УДК 004.45

С.А. Рожков

Защищенные терминальные системы

Терминальная система, построенная по схеме сильный сервер – слабая рабочая станция, очень экономична и легко управляема. Однако она подвержена новым специфическим атакам на ее безопасность. Некоторые из этих атак и способы противодействия им изучены в данной статье. Исследования проводились на базе разработанной автором терминальной системы WTPRO. Предложена и реализована система взаимной аутентификации клиента и сервера WTPRO.

Ключевые слова: терминальная система, защита информации, аутентификация, идентификация, безопасность.

В данной статье рассматриваются программные решения, позволяющие заменить ОС Linux или Windows на машине пользователя, на терминал, к оторый реализует перенаправление рабочего стола с сервера на клиентскую машину.

Терминальная система упрощает администрирование компьютерной сети и ее защиту. Вместе с тем такая система подвержена новым атакам, актуальным только для терминальных систем. Источником большинства проблем безопасности является то, что на терминале нет предустановленной ОС, а она загружается по сети. Используемые при этом протоколы разрабатывались в 80-х годах прошлого века [1, 2] и не обеспечивают необходимого сегодня уровня защищенности.

Обеспечить приемлемый уровень безопасности можно, установив сетевое оборудование, например корпорации CISCO, и правильно его сконфигурировав. Однако терминальные системы часто создаются на морально устаревшем оборудовании и используют недорогие серверы, следовательно, покупка сетевого оборудования, по цене сравнимая со стоимостью всей сети, не оправдана.

Для терминальных систем актуальной является задача обеспечения безопасности недорогими программно-аппаратными средствами, укладывающимися в норматив – не более 10–20% от стоимости информационной системы [3, 4].

В 2005 г. на основе ядра Linux 2.6 был разработан дистрибутив Elinux [5], позволяющий проводить анализ сети, восстанавливать ОС, работать в качестве терминального сервера и рабочей станции. Достоинством дистрибутива был его небольшой размер (30 Мб). В 2006 г. был создан тонкий клиент ElinuxT (торговая марка WTPRO) [6–8, см. также 9, с. 447]. В настоящее время WTPRO единственная разрабатываемая в РФ терминальная система, в которую встроен модуль взаимной аутентификации и в которой имеется поддержка MacOS-серверов.

Проблема аутентификации. Стандартные методы аутентификации [10, 11], основанные на знании клиентом какой-либо уникальной информации о сервере и хранении этой информации на клиенте, не могут использоваться, т.к. тонкие клиенты загружаются по сети и не имеют локальных носителей информации.

В то же время решение проблемы аутентификации должно быть совместимым с существующими технологиями, простым и недорогим.

Аутентификацию клиента можно осуществить, используя аппаратные ключи Etoken или RuToken, т.к. они не поддаются клонированию и выполняют криптографические операции на собственном процессоре. Аналогично, оснастив сервер аппаратным ключом, можно решить проблему аутентификации сервера.

Автором статьи разработаны расширения для виртуальных каналов RDP протокола, расширяющие функциональные возможности сервера терминалов, позволяющие производить идентификацию и аутентификацию клиента и сервера.

Алгоритм идентификации и аутентификации в виртуальных каналах. При создании новой терминальной сессии на сервере создается новый виртуальный канал, в дальнейшем все данные передаются через этот виртуальный канал.

Сервер получает запрос на доступ к сессии, генерирует ЭЦП и случайную последовательность данных, передает эти данные клиенту.

Клиент средствами аппаратной идентификации (ключ Etoken) проверяет данные сервера. В случае успеха добавляет к случайной последовательности данных свою случайную последовательность и генерирует собственную ЭЦП. Отправляет эти данные серверу.

Сервер, получив данные от клиента, проверяет их.

В случае успеха взаимной проверки клиента и сервера разрешается старт терминальной сессии. В противном случае сессия прерывается.

Периодическая взаимная аутентификация позволяет гарантировать подлинность клиента и сервера на протяжении всего сеанса работы.

На основе переданных от клиента к серверу и от сервера к клиенту случайных данных можно создать сессионный ключ шифрования и на его основе зашифровать передаваемые по виртуальному каналу данные.

Альтернативное решение – помещение в загрузчик сетевой карты открытого ключа сервера, при условии, что злоумышленнику блокирован физический доступ внутрь системного блока клиента. Алгоритм взаимной аутентификации аналогичен приведенному выше, за исключением того, что все ключи хранятся в bootrom и проверка ключей производится средствами центрального процессора, а не Etoken.

Рассмотрим аутентификацию сервера на базе протокола SSH средствами визуализации открытого ключа сервера. При подключении клиента к серверу на экране клиента появляется картинка – например, графический примитив дома или стула, изменяется ключ – изменяется картинка. Графические изображения можно сделать состоящими из большого количества элементов, в зависимости от длины ключа. Если длина ключа равна 256 бит, то часть бит задают цвет фона, часть – цвет элементов, количество элементов и т.д.

Один из возможных алгоритмов реализации этой идеи включен в программный продукт [12].

Также решением проблемы аутентификации является расширение протоколов DHCP и TFTP с сохранением совместимости путем добавления алгоритмов для аутентификации сервера и клиента, например приведенных выше. Данное расширение протоколов будет включено в очередные версии терминала WTPRO.

Выводы. Терминальные системы, в силу своей архитектуры защищены от многих угроз безопасности, которые актуальны для полноценных рабочих станций. В то же время они подвержены новым специфическим атакам. Поскольку тонкий клиент загружается по сети и не имеет локальных носителей информации, то очень важна аутентификация как клиента, так и сервера. В работе предложены три метода аутентификации терминальных серверов и клиентов: виртуальные каналы RDP протокола; расширение протокола DHCP; графическая аутентификация. Программно-аппаратные реализации этих методов включены в очередную версию терминального клиента WTPRO, разработанного и поддерживаемого автором.

Литература

1. Джамса К. Программирование для Internet в среде Windows / К. Джамса, К. Коуп. – СПб.: Питер, 1996. – 672 с.

2. RFC1533 http://www.faqs.org/rfcs/rfc1533.html

3. ГОСТ Р ИСО/МЭК 17799–2005

4. Петренко С. Информационная безопасность: экономические аспекты / С. Петренко, С. Симонов, Р. Кислов // Jet Info Online. – 2003. – №10.

5. Рожков С.А. Дистрибутив Elinux // Матер. Всеросс. науч.-практ. конф: «Безопасность информационного пространства». – Екатеринбург: УГТУ-УПИ, 2005. – С. 83–84.

6. Рожков С.А. Защищенная терминальная система WTPRO: Свидетельство об отраслевой регистрации разработки № 12153; заявл. 08.12.2008.; опубл. 16.01.2009. № 50200900159.

7. Рожков С.А. Терминальная система ElinuxT: Свидетельство об отраслевой регистрации разработки № 5491/ Гос. координац. центр информ. технологий. Отраслевой фонд алгоритмов и программ. – М., 2005. 29.12.05, № 50200501788.

8. Рожков С.А. Терминальные системы для предприятий // Сб. науч. тр. междунар. науч.-практ. конф. «Снежинск и наука – 2006». – Снежинск: СГФТА, 2006. – С. 184–186.

9. Стахнов А. Linux-сервер в Windows-окружении. – СПб.: БХВ, 2007. – 656 с.

10. Белов Е.Б. Основы информационной безопасности: учеб. пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2006. – 544 с.

11. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. – Екатеринбург: Изд-во УрГУ, 2003. – 328 с.

12. Рожков С.А. Защищенная терминальная система WTPRO: Свидетельство о государственной регистрации программы для ЭВМ № 2009611320. Зарегистрировано в Реестре программ 04.03.2009.

Рожков Сергей Александрович
ГОУ ВПО «Южно-Уральский государственный университет»,
аспирант каф. цифровых радиотехнических систем
Эл. адрес: z@zserg.ru

S.A. Rozkhov
Protected terminal system
The terminal system constructed under the circuit a strong server – a weak workstation, is very economic and manageable. However, it is subject to new specific attacks on its safety. Some of these attacks and ways of counteraction are investigated by him in given article. Researches were carried spent on the basis of terminal system WTPRO developed by the author.
Keywords: terminal system, information security, autentification, identification, protection.