6. *Denning D.* An Intrusion Detection Model. IEEE Transactions on Software Engineering. – 1987. – Vol. 13. – P. 222–232.

7. *Guofei G., Fogla P.* Measuring intrusion detection capability: an information-theoretic approach. ACM Symposium on Informaion, Computer and Communications Security. – 2006. P. 90–101.

8. *McHugh J.* Testing intrusion detection systems: A critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory. ACM Transactions on Information and System Security. – 2000. – P. 262–294.

Е.В. Горковенко
Казахстан, г. Алматы, Институт проблем информатики и управления

ОРГАНИЗАЦИЯ ИНТЕРФЕЙСА И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ С МАНДАТНЫМ УПРАВЛЕНИЕМ ДОСТУПА

Технология создания безопасного канала предусматривает как шифрование данных, так и разграничение доступа к сетевым ресурсам. Контроль доступа пользователей к ресурсам локальной сети должен осуществляться в соответствии с политикой безопасности организации, которой принадлежит локальная сеть. Эффективное разграничение доступа к сетевым ресурсам может быть обеспечено только при надежной аутентификации всех пользователей. При взаимодействии с физически удаленными пользователями значительно сложнее обеспечить доступ к сетевым ресурсам только лиц, имеющих на это определенные полномочия. При удаленном взаимодействии важна надежная аутентификация и пользователя и оборудования, поскольку подмена пользователя или маршрутизатора приводит к тому, что данные из корпоративной сети могут передаваться не тем лицам, которым они предназначены, что ведет к реализации несанкционированного доступа (НСД). В классических моделях мандатного управления доступом процесс проецирования прав на защищаемые субъекты осуществляется логически, на основе вывода (да/нет) об аутентичности субъекта. Это наиболее уязвимое место, которое разработчики информационных систем пытаются устранить за счет организации различных схем аутентификации субъектов, в том числе с использованием средств криптографии. Другим подходом в решении данной проблемы является создание так называемой "доверительной компьютерной базы" (ДКБ), цель которой - гарантировать защищенность вычислений заданного пространства. Практика доказывает отсутствие четких гарантий в части обеспечения безопасности ДКБ.

Предлагается рассмотреть организацию многоуровневой защиты, отвечающей полномочной политике информационной безопасности и реализовывающей функции защиты в сетевом многопользовательском варианте в распределенных компьютерных системах. Организация интерфейса в информационных системах с мандатным управлением – доступом (рис.1) направлена, с одной стороны, на выполнение запросов пользователей к информационным ресурсам, а с другой, на поддержку работы администратора без нарушения правил доступа по разрешению запросов к информации различного уровня секретности. Интерфейс организован таким образом, что администратор имеет возможность работать только с базой данных многоуровневой защиты, однако не имеет непосредственного доступа к информационных ресурсам.

Интерфейс пользователя включает в себя:

- процесс аутентификации пользователя;
- формирование текущего запроса к информационным ресурсам;

- работа в диалоговом окне с выбранной информацией в соответствии с разрешенным видом доступа;
- пересылка информации в открытом канале связи.

Выделим несколько классов пользователей среди субъектов защиты: доверенные, удаленные и локальные. Доверенные субъекты – это процессы (специальные программы), которые функционируют только в интересах администраторов компьютерных систем. Удаленные субъекты – авторизованные пользователи, которым организован доступ к ресурсам локальной сети через выделенный сервер удаленного доступа с применением стандартных протоколов сетевого уровня, например на основе протокола *PPP*. Аутентификации локальных, удаленных и доверенных абонентов осуществляется через функцию подтверждения подлинности на основе пароля. Пароль возможно хранить в зашифрованном виде, что существенно снижает риск его раскрытия. При аутентификации введенный пользователем пароль также зашифровывается и сравнивается с хранящимся зашифрованным значением. Естественно, что файл, хранящий пароль, должен быть сам защищен от попыток НСД также как и информация о грифе секретности объектов и уровне допуска субъектов системы. Предусмотрены динамический контроль качества назначаемых паролей и обработка статистических данных (дата и время предыдущего входа и окончание сеанса работы), позволяющих обнаружить факт несанкционированного входа в систему под именем легального пользователя.

Формирование текущего запроса к информационным ресурсам происходит только после успешной аутентификации субъекта. В диалоговых окнах пользователю необходимо выбрать интересующую его информацию и определить вид доступа (чтение, редактирование, копирование и т.д.). Монитор обработки запросов анализирует поступивший запрос. Если уровень допуска субъекта противоречит правилам доступа выбранной модели многоуровневой защиты или субъект не имеет права на реализацию подобного запроса, то субъекту будет отказано в доступе, а в журнале подобный запрос зарегистрируется как попытка НСД. Если доступ разрешен, то субъект работает в диалоговом окне с выбранной информацией в соответствии с разрешенным видом доступа. Для субъектов с высокой категорией допуска часть информации может быть представлена в зашифрованном виде. В функции монитора не включены процедуры, поддерживающие процессы шифрования или дешифрования. Для подобной информации монитор проверяет вид доступа и пересылает абоненту. В журнале регистрируется шифр субъекта, шифр объекта, все действия, время работы. Некоторые виды доступа, например копирование, предусматривают пересылку информации по открытым каналам. При значительных объемах затребованной информации, перед пересылкой она предварительно архивируется. Интерфейс администратора включает в себя:

- процесс аутентификации администратора;
- редактирование в диалоговом окне характеристик объектов защиты;
- редактирование в диалоговом окне характеристик субъектов защиты;
- редактирование в диалоговом окне матрицы доступа;
- управление в диалоговом окне правами доступа субъектов защиты к объектам защиты;
- ведение журнала регистрации всех запросов к информационным ресурсам с выделением попыток НСД.

Аутентификация администратора также организована через парольную защиту. Дважды неправильный ввод пароля – блокировка системы. Использование строгой двухфакторной аутентификации на основе электронных ключей больше подойдет для контроля действий пользователей.

Рис. 1 Структура интерфейса в информационных системах с мандатным управлением – доступом

Редактирование в диалоговом окне характеристик субъектов защиты: шифр субъекта, пароль, категория допуска, должность, код классификации. Классификация выделяет подмножество субъектов, имеющих право подписи документов (владельцы объектов), право переписки, право на разрешение доступа к объектам и право ликвидации доступа.

Редактирование в диалоговом окне характеристик объектов защиты: шифр объекта, степень секретности информации, место хранения, субъект-владелец, код классификации, текущий уровень защиты. Понижение уровня секретности объекта происходит из-за естественного старения информации.

Редактирование в диалоговом окне матрицы доступа может осуществляться по двум направлениям: задание шифра субъекта, тогда редактирование видов доступа ко всем его объектам или задание шифра объекта, тогда редактирование видов доступа всех объектов, которые имели различные права доступа к данному объекту.

Управление в диалоговом окне правами доступа субъектов защиты к объектам защиты состоит в определении администратором следующих функций в соответствии с классификацией и категорией допуска субъектов: наделение правами; передача прав; лишение прав; наделение правом владения, наделение правом реализации. Лишение прав субъекта предусматривает удаление из матрицы доступа данного субъекта, что автоматически лишает его всех прав над объектами. Решающие правила по разрешению запросов и изменению состояний системы подробно рассмотрены в [1,2].

Выбор действий над журналом регистрации запросов предусматривает:

- просмотр журнала с установкой фильтра просмотра по дате, по типу транзакций, по имени файла;
- реагирование на попытки несанкционированного доступа неавторизованных пользователей.

В настоящее время сотрудниками Института проблем информатики и управления разрабатывается комплекс программ «Security Access Monitor -монитор безопасного доступа», который может быть применен для систем управления государственными органами с древовидной структурой субъектов и объектов защиты информации, в которых функционирует информация различной степени чувствительности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Горковенко Е.В.* Параметры безопасности в многоуровневой модели разграничения доступа.// Известия ТРТУ, тематический выпуск материалов 8-й Международной научно-практической конференции «Информационная безопасность », Россия, – Таганрог: Изд-во ТРТУ, 2006, №7(62), – С 87–91.

2. *Горковенко Е.В.* Формализованное представление механизмов защиты при мандатном разграничении доступа. Известия Национальной Академии Наук Республики Казахстан, №3, 2006, – С 79–85.

Е.П. Тумоян
Россия, г. Таганрог, Технологический институт ЮФУ

МЕТОДЫ ФОРМАЛЬНОГО МОДЕЛИРОВАНИЯ СЕТЕВЫХ АТАК

Введение

В последние годы вопросы защиты информационных систем от атак приобретают чрезвычайно большое значение. Одним из наиболее важных направлений обеспечения такой защиты является разработка методов и средств, которые позво-