



# Тема: Методы и средства удаленного доступа

СТУДЕНТ: АБДУРЗАКОВ Т.М.

РУКОВОДИТЕЛЬ: ЗАКРИЕВ З.И.

**Актуальность** безопасности передаваемых данных и их защиты от несанкционированного доступа в системах удаленного доступа требует особенно пристального внимания и применения специальных методик, которые гарантировали бы достаточную конфиденциальность и достоверность данных. В противном случае, хакер, подключившийся в качестве удаленного клиента или перехватывая трафик реально существующего клиента, сможет украсть данные являющиеся коммерческой тайной или фальсифицировать их.

- **Цель дипломной работы** изучить методы и средства удаленного доступа.
- **Задача, решаемая данной работой связана с рассмотрением:**
  - проанализировать и исследовать существующие способы обеспечения безопасности работы в системах удаленного доступа;
  - выработать рекомендации по выбору конкретного способа.

# Методы и средства удаленного доступа

- Под средствами удаленного доступа понимаются средства, необходимые для связи небольших локальных сетей и даже удаленных отдельных компьютеров с центральной локальной сетью предприятия. В качестве отдельных удаленных узлов могут также выступать банкоматы или кассовые аппараты, требующие доступ к центральной базе данных о легальных клиентах банка, пластиковые карточки которых необходимо авторизовать на месте.

# Терминальный доступ

**Терминальный доступ** — доступ к информационной системе (ИС), организованный так, что локальная машина-терминал не выполняет вычислительной работы, а лишь осуществляет перенаправление ввода информации (от мыши и клавиатуры) на центральную машину (терминальный сервер) и отображает графическую информацию на монитор. Причем вся вычислительная работа в терминальной системе выполняется на центральной машине.

# Удаленный узел

Одним из вариантов удаленного доступа типа компьютер - сеть является режим удаленного узла (remote node). Программное обеспечение удаленного узла на клиентской машине позволяет последовательному порту и модему (или терминальному адаптеру ISDN) стать медленным узлом удаленной локальной сети, взаимодействующим обычным способом с сетевыми операционными системами при разделении их ресурсов.



# Удаленный доступ к exchange 2003 по каналам HTTP

- Новая возможность Outlook 2003 для доступа к почтовому ящику Exchange. Благодаря сочетанию Microsoft Outlook 2003, Windows Server 2003 и Microsoft Exchange Server 2003 открываются новые возможности для подключения клиента Outlook 2003 к Exchange 2003 по каналам HTTP. Соединение не просто использует HTTP: Outlook заключает вызов удаленных процедур (RPC) к Exchange 2003 в оболочку HTTP, обеспечивая соединение локального клиента Outlook 2003 с удаленным сервером Exchange 2003 с любой машины.

# Протокол SLIP

SLIP (Serial Line Internet Protocol) — устаревший сетевой протокол канального уровня эталонной сетевой модели OSI для доступа к сетям стека TCP/IP через низкоскоростные линии связи путём простой инкапсуляции IP-пакетов. Используются коммутируемые соединения через последовательные порты для соединений клиент-сервер типа точка-точка. В настоящее время вместо него используют более совершенный протокол PPP. SLIP был разработан в начале 80-х компанией 3COM.

# Протокол PPP

Основная функция программного обеспечения SLIP/PPP - организовать пересылку IP -пакетов по последовательной линии, которая не предусматривает деления пересылаемой информации на какие-либо отдельные блоки и пересылает все данные единым непрерывным потоком. SLIP/PPP как раз и занимается организацией такой пересылки, чтобы на другом конце можно было этот сплошной и непрерывный поток данных разделить на составляющие его IP -пакеты, выделить их и передать дальше уже как IP –пакеты.



# Протоколы защищенных каналов SSL, PPTP, ipsec

- Протокол PPTP позволяет создавать защищенные каналы для обмена данными по различным сетевым протоколам — IP, IPX или NetBEUI. Данные этих протоколов инкапсулируются с помощью протокола PPTP в пакеты протокола IP, с помощью которого переносятся в зашифрованном виде через любую сеть TCP/IP. Инкапсулируется исходный кадр PPP, поэтому протокол PPTP можно отнести к классу протоколов инкапсуляции канального уровня в сетевой.

# **Усугубление проблем безопасности при удаленном доступе**

Обеспечение безопасности данных при удаленном доступе - проблема если и не номер один, то, по крайней мере, номер два, после проблемы обеспечения приемлемой для пользователей пропускной способности. А при активном использовании транспорта Internet она становится проблемой номер один.

# Настройка клиента

Некоторые изменения требуется внести и в профиль Messaging API (МАPI), чтобы позволить клиенту Outlook 2003 установить связь с сервером по HTTP. Если у пользователя уже имеется профиль MAPI, то доступ к его свойствам можно получить, выбрав соответствующий профиль MAPI в утилите Mail панели управления. Нужно выбрать пункты Change, More Settings, а затем перейти к вкладке Connection. Затем следует установить флажок Connect to my Exchange mailbox using HTTP и щелкнуть на кнопке Exchange Proxy Settings, чтобы завершить настройку конфигурации.

# Безопасные соединения

Соединения RPC over HTTP желательно устанавливать по каналам SSL, избегая незащищенных линий. В рекомендуемой конфигурации ретрансляционный прокси-сервер HTTP (ISA Server) завершает любые клиентские SSL-соединения и устанавливает отличные от SSL соединения с прокси-сервером RPC. Для этого необходимо установить серверный сертификат на ретрансляционном посреднике HTTP.

# Ограничение соединений RPC-посредника

Диапазон портов проху-сервера RPC определяет область функционирования RPC over HTTP. Однако можно явно назначить порты, которые будут использоваться каждым сервером — участником соединений RPC over HTTP. Следует обратить внимание, что в бета-версиях Exchange 2003 в разделе реестра ValidPorts можно указать принимаемый по умолчанию диапазон 1024-65535, и любые внутренние серверы или GC будут динамически выбирать рабочие порты в этом диапазоне без дополнительной настройки. Из версии Release Candidate 0 эта функция удалена.



# Заключение

Для того чтобы обеспечить доступ к услугам локальной сети при отсутствии непосредственного подключения к ней, служат средства удаленного доступа к сети. Эти средства используют для связи удаленного (то есть не имеющего непосредственного подключения к локальной сети) компьютера с сетью коммутированные линии телефонных сетей общего пользования, аналоговые выделенные линии.

The background is a blue gradient. In the corners, there are decorative white lines resembling circuit traces or a stylized city skyline, with small circles at the end of the lines.

**Спасибо за внимание**