УДАЛЕННЫЕ УЧЕБНЫЕ РАБОЧИЕ МЕСТА НА ОСНОВЕ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

М.П. Ревотюк, Р. Хормози

Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь, rmp@bsuir.by

Abstract. Plug-in technology of distance learning process support system on virtual privacy network and electronic mail standard channels frame was presented.

Учебный процесс традиционно предполагает интерактивное взаимодействие студента и преподавателя при проведении лабораторных и практических занятий. При этом исполнение задания прерывает диалог до момента его исполнения, после чего проводится этап оценивания работы. В случае дистанционной формы обучения возникает ряд проблем, порождаемых физическим отсутствием обучаемого на рабочем месте преподавателя. Сюда можно отнести сложность построения системы синхронизации деятельности студента и преподавателя, необходимость освоения ими такой системы. В большинстве случаев преподаватель и студент обладают лишь доступом к персональной универсальной ЭВМ. Наличие на домашней ЭВМ студента программного обеспечения лабораторного практикума не избавляет от необходимости взаимодействия с преподавателем, например, для консультаций по системным вопросам.

Технологический процесс прохождения дисциплины допускает и практически всегда предусматривает разбиение на контролируемые этапы. Объект рассмотрения – технология создания удаленных учебных рабочих мест, автоматически связывающих не только электронные версии документов заданий и отчетов по этапам учебной работы, но и промежуточные результаты их подготовки. Основа рассматриваемой технологии – виртуальные частные сети (Virtual Privacy Network, VPN).

Технология VPN – надежный канал связи в распределенных системах, требующих реализации взаимодействия в реальном времени в рамках открытых сеансов. Современные операционные системы, как правило, предусматривают поддержку VPN, но при этом его стандартная конфигурация включает дополнительную аппаратуру, а настройка требует нетривиального администрирования. Однако в последнее время доступны средства виртуализации даже VPN. Например, к таким средствам относится Hamachi – программное обеспечение для построения VPN поверх Интернета [1], доступное бесплатно для некоммерческого использования.

Любые приложения, которые работают через локальную сеть, могут работать через сети Hamachi. При этом передаваемые данные защищены стандартными средствами обмена между приложениями в стиле “точка-точка”. Hamachi организует VPN на основе протокола UDP. В такой сети узлы для установления соединения между собой используется третий узел, а передача информации производится непосредственно между узлами. Взаимодействующие узлы могут находиться за NAT или фаерволом. Возможна организация VPN со шлюзом, с топологией «звезда» и ячеистых сетей. Последний вариант позволяет быстро соединять удаленные компьютеры непосредственно друг с другом, предоставляя пользователям базовый сетевой доступ ко всем необходимым сетевым ресурсам без дополнительного оборудования. Для этого необходимо лишь провести установку программного обеспечения клиента сетей Hamachi, загружаемого с сайта фирмы LogMeIn, указав идентификаторы VPN и компьютера пользователя для логической адресации в VPN.

Сервис сети Hamachi представлен драйвером виртуального сетевого устройства с отдельным адресом, который во включенном логически состоянии обеспечивает

стандартный сетевой интерфейс доступа к зарегистрированным компьютерам VPN. Базовый сетевой доступ позволяет получить доступ к рабочему столу удаленного компьютера и открытым для общего доступа другим ресурсам. Управление доступом на этом уровне выполняется стандартными средствами локального администрирования в рамках выбранных пользователем и администратором политик безопасности.

Учитывая, что действия локального администратора инварианты к пользователю, предлагается привязать их к графику прохождения дисциплины, и автоматизировать рутинные операторные действия. При этом инициатором процесса является запрос пользователя по электронной почте процедуры автоматической установки клиента VPN с назначенными параметрами. Основой защиты электронной почты является использование сертифицированных несимметричных криптосистем [2].

Укрупненная объектная модель организации защищенного канала типа “точка-точка” представлена на рисунке 1 в терминах расширенных сетей Петри.

Доставка информации от отправителя А получателю В реализуется по стандартным правилам несимметричной криптосистемы. Субъекты А и В предварительно генерируют личные ключи KA, KB и обмениваются открытыми ключами PA, PB. Отправитель А порождает зашифрованное письмо I(A,B), предъявив личный ключ KA. Получатель В выбирает и расшифровывает письмо в произвольный момент, предъявив личный ключ KB. Фильтрация писем на стороне получателя производится на основе соответствия их сигнатур множеству открытых ключей. Так как возможно скрытие шифрованием и пути доставки от А до В (назначаемого системой), то адресные параметры раскрываются только после предъявления личного ключа.

Переходы А и В расширенной сети Петри – инсталлируемые и частично хранимые на носителе ключа оконечные компоненты виртуального канала. Их программная реализация шаблонами полиморфных классов позволяет интегрировать приемы защиты программного кода операций транспортного уровня, а также автоматизировать действия пользователей по организации как обмена [3], так и построению VPN.

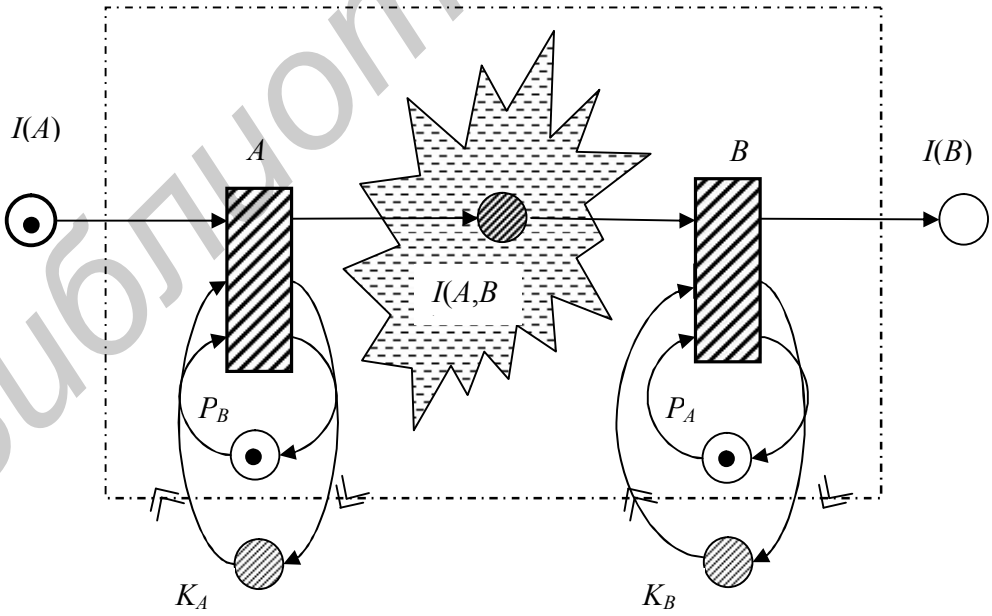

Рисунок 1 - Модель виртуального канала защищенной передачи документа.

Почтовый сервер является посредником для транспортировки зашифрованных сообщений, реализуя функции буферизации и синхронизации. Одним из приемов

скрытия канала обмена является минимизация интервала его доступности для реализации угроз раскрытия пароля. Предлагается все адресную информацию, касающуюся установления связи, хранить в зашифрованном виде, а расшифровку выполнять на стороне сервера и клиента лишь при выявлении потребности в приеме или передачи сообщений. При этом выбор и установка адресных параметров может быть автоматизирован и выполняться в момент инсталляции прикладной системы [2,3].

Необходимость установления персонифицированной связи “преподаватель-студент”, очевидно, может быть реализована даже на единственной учетной записи некоторого почтового сервера. В качестве места хранения адресных параметров удобно использовать носитель закрытого ключа несимметричной криптосистемы. Другой альтернативой может быть дополнение записей сертификата PKI [3]. Основанием подобного выбора является потребность наличия носителя либо доступа к хранилищу сертификатов непосредственно перед операциями обмена.

В конкретной прикладной системе набор типов передаваемых сообщений ограничен, поэтому несложно организовать фильтрацию таких сообщений в почтовых ящиках. В качестве надежного ключа достаточно использовать идентификаторы пользователей в сертификатах. Использование SSL предполагает наличие доступа к хранилищу сертификатов всех субъектов обмена. Удаление спама легко организуется по инициативе получателя по принципу “свой-чужой”.

Каждый документ соответствует позиции в схеме технологического процесса прохождения дисциплины. Такую схему удобно рассмотреть в терминах диаграмм потоков работ, тогда для автоматизации контроля процесса можно предложить подход, применяемый для моделирования поведения расширенной сети Петри (рисунок 1). Операции приема и передачи документов могут выполняться автоматически как реагирование на факт предъявления файла входного документа.

В среде Windows 2000/XP/2003 и их более поздних версиях съемные носители могут, как известно, обслуживаться в режиме автозапуска: подключение носителя, содержащего файл AutoRun.inf автоматически порождает порождение предопределенного процесса. Безопасность такой технологии гарантирована возможностью установки запрета ключами реестра NoDriveAutoRun и NoDriveTypeAutoRun. Таким образом, преподаватель и студент переходят в рабочий режим после физического подключения съемного носителя к разъему USB.

Результат работы – объектно-ориентированная реализация средствами шаблонов классов языка C++ итератора распределенной прикладной системы с каналом двустороннего защищенного обмена между обладателями ключей несимметричной криптосистемы в форме исполняемого модуля, оснащенного средствами самозащиты от известных угроз взлома программного обеспечения.

Литература

1. Функции LogMeIn Hamachi[Электрон. Ресурс]/LogMeIn, Inc., 2003-2011 – Режим доступа: https://secure.logmein.com/RU/products/hamachi/features.aspx

2. Ревотюк, М.П. Шаблоны систем обеспечения безопасности разрабатываемых программ в вычислительных средах с открытой архитектурой/ М.П. Ревотюк//Компьютерные технологии в обеспечении безопасности электронной информации: Мат. междунар. конф. (Минск, 4-9 ноября 2002 г.) – Мн.: БелИСА, 2002. – С. 107-117.

3. Жолудев, Н.Н. Защита прикладных процессов в распределенных системах на основе Windows 2000/XP/2003/Н.Н.Жолудев, М.П.Ревотюк, Ю.М.Ревотюк//Материалы XI Междунар. конф. “Комплексная защита информации”(Новополоцк, 20-23 марта 2007 г.) – Мн.: Амалфея, 2007. – С.99-102.