УДК 004

ПРОБЛЕМАТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СЕТЯХ: СЕТЕВЫЕ ПРОТОКОЛЫ И ИХ ОСОБЕННОСТИ

Василенко К. А., Щетилин В. А.

В современном мире, в веке стремительной компьютеризации и различных методов цифровой обработки информации, она становится весьма значимым звеном. Банковские счета, ПИН-коды от кредитных карт, биржевые котировки, место проживания, пароли от аккаунтов, оценки учеников в школе — все это сейчас приобретает вид нулей и единиц. Развитие коммуникаций привело к новой эре, где информация сравнима с золотом. И это золото необходимо должным образом защитить.

С точки зрения безопасности компьютерные сети обладают следующими недостатками:

- недостаточный контроль над клиентскими компьютерами; - отсутствие механизма настраиваемого доступа нескольких пользователей к разным ресурсам на одном компьютере;
- необходимость подготовленности пользователя к разным административным мерам — обновлению антивирусной базы, архивированию данных, определению механизмов доступа к раздаваемым ресурсам и т.д.;
- разделение ресурсов и загрузка распределяются по различным узлам сети, многие пользователи имеют потенциальную возможность доступа к сети как к единой компьютерной системе;
- операционная система, представляющая сложный комплекс взаимодействующих программ.

Учитывая вышеизложенное, имеются сложности в формулировке каких-либо четких критериев и требования к информационной безопасности, особенно это относится к сетям общего пользования (общецелевым), разработка которых обычно ведется без учета каких-либо средств защиты информации [2]. Это также зависит от точных границ и пределов разработанной компьютерной сети и имеющихся при этом функционирующих периферийных устройств.

Узел компьютерной сети имеет возможность синхронизированной работы в нескольких вычислительных сетях. В данном процессе весь функционал, инструменты и ресурсы данной одной компьютерной сети также могут эксплуатироваться с узлов и сегментов, находящихся в составе иной вычислительной сети.

С какой-то стороны это может показаться относительно уместным преимуществом с обычных пользователей, поскольку такое разделение имеющихся в компьютерной сети ресурсов должно иметь широкомасштабное распространение. Однако для злоумышленников данное обстоятельство является ничуть не меньшей удачной возможностью для соответствующей атаки в имеющиеся множества уязвимых точек атаки вычислительной системы, при этом может вестись контроль точек доступа к самой системе пользователей, учитывая что указанны доступ ведется с определенных терминалов вычислительной системы.

В компьютерной сети может возникнуть такое обстоятельство, при котором с различных рабочих станций, узлов или сегментов сети может быть запрошен удаленный доступ для входа и управления данными. В связи с чем, главный пользователь или администратор отдельной вычислительной системы может вести активные меры информационной безопасности для своей компьютерной системы, в том время как администратор узла сети не имеет таких функций и возможностей. При этом бывает ситуация, когда траектория доступа к сети остается не распределенной до конца, и ее не возможно определить. Злоумышленник с целью проникновения к ресурсам компьютерной сети может запросить к ним соответствующий доступ, при этом выбрать определенный узел сети или сегмент, с которыми нет прямой связи с данной вычислительной сетью.

В таких случаях доступ осуществляется через некоторый промежуточный узел, связанный с обоими узлами, или даже через несколько промежуточных узлов. В компьютерных сетях весьма непросто точно определить, откуда именно пришел запрос на доступ, особенно если захватчик приложит немного усилий к тому, чтобы скрыть это; слабая защищенность линии связи.

Сеть тем и отличается от отдельной системы, что непременно включает в себя линии связи, по которым между узлами передаются данные. Это может быть элементарный провод, а может быть линия радиосвязи, в том числе и спутниковый канал.

При наличии определенных условий (и соответствующей аппаратуры) к проводу можно незаметно (или почти незаметно) подсоединиться, радиолинию можно успешно прослушивать — т.е. ничто не препятствует тому, чтобы «выкачивать» передаваемые сообщения из линий связи и затем выделять из всего потока требуемые.

Ограничить доступ к информации злоумышленникам возможно при помощи: криптосистем, разграничения прав доступа, исключения несанкционированного копирования баз данных и т.д. Но как защитить информацию в сети? Для безопасной передачи информации в сети используют защищенные протоколы передачи данных и многие другие способы защиты, о которых и пойдет речь.

Вначале рассмотрим несколько криптографических протоколов.

SSL(SecureSocketsLayer) — криптографический протокол, который подразумевает безопасную связь. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений. Протокол широко использовался для обмена мгновенными сообщениями и передачи голоса через IP (англ. VoiceoverIP — VoIP), в таких приложениях, как электронная почта, Интернет-факс и др. Ниже приведена схема работы данного протокола (см. рис. 1).

1. ПК1 отправляет запрос на получение сертификата: открытый ключ и идентификационную информацию.
2. Центр сертификатов выдает сертификат ПК1: открытый ключ ПК1 подписан закрытым ключом.
3. ПК1 устанавливает сертификат на SSL-сервер.
4. ПК2 генерирует запрос к SSL-серверу ПК1 и автоматически скачивает сертификат ПК1.
5. ПК2 берет открытый ключ SSL-сервера и дешифрует сертификат ПК1. (Так как SSL-сервер подписал сертификат с открытым ключом ПК1, то ПК2 знает, что он работает именно с ПК1 и может устанавливать безопасное соединение с веб-сервером ПК1).
6. ПК2 посылает сообщение, внутри которого находится сессионный ключ(-симметричный)и шифрует его с помощью открытого ключа ПК1.
7. ПК1 дешифрует сообщение с помощью своего закрытого ключа, извлекает сессионный ключ и теперь может

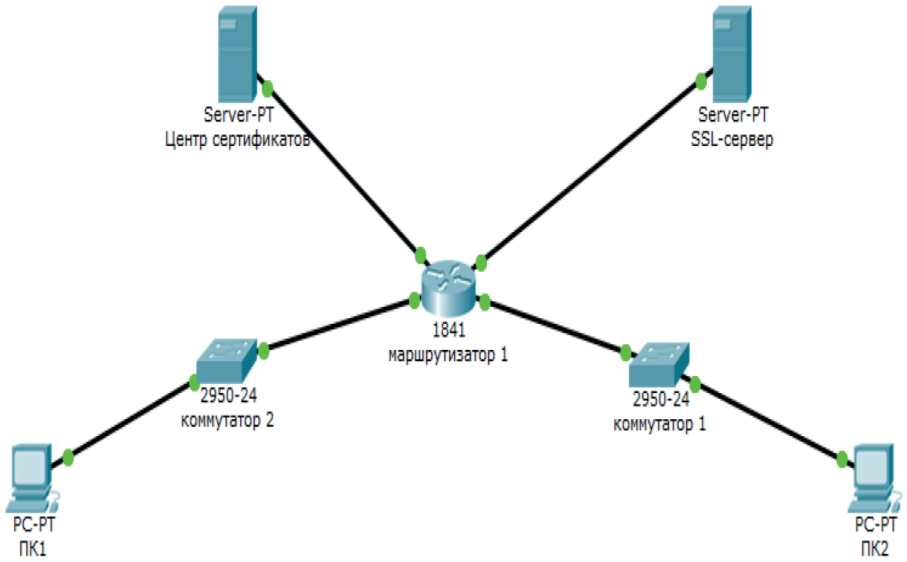

Рисунок 1. Схема работы протокола SSL

безопасно обмениваться сообщениями с ПК2.

В настоящее время доказано, что рассмотренный выше протокол не является абсолютно безопасным. В связи с этим появился протокол TLS, который является улучшенной версией в предыдущего протокола.

Изменения повлекли за собой такую особенность, что между участниками соединения должен использоваться одинаковый протокол (либо TLS, либо SSL). Совместное их использование не уместно.

SSL/TLS протоколы применяются совместно с протоколами, которые используются при передаче данных. К примеру, многие наверняка знают о протоколе HTTP, который используется для получения информации с WEB-сайтов. Протокол HTTP, к которому прикрепляется протокол SSL/TLS, называется HTTPS. Данный протокол можно наблюдать, например, при переходе на сайт «Сбербанк онлайн».

Следующий протокол, о котором пойдет речь, — это протокол SSH. Этим протоколом мы пользуемся зачастую тогда, когда необходимо установить защищённое соединение с сетевым оборудованием. Для работы с SSH необходимы SSH-сервер и SSH-клиент. Данную реализацию можно произвести на любых операционных системах (ОС), но так как поддержка SSH реализована практически на всех UNIX-системах, то рекомендуется использовать именно их. Они проявляют себя более стабильно в отличие от того же семейства Windows, так как UNIX-системы является открытыми операционными системами, то их возможности более обширны.

К слову сказать, если, к примеру, у вас имеется информация или оборудование, к которому необходим ограниченный доступ, то для повышения их безопасности необходимо использовать открытые ОС. Проще говоря, в открытых ОС вы всегда можете посмотреть, что происходит в вашей системе. После небольшого отступления возвратимся к протоколу SSH.

SSH (SecureShell — безопасная оболочка) — сетевой протокол прикладного уровня, позволяющий производить удаленное подключение. Если имеется какой-либо незащищенный канал связи, то при помощи данного протокола можно установить безопасное соединение, и передавать практически любой другой сетевой протокол и любой трафик. Для организации соединения необходимо создать пары ключей — открытый и закрытый. И, как принято в асимметричных системах шифрования, обмен происходит только открытым ключом, причем иногда используется также пароль.

Приведем некоторые факты, которые позволяют обезопасить SSH–соединение.

1. Шифрованное соединение, которое может выполняться одним из мето-

дов, выбранных в процессе переговоров. Шифрованное соединение не позволяет просто перехватить и использовать трафик. Выбор алгоритма шифрования делает систему более гибкой, позволяя не использовать алгоритмы, в которых обнаружены слабые места или которые не может поддерживать одна из сторон.

2. Аутентификация сервера выполняется при любом соединении. Это не позволяет выполнить подмену сервера или подмену трафика.
3. Аутентификация клиента может выполняться одним из нескольких доступных способов. Это, с одной стороны, может повысить надежность аутентификации, с другой — делает систему более гибкой и упрощает ее использование.
4. Проверка целостности пакетов позволяет отследить любые незаконные изменения в трафике соединения. При обнаружении таких изменений соединение немедленно разрывается.
5. Временные параметры аутентификации не позволяют воспользоваться данными соединения в том случае, если, спустя некоторое время после перехвата, оно все-таки было расшифровано. Устаревание обычно происходит через час.

Также в рассматриваемом протоколе есть такая функция, как аутентификация сервера. Она осуществляется при помощи инфраструктуры открытых ключей. Если клиент хочет установить соединение с сервером, то он шифрует данные при помощи открытого ключа сервера, который получил при первом соединении, и отправляет их на сервер. Сервер, в свою очередь, должен расшифровать это сообщение при помощи своего закрытого ключа. Если все проходит успешно, то соединение устанавливается. Таким образом, клиент и сервер распознают друг друга.

SSH помогает защититься от следующих несанкционированных действий:

1. Подмены IP-адресов, когда удаленный хост посылает пакеты от имени другого хоста.
2. Подмены DNS-записей, в результате которой соединение устанавливается с нежелательным хостом.
3. Перехвата данных и открытых паролей.

На данный момент рассмотренный протокол достаточно актуален и широко используется в информационных технологиях.

Следующий способ защиты информации — это контрольные суммы. В том случае, если послание полностью зашифровано, есть вероятность что его могут исказить или вовсе заменить. Чтобы избежать этого используют контрольную сумму. Данный способ является частью определенного сообщения, его элементом. Разработка алгоритмов, относящихся к расчету контрольных сумм, имеет свою соответствующую уникальность для каждой передаваемой информации или сообщения. В результате чего, ликвидируется какой-либо способ подменить или изменить данную информацию. Но при этом, может образоваться определенная сложность в передачи получателю контрольных сумм алгоритма, но решении было найдено в использовании электронной подписи.

ЭЦП (электронная цифровая подпись). При помощи ЭЦП получатель может убедится, что письмо было отправлено не сторонним лицом, а отправителем. ЭЦП создаются путем шифрования контрольных сумм и дополнительной информации при помощи открытого ключа отправителя.

Еще один тривиальный способ ограничения информации от злоумышленника — это аутентификация.

Аутентификация — один из основополагающих способов защиты. Прежде чем пользователь получит доступ к информации, ему необходимо доказать, что он действительно тот, за кого себя выдает. При получении запроса от пользователя на предоставление доступа, сервер аутентификации запрашивает секретное слово

или несколько слов. Чаще всего это бывают «логин» и «пароль». Но есть вероятность, что пароль могут перехватить и воспользоваться им. В этом случае можно использовать криптографическую защиту при передаче пароля, либо генерировать каждый раз новый пароль. Генерация пароля возможна как программными, так и аппаратными средствами.

Последний метод защиты, который мы рассмотрим, — это фильтрация MACи IP-адресов. При использовании этого метода необходимо соблюсти следующие условия:

1) Доверенным устройствам необходимо присвоить статические IP-адреса.
2) Должны быть известны MAC-адреса доверенных устройств.
3) Должен быть маршрутизатор или сервер, на котором будет осуществляется фильтрация.

Если соблюсти это условия, то можно осуществить фильтрование устройств, которые могут осуществлять доступ к внутренней сети или данным. Так же данное решение помогает защититься от многих атак из всемирной паутины.

Область защиты информации стала очень актуальна. Из-за утечки секретных данных в сеть многомиллиардные компании могут оказаться в большом убытке, поэтому они тратят огромные средства для своей защиты. Атаки в сети с каждым годом увеличиваются в геометрической прогрессии. Становится все сложнее защищать информацию, и многие заинтересованные компании сейчас в поиске более эффективных способов защиты. Можно только предположить, что будущее будет еще более информативнее — соответственно возникнет необходимость в изменении политики и способах защиты информации.

Литература

1. *Дансмор Б., Скандьер Т. Справочник по телекоммуникационным технологиям. М: Издательский дом Вильямс, 2017. 630 с.*
2. *Рудакова Е. В. К вопросу об обеспечении безопасности электронного документооборота // Актуальные проблемы социально-гуманитарного и научно-технического знания. 2017. № 1 (10). С. 1–2.*
3. *Рудакова Е. В. Признаки, виды и особенности информационных систем // Духовная ситуация времени. Россия XXI век. 2019. № 3 (18). С. 1–4.*
4. *Столлингс В. Криптография и защита сетей. Принципы и практика. М: Издательский дом Вильямс, 2016. 671 с.*
5. *Столлингс В. Передача данных. СПб: Питер, 2017. 750 с.*
6. *Уэнстром М. Организация защиты сетей Cisco. М: Издательский дом Вильямс, 2017. 768 с.*
7. *Хилл Б. Полный справочник по Cisco. М: Издательский дом Вильямс, 2016. 1068 с.*