ISBN 5-94052-066-0 ПРОГРАММНЫЕ СИСТЕМЫ: ТЕОРИЯ И ПРИЛОЖЕНИЯ. ПЕРЕСЛАВЛЬ-ЗАЛЕССКИЙ, 2004

УДК 681.324

С. В. Бурчу

Методы хостинга веб-сайтов, применимо к системе телекоммуникаций «Ботик»

Аннотация. Данная работа является описанием технологий для услуги аренды WWW-пространства. Это включает в себя описание как уже существующих технологий, так и принципиально новых.

1. Введение

В данной статье описываются некоторые методы и технологии, которые используются в системе телекоммуникаций (СТ) «Ботик» для развития услуги аренды WWW-пространства (веб-хостинг).

Термин *веб-хостинг (web hosting)* буквально переводится как "содержание/размещение в сети" и означает размещение сайтов Заказчика на компьютерных площадях Исполнителя этой услуги.

1.1. Немного истории. Со времени своего первого шага по глобальной сети Интернет каждый человек мечтает создать и разместить в Сети свою собственную страничку, свой сайт. Но не у каждого человека есть свой собственный сервер с постоянным выходом в Сеть, чаще всего такая возможность есть у людей, тесно связанных с компьютерами и Интернет. Но как быть простому пользователю? Что делать деловому человеку, желающему рассказать всем с помощью Интернета о своей компании, о своем деле? Услуга аренды WWW-пространства (web hosting) как раз и позволяет ответить на эти вопросы. Услуга аренды позволяет решить множество проблем, которые встают перед желающим иметь свой собственный сайт в Интернет. Пользователю уже не нужно обладать своим собственным сервером с постоянным выходом в Сеть, постоянно включенным и под постоянным присмотром квалифицированного системного администратора, которому нужно платить зарплату. К тому же чаще всего сервер, на котором осуществляется аренда, располагают более

Работа выполнялась при частичной поддержке суперкомпьютерной программы «СКИФ» Союзного государства и программы фундаментальных научных исследований ОИТВС РАН «Новые физические и структурные решения в инфотелекоммуникациях».

удачно (чем это бывает для обычных абонентских подключений) в смысле скорости доступа к внешнему Интернету. Поэтому данная услуга весьма привлекательна для широкого круга Абонентов.

1.2. История развития хостинга в СТ «Ботик». СТ «Ботик» предоставляет пользователям услуги аренды WWW-пространства с 1995 года. Услуги аренды реализуются центральным сервером Системы Телекоммуникаций «Ботик» (http://www.botik.ru). Предоставляемые возможности (размещение статических документов, доступ к арендованному пространству по протоколу FTP) на момент появления этого сервиса вполне соответствовали потребностям пользователей. Но за прошедшее с тех пор время обстановка в Интернет существенно изменилась: получили широкое распространение технологии создания Интернет-сайтов с динамическим содержанием (CGI [4], PHP [5], ASP [6]); пользователи требуют размещения на сервере аренды не только готовых документов, но и программ и баз данных. Сеть развивается, в том числе и внутренняя локальная сеть СТ «Ботик», появляются клиенты, которых статические сайты уже не устраивают и которым нужны дополнительные возможности, например, для создания специализированного сетевого магазина.

1.3. Что нужно? Предоставление услуг аренды на этом новом уровне выходит за пределы возможностей (и целей тоже) центрального сервера СТ «Ботик». Прежде всего, на этом новом уровне требуются механизмы контроля использования ресурсов сервера пользователями. Кроме того, требуется продуманная схема обеспечения безопасности сервера с позиций “недоверия к пользователю”. Наконец, требуется включение сервера в обработку учетно-статистической системой СТ «Ботик» (Nadmin [2]).

Описанию уже существующих методов и разработке новых и посвящена данная статья.

2. Краткий обзор уже существующих технологий

Для оказания услуги аренды WWW-пространства нужно как минимум две вещи:

(1) Компьютер с установленной на нем операционной системой.
(2) Программное обеспечение, реализующее функции веб-сервера.

Операционной системой (ОС) была выбрана ОС Debian GNU/Linux ([12]) как наиболее привычная и удобная, а в качестве веб-сервера — Apache ([7]), отличающийся от обычного только модификациями, позволяющими ему на лету делать перекодировку документов. Для генерации динамического контента был выбран скриптовый язык PHP ([5]), а в качестве сервера баз данных — MySQL ([8]).

3. Что еще нужно?

При разработке услуги аренды веб-пространства для СТ «Ботик» практически сразу возникла проблема с учетом трафика пользователей сервера аренды. Предоставив пользователям возможность выполнять программы на сервере, мы открываем ему полный и бесплатный доступ к ресурсам Интернет. Конечно, никто не мешает административно решить эту проблему, практически разделив расходы на трафик сервера аренды между всеми его пользователями, но данное решение было бы не совсем правильным с точки зрения тех самых пользователей. Поэтому возникла и была решена задача количественного определения трафика по каждому пользователю отдельно. Еще одной задачей являлось включение услуги аренды веб-пространства в учетно-статистическую систему Nadmin. Так же здесь будут рассмотрены некоторые решения в области безопасности.

3.1. Решение задачи определения трафика по каждому пользователю. Получение данных о трафике пользователей оказалось делом непростым. Стандартных и эффективных решений данной проблемы найдено не было. Поэтому пришлось реализовать собственную компоненту для решения этой проблемы.

Реализация данной компоненты основывалась на механизме работы с сетью пользовательских приложений и в ядре ОС Linux. Суть идеи такова: поскольку работа с сетью происходит через несколько различных системных вызовов, то нужно в нескольких местах поправить ядро ОС Linux таким образом, чтобы гарантированно получать данные о трафике. В целом реализация данной идеи оказалась достаточно простой, за исключением процедуры вывода данных.

В рамках данной работы было разработано две версии подсистемы получения данных о трафике пользователей. Они были названы Socket Accounting V1 (sacct1) и Socket Accounting V2 (sacct2).

Первая версия Socket Accounting. В первой версии подсистемы получения данных о трафике пользователей данные о трафике представлены следующим образом:

- *uid/gid* пользователя, открывшего соединение;
- протокол соединения (TCP, UDP);
- локальные ip-адрес и порт соединения;
- удаленные ip-адрес и порт соединения.

Вывод данных из ядра ОС Linux был реализован через системный лог-файл сервера (syslog). Примерная строка вывода данных представлена на рисунке 1.

```
SACCT u 285 g 10 t 2 l 193.232.174.76:4171 r 193.232.174.1:53 tx 47 rx 98
SACCT u 285 g 10 t 2 l 193.232.174.76:4171 r 193.232.174.1:53 tx 32 rx 15
SACCT u 285 g 10 t 2 l 193.232.174.76:4171 r 193.232.174.1:53 tx 44 rx 20
SACCT u 135 g 30 t 2 l 193.232.174.76:4171 r 193.232.174.1:53 tx 31 rx 12
SACCT u 135 g 30 t 1 l 193.232.174.76:5087 r 194.226.220.7:80 tx 25 rx 54
SACCT u 135 g 30 t 2 l 193.232.174.76:4171 r 193.232.174.1:53 tx 31 rx 12
```

Рис. 1. Пример вывода данных о трафике в системный лог-файл

Однако это решение оказалось неоптимальным. Даже на небольшом сервере со средней загрузкой системный лог-файл быстро увеличивался в размерах и за несколько дней вырастал до размеров нескольких гигабайт.

Вторая версия Socket Accounting. Вторая версия подсистемы получения данных о трафике пользователей была разработана на базе собственного механизма вывода данных из ядра в файл. С помощью файловой системы *proc*[1] ядру сообщают о файле, в который нужно записывать данные о трафике пользователей. Данные о трафике были нами изменены — добавились данные о том, было ли соединение создано посредством функции *accept*[2], кроме того, данные записывались в бинарном виде. Это позволило существенно сократить размеры лог-файлов: лог-файл второй версии подсистемы по сравнению с лог-файлом первой версии подсистемы в среднем отличается размерами в 50–70 раз.

[1]Псевдофайловая система *proc* используется для получения информации о компьютерной системе и изменения некоторых параметров ядра после загрузки ОС.

[2]Употребляется в tcp/ip-соединениях. Забирает первый запрос на соединение из очереди запросов и создает соединение.

Тем самым вторая версия подсистемы получения данных о трафике пользователей оказалась эффективной и была принята в опытную эксплуатацию как одна из компонент программного обеспечения сервера аренды.

3.2. Включение услуги аренды веб-пространства в систему Nadmin. Решение этой задачи было реализовано как для старой версии Nadmin, так и для новой. На старой не стоит останавливаться, можно только сказать, что решение было реализовано, но не испытано в реальных условиях. Решение же для новой версии Nadmin([3]) было точно так же реализовано, но только уже с учетом архитектурных особенностей этой системы.

Были реализованы два сенсора для считывания данных о трафике пользователей сервера: для "Socket Accounting" (смотри пункт 3.1) и для учета трафика виртуальных хостов сервера аренды.

Были так же добавлены и дополнены соответствующие скрипты из системы Nadmin.

3.3. Некоторые решения в области безопасности. Решением проблемы безопасности заключается в некотором общем подходе, который позволил бы убрать хотя бы большинство первопричин возникновения "уязвимостей" в программном обеспечении сервера, а не следствия. Таким общим подходом является пакет **GrSecurity** [11] — набор заплат для ядра ОС Linux. В возможности данного пакета входит:

- наложение дополнительных ограничений на реализацию системного вызова chroot[3];
- защита от изменения адресов возврата в стеке программ; Существует целый ряд "уязвимостей", основанных на изменении адресов возврата в стеке, что позволяет злоумышленнику исполнить какой-либо код с правами атакуемой программы.
- возможность слежения (аудита) за некоторыми важными системными событиями;
- увеличение "энтропии" в ядре, что позволит защититься от предсказания злоумышленником некоторых будущих действий;

[3]Системный вызов chroot обеспечивает возможность для какого-либо процесса изменить корневой каталог. Однако в некоторых случаях возможно обойти chroot–ограничения и получить доступ к реальному корневому каталогу сервера.

- различные ограничения на получение информации о системе.

Еще одной проблемой является не всегда корректное написание CGI-скриптов пользователями. Невозможно полностью решить такую проблему как ошибки пользователей в разработанных ими CGI-скриптах. Суть проблемы состоит в том, что Абонент, арендующий веб-пространство, может написать уязвимый CGI-скрипт. После чего внешний злоумышленник способен будет *удалённо* исполнить некий код на сервере аренды. Отметим, что все скрипты пользователей исполняются с одним и тем же *uid*[4]*/gid*[5]: www-data. Таким образом данные пользователей оказываются не защищёнными от другого пользователя. Например, открывая файл на доступ своему скрипту, пользователь автоматически делает его доступным для всех остальных скриптов. То есть даже при отсутствии "уязвимостей" в скриптах пользователи оказываются не защищены друг от друга, оказывается обойдён механизм *многопользовательской защиты*[6] Linux. Описанное классифицируется как *локальная* угроза, но в сочетании с возможными "уязвимостями" в скриптах некоторых пользователей она может стать *удалённой*.

От "уязвимостей" в скриптах пользователей мы не можем защититься, поскольку пользователи пишут скрипты сами. Но мы хотим обеспечить такую защиту сервера от пользователей и пользователей друг от друга, чтобы в случае обнаружения и использования "уязвимости" в скрипте пострадал только владелец скрипта, но не другие пользователи и не работоспособность сервера в целом.

В качестве подобной защиты решено использовать компоненту **suexec** веб-сервера Apache. Данная компонента позволяет исполнять скрипты пользователей с *uid/gid* владельца скрипта (то есть отличными от www-data и различными для каждого владельца скрипта). Тем самым убирается возможность обхождения *многопользовательской защиты* Linux.

---

[4]Идентификатор пользователя — *uid*.

[5]Идентификатор группы — *gid*.

[6]Многопользовательской защитой Linux называют способ ограничения доступа к файлу, который позволяет разрешить доступ на запись, чтение и исполнение одному конкретному пользователю (владельцу файла), группе пользователей и всем остальным пользователям системы.

4. Заключение

Описанные здесь технологии позволяют успешно реализовать услугу аренды веб-пространства. На данный момент все это уже тестируется на тестовом сервере СТ «Ботик».

Благодарности. Автор благодарен всем, кто помогал ему в написании этой статьи. Особые благодарности Юрию Владимировичу Шевчуку и Сергею Михайловичу Абрамову за их бесконечное (автор надеется) терпение.

Список литературы

[1] Т. Кристиансен, Н. Торкингтон PERL: библиотека программиста: Издание официальное. — СПб: Питер, 2001. ↑

[2] Шевчук Ю. В.. 1999. *Методы построения экономически эффективных региональных компьютерных сетей*, Диссертация на соискание степени кандидата технических наук, Институт программных систем РАН, Переславль-Залесский. ↑1.3

[3] Ермилова Екатерина В., Карлаш Анастасия В., Нестеров Александр С., Жбанов Павел Г., Шевчук Юрий В.. 2004. *Nadmin — система администрирования для региональных сетей*, Переславль-Залесский. ↑3.2

[4] Ken A. L. Coar, David Robinson The WWW Common Gateway Interface Version 1.1. — http://cgi-spec.golux.com/draft-coar-cgi-v11-03.txt. ↑1.2

[5] PHP scripting language. — http://www.php.net. ↑1.2, 2

[6] Microsoft Corporation Active Server Pages. — http://msdn.microsoft.com/asp/. ↑1.2

[7] Apache Software Foundation The Apache HTTP Server Project. — http://www.apache.org. ↑2

[8] MySQL AB MySQL: The World's Most Popular Open Source Database. — http://www.mysql.com. ↑2

[9] The PostgreSQL Global Development Group PostgreSQL Database Management System. — http://www.postgresql.org. ↑

[10] Linus Torvalds Linux Kernel Archives. — http://www.kernel.org. ↑

[11] GrSecurity Team Greater Security. — http://www.grsecurity.net. ↑3.3

[12] Debian Project Team Debian GNU/Linux – The Universal Operating System. — http://www.debian.org. ↑2

[13] Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet: Издание официальное. — ДМК: Москва, 1999. ↑

Исследовательский центр мультипроцессорных систем ИПС РАН

S. V. Burchu. *Methods of Web Hosting used in Telecommunication Laboratory "Botik".* (in russian.)

Abstract. This work is about World Wide Web hosting technologies used in Telecommunication Laboratory "Botik". That includes the description both already existing technologies and essentially new.