Лекция 11. Модель сетевой безопасности

Цель лекции: познакомиться с компьютерными сетями, уровнями модели OSI, стеками протоколов; рассмотреть угрозы безопасности в глобальных сетях, сетевые атаки и защиту данных.

План лекции:

1. Компьютерная сеть. Основные понятия
2. Уровни в модели OSI
3. Стеки протоколов
4. Уязвимость компонентов распределенных АС
5. Угрозы безопасности в глобальных сетях
6. Сетевые атаки и защита данных

Компьютерная сеть (Computer NetWork, net - сеть, и work - работа) - это система обмена информацией между компьютерами. Основная цель: обеспечение пользователям потенциальной возможности доступа к локальным ресурсам всех компьютеров сети.

Компьютерные сети классифицируются по следующим признакам:

- степень географического распространения;
- масштаб производственного подразделения;
- способ управления;
- структура (топология) связей.

По степени географического распространения различают:

- локальные сети (Local Area Network, LAN);
- глобальные сети (Wide Area Network, WAN);
- городские сети (Metropolitan Area Network, MAN).

По топологии связей различают:

- сети с топологией «Общая шина»;
- сети с топологией «Звезда»;
- сети с топологией «Кольцо»;
- сети с древовидной топологией;
- сети со смешанной топологией.

Проблемы взаимодействия компьютеров в сети:

- Согласование сигналов в линиях связи
- Определение правил доступа к среде передачи
- Согласование способов повышения надежности передачи информации
- Определение маршрута передачи информации и способов адресации

Модель OSI

Сетевая модель OSI (The Open Systems Interconnection model) — сетевая модель стека (магазина) сетевых протоколов OSI/ISO. Посредством данной модели различные сетевые устройства могут взаимодействовать друг с другом. Модель определяет различные уровни взаимодействия систем. Каждый уровень выполняет определённые функции при таком взаимодействии.

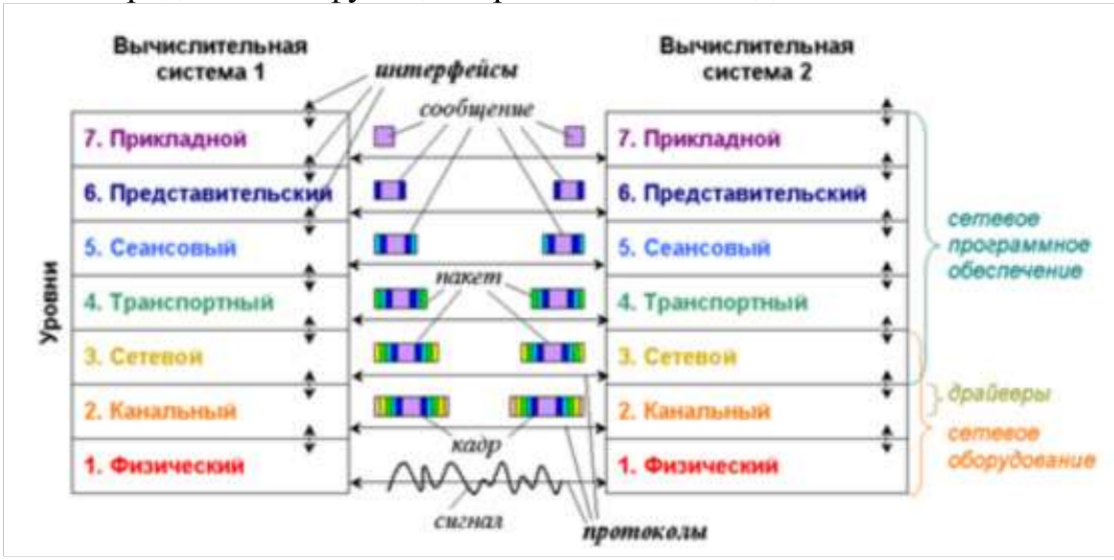

Рисунок 1 Модель OSI

Модель OSI была разработана в конце 1970-х годов для поддержания разнообразных методов компьютерных сетей, которые в это время конкурировали за применение в крупных национальных сетевых взаимодействиях во Франции, Великобритании и США. В 1980-х годах она стала рабочим продуктом группы взаимодействия открытых систем Международной организации по стандартизации (ISO).

Уровни в модели OSI

прикладной	Общий доступ к сети, поток данных, Ex: telnet.
представления данных	Определяет формат для обмена данными (переводчик), перевод данных свыше в общепринятый стандарт, шифрование, смена кодовой таблицы, сжатие данных.
сеансовый	Установление, использование и завершение сеанса связи, распознавание имен и защита, расстановка checkpoints, чтоб в случае неудачной передачи начинать с плохого места, некорректное завершение сеанса.

транспортный	Гарантирует доставку пакетов без ошибок, в той же последовательности, без потерь и дублирования. Переупаковка пакетов: длинные разбиваются, короткие объединяются. Сигнал подтверждения приема.
сетевой	Адресация и маршрутизация в глобальных сетях. На основании конкретных сетевых условий, приоритета услуги определяется маршрут пакета. Коммутация пакетов, маршрутизация, перегрузки. Деление на более мелкие пакеты, если адаптер компьютера не может передавать пакеты поступившей длины. Принимающая сторона их обратно соберет.
канальный	Передача кадров с сетевого в среду передачи (паралл. в послед. и наоборот), иногда спец. кодирование. Кадр содержит: адреса получателя и отправителя, управляющую инфу (данные о верхнем уровне), данные и CRC поле. Сетевой уровень считает передачу данных безошибочной.
физический	Сырой поток битов. Электрический, оптический, механический (разъемы) и функциональный (способ передачи данных) интерфейсы сетевой платы с кабелем. Устанавливается длительность передачи каждого бита и правила перевода его в эл.- и опти-сигналы.

Стеки протоколов

- TCP/IP (Transmission Control Protocol / internet Protocol) - стандарт для гетерогенных сетей, популярный межсетевой протокол, спец. разработанные для него протоколы SMTP, FTP, SNMP. Недостатки - большой размер и неторопливость. Проблемы с нехваткой IP адресов.
- NetBEUI (Network Basic Extended User Interface) - связан с NetBIOS (IBM интерфейс сеансового уровня с ЛВС), а сам NetBEIU - трансп. протокол Микрософта. Небольшой, быстрый, эффективный. Не поддерживает маршрутизацию.
- X.25 - сети с коммутацией пакетов, полное соответствие OSI/RM.
- XNS - Xerox Network System. Большой и медленный, много широковещательных пакетов.
- IPX/SPX и NWLink (реализация от Microsoft) - наследник XNS, небольшой и достаточно быстрый.
- DECnet - собственный стек маршрутизируемых протоколов, на нем впоследствии вырос И-нет, т.к. он ставился на VAX (Virtual Address Extension) машины с операционной системой VMS.
- Набор протоколов OSI

Сетевая безопасность — прикладная научная дисциплина, отрасль информатики, которая занимается вопросами обеспечения информационной безопасности компьютерной сети и её ресурсов, в частности,

хранящихся в ней и передающихся по ней данных и работающих с ней пользователей.

Система сетевой безопасности — это комплекс мер, направленных на поддержание удобства использования и защиту целостности сети и данных.

- Она использует аппаратные и программные технологии
- Она борется с различными угрозами
- Она блокирует их проникновение и распространение в сети
- Эффективная система сетевой безопасности управляет доступом к сети.

Уязвимость компонентов распределенных АС

В общем случае ЛВС состоит из следующих основных структурно-функциональных элементов:

- рабочих станций;
- серверов;
- межсетевых коммуникационных узлов (шлюзов, мостов, маршрутизаторов);
- каналов связи.

Рабочие станции считаются наиболее доступными компонентами сетей и именно с них могут быть предприняты наиболее многочисленные попытки совершения несанкционированных действий.

С рабочих станций осуществляется управление процессами обработки информации, запуск программ, ввод и корректировка данных, на дисках рабочих станций могут размещаться важные данные и программы обработки.

Серверы и коммуникационное оборудование нуждаются в особой защите, поскольку наиболее привлекательны с точки зрения злоумышленников. Первые — как концентраторы больших объемов информации, вторые — как элементы, в которых осуществляется преобразование (возможно через открытую, нешифрованную форму представления) данных при согласовании протоколов обмена в различных участках сети.

Каналы связи, в силу большой пространственной протяженности через неконтролируемую или слабо контролируемую территорию, представляют возможность как прямого подключения к ним, так и вмешательства в процесс передачи данных.

Угрозы безопасности в глобальных сетях

Атаки типа «отказ в обслуживании» (denial of service, DoS). Под этим названием объединены методы, призванные расстроить работу некоторого сетевого устройства путем перегрузки какого-либо ограниченного ресурса,

отказа устройства, изменения его настроек. Ограниченными ресурсами являются оперативная память, емкость жесткого диска, процессорное время. Типичная DoS атака представляет собой генерацию большого потока сетевых пакетов, которые не успевают обрабатываться сетевыми серверами, что приводит либо к отказам в их работе, либо к невозможности обрабатывать запросы обычных пользователей.

Очень распространенными являются *атаки с использованием протокола ICMP*. Протокол управляющих сообщений ICMP (Internet Control Message Protocol) носит вспомогательный характер (популярная утилита ping использует этот прото-кол).Протокол ICMP не содержит методов аутентификации источника сообщения, что активно используется злоумышленниками. Например, для блокировки обслужи-вания используются icmp-сообщения “time exceeded” (превышено время) или “destination unreachable” (адресат недоступен). Первое сообщение означает, что предел, указанный в поле TTL заголовка пакета, превышен. Такое может произойти из-за зацикливания пакетов или когда адресат расположен очень далеко.

Популярными являются также *атаки на серверы некоторых сетевых служб (*Web, mail), когда из-за ошибок в программном обеспечении запросы определенной конфигурации способны вызвать ошибки типа переполнение буфера, предоставить злоумышленнику доступ с правами администратора.

Важным аспектом безопасности является обеспечение конфиденциальности сетевого трафика, поскольку пакеты сообщения могут быть перехвачены на любом промежуточном узле по пути следования к получателю, а встроенных средств шифрования классический протокол IP не предоставляет.

Глобальная сеть является благоприятной средой для распространения вирусов и «троянских коней». Развитие Интернет привело к появлению такого феномена как вирусы – черви. Остановимся подробнее на сетевом черве Klez. Этот экземпляр заражает компьютер через ошибку в почтовой программе Outlook: когда пользователь пытается прочитать письмо, содержащее вирус, Klez инфицирует систему. После попадания в ОС сетевой червь сканирует жесткие диски, ищет электронные адреса и рассылает на них письма, прикрепляя свое тело в качестве вложения, создавая очень большой исходящий трафик. Таким образом, скорость распространения сетевого червя становилась очень высокой.

Сетевые атаки

- сбор информации
  - изучение сетевой топологии,
  - определение типа и версии ОС атакуемого узла,
  - доступных сетевых сервисов
- выявление уязвимых мест атакуемой системы
  - анализ наличия уязвимостей в ПО и его настройках

- реализация выбранной атаки
  - отправка сетевых пакетов на определенные сетевые службы
  - SYN Flood, Teardrop, UDP Bomb, подбор паролей

Исследование сетевой топологии

- ICMP-сканирование
  - команда ECHO_REQUEST протокола ICMP
  - ответное сообщение ECHO_REPLY
- TCP-сканирование
  - последовательная установка сетевого соединения по определенному порту с перебором IP-адресов

Система межсетевой защиты, позволяющая разделить общую сеть на две части и более и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. (Firewall, брандмауэр).

Защита сетей с использованием межсетевых экранов. Стандартные требования:

- К Web-серверам организации должен быть разрешен доступ из Интернет
- В организацию должна приходить почта
- Из внутренней сети должен быть разрешен доступ к внешним Web- и FTP-серверам
- Необходимо разрешить отправлять исходящую почту

Протокол защитной оболочки (SSH - Secure Shell protocol) использует окрытый ключ для создания соединения и проведения авторизации. Используется для безопасного удалённого доступа к компьютеру, а также для передачи данных при помощи SFTP (Secure File Transfer Protocol) протокола.

Honeypot - это информационная система, предназначенная для неправомерного доступа. Фактически это обманка, привлекательный объект для атаки, при этом находящийся под полным контролем специалистов по безопасности. Информационная система honeypot может представлять собой как отдельный хост в сети, так и сеть, наполненную разного рода объектами: маршрутизаторами, серверами, рабочими станциями, реальными или виртуальными.

План защиты сети должен состоять из следующих структурных элементов:

- описание способов профилактики и устранения последствий атак на корпоративную сеть;
- применяемые базовые принципы защиты информации;
- методы моделирования угроз;
- описание ответных действий при атаке;
- описание процедуры аварийного восстановления;

- описание сетевых сегментов.

При разработке плана защиты около 30 процентов времени необходимо выделять моделированию угроз. В конечном итоге это снизит риск уязвимости системы. Процесс моделирования угроз необходимо проводить следующим образом:

1. сформировать команду по моделированию (в нее должны входить специалисты, имеющие опыт работы с внедряемым оборудованием и программным обеспечением);
2. использовать данные анализа, проведенного на предыдущих этапах построения концептуального плана защиты (на этой стадии выявляются недостатки собранной и разработанной к данному моменту документации);
3. поиск угроз (обсуждаются и прорабатываются все высказанные варианты атак с указанием степени их опасности и разработкой плана реакции на каждую из угроз);
4. выбор механизмов и методов предотвращения смоделированных угроз (при выборе технических средств необходимо учитывать их совместимость с уже имеющимися в корпоративной сети устройствами и программами. После проведения аудита имеющихся систем необходимо иметь список их технических ограничений для того, чтобы можно было в полной мере использовать возможности нового оборудования и программ и во избежание конфликтов новых систем с уже имеющимися).

Средства обеспечения сетевой безопасности

- Межсетевые экраны
- Защита электронной почты
- Антивирусы и программы для защиты от вредоносного ПО
- Сегментация сети
- Управление доступом
- Безопасность приложений
- Поведенческая аналитика
- Предотвращение утечки данных (DLP)
- Системы предотвращения вторжений (IPS)
- Управление событиями и данными об информационной безопасности (SIEM)
- Сеть VPN
- Безопасность веб-трафика
- Безопасность беспроводного доступа

Модель безопасного сетевого взаимодействия в общем виде можно представить следующим образом:

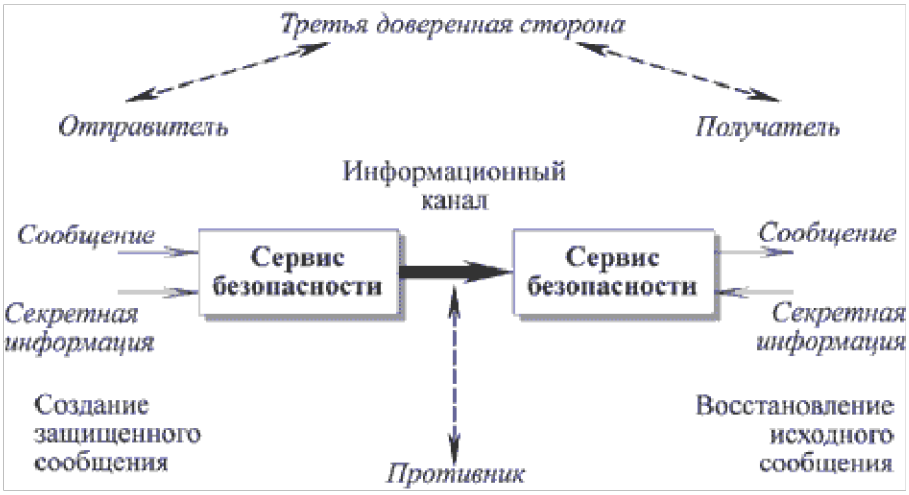

Рисунок 2 Модель сетевой безопасности

Сообщение, которое передается от одного участника другому, проходит через различного рода сети. При этом будем считать, что устанавливается логический информационный канал от отправителя к получателю с использованием различных коммуникационных протоколов (например, TCP/IP).

Средства безопасности необходимы, если требуется защитить передаваемую информацию от противника, который может представлять угрозу конфиденциальности, аутентификации, целостности и т.п. Все технологии повышения безопасности имеют два компонента:

Относительно безопасная передача информации. Примером является шифрование, когда сообщение изменяется таким образом, что становится нечитаемым для противника, и, возможно, дополняется кодом, который основан на содержимом сообщения и может использоваться для аутентификации отправителя и обеспечения целостности сообщения.

Некоторая секретная информация, разделяемая обоими участниками и неизвестная противнику. Примером является ключ шифрования.

Кроме того, в некоторых случаях для обеспечения безопасной передачи бывает необходима третья доверенная сторона (third trusted party - TTP). Например, третья сторона может быть ответственной за распределение между двумя участниками секретной информации, которая не стала бы доступна противнику. Либо третья сторона может использоваться для решения споров между двумя участниками относительно достоверности передаваемого сообщения.

Из данной общей модели вытекают три основные задачи, которые необходимо решить при разработке конкретного сервиса безопасности:

- Разработать алгоритм шифрования/дешифрования для выполнения безопасной передачи информации. Алгоритм должен быть таким, чтобы противник не мог расшифровать перехваченное сообщение, не зная секретную информацию.

- Создать секретную информацию, используемую алгоритмом шифрования.
- Разработать протокол обмена сообщениями для распределения разделяемой секретной информации таким образом, чтобы она не стала известна противнику.

Список использованной литературы

1. Adam Shostack. “Threat Modeling: Designing for Security”. Published by John Wiley & Sons, Inc., Canada 2014.- 626 p.
2. Richard Bejtlich. “The Practice of Network Security Monitoring”. Published by No Starch Press, Inc., USA 2013. – 380 p.
3. Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams and Abdul Aslam. “Enterprise Cybersecurity: how to build a successful Cyberdefense program against advanced threats”. Published by Apress, 2015. – 508 p.
4. Хорев А. А. Организация защиты конфиденциальной информации в коммерческой структуре // Защита информации. Инсайд : журнал. — 2015. — № 1. — С. 14—17. — ISSN 2413-3582
5. Carl A. Sunshine. Computer Network Architectures and Protocols. — Springer Science & Business Media, 2013-06-29. — 542 с. — ISBN 978-1-4613-0809-6.
6. Keith Shaw. The OSI model explained and how to easily remember its 7 layers (англ.). Network World (14 October 2020). Дата обращения: 1 ноября 2021.