УДК 004.45

ТЕРМИНАЛЬНАЯ СИСТЕМА WTPRO: АРХИТЕКТУРА, ФУНКЦИОНАЛЬНОСТЬ, СХЕМА ПРИМЕНЕНИЯ

С.А. Рожков

TERMINAL SYSTEM WTPRO: ARCHITECTURE, FUNCTIONALITY, APPLICATION CIRCUIT

S.A. Rozkhov

В последнее время возрос интерес к терминальным системам. Во многих компаниях накоплен обширный парк компьютерной техники, как правило, морально устаревшей, но технически исправной. Чрезмерная требовательность к аппаратным ресурсам со стороны, например, Windows Vista, требует замены техники. Однако, для офисной работы, имеющиеся средства пригодны. С другой стороны, применение терминалов позволит централизовать управление сетью, что позволит проводить единую политику в области информационной безопасности и не допустить установку вредоносного кода, который может быть внесен недобросовестными или беспечными пользователями рабочих станций. В-третьих, терминальные системы позволяют снизить лицензионные отчисления за использование программного обеспечения. В статье описывается компактная система для работы в тонких клиентах, созданная автором статьи.

Ключевые слова: тонкий клиент, сетевая загрузка, терминал, безопасность, Linux, Windows.

An interest to terminal system increases at the last time. There are a fleets of obsolete computers in many firms. But they are technicaly in a good repare. The unreasonable demand of Windows Vista to apparatus resourse demands to change this technic. But it is enough for work at the office. On the other hand using of terminal systems allows to centralize net-administration. It allows to conduct united politic of informatiom security and doesn't allow a putting of harmful code, that can be brought in by the careless users At thirds the using of terminat systems allows to pay not so high assigments for programs. Text runs about using of think clients, created by the auther of article.

Keywords: thin client, netboot, terminal, security, Linux, Windows.

Введение

WTPRO - терминальный клиент для подключения к Windows и Unix серверам. Он не требует операционной системы и жесткого диска. В настоящее время эта разработка используется в более чем ста организациях на территории бывшего СССР. Получены свидетельства авторские и об отраслевой регистрации разработки [1, 2-5]. Создан и поддерживается сайт http://www.WTPRO.ru. Разработка отражена в монографической литературе [6].

Терминалом называется устройство ввода и отображения информации. По сути дела - это бездисковая (без HDD-дисковая) рабочая станция, загрузка которой осуществляется по сети. На сервер с клиента передаются нажатия клавиш и движения мыши. Обратно приходят снимки экрана. Все прикладные программы выполняются на терминальном сервере, но для пользователя все выглядит так, как если бы компьютер с такой же вычислительной мощностью, как сервер стоял у него на столе.

1. Схема применения

Выделяется сервер. Сервером может быть обычная рабочая станция с большим объемом оперативной памяти. На сервер устанавливается операционная система и все необходимые пользователю программы. Клиентскими машинами могут быть как специализированные тонкие клиенты, так и обычные морально устаревшие компьютеры. На клиентах отсутствуют жесткие диски, а загрузка операционной системы происходит по сети.

Настройка WTPRO производится через web-интерфейс. Возможно также использование Windows-утилиты для редактирования файла конфигурации.

Чаще всего WTPRO применяют:

• для создания мобильного офиса. В этом случае сервер находится на ноутбуке, а в качестве терминалов используются доступные в данный момент компьютеры. Развернуть подобный учебный класс или мобильный офис можно за считанные минуты;

Рожков Сергей Александрович аспирант ЮУрГУ; zserg@zserg.ru

Rozkhov Sergey Aleksandrovich - postgraduate student of SUSU; zserg@zserg.ru

• организации учебных классов. Используется один мощный сервер, который обновляется, в случае необходимости. Терминальные клиенты, в силу нетребовательности к их ресурсам, обновлять не нужно. Преподаватель имеет возможность со своего рабочего места общаться с учеником;

• организации презентаций. Не всегда есть возможность демонстрировать презентации на большом экране. Но если есть компьютерный класс, то можно вывести изображение на все компьютеры в классе;

• развертывания операторных залов. Организация рабочих мест для большого числа пользователей, работающих с одним набором ПО;

• организации работы бухгалтерии или отдела кадров и т.д.

Минимальные системные требования для работы терминальной системы WTPRO:

• процессор: i486;
• Оперативная память:
- 6 Mb - без графического режима,
- 8 Mb - без перенаправления устройств,
- от 12 Mb - с перенаправлением устройств,
- от 16 Mb - с библиотекой Xwindow;
• Видеокарта VGA, монитор;
• Клавиатура, мышь;
• Сетевая карта.

2. Архитектура

WTPRO поддерживает четыре терминальных протокола - два текстовых:

• telnet - небезопасный протокол, позволяет перехватить имя пользователя и пароль,

• ssh - защищенный аналог telnet

и два графических:

• RDP - удаленный рабочий стол Windows,

• VNC - открытый протокол для доступа как к Windows, так и к ТЖГХ-серверам [8].

Основной сложностью при разработке программного комплекса был компромисс для выполнения двух противоречивых требований:

• Необходимо поддерживать большое количество оборудования.

• Размер комплекса должен быть небольшим. Чтобы поместиться в оперативную память даже морально устаревших машин.

Для экономии оперативной памяти основная программа RDP, которая служит для подключения к терминальным серверам, была разбита на несколько модулей:

• RDP - содержит графическую подсистему, которая обеспечивает видеовывод, обработку операций мыши и клавиатуры;

• librdesktop.so - библиотека, основанная на коде проекта rdesktop, для доступа к функциям протокола rdp;

• libvnc.so — библиотека, основанная на открытых реализациях протокола vnc, предоставляет доступ к функциям протокола vnc;

• libscard.so - библиотека, основанная на патче Алексея Волкова [16] к программе rdesktop для поддержки перенаправления на сервер смарт-карт;

• xrdp - аналог программы RDP, использующей библиотеку видеовывода xorg.

В WTPRO использует три вида драйверов для видеовывода.

Svgalib - облегченная библиотека, рекомендуется для использования на слабых машинах. Поддерживает не все видеокарты, а некоторые современные работают некорректно.

FrameBuffer - данные видеодрайвера включены в ядро Linux. Для своей работы требуют больший объем оперативной памяти, рекомендуется использовать в том случае, если драйвера svgalib работают некорректно.

Xorg - наиболее ресурсоемкая библиотека, хорошо работает с современными видеокартами на машинах с объемом оперативной памяти от 16 Mb.

Так как терминал должен эмулировать полноценную рабочую станцию, то необходимо передавать на сервер не только нажатия клавиш и движения мыши, но и действия локальных устройств: CD-ROM, дисководов, принтеров и т.д.

Рассмотрим, какие возможности поддерживает WTPRO для перенаправления устройств.

CDROM. Перенаправление локально установленного привода для чтения компакт дисков осуществляется средствами протокола RDP, который, начиная с Windows 2003, поддерживает перенаправление дисков. Проблема перенаправления данного привода заключается в следующем. В Windows при вставке компакт-диска в привод CD-ROM происходит автоматическое монтирование (подключение) данного диска, в результате чего он становится доступным пользователю. В UNIX системах принято, что пользователь вручную монтирует необходимые ему устройства. Вторая сложность заключается в том, что пользователь Windows может в любое время извлечь компакт диск, а пользователь UNIX не имеет такой возможности, поскольку при монтировании компакт диска кнопка для извлечения дисков блокируется программно. Для решения этих задач был написан демон (сервис в терминологии Windows), который каждые 5 секунд проверяет статус привода компакт дисков. Если статус изменился на «CDSDISCOK» и тип диска определен как диск с данными, то пробуем примонтировать сначала его как CD-диск, а в случае неудачи как DVD-диск. Для того чтобы можно было извлечь примонтированный компакт-диск вызываем функцию ядра ioctl (cd, CDROMJLOCKDOOR, 0), которая запрещает блокировку клавиши извлечения диска. Если статус привода изменился на CDSNOINFO, CDS_NO_DISC, CDS_TRAY_OPEN или CDS_DRIVE_NOT_READY, то отмонтируем подключенную файловую систему.

Дисковод. Перенаправление дисковода реализовано аналогично перенаправлению CD-ROM. Различия состоят в том, что дискета может быть

доступна не только для чтения, но и для записи. В силу этого нужен способ для записи данных без стандартного ручного монтирования. Второй сложностью является то, что опрашивать дисковод каждые N секунд нерационально, так как дисковод не имеет состояний как CD-ROM. У дисковода доступно только два состояния - данные читаются и данные недоступны. В любом случае при доступе к дисководу производится шум, а непрерывное гудение дисковода не понравится пользователю. Поэтому было решено использовать патч к ядру supermount. Этот патч позволяет один раз примонтировать устройство и в дальнейшем, только при обращении к каталогу, в который примонтировано устройство, обращаться к этому устройству. В отличие от стандартного монтирования данные, которые пишутся на устройство, не кэшируются, а сразу записываются, что исключает потерю информации при извлечении дискеты. Пример для монтирования дисковода

```
mount –t supermount –o fs=vfat,
dev=/dev/floppy/0,-,nosuid,nodev,noexec,
noatime none /ram/mnt/floppy.
```

Локальные диски. Если на терминале находится локальный жесткий диск, то можно использовать и его. Для этого используется стандартное монтирование при старте системы. Bash-скрипт просматривает доступные диски и пытается их примонтировать стандартным способом.

Flash диски. При монтировании flash-дисков основной проблемой является сохранность данных при извлечении диска из системы. Эта проблема решена аналогично задаче с дисководом. Следующей сложностью является автоматическое монтирование flash-дисков. В данном случае нельзя использовать алгоритм как в случае с локальными дисками, потому что внутренне имя flash-диска в ОС LINUX постоянно меняется при подключении и отключении устройства. Для решения этой задачи был написан основанный на devfsd демон [8]. Devfs - виртуальная файловая система, которая динамически создает файлы устройств при их подключении и удаляет их после отключения. В ядрах Linux, начиная с 2.6.13 поддержка devfs удалена, вместо этого рекомендуется использовать файловую систему udev, которая выполняет аналогичные функции, но не на уровне ядра, а на уровне пользовательского приложения. Эта файловая система довольно медлительна (на компьютере Pentium 100 создание устройств занимает около трех минут). Поэтому мною ведется поддержка devfs в современных ядрах. Написанный devfs-демон реагирует на создание нового устройства определенного типа и монтирует данные с него.

Звук. Перенаправление звука реализовано средствами rdp-протокола.

Смарт-карты. Перенаправление осуществляется средствами протокола RDP. Так как поддержка смарт-карт ресурсоемкая задача, то библиотека для доступа к функциям смарт-карт была вынесена из библиотеки librdesktop.so. Если в файле конфигурации указано, что необходимо использовать перенаправление смарт-карт, то с сервера загружаются необходимые приложения и библиотеки. Запускается поддержка смарт-карт, и библиотека librdesktop.so динамически подключает библиотеку libscarcLso.

COM-порты. В настоящее время перенаправление COM-портов реализовано двумя способами: средствами протокола RDP, средствами дополнительного сервиса. В протоколе RDP перенаправление портов реализовано не полностью, например подключиться к интернету, используя модем, подключенный к COM-порту терминала не получится. Дополнительный сервис прослушивает TCP порт на терминале? При поступлении команд на этот порт они перенаправляются в com-порт, в результате большинство устройств на этом порту работают корректно.

Принтеры. В первых версиях WTPRO использовалось перенаправление принтера средствами RDP протокола, но оно имело ряд минусов. Принтер был доступен только при подключении к терминальному серверу. Для подключения принтера необходимо обладать правами администратора. При каждом новом подключении к терминальному серверу необходимо было его переподключать. Поэтому было решено использовать эмуляцию аппаратного принт-сервера от HP.

Аппаратный принт-сервер работает так:

- прослушивается tcp-порт;
- в этот порт поступают «сырые» данные для принтера;
- данные перенаправляются напрямую в устройство.

Для корректной работы принтера достаточно установить стандартные Windows-драйвера на сервер. При использовании этого способа не будут работать «win-принтеры». То есть принтеры, которые не имеют драйверов в стандартной поставке и не работающие под DOS.

3. Этапы загрузки терминальной системы

На первом этапе запускается программа, прошитая в загрузочный образ сетевой карты. Эта программа отправляет запрос по протоколу BOOTP/DHCP и узнает у сервера IP-адрес tftp-сервера [9]. С этого сервера скачивается загрузчик pxelinux. Pxelinux загружает с tftp-сервера свой файл конфигурации, в котором указано, какое ядро необходимо загрузить.

На следующем шаге загружается ядро Linux и образ initrd [10]. В WTPRO файл Initrd.gz был заменен образом с файловой системой SquashFS. В этом образе содержится микро-версия терминала, пригодная для работы на компьютерах с 8 Mb оперативной памяти. При необходимости, по протоколу tftp подгружаются необходимые образы.

Например, так реализована поддержка звука на терминале. Рассмотрим ее подробнее. После

запуска системы, перед подключением к терминальному серверу, проверяется какие расширения необходимо загрузить [11] с tftp сервера. Далее скачивается файл содержащий образ файловой системы SquashFS, в котором находятся модули к ядру Linux с драйверами звуковых карт. После этого запускается программа, определяющая какой модуль необходимо загрузить (используется алгоритм, определяющий по PCI ID нужный модуль) [12]. Загружается необходимый модуль. Отмонтируется образ с драйверами и удаляется файл, в котором этот образ находится. В результате оперативная память расходуется экономно.

4. Терминальный протокол RFB

Одним из терминальных протоколов является протокол VNC (RFB). Рассмотрим некоторые его особенности. Virtual Network Computing (VNC) система удаленного доступа к компьютеру, использующая RFB-протокол (Remote FrameBuffer). Она передает нажатия клавиш на клавиатуре и движения мыши с одного компьютера на другой, транслируя обновления экрана в обратном направлении по сети.

По протоколу VNC нельзя перенаправлять устройства. VNC очень простой протокол, основанный на графических примитивах: «Положить прямоугольник пикселей на заданную позицию x, y».

Сервер посылает небольшие прямоугольники framebuffer'a клиенту. Такая схема в своей примитивной форме потребляет большую часть пропускной возможности канала. Для снижения нагрузки на канал используются различные методы. Существует вариант использования сжатия - метод определения наиболее эффективного способа передачи прямоугольников пикселей.

VNC-протокол позволяет клиенту и серверу договориться об используемом методе кодирования. Самый простой метод кодирования, поддерживаемый всеми клиентами и серверами - «raw encoding». В этом случае пиксели передаются в порядке слева-направо, сверху-вниз. А после передачи первоначального состояния экрана, передаются только изменившиеся пиксели.

Этот метод работает очень хорошо при незначительных изменениях изображения на экране. Например, при движении указателя мыши по рабочему столу, в случае набора текста под курсором и т.д. Однако загрузка канала становится очень высокой при одновременном изменении большого количества пикселей, например при просмотре видео.

В отличие от RDP-протокола VNC-сервер для авторизации не использует системные имена пользователей и пароли. Он вообще не использует имена пользователей. Вместо имени пользователя используется номер порта [13]. На Unix-машинах можно запустить несколько VNC-серверов. На Windows-машинах мы ограничены только одним сеансом. То есть при работе в Unix наш сервер поддерживает столько клиентов, сколько VNC-серверов запущено. В Windows все пользователи работают с одним сеансом, а именно с локальной консолью сервера. Все пользователи используют одну и ту же клавиатуру и одну и ту же мышь. Поэтому вероятны конфликты, когда пользователи на различных компьютерах будут тянуть в разные стороны одну и ту же мышь. В связи с этим в VNC-сеансе существует два вида паролей: пароль на чтение и запись (зная этот пароль, пользователь полностью управляет сеансом); пароль только на чтение (пользователь видит, что происходит в сеансе, но не может вмешиваться - данный режим удобен для презентаций).

Еще одной особенностью протокола является возможность «разделить» сессию - разрешить нескольким пользователям параллельно работать с одним портом и использовать общий сеанс. В этом режиме целесообразно использовать пароль «только на чтение». В режиме презентации мы делаем общедоступной одну сессию, а все остальные пользователи подключаются, используя пароль только на чтение. В результате, все, что происходит на центральном компьютере транслируется на все остальные машины. В ряде случаев это удобней использования проектора, так как изображение находится в непосредственной близости от пользователя.

5. Оптимизация

Для того чтобы WTPRO мог работать на системах с очень ограниченными ресурсами, нами было проведено множество оптимизаций. В частности стандартная, но «тяжелая» библиотека glibc была заменена на легкую, но урезанную функционально библиотеку uclibc. Многие программы были перекомпилированы со статическим включением библиотек [14]. При статической линковке приложений в полученную программу включается только используемый код, а при динамической линковке в библиотеке остается даже тот код, который не используется в программе. Некоторые программы, например, librdesktop.so, требуют установки дополнительных библиотек, таких как libiconv.so, которые занимают много места. Эти библиотеки были заменены эквивалентным кодом, достаточным для выполнения программ. Таким образом, удалось на 70 % сократить размер бинарного кода. Многие стандартные утилиты были нами переписаны таким образом, что теперь используют только вызовы ядра и не требуется ни одной библиотеки. Например, программа перезагружающая компьютер, которая идет с дистрибутивом Fedora Core 4 занимает 11 Kb и требует две библиотеки libc (1,5 Mb) и ld (124 Kb). После компиляции наша версия программы занимает 624 байта и не требует ни одной библиотеки.

Также сильной модификации подверглось ядро Linux. Как уже было сказано выше, в нашем ядре присутствует поддержка devfs. В ядро вклю-

чены патчи для нестандартных файловых систем SquashFS, supermount. Также в ядро мною был включен патч Linux-tiny, который позволяет запускать операционную систему на машинах с весьма ограниченными системными ресурсами [15]. Данный патч уже не поддерживается разработчиками Linux, начиная с версии ядра 2.6.14. Теперь он поддерживается нами.

Этот патч реализует следующие функции: удаляет неиспользуемые системные вызовы, в нем отсутствует вывод сообщений ядра, «тяжелый» код заменен на менее функциональный, но существенно меньший по размеру.

Так же большим ограничением является то, что на терминальном клиенте нельзя хранить настройки (отсутствует жесткий диск). Поэтому используется несколько способов конфигурации клиента. Часть параметров, о конфигурации сети и IP-адресах терминальных серверов, передаются по DHCP. Остальные настройки, в случае необходимости, загружаются посредством протокола TFTP. Некоторые параметры - видеокарта, разрешение, тип мыши т. д. определяются автоматически [16].

Заключение

Результатом данной работы является разработка, внедрение и поддержка терминального клиента WTPRO. Тонкий клиент имеет модульную архитектуру. Это позволяет запускать его как на устаревших, так и на современных компьютерах. Нами была произведена оптимизация кода и реализованы алгоритмы, для автоматического определения оборудования и загрузки его на терминал. Получившийся продукт может подключаться как к Windows, так и UNIX подобным серверам.

Литература

1. А. с. РФ. Препроцессор «Elinux»: свидетельство об отраслевой регистрации разработки № 5399 / С.А. Рожков. - № 50200501646; заявл. 08.11.2005.; опубл. 05.12.2005; Компьютерные учебные программы и инновации № 9(10). -1с.

2. А. с. РФ. Терминальная система ElinuxT: свидетельство об отраслевой регистрации разработки № 5491 / С.А. Рожков. - № 50200501788; заявл. 08.11.2005.; опубл. 20.12.2005; Компьютерные учебные программы и инновации №9(10). — 1с.

3. А. с. РФ. Терминальная система «ElinuxT»: свидетельство об официальной регистрации программы для ЭВМ № 2006611848. Зарегистрировано в Реестре программ 30.05.2006.

4. Рожков, С.А. Защищенная терминальная система WTPRO: свидетельство о государственной регистрации программы для ЭВМ/ С.А. Рожков. — № 2009611320. Зарегистрировано в Реестре программ 04.03.2009.

5. А. с. РФ. Защищенная терминальная система WTPRO: свидетельство об отраслевой регистрации разработки № 12153 / С.А. Рожков. — № 50200900159; заявл. 08.12.2008.; опубл. 16.01.2009.

6. Стахнов, А. Linux-сервер в Windows-окружении / А. Стахнов. — СПб.: БХВ, 2007. — 656 с.

7. httpJ/sourceforge. net/tracker/index.php?func=detail&aid=1314556&groupJd=24366&atid=381349

8. Вахалия, Ю. UNIX изнутри/ Ю. Вахалия. - СПб.: Питер, 2003. - 844 с.

9. Таненбаум, Э. Современные операционные системы /Э. Таненбаум. — 2-е изд. - СПб.: Питер, 2002. -1040 с.

10. Таненбаум, Э. Распределенные системы. Принципы и парадигмы / Э. Таненбаум. - СПб.: Питер, 2003. - 877 с.

11. Хелд, Г. Технологии передачи данных / Г. Хелд. - СПб.: Питер, 2003. - 720 с.

12. Рожков, С.А. Дистрибутив Elinux [Текст] / С.А. Рожков // Безопасность информационного пространства: материалы Всерос. науч.-практ. конф. -Екатеринбург: УТТУ-УПИ, 2005. - С. 83-84.

13. Рожков, С.А. Терминальные системы для предприятий / С.А. Рожков // Снежинск и наука — 2006: сб. науч. тр. междунар. науч.-практ. конф. — Снежинск: СГФТА, 2006. - С. 184-186.

14. Рожков, С.А. Разработка терминальной системы ElinuxT / С.А. Рожков // Каталог тезисов проектов научно-технических коллективов молодых ученых, аспирантов и студентов, представленных на всероссийский конкурсный отбор по приоритетным направлениям науки и высоких технологий. -М: РГУИТИ, 2006. - С. 109-111.

15. Рожков, С.А. Терминальные системы для предприятий / С.А. Рожков // Безопасность информационного пространства: материалы междунар. науч.-практ. конф. -Екатеринбург: УрГУПС, 2006. - С. 96-97.

16. Рожков, С.А. Сравнение терминальных систем / С.А. Рожков // Безопасность информационного пространства VI: сб. тр. межвуз. науч.-практ. конф. студентов, аспирантов и молодых ученых. - Тюмень: Изд-во ТюмГУ, 2007. - С. 183-188.

Поступила в редакцию 10 апреля 2009 г.