, системы бесперебойного питания, видеокамеры, охрана.

По целям можно выделить семь категорий управления доступом:

1. Превентивное (preventative access control) – направлено на предотвращение нежелательных или неавторизованных действий. Примерами превентивного управления доступами могут быть: отбор и тренинг персонала, тестирование системы на проникновение и шифрование данных, ограждение и экранирование кабеля.

2. Детективное (detective access control) – направлено на обнаружение нежелательных или неавторизованных действий. Например: проверка на полиграфе и расследование инцидента, аудит системных журналов и применение HIDS-систем, использование розыскных собак и анализ материалов, полученных со скрытых камер.

3. Коррективное (corrective access control) – требуется при возобновлении нормального функционирования системы в случае факта нежелательных или неавторизованных действий. Это может быть: процедуры по оперативному восстановлению системных файлов на случай сбоя, антивирусные средства, шлагбаум.

4. Отпугивающее (deterrent access control) – направленное на предотвращение попыток нежелательных или неавторизованных действий. Примеры: зачет на знание Уголовного кодекса, демонстративные IDS-системы и аудит, вахтерши и муляжи.

5. Восстановительное (recovery access control) – направлено на восстановление и исправление ресурсов в случае нарушений. Примерами являются план восстановления, кластерные и RAID-системы, дублеры.

6. Компенсационное (compensation access control) – дополняет другие категории управления доступом путем применения альтернативных мер и средств. Например, это может быть страхование, введение ограничений на использование продукта, дополнительное резервное копирование, включение записывающих скрытых камер в выходные дни.

7. Директивное (directive access control) – включает указания, директивы, управление действиями субъекта с целью усиления и локализации нарушений ПБ. Пример: сертификация, межсетевой экран, вход по пропускам.

По этапам работы и компонентам, реализующим подсистему управления доступом, выделяют подсистемы идентификации, аутентификации, авторизацию и, иногда, аудита. На этапе идентификации определяются и проверяются идентификаторы субъекта и объекта системы. При аутентификации проверяется достоверность субъекта, действительно ли он тот, за которого себя выдает, например, путем ввода и проверки пароля. Если субъект аутентифицирован и имеет соответствующие права на объект, он будет авторизован, т.е. ему предоставляется доступ к запрошенному им объекту. Аудит подразумевает протоколирование и анализ событий безопасности.

1.2. Свойство подотчетности и подсистемы управления доступом

Кроме базовых свойств системы ИБ (конфиденциальность, целостность и доступность) при описании систем управления доступом выделяют свойство подотчетность (accountability). Подотчетность – свойство, характеризующее то, что все события и действия субъекта в системе идентифицируются, регистрируются и могут быть проверены. Свойство подотчетности в системе реализуется четырьмя механизмами: идентификацией, аутентификацией, авторизацией и аудитом.

Идентификация (identification) - процесс, при котором происходит регистрация и последующая проверка имени (идентификатора) субъекта (активного объекта) системы. Идентификация является базовым элементом любой сложной системы, так как для ее управления все компоненты должны быть поименованы. Примерами идентификаторов могут быть: идентификатор пользователя (username, logon ID, PIN - personal identification number) или устройство идентификации в физи-

ческих системах контроля доступа, таких как магнитная карточка, электронный ключ и др.

Аутентификация (authentication) – процесс проверки подлинности идентифицированного субъекта: действительно ли он тот, за кого себя выдает. При аутентификации субъект должен предоставить дополнительную информацию, которая может подтвердить его подлинность. Наиболее известными примерами систем аутентификации являются парольные системы и системы, основанные на вводе электронного ключа.

Авторизация (authorization) - установление полномочий, а именно: присвоение аутентифицированному субъекту прав и привилегий на доступ к объекту или выполнение определенных действий. В большинстве программных систем установление полномочий осуществляется на базе списков доступа (ACL) или матрицы управления доступом.

Аудит (auditing) – процесс протоколирования в системных журналах событий и действий субъектов. Следует отметить, что аудит в широком смысле подразумевает не просто протоколирование, а и идентификацию и анализ возможных нарушений в системе. Системы, выполняющие анализ системных журналов в реальном времени на предмет нарушений безопасности, называют системами обнаружения вторжений (IDS-системы), основанными на системных журналах (log). На практике, более распространены системы обнаружения вторжений, основанные на мониторинге и анализе трафика. Поэтому часто процесс аудита рассматривают совместно с процессом мониторинга (monitoring).

При изучении данного домена удобно спроецировать названные механизмы на классы средств, протоколов и методов.

2. Средства идентификации и аутентификации

Идентификация и аутентификация являются первым рубежом в процессе управления доступом и, как правило, связаны между собой. Некоторые устройства и механизмы в различных вариантах исполнения системы могут быть как компонентами подсистемы идентификации, так и аутентификации. Поэтому целесообразно рассматривать средства идентификации и аутентификации в едином ключе.

Традиционно указанные средства разделяют по, так называемым, аутентификационным факторам на три типа:

Тип 1. Средства, основанные на знании некоторой закрытой информации (something you know), например: пароля, секретного PIN-кода, комбинации клавиш или фраз.

Тип 2. Средства, основанные на использовании уникального устройства, метода или набора данных (something you have), например: смарт-карты, электронного ключа, магнитной карточки, цифрового сертификата.

Тип 3. Биометрические средства, основанные на физиологических (something you are) или поведенческих (something you do) атрибутах живого организма, например: радужной оболочке глаза или подписи.

В некоторых классификациях можно встретить еще один тип средств, основанных на информации, связанной с местоположением пользователя (somewhere you are). Так как на практике здесь аутентификационным фактором выступает номер телефона (код страны, города, района) или IP-адрес, то часто такие средства аутентификации относят ко 2-му типу (something you have).

Если в системе используются средства, совмещающие различные типы аутентификационных факторов, то говорят о многофакторной аутентификации. Такие системы относят к категории многоуровневой защиты (defense in depth), поэтому они, как считают, обладают большей устойчивостью к компрометации, чем системы, использующие устройства только одного из типов.

2.1. Парольные системы

Традиционными средствами аутентификации являются системы, основанные на секретных идентификаторах – паролях (password).

К сожалению, парольные системы уязвимы по объективным и субъективным причинам.

Во-первых, парольные системы, находятся под пристальным вниманием взломщиков систем. Ведь, подобрав и взломав парольную защиту можно стать санкционированным с точки зрения системы пользователем, еще лучше, привилегированным пользователем. К примеру, более 80% инцидентов в области ИБ связано с взломом именно парольной защиты. Подавляющее большинство компьютерных атак сводятся к получению именно пароля администратора. В Интернете представлено огромное количество методик и программ взлома, подбора и перехвата парольной информации, библиотек с часто используемыми паролями, мастерпаролями (встроенными паролями) и паролями, устанавливаемыми системами по умолчанию. Следует подчеркнуть, что многие системы аутентификации уязвимы по причине некорректной реализации, например в некоторых системах пароль передается или

хранится в открытом виде (пример, по протоколу PAP), а протоколы и средства шифрования парольной информации недостаточно криптостойки.

Во-вторых, сами пароли зачастую можно просто подобрать или угадать. Дело в том, что пароль может быть сгенерирован системой (датчиком случайных чисел) и, следовательно, его трудно запомнить. В таких случаях пользователи зачастую записывают такие псевдослучайные пароли на клочках бумаги, в файлах на компьютере, внешних мобильных устройствах и т.д., что весьма приятно для потенциальных взломщиков.

С другой стороны, легко запоминаемый пароль, как правило, простейший (короткий или примитивный, как: 1, ф1, qwerty, 123, ааа), либо ассоциирован с личной жизнью и окружением конкретного пользователя, а значит, может быть подобран.

Как можно усилить стойкость парольной защиты? Есть несколько путей:

- использование одноразовые паролей вместо постоянных (static) паролей;

- усиления политики безопасности парольной защиты и учетных записей.

Для исключения угрозы использования скомпрометированного пароля используют механизмы динамически меняющихся (dynamic) паролей, которые обеспечивают генерацию и использование нового пароля через какой-то промежуток времени. На практике, в первую очередь в системах централизованной аутентификации, в качестве динамически меняющихся паролей получили распространение одноразовые (one-time, single-use) пароли, действующие на один сеанс работы субъекта. Примерами таких систем является S/KEY (RFC 1938) и OPIE.

Усиление политики безопасности парольной защиты предусматривает соблюдение требований при выборе пароля, затрудняющее, подбор и угадывание пароля, а также требований по его хранению и передачи по сети.

Оригинальными вариантами усиления парольной защиты является использование парольных фраз (pass phrase) и когнитивных (cognitive) паролей. Длинная, но легкая для запоминания парольная фраза представляет собой вид виртуального пароля, преобразованная или хеширования в пароль, сложный для угадывания или подбора. Сравним известную фразу поэта, преобразованную путем замены символов и с помощью алгоритма md5:

- «Молила(ь /\и ты на но4ь, Дездем0на?»;

- 99d87ae239a52edf71e66fb70edccfd6.

Когнитивный пароль представляет собой подмножество ответов на, как правило, случайным образом выбранные, но секретно предопределенные вопросы.

В заключение подраздела следует отметить, что радикальным методом усиления парольной защиты является переход к двухфакторной аутентификации за счет дополнительного использования уникального электронного устройства.

2.2. Электронные устройства

Ко 2-му типу средств идентификации и аутентификации (something you have) относят электронные устройства, содержащие или генерирующие некоторую уникальную информацию о субъекте. Такое устройство должно быть вместе с пользователем. Для усиления стойкости аутентификации можно использовать PIN-код, который дополнительно вводится при инициировании идентификации и аутентификации с помощью устройства.

Указанные устройства классифицируют:

- по типу реализации на пассивные (только с памятью) и активные (включающие еще и микропроцессор, т.е. интеллектуальные);

- по наличию устройства считывания: использующие отдельный считыватель (reader), использующие считыватель, интегрированный с ключом (который, например, подключается к USB-порту) и использующие устройство ввода и оперативную память собственно компьютера;

- по функциональному назначению.

По функциональному назначению выделяют четыре типа устройств:

- статические (static password tokens);

- синхронные динамические (synchronous dynamic password tokens);

- асинхронные динамические (asynchronous dynamic password tokens);

- запрос-ответные (challenge-response tokens).

1. Статические устройства обеспечивают хранение постоянной уникальной информации, которая используется для аутентификации или идентификации субъекта. Простейшим статическим устройством может быть: дискета, флеш-карта, карта с магнитной полосой (как в московском метро), АТМ-карта, содержащей идентификатор, пароль, хэшерованный пароль, закрытый ключ или цифровой сертификат.

К современным статическим устройствам относят:

- смарт-карты (smart card) - карты в формфакторе обычной кредитной карты с встроенным микропроцессором;

- USB-ключи (USB-token) - устройства, комбинирующие ключ со встроенным микропроцессором и считыватель, подключаемый напрямую к USB-порту компьютера,

- электронные таблетки iButton (information button), известные в нашей стране как Touch Memory (например, в домофоне в парадной);

- RFID-радиометки (radio-frequency ID) - бесконтактные радиочастотные идентификаторы.

Остальные типы устройств обеспечивают систему динамически меняющихся или одноразовых паролей.

2. Синхронные устройства генерируют пароль в фиксированные интервалы времени. Системное время на сервере и на токене должно быть синхронизировано.

3. Асинхронные устройства генерируют очередной пароль при наступлении некоторого события, например нажатия клавиши на сервере и токене.

Пароль, генерируемый синхронным или асинхронным устройством, может обеспечивать идентификацию, а вводимый PIN-код или пароль - аутентификацию, либо такие системы, используя имя пользователя, позволяют организовать двухфакторную аутентификацию.

4. Запрос-ответные устройства реализуют одноименный механизм аутентификации. Клиент (ключ) инициирует запрос, в ответ на который сервер, выполняющий функции аутентификации, генерирует некоторый псевдослучайный код или фразу и передает назад на ключ. Электронное устройство на основании полученных данных по встроенному алгоритму вычисляет ответ, который пересылается обратно серверу. Сервер, знающий алгоритм, реализованный в ключе, выполняет аутентификационную операцию проверки правильности ответа от клиента.

Несмотря на возможность построения системы многофакторной аутентификации, электронные устройства имеют ряд недостатков:

- устройство можно нечаянно сломать, а если устройство энергозависимо, то необходимо отслеживать его энергоемкость;

- устройство может быть отобрано, похищено, изъято, утеряно или им просто может кто-то воспользоваться, если вы оставили его без присмотра, скажем, на рабочем месте;

- простейшие устройства могут быть клонированы или эмулированы;

- кроме USB-токенов, большинству устройств требуется дополнительное устройство считывания.

2.3. Билеты

Второй тип идентификации и аутентификации может быть представлен не только электронными устройствами, но и самостоятельным уникальным набором данных, обычно криптографическим. Наиболее известными являются сеансовые билеты или мандаты (tickets), которые выдаются участникам на заданное время взаимодействия во время этапа аутентификации в сети. К системам, реализующим механизм аутентификации с использованием билетов относят Kerberos, которую мы рассмотрим ниже.

2.4. Биометрические системы

К третьему типу средств идентификации и аутентификации относят биометрические устройства, основанные на уникальных физиологических или поведенческих (подсознательных) характеристиках живого организма. Рассмотрим наиболее популярные биометрические методы.

1. ***По отпечаткам пальцев*** (fingerprint). Метод сканирования отпечатков пальцев основан на уникальности папиллярных рисунков пальцев каждого человека. Сканеры пальцев имеют небольшой размер, универсальны, недороги и имеют широкое распространение. Сама технология имеет исторические корни в работах антикриминальных и правительственных структурах многих стран.

2. ***По геометрии ладони*** (palm). Метод основан на форме кисти руки. Эффективность средств сканирования ладони сопоставима со сканерами пальцев.

3. ***По сетчатке глаза*** (retina). Здесь используется луч инфракрасного света, направленный через зрачок к кровеносным сосудам на задней стенке зеницы. Просвеченное таким образом глазное дно сканируется специальной камерой.

4. ***По радужной оболочке*** (iris). Образ пятен на радужной оболочке является одной из самых уникальных характеристик человека. Преимущество метода состоит в том, что видеоизображение глаза может быть отсканировано на расстоянии более метра, что делает возможность интегрирования сканеров с камерами наблюдения.

5. ***По форме лица*** (face). Метод основан на построении многомерного образа лица человека.

6. ***По рукописному почерку*** (signature). Метод основан на графической идентификации подписи или специальной фразы.

7. ***По клавиатурному почерку*** (keystroke). Метод основан на особенностях набора, как правило, заранее определенного текста на клавиатуре.

8. ***По голосу*** (voice). Метод основан на профиле частотных или статических характеристик речи человека. К сожалению, метод зависит от состояния человека (осип, напряжен, легкое недомогание).

В принципе, человеческий организм «не исчерпаем, как атом», и, если верить прессе, то таможенники смотрят на ушные раковины, сотрудники МВД ловят уголовников по запаху, спецслужбы идентифицируют «объект» по повороту ключа в отеле. Один полковник военной разведки даже предложил использовать отпечатки губ в качестве способа идентификации личности. К этому открытию он пришел, просматривая на досуге следы губной помады от поцелуев, оставленные на визитках, которые ему дарили официантки баров в Европе.

Самым надежным из биометрических систем являются сканеры радужной оболочки или сетчатки глаза, затем идут сканеры пальцев, ладони, лица, существенно отстают сканеры подписи или голоса. В настоящее время наибольшей точностью обладают комбинированные устройства, такие как сканер пяти пальцев и системы, использующие одновременно отпечаток пальца и радужную оболочку глаза.

Интересным приложением биометрических устройств является потенциальная возможность использования их в качестве верификаторов личности, т.е. детекторов лжи и полиграфов. Это связано с тем, что внешние атрибуты человека являются, в конце концов, отражением его центральной нервной системы.

Так как работа биометрических устройств носит вероятностный характер, то для оценки их точности используют следующие показатели:

- FAR (false acceptance rate) - частота ложных разрешений на допуск (ошибка II рода);
- FRR (false rejection rate) - частота ложных отказов на допуск (ошибка I рода);
- EER (equal error rate) или CER (crossover error rate) – коэффициент равной вероятности ошибок I и II рода.

Показатели FAR и FRR связаны между собой обратно пропорциональной зависимостью: чем лучше один параметр, тем хуже другой. Некоторые системы позволяют регулировать порог чувствительности. Надо понимать, что увеличение чувствительности (снижение FAR) одновременно сопровождается увеличением вероятности ложного отказа на допуск (FRR), а также времени идентификации (рис.1).

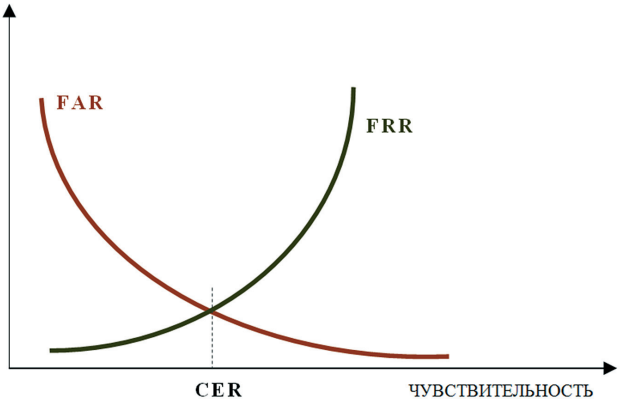

Рис. 1*. Зависимость ошибок 1-го и 2-го рода от настройки устройства*

Аутентификация по биометрическим атрибутам обладает рядом преимуществ по сравнению со средствами аутентификации I и II типа, но у нее есть свои особенности и недостатки:

- сориентирована только на живой организм;
- носит вероятностный характер, необходимо учитывать чувствительность прибора;
- многие средства зависят от окружающей среды и здоровья человека;
- кроме сканеров пальцев, остальные устройства на сегодня достаточно дорогостоящие;
- имеются недоверие у пользователей по поводу угрозы тотального контроля со стороны государства.

3. Протоколы сетевого доступа

В системах распределенной обработки данных для проверки подлинности субъектов сетевого доступа применяются протоколы и сервисы удаленной аутентификации. Клиент выполняет процедуру сетевой аутентификации путем обращения по сетевому протоколу к серверу удаленного доступа, который предоставляет необходимые сетевые сервисы и ресурсы.

3.1. Протоколы удаленного доступа

Простейшим протоколом сетевого доступа является PAP (Password Access Protocol). Согласно протоколу клиент посылает пароль на сервер, на котором хранится пароль для проверки подлинности. Обычно соединение на основе PAP устанавливается, когда клиент и сервер удаленного доступа не могут договориться о более безопасной форме проверки подлинности. Очевидно, что использование данного протокола уязвимо в случае перехвата трафика.

Для исключения данного недостатка применяются протоколы по методу «запрос-ответ», позволяющие выполнить аутентификацию без передачи пароля по сети. Наиболее известным таким протоколом является CHAP[1] (Challenge-Handshake Authentication Protocol). Аутентификация согласно CHAP включает следующие этапы:

- клиент посылает серверу запрос на доступ;
- сервер генерирует *случайное* число и отправляет его назад клиенту;
- клиент шифрует («хэширует») полученное от сервера случайное число и отправляет его назад клиенту (ответ тоже будет *случайным*, так как аргумент функции случайный);
- сервер расшифровывает полученное число и сравнивает его с исходным сгенерированным числом.

Так как парольная информация не передается по сети, то такую схему аутентификации относят к категории усиленной аутентификации. Основной недостаток такой схемы аутентификации является необходимость в установке на каждом компьютере аналогичного модуля шифрования.

3.2. Протокол централизованной аутентификации Kerberos 5

Типовым примером централизованной аутентификации является Kerberos. Этот протокол сетевой аутентификации основан на симметричном алгоритме шифрования и обеспечивает единую одновходовую аутентификацию (а также конфиденциальность и целостность аутентификационного трафика между взаимодействующими компонентами сети) путем использования третьей доверительной стороны.

Основными особенностями системы является следующее:

- каждый абонент имеет долгосрочный секретный ключ, который хранится и на сервере Kerberos, а именно: KDC (key distribution center);
- в случае необходимости взаимодействия абонентов сервер Kerberos создает секретный сеансовый ключ и билет именно для выполнения конкретного обмена между абонентами;
- основным элементом аутентификации являются билеты, содержащие зашифрованный закрытый ключ, характеристику запроса, временной интервал обмена и т.д.

Например, сокращенно алгоритм начальной аутентификации между клиентом и сервером с участием сервера Kerberos выглядит следующим образом:

1) клиент посылает серверу Kerberos запрос, содержащий идентификатор клиента и запрашиваемый сервис сервера;

2) сервер Kerberos посылает обратно клиенту сформированный билет (ticket), зашифрованный секретным ключом сервера, и копию части информации из билета, зашифрованную секретным ключом клиента;

3) клиент расшифровывает вторую часть билета и отсылает ее вместе с билетом серверу.

4) сервер, расшифровав билет, может сравнить его содержимое с дополнительной информацией, присланной клиентом. Совпадение свидетельствует, что клиент и сервер уполномоченные абоненты взаимодействия.

Шифрования билета выполняется по симметричным алгоритмам DES и TripleDES, в версии 5.0 протокола – AES.

К основным недостаткам системы Kerberos относят централизованное хранение секретных ключей в KDC.

Следует заметить, что вместо симметричного шифрования, как это реализовано в системе Kerberos в протоколах аутентификации может применяться асимметричное шифрование и электронная цифровая подпись.

3.3. Сервисы и протоколы централизованного управления доступом

Как показано в предыдущем подразделе, разделяют сервисы централизованного и децентрализованного управления доступом. Среди централизованных систем выделяют так называемые AAA-сервисы (AAA - аутентификация, авторизация, аудит) сеансового уровня, которые могут включать комбинированные и выделенные сервера аутентификации, авторизации и т.д. Наиболее известны два AAA-протокола: RADIUS (Remote Authentication Dial In User Service) и TACACS+ (Terminal Access Controller Access Control System plus) (табл.1). Одно-ранговой версией RADIUS является протокол DIAMETR.

Таблица 1.

AAA-протоколы

Критерии	TACACS+	RADIUS
Транспортный протокол	TCP (надежность)	UDP (производительность)
RFC	RFC 1492	RFC 2865, 2866
Шифрование	Весь пакет	Только пароль
Поддержка мульти-протоколов	IP, IPX, X.25, Apple и др.	IP
Протоколы аутентификации	PAP, CHAP и др.	PAP, CHAP

1 Microsoft-версия стандарта CHAP (MS-CHAP) версии 2 соответствует протоколу NTLM 0.12.

3. Методы управления доступом

В основе подсистемы авторизации лежит формальный метод управления доступом.

На практике встречаются три метода управления доступом:

- дискреционный (discretionary access control, DAC);
- мандатный (mandatory access control, MAC);
- ролевой (role-base access control, RBAC).

3.1. Дискретный метод управления доступом

Дискреционным (или произвольным) методом называют метод управления доступом между поименованными субъектами и поименованными объектами, в котором владелец объекта *сам решает*, кто имеет доступ к объекту, а также их вид доступа. Данный метод управления доступом ориентирован на идентификационную информацию субъекта и ассоциированный с ним ряд операций доступа (чтение, запись и т.д.). Такая политика может быть реализована с помощью:

- списка доступа (access control list, ACL);
- матрицы доступа (access control matrix).

Метод прост и распространен в большинстве систем защиты информации.

Проблема метода в том, что он не обеспечивает контроль передачи прав. Субъект с определенным правом доступа может передать это право любому другому субъекту без уведомления владельца объекта.

3.2. Мандатный метод управления доступом

Мандатный метод основан на иерархической классификации объектов и субъектов системы. Каждому субъекту и объекту системы назначается некоторый иерархический уровень безопасности. Уровень безопасности объекта характеризует ценность объекта (возможный ущерб в случае нарушения конфиденциальности, целостности и доступности). Каждый объект в соответствии с уровнем имеет метку безопасности (security label)[2].

Уровень безопасности субъекта характеризует степень доверия к нему. Каждый субъект имеет допуск к соответствующему уровню. В отличие от дискретного метода в мандатном методе пользователи не могут изменять стратегию доступа в отношении объектов системы. При создании объекта собственно сама операционная система автоматически назначает ему соответствующие атрибуты. В этом смысле метод называют еще принудительным или обязательным. Формально мандатный метод управления доступом описывается моделью Ла-Падули и моделью Биба [6].

Наряду с уровнями безопасности мандатный метод допускает использование смысловых категорий (областей использования), к которым субъекты и объекты относятся. Введение смысловых категорий позволяет реализовать принцип «положено знать только то, что относится к должностным обязанностям» (need-to-know) [2].

Очевидно, что мандатный метод применяется при реализации систем с высшими уровнями доверия, например, обрабатывающих информацию уровня государственной тайны.

3.3. Ролевой метод управления доступом

Ролевой метод ориентирован на роли или функции безопасности системы. Например, в системе вводится активный «ролевой» объект (organization role), выполняющий некоторую дежурную роль и, соответственно, имеющий требуемые права на доступ к заданным объектам системы. В таком случае сопровождение системы безопасности заключается в назначении (в случае надобности) отношения эквивалентности между субъектами системы и ролевым объектом.

Использование ролевого метода упрощает администрирование системы, когда есть дежурные роли, чтобы не переопределять права в случае постоянной смены обязанностей пользователей. На некоторые роли может быть наложена некоторая семантика, например, запрещено совмещать привилегированные роли. Допускается построение иерархических ролей.

В смысле безопасности метод полезен, чтобы исключить абсолютную диктатуру одного администратора системы. Например, роль администратора сети разделяют на две отдельные роли: ответственного за восстановление/копирование системы и ответственного за оперативное функционирование системы. В случае, при каком-нибудь, не дай Бог, эксцессе, поодиночке они не смогут в миг пустить по миру всю фирму. Кроме того, ролевой метод позволяет реализовать принцип наименьших привилегий.

Ролевой метод принципиально отличается от предыдущих тем, что в методе политика безопасности не предопределена и настраивается в процессе изменения ролей пользователей (и определения их прав) по требованиям бизнес-процессов организации. В противоположность этому, в DAC и MAC политика безопасности уже предопределена

2 К примеру, в России для информации, составляющей гостайну, определены метки конфиденциальности в виде грифа секретности: «особой важности», «совершенно секретно», «секретно».

(либо, например, посредством ACL, либо с помощью меток безопасности), ее только настраивают для конкретной ситуации. С другой стороны, в отличие от дискреционного метода, управление правами осуществляется централизованно в соответствии с ролями и должностями субъектов. По этой причине ролевой метод относят к недискреционным методам (nondiscretionary access control).

Кроме названных методов в литературе можно встретить и другие методы, например: TBAC (task-based access control), на основе правил Rule-BAC (Rule-based Access Control, типа «if-else»), контекстно-зависимое управление (context-dependent access control) и др.

Заключение

Перечислим, что осталось за рамками данной публикации, а именно: технические средства защиты информации, формальные (концептуальные) модели, политики безопасности, типовые атаки.

Из применяемых средств защиты информации следует выделить системы обнаружения вторжений (IDS/IPS), ложные системы (Honeypot), SIEM-системы и в качестве основного средства разграничения сетевого доступа – межсетевые экраны. Однако они, как и сетевые атаки, подробно рассматриваются в рамках домена, посвященного сетевой безопасности. Формальным моделям разграничения доступом посвящен отдельный домен, касающийся архитектуры безопасности [6]. Политики упоминаются в домене по операционной безопасности.

Всего, по авторской оценке, знание положений рассмотренного домена обеспечит не менее 30% успеха при сдаче экзамена CISSP.

Литература

1. Дорофеев А.В. Статус CISSP: как получить и не потерять? // Вопросы кибербезопасности. 2013. № 1(1). С.65-68.
2. Дорофеев А.В., Марков А.С. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. № 1 (2). С. 67-73.
3. Дорофеев А.В. Менеджмент информационной безопасности: управление рисками // Вопросы кибербезопасности. 2014. № 2(3). С.66-73.
4. Дорофеев А.В. Менеджмент информационной безопасности: переход на ISO 27001:2013 // Вопросы кибербезопасности. 2014. № 3(4). С.69-73.
5. Дорофеев А.В. Подготовка к CISSP: телекоммуникации и сетевая безопасность // Вопросы кибербезопасности. 2014. № 4(7). С. 69-74.
6. Барабанов А.В. Подготовка к сдаче CISSP: модели информационной безопасности // Вопросы кибербезопасности. 2014. № 5(8). С. 59-67.
7. Марков А.С., Цирлов В.Л. Основы криптографии: подготовка к CISSP // Вопросы кибербезопасности. 2014. № 1(9).
8. James M. Stewart, Mike Chapple, Darril Gibson. CISSP: Certified Information Systems Security Professional Study Guide, 7th Edition. - Sybex, 2015. 1104 p.
9. Shon Harris, CISSP All-in-One Exam Guide, 6th Edition -McGrawHill, 2012. 1216 p.

Reference

1. Dorofeev A.V. Status CISSP: kak poluchit' i ne poteryat'? Voprosy kiberbezopasnosti (Cybersecurity issues, in Russia), 2013, No 1(1), pp.65-68.
2. Dorofeev A.V., Markov A.S. Menedzhment informatsionnoy bezopasnosti: osnovnye kontseptsii, Voprosy kiberbezopasnosti, 2014, No 1 (2), pp. 67-73.
3. Dorofeev A.V. Menedzhment informatsionnoy bezopasnosti: upravlenie riskami, Voprosy kiberbezopasnosti, 2014, No 2(3), pp.66-73.
4. Dorofeev A.V. Menedzhment informatsionnoy bezopasnosti: perekhod na ISO 27001:2013, Voprosy kiberbezopasnosti, 2014, No 3(4), pp.69-73.
5. Dorofeev A.V. Podgotovka k CISSP: telekommunikatsii i setevaya bezopasnost', Voprosy kiberbezopasnosti, 2014, No 4(7), pp. 69-74.
6. Barabanov A.V. Podgotovka k sdache CISSP: modeli informatsionnoy bezopasnosti, Voprosy kiberbezopasnosti, 2014, No 5(8), pp. 59-67.
7. Markov A.S., Tsirlov V.L. Osnovy kriptografii: podgotovka k CISSP, Voprosy kiberbezopasnosti, 2014, No 1(9).
8. James M. Stewart, Mike Chapple, Darril Gibson. CISSP: Certified Information Systems Security Professional Study Guide, 7th Edition. - Sybex, 2015. 1104 p.
9. Shon Harris, CISSP All-in-One Exam Guide, 6th Edition -McGrawHill, 2012. 1216 p.