**Аспекты сетевой безопасности**

*Введение*

В двадцать первом веке движущей силой и главным объектом всех отраслей человеческой деятельности становится *информация*. К сожалению, сложные сетевые технологии достаточно уязвимы для целенаправленных атак. Причем такие атаки могут производиться удаленно, в том числе и из-за пределов национальных границ. Все это ставит новые проблемы перед разработчиками и строителями информационной инфраструктуры. Некоторые современные формы бизнеса полностью базируются на сетевых технологиях (электронная *торговля*, *IP*-телефония, сетевое провайдерство и т.д.) и *по* этой причине особенно уязвимы. Потребуется здесь и международное сотрудничество в сфере законодательства и установления барьеров для сетевых террористов. Не исключено, что придется со временем модифицировать некоторые протоколы и программы с учетом требований безопасности.

*Что такое сетевая безопасность?*

Это прикладная научная дисциплина, отрасль информатики, занимающаяся вопросами обеспечения информационной безопасности компьютерной сети и её ресурсов, в частности, хранящихся в ней и передающихся по ней данных и работающих с ней пользователей. Является расширением компьютерной безопасности и подразделом информационной безопасности. Занимается изучением и разработкой методов и практических правил работы с сетью, в том числе протоколами связи, обмена данными и криптографическими методами защиты информации.

Кроме дисциплины, под термином «сетевая безопасность» может пониматься комплекс процедур, стандартов, правил и средств, призванных обеспечить безопасность компьютерной сети.

Обеспечение сетевой безопасности является важным аспектом деятельности любой компании.

Существуют *юридические* аспекты сетевой безопасности, *организационные* и *программно-технические*.

Я рассмотрю два последних.

Рассмотрим сначала факторы, влияющие на надежность сети. Источниками ненадежности сети могут быть:

* стихийные явления, к которым можно отнести отказы оборудования или питания, а также некомпетентность обслуживающего персонала;
* несанкционированные действия операторов удаленных ЭВМ.

*Уязвимости и атаки*

Общей уязвимостью, существующей как в проводных, так и в беспроводных сетях, является «несанкционированный доступ» к сети. Злоумышленник может подключить свое устройство к сети через незащищенный порт концентратора / коммутатора. В связи с этим беспроводная сеть считается менее безопасной, чем проводная сеть, поскольку к беспроводной сети можно легко получить доступ без какого-либо физического соединения.

После получения доступа злоумышленник может использовать эту уязвимость для запуска таких атак, как:

* Получение пакетных данных, чтобы украсть ценную информацию.
* Отказ в обслуживании законным пользователям в сети.
* Подмена физических идентификаторов (MAC) законных хостов, а затем кража данных или дальнейшее начало атаки «человек посередине».

*Сетевой протокол*

Это набор правил, управляющих связью между устройствами, подключенными к сети. Они включают в себя механизмы создания соединений, а также правила форматирования для упаковки данных для отправленных и полученных сообщений.

Было разработано несколько протоколов компьютерных сетей, каждый из которых предназначен для определенных целей. Популярными и широко используемыми протоколами являются TCP / IP со связанными протоколами более высокого и более низкого уровня.

*Цели сетевой безопасности*

В сети существует большое количество уязвимостей. Таким образом, во время передачи данные очень уязвимы для атак. Злоумышленник может нацелиться на канал связи, получить данные и повторно отправить их, вставив ложное сообщение для достижения своих целей.

Безопасность сети касается не только безопасности компьютеров на каждом конце коммуникационной цепочки; однако, это стремится гарантировать, что вся сеть безопасна.

Безопасность сети подразумевает защиту удобства использования, надежности, целостности и безопасности как самой сети, так и данных. Эффективная сетевая безопасность защищает от множества угроз от проникновения или распространения в сети.

Основной целью сетевой безопасности являются конфиденциальность, целостность и доступность. Эти три столпа сетевой безопасности часто представлены в виде **треугольника ЦРУ**.

* **Конфиденциальность** — функция конфиденциальности заключается в защите ценных деловых данных от посторонних лиц. Часть обеспечения безопасности сети гарантирует, что данные доступны только предполагаемым и уполномоченным лицам.
* **Целостность** — эта цель означает поддержание и обеспечение точности и согласованности данных. Функция целостности заключается в том, чтобы гарантировать, что данные надежны и не изменены посторонними лицами.
* **Доступность** — функция доступности в Network Security состоит в том, чтобы гарантировать, что данные, сетевые ресурсы, сервисы постоянно доступны для законных пользователей, когда они этого требуют.

*Достижение безопасности сети*

Обеспечение безопасности сети может показаться очень простым. Цели, которые должны быть достигнуты, кажутся простыми. Но на самом деле механизмы, используемые для достижения этих целей, очень сложны.

**Международный союз электросвязи** (МСЭ) в своей рекомендации по архитектуре безопасности X.800 определил определенные механизмы для стандартизации методов обеспечения безопасности сети.

*Некоторые из этих механизмов*

* **Зашифрование** — этот механизм предоставляет услуги конфиденциальности данных путем преобразования данных в нечитаемые формы для посторонних лиц. Этот механизм использует алгоритм шифрования-дешифрования с секретными ключами.
* **Цифровые подписи** — этот механизм является электронным эквивалентом обычных подписей в электронных данных. Это обеспечивает достоверность данных.
* **Контроль доступа** — этот механизм используется для предоставления услуг контроля доступа. Эти механизмы могут использовать идентификацию и аутентификацию объекта для определения и обеспечения прав доступа объекта.

Разработав и идентифицировав различные механизмы безопасности для обеспечения безопасности сети, важно решить, где их применять; как физически (в каком месте), так и логически (на каком уровне архитектуры, такой как TCP / IP).

*Механизмы безопасности на сетевых уровнях*

Несколько механизмов безопасности были разработаны таким образом, что они могут быть работать на определенном уровне модели сетевого уровня OSI.

**Безопасность на уровне приложений** — меры безопасности, используемые на этом уровне, зависят от конкретного приложения. Различные типы приложений потребуют отдельных мер безопасности.

Считается, что разработка криптографически обоснованного протокола приложения очень сложна, а правильная его реализация еще сложнее. Следовательно, механизмы защиты прикладного уровня для защиты сетевых коммуникаций предпочтительны, чтобы быть только основанными на стандартах решений, которые использовались в течение некоторого времени.

Примером протокола безопасности прикладного уровня является Secure Multipurpose Internet Mail Extensions (S / MIME), который обычно используется для шифрования сообщений электронной почты.

**Безопасность на транспортном уровне -** меры безопасности на этом уровне могут использоваться для защиты данных в одном сеансе связи между двумя хостами. Наиболее распространенным применением протоколов безопасности транспортного уровня является защита трафика сеансов HTTP и FTP. Transport layer security (TLS) и Secure Sockets Layer (SSL) являются наиболее распространенными протоколами, используемыми для этой цели.

**Сетевой уровень** — меры безопасности на этом уровне могут применяться ко всем приложениям; таким образом, они не зависят от приложения. Все сетевые коммуникации между двумя хостами или сетями могут быть защищены на этом уровне без изменения какого-либо приложения.  Однако протоколы безопасности на этом уровне обеспечивают меньшую гибкость связи, которая может потребоваться некоторым приложениям.

Механизм безопасности, предназначенный для работы на более высоком уровне, не может обеспечить защиту данных на более низких уровнях, потому что более низкие уровни выполняют функции, о которых более высокие уровни не знают. Следовательно, может быть необходимо развернуть несколько механизмов безопасности для повышения безопасности сети.