УДК 004.514.6

ПРИНЦИПЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Храмогин П.А.
Научный руководитель: Арнаутов А.Д.
Сибирский федеральный университет. Институт цветных металлов и материаловедения.

Введение

Информационная безопасность подчеркивает важность информации в современном обществе - понимание того, что информация - это ценный ресурс, нечто большее, чем отдельные элементы данных.

Информационной безопасностью называют меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода.

Целью информационной безопасности является обезопасить ценности системы, защитить и гарантировать точность и целостность информации, и минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена. Информационная безопасность требует учета всех событий, в ходе которых информация создается, модифицируется, к ней обеспечивается доступ или она распространяется.

Информационная безопасность дает гарантию того, что достигаются следующие цели:

1. конфиденциальность критической информации;
2. целостность информации и связанных с ней процессов(создания, ввода, обработки и вывода);
3. доступность информации, когда она нужна;
4. учет всех процессов, связанных с информацией.

Некоторые технологии по защите системы и обеспечению учета всех событий могут быть встроены в сам компьютер. Другие могут быть встроены в программы. Принятие решения о выборе уровня сложности технологий для защиты системы требует установления критичности информации и последующего определения адекватного уровня безопасности.

Методы защиты информации

Управление доступом - метод защиты информации регулированием использования всех ресурсов системы, включающий следующие функции:

1. идентификация ресурсов системы;
2. установление подлинности (аутентификация) объектов или субъектов системы по идентификатору;
3. проверка полномочий в соответствии с установленным регламентом;
4. реагирование при попытках несанкционированных действий.

Препятствие - метод физического преграждения пути нарушителю к защищаемым ресурсам системы.

Маскировка - метод закрытия информации путем ее шифрованного закрытия.

Регламентация - метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи информации, при которых возможности несанкционированного доступа к ней минимизированы.

Шифрование данных - обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней.

Подробнее в своей работе я хотел бы рассмотреть такой метод защиты информации, как шифрование.

Шифрование данных

Шифрование служит задачей соблюдения конфиденциальности передаваемой информации. Важной особенностью любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного преобразования из совокупности возможных преобразований для данного алгоритма.

С помощью шифрования обеспечиваются три состояния безопасности информации:

1)Конфиденциальность - используется для скрытия информации от неавторизованных пользователей при передаче или при хранении.

2)Целостность - используется для предотвращения изменения информации при передаче или хранении

3) Идентифицируемость - используется для аутентификации источника информации и предотвращения отказа отправителя информации от того факта, что данные были отправлены именно им.

Шифрование данных в компьютерной сети

Одной из отличительных характеристик любой компьютерной сети является ее деление на так называемые уровни, каждый из которых отвечает за соблюдение определенных условий и выполнение функций, которые необходимы для общения между собой компьютеров, связанных в сеть. Это деление на уровни имеет фундаментальное значение для создания стандартных компьютерных сетей. Поэтому в 1984 году несколько международных организаций и комитетов объединили свои усилия и выработали примерную модель компьютерной сети, известную под названием OSI(Open Systems Interconnection).

OSI разносит коммуникационные функции по уровням. Каждый из этих уровней функционирует независимо от ниже- и вышележащих. Он может непосредственно общаться только с двумя соседними уровнями, но полностью изолирован от прямого обращения к следующим уровням. Модель OSI выделяет семь уровней: верхние три служат для связи с конечным пользователем, а нижние четыре ориентированы на выполнение коммуникационных функций в реальном масштабе времени.

В теории шифрование данных для передачи по каналам связи компьютерной сети может осуществляться на любом уровне модели OSI. На практике это обычно делается либо на самых нижних, либо на самых верхних уровнях. Если данные шифруются на нижних уровнях, шифрование называется **канальным.** Если шифрование данных выполняется на верхних уровнях, то оно называется **сквозным.** Оба этих подхода к шифрованию данных имеют свои преимущества и недостатки.

Канальное шифрование

При канальном шифровании шифруются абсолютно все данные, проходящие через каждый канал связи, включая открытый текст сообщения, а также информацию о его маршрутизации и об используемом коммуникационном протоколе. Однако в этом случае любой интеллектуальный сетевой узел (например, коммутатор) будет вынужден расшифровывать входящий поток данных, чтобы соответствующим образом его обработать, и снова зашифровывать, чтобы передать на другой узел сети.

Тем не менее канальное шифрование представляет собой очень эффективное средство защиты информации в компьютерных сетях. Поскольку шифрованию подлежат все данные, движущиеся от одного узла сети к другому, у криптоаналитика нет никакой дополнительной информации о том, кто служит источником передаваемых данных, кому они предназначены, какова их структура и так далее.

Самый большой недостаток канального шифрования связан с тем, что данные приходится шифровать при передаче по каждому физическому каналу компьютерной сети. Отправка информации в незашифрованном виде по какому-то из каналов ставит под угрозу обеспечение безопасности всей сети в целом. В результате стоимость реализации канального шифрования в больших сетях может оказаться чрезмерно велика.

Кроме того, при использовании канального шифрования дополнительно потребуется защищать каждый узел компьютерной сети, через который проходят передаваемые по сети данные. Если абоненты сети полностью доверяют друг другу, и каждый ее узел размещен в защищенном от проникновения злоумышленников месте, на этот недостаток канального шифрования можно не обращать внимание. Однако на практике такое положение встречается чрезвычайно редко. Ведь в каждой фирме есть конфиденциальные данные, знакомиться с которыми могут только сотрудники одного определенного отдела, а за его пределами доступ к этим данным необходимо ограничивать до минимума.

Сквозное шифрование

При сквозном шифровании криптографический алгоритм реализуется на одном из верхних уровней модели OSI. Шифрованию подлежит только содержательная часть сообщения, которое требуется передать по сети. После зашифровывания к ней добавляется служебная информация, необходимая для маршрутизации сообщения, и результат переправляется на более низкие уровни с целью отправки адресату.

Теперь сообщение не требуется постоянно расшифровывать и зашифровывать при прохождении через каждый промежуточный узел сети связи. Сообщение остается зашифрованным на всем пути от отправителя к получателю.

Основная проблема, с которой сталкиваются пользователи сетей, где применяется сквозное шифрование, связана с тем, что служебная информация, используемая для маршрутизации сообщений, передается по сети в незашифрованном виде. Опытный криптоаналитик может извлечь для себя массу полезной информации, зная кто с кем, как долго и в какие часы общается через компьютерную сеть. Для этого ему даже не потребуется быть в курсе предмета общения.

По сравнению с канальным, сквозное шифрование характеризуется более сложной работой с ключами, поскольку каждая пара пользователей компьютерной сети должна быть снабжена одинаковыми ключами, прежде чем они смогут связаться друг с другом. А поскольку криптографический алгоритм реализуется на верхних уровнях модели OSI, приходится также сталкиваться со многими существенными различиями в коммуникационных протоколах и интерфейсах в зависимости от типов сетей и

объединяемых в сеть компьютеров. Все это затрудняет практическое применение сквозного шифрования..

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Медведовский И.Д., Семьянов П.В., Леонов Д.Г. “Атака на интернет”
2. Издательского дома "Открытые Системы" (Lan Magazine/Журнал сетевых решений, 1996, том 2, #7)
3. Издательского дома "Открытые Системы"(Сети, 1997, #8)
4. “Office” N5 1999 Александр Буров “Человеческий фактор и безопасность”