УДК 004.056.5

МОДЕЛЬ OSI В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ахмедов Максим Рафильевич, ГБОУ лицей №533

Научный руководитель – Минеев Дмитрий Юрьевич

Аннотация. Данная работа посвящена, рассмотрению модели OSI в информационной безопасности**.**

Введение. Каждый день, мы заходим в интернет и оставляем там определенную информацию. Каждую минуту, все люди, пользующиеся интернетом, генерируют огромное количество данных. От данных по перемещению внутри мировой сети и вплоть до информации о покупках, таки как электронные чеки, подтверждения об оплате, пароли и многое другое.

Все компании, внутри которых эта информация генерируется, собирают её и анализируют, для построения своей политики в будущем.

Как и другую любую информацию, эти данные необходимо защищать от злоумышленников, которые хотят воспользоваться ими в своих корыстных целях. По большей части, им необходима личная информация о пользователях, такая как: номера банковских карт, пароли от личного профиля, коды подтверждения и т.п. Защитой таких данных занимается Информационная безопасность.

Основная часть. Для начала уточним термин “Информационная безопасность”.

Информационная безопасность – это практика по предотвращению несанкционированного доступа, какого-либо искажения или изменения, исследования, перезаписи или же уничтожения информации. Данный термин относится не только к IT – индустрии, но и к физическим данным в том числе.

В этой работе мы рассмотрим информационную безопасность на примере модели OSI, которая представляет из себя сетевую модель стека (магазина) сетевых протоколов OSI/ISO. При помощи данной модели различные сетевые устройства могут взаимодействовать друг с другом. Модель определяет различные уровни взаимодействия систем. Каждый уровень выполняет определённые функции при таком взаимодействии.

Начнем рассматривать данную систему с нулевого уровня. В самой модели OSI такой уровень не выделяют, но говоря о информационной безопасности, следует упомянуть его.

0. Уровень проектирования. Самые основные и базовые понятия о защите информации, мы представляем в виде теоретической модели. Как например, при проектировании плана, по установке серверного оборудования: где и как должна располагаться электроника, как правильно разместить предметы пожарной безопасности т.п.

Плохой пример: из-за скачка электроэнергии произошло короткое замыкание, вследствие чего началось возгорание электроники. Сработала система пожаротушения и залила всё водой. В данный момент, если не была спроектирована система “Бэкапов” (систематичное копирование данных), то возможности, полного восстановления данных попросту нету. На этом примере мы можем увидеть, что были нарушены\не предусмотрены два условия:

1. Не была предусмотрена защита электроники от скачков напряжения. (решается установкой более качественного и сертифицированного оборудования)
2. Сервер расположен в помещении с водяной системой пожаротушения.

Чтобы избежать таких проблем, данной задачей занимается отдельный человек: Архитектор системы безопасности.

1. Физический уровень. На данном уровне, прорабатывается физическая защита информации:

Замок на двери, охранник возле входа, сигнализация, пропускной пункт и т.д.

Все это является физической защитой информации.

Плохой пример: Злоумышленник, пробирается в офис компании, за счет отсутствия контрольно-пропускного пункта, далее проходит в серверную из-за отсутствия замков и крадет физический носитель информации.

2. Канальный уровень – на данном этапе, определяются, методы передачи данных в локальной сети при помощи блоков данных (далее. Фреймы). Эти фреймы не пересекаются с общесетевым уровнем, т.к. они работают только в области локальной сети. Разделение канального и общесетевого уровня, нужен для распределения нагрузки. Вследствие чего, протоколы канального уровня, могут сосредоточится только на локальной доставке и адресации. Канальный уровень, можно разделить на 2 подуровня:

1. уровень управления логическим каналом (logical link control, LLC).

2. уровень доступа к среде (media access layer, MAC),

Главная задача MAC уровня, это процедура доступа к самой среде.

Для чего вообще нужен данный канальный уровень?

Пояснение: В случае, когда все устройства пытаются использовать среду одновременно, происходит несостыковка (коллизия) в наложении фреймов, в итоге данные устройства не могут синхронизироваться. Протоколы канального уровня же, выявляют такие случаи и обеспечивают среду механизмами для уменьшения случаев коллизии или же их полного предотвращения. Кроме этого, главной задачей, на которую нужно обратить внимание на данном уровне, это система доступа к среде работающий по системе ролей. Каждому пользователю присваивается определенная роль, которая включает в себя определенные разрешения и запреты.

3. Сетевой уровень – на данном этапе, протоколы сетевого уровня нужны для определения пути передачи данных, среди удаленных друг от друга серверов.

При формировании защищенных виртуальных каналов на сетевом уровне рассматриваемой модели OSI достигается оптимальное соотношение между прозрачностью и качеством защиты. Размещение средств защиты на сетевом уровне делает их невидимыми для приложений, так как между сетевым уровнем и приложением, реализуется протокол транспортного уровня. Для пользователей процедуры защиты оказываются такими же прозрачными, как и сам протокол IP (internet protocol). На сетевом уровне существует возможность достаточно полной реализации функций защиты трафика и управления ключами, поскольку именно на сетевом уровне выполняется маршрутизация пакетов сообщений.

Для защиты сетевого уровня, используется стек протоколов IPSec (Internet Protocol Security) который используется для аутентификации участников обмена, туннелирования трафика и шифрования IP-пакетов. Основное назначение протокола IPSec — обеспечение безопасной передачи данных по сетям IP. Поскольку архитектура IPSec совместима с протоколом IPv4 (internet protocol version 4, благодаря которому и работает весь современные интернет), ее поддержку достаточно обеспечить на обоих концах соединения; промежуточные сетевые узлы могут вообще ничего «не знать» об IPSec. Протокол IPSec может защищать трафик как текущей версии протокола IPv4, применяемой сегодня в Internet, так и трафик новой версии IPv6, которая постепенно внедряется в Internet.2

4. Транспортный уровень — это первый уровень, который встречает данные приложения и начинает процедуру по их подготовке к передаче, если сетевой уровень определяет, по какому пути отправятся данные, то транспортный уровень, подготавливает и отправляет их.

На транспортном уровне функционируют как правило два протокола: TCP и UDP.

TCP (Transmission Control Protocol) – основная задача данного протокола - сегментация данных, приходящих с уровня приложений и адресация приложений при помощи портов. Так же TCP обеспечивает:

1. Надёжную доставку сегментов.
2. Упорядочивание сегментов при получении.
3. Работу с сессиями.
4. Контроль за скоростью передачи.

UDP – (User datagram protocol) – основная задача данного протокола схожа с TCP но помимо этого, она умеет:

1. Сегментировать данные, полученные с уровня приложений.
2. Адресовать работающие приложений при помощи портов

Основные протоколы по защите транспортного уровня: TLS (transport layer security) как и его предшественник SSL (secure sockets layer далее, разберем его более подробнее) — являются криптографическими протоколами, которые обеспечивают защищённую передачу данных между узлами в сети Интернет. TLS и SSL используют:

1. Асимметричное шифрование для аутентификации.
2. Симметричное шифрование для конфиденциальности
3. Коды аутентичности сообщений для сохранения целостности сообщений.

Данный протокол широко используется в приложениях, работающих с сетью Интернет, таких как веб-браузеры, работа с электронной почтой, обмен мгновенными сообщениями и IP-телефония.

5. Сеансовый уровень - данный уровень используется относительно редко, многие протоколы реализуют его функциональные возможности на своих транспортных уровнях.

Основная функция сеансового уровня - организация сеанса, т. е. передачи управления во время связи между двумя компьютерными системами. Сеанс определяет направленность передачи данных (это может быть одно или двухсторонняя направленность), а также гарантирует завершение обработки одного запроса до принятия следующего.

Сеансовый уровень также может поддерживать некоторые из следующих дополнений:

- управление диалогом.
- управление маркерами.
- управление операциями.

Для работы некоторых протоколов очень важно, чтобы в любой момент времени попытки выполнения критических операций могли выполняться лишь одной из сторон. Чтобы обе стороны не пытались одновременно выполнить одну и ту же операцию, реализован специальный механизм управления, который основан на использовании маркеров. В этом случае выполнение операции разрешается только той стороне, которая в настоящий момент удерживает маркер. Определение того, на какой стороне находится маркер и как он передается между двумя сторонами, как раз-таки и называется управление маркером.

Для передачи данных и обеспечения достоверности передаваемой информации в поток данных вставляются контрольные точки. В этом случае при возникновении сбоя сеансовый уровень может продолжить пересылку данных с предыдущей контрольной точки. Эти контрольные точки называются точками синхронизации. Управление точками синхронизации называется управлением операциями.

В случае с сеансовым уровнем, нам необходимо озаботится созданием защищенного канала связи, для передачи определенной информации.

В таком случае используется протокол SSL. (Мы упоминали его на транспортном уровне)

Протокол SSL (Secure Sockets Layer) применяется в качестве протокола защищенного канала, работающего на сеансовом уровне модели OSI и работавшего до какого-то момента на транспортном уровне, пока его не заменил TLS. Этот протокол использует

криптографические методы защиты информации для обеспечения безопасности информационного обмена. Протокол SSL выполняет все функции по созданию защищенного канала между двумя абонентами сети, включая их взаимную аутентификацию, обеспечение конфиденциальности, целостности и аутентичности передаваемых данных. Конфиденциальность обеспечивается шифрованием передаваемых сообщений с использованием симметричных сессионных ключей, которыми стороны обмениваются при установлении соединения. Сессионные ключи передаются также в зашифрованном виде, при этом они шифруются с помощью открытых ключей, извлеченных из сертификатов абонентов. Использование для защиты сообщений симметричных ключей связано с тем, что скорость процессов шифрования и расшифрования на основе симметричного ключа существенно выше, чем при использовании несимметричных ключей. Подлинность и целостность циркулирующей информации обеспечивается за счет формирования и проверки электронной цифровой подписи.

Согласно протоколу SSL криптозащищенные туннели создаются между конечными точками виртуальной сети. Инициаторами каждого защищенного туннеля являются клиент и сервер, функционирующие на компьютерах в конечных точках туннеля.

Существуют так же еще два уровня модели OSI, но они менее подвержены опасности, т.к. они лишь позволяют пользователю осуществлять связь с сетью. И зачастую информационную безопасность из себя представляет установка паролей, антивирусов и т.д.

Заключение. Итак, в заключение хочется сказать, что: в наше время, чтобы защитить информацию необходимо выстроить грамотную многоуровневую систему защиты и ограничений для создания безопасной информационной среды

В данной работе мы рассмотрели информационную безопасность компаний на примере модели OSI. разобрали закономерности в проектировании безопасной среды для обмена, накопления, редактирования и создания информации на различных уровнях OSI модели. И то, как работают различные сетевые протоколы, и их влияние на структуру сети.

Сфера защиты данных является наиболее перспективной в наше время, из-за перехода от индустриального общества к информационному. Мы можем наблюдать глобальную цифровизацию во всех сферах нашей жизни. Огромное количество информации попадает во всемирную сеть, и защита этих данных сейчас наиболее востребована.