Магия ПК

О сложном просто и понятно

#10 (87)

октябрь 2005

Издательство "Техно-Пресс", Санкт-Петербург

- Безопасность с позиции силы
- Твой скорострельный шотган
- Windows XP: ядерная война
- Осторожно, злая@

Мой компьютер — моя крепость

БЕЗОПАСНОСТЬ
Linux vs. Windows

Михаил Емельченков (г. Красногорск)

Безопасность — постоянная забота системных администраторов. Попробуем сравнить с этой точки зрения две наиболее популярные операционные системы — Linux и Windows.

Существует множество версий операционных систем Windows — Windows 95/98, Windows NT/2000, Windows XP, Windows 2003 Server. Дистрибутивы Linux отличаются версиями ядра (2.2, 2.4, 2.6) и версиями поставляемых с ними пакетов программного обеспечения.

Надо понимать, что существует фундаментальное различие между архитектурой Linux и Windows. Windows разработана таким образом, что в ее ядре сосредоточена большая функциональность, позволяющая глубже интегрировать приложения в ядро. Linux отличается от Windows тем, что в ней присутствует разделение между ядром и прикладным ПО. Это имеет большое значение, потому что безопасность ОС зависит от ее архитектуры.

Растущая популярность Linux заставила Microsoft вкладывать гораздо больше ресурсов в безопасность Windows. Несомненным прогрессом в этой области можно считать выпуск Service Pack 2 для Windows XP. Этот пакет усиливает безопасность Windows посредством отключения некоторых сервисов по умолчанию, а также добавляет несколько новых security-инструментов, таких как улучшенный брандмауэр Windows. В большинстве случаев отключение сервисов делает систему в целом безопаснее, но не стоит это делать в ущерб гибкости или функциональности.

Microsoft сконцентрировалась на усилении безопасности через повыше-

ние удобства работы. Вспомним, что появление нескольких эксплоитов в 2003 году вылилось в эпидемию e-mail-вложений, рапространяемых как исполняемый файл (например, MyDoom). Service Pack 2 вводит специальный сервис для обработки вложений Outlook/Exchange, Windows Messenger и Internet Explorer вместо того, чтобы исправлять неработающую инфраструктуру и безопасность коммуникаций. В Linux подобного никогда не происходило.

Service Pack 2 внес много нововведений для пользователя Windows, но все равно обеспечение безопасности лежит на плечах системных администраторов и пользователей Windows, а не обеспечивается исходным кодом системы.

Фундаментальное различие между Linux и Windows состоит и в моделях лицензирования. Linux лицензируется под GNU General Public License, которая дает возможность пользователю копировать, изменять и распространять исходный код. Windows же, напротив, — закрытая ОС, безопасность которой обеспечивается недоступностью исходного кода. Правда, в 2001 году Microsoft открыла часть кода Windows для своих партнеров. Некоторые нашли это полезным для отладки приложений и, таким образом, обеспечения большей безопасности.

Скрытая угроза безопасности Windows — мнимая простота администрирования. Как известно, в Windows все действия по настройке и эксплуатации ОС выполняются с помощью графического интерфейса, а в Linux — с помощью командой строки (шелла). Графический интерфейс подкупает своей простотой, позволяя администрировать систему даже новичку, не обладающему глубокими знаниями в вопросах обеспечения безопасности. Этим он подвергает риску не только администрируемую систему, но и финансы компании, нанявшей такого системного администратора.

Еще одно фундаментальное различие Windows и Linux — в их принципе построения. Windows — монолитная, а не модульная система, в отличие от Linux. По сути это означает, что слишком много компонентов интегрировано в ядро Windows. Например, интеграция в ядро Internet Explorer скрывает в себе потенциальные дыры в безопасности всей системы. Или, скажем, интеграция подсистемы рендеринга изображений в ядро при ее крахе приведет к краху ядра в целом, а не отдельной подсистемы. Монолитная структура нестабильна по своей природе. Каждая подсистема такого ядра имеет множество зависимостей, и при ее модификации приходится следить за всеми зависимостями, что, естественно, довольно трудно.

Сетевая безопасность и протоколы

И Linux, и Windows включают IPSec как отрытый стандарт криптографической защиты IP-протокола. IPSec проверяет, не было ли каких модификаций передаваемой по сети информации, и шифрует ее. OpenSSH, OpenSSL и OpenLDAP реализованы на Linux, их закрытые реализации SSH, SLL и LDAP — на Windows.

Безопасность приложений

Linux превосходит Windows в вопросе безопасности приложений, осо-

бенно в связи с постоянными дырами в безопасности Microsoft ISS и Exchange/Outlook. Apache и Postfix — кросс-платформенные приложения, они имеют лучшую защищенность по сравнению с продуктами Microsoft. Безопасность Linux также обеспечивает брандмауэр, встроенный в ядро, и Snort — де факто стандарт систем защиты от вторжения.

Настораживает тенденция Microsoft смешивать данные и код в приложениях. Например, ActiveX приносит непроверенные данные из внешних систем и запускает непроверенный код.

Одна из основных проблем Windows — переполнение буфера. Пользователи Linux оценят возможность использовать защиту от выполнения, появившуюся в ядре Linux 2.6. Она обеспечивает защиту от эксплоитов, которые перезаписывают структуры данных или вставляют код в эти структуры.

Еще одно подспорье в безопасности — использование User-Mode Linux (UML), специального патча для ядра, который позволяет запускать несколько независимых ядер Linux одновременно. Таким образом можно тестировать приложения, не опасаясь за безопасность рабочей системы.

Безопасность пользователей

Windows XP — первая ОС семейства MS Windows, относительно полноценно поддерживающая многопользовательскую работу за ПК. Файлы пользователей отделены друг от друга, и каждый пользователь имеет свои приватные файлы, недоступные для других, а также ограниченные системные привилегии. Функция «Fast User Switching» позволяет работать одновременно нескольким пользователям за одним ПК, но имеет одно существенное ограничение: в таком режиме компьютер не может входить в домен Windows. В Linux многопользовательская поддержка работает с самой первой версии системы.

Открытые стандарты

Закрытые стандарты, которые так любит Microsoft, несут в себе потенциальные дыры в безопасности. Об этом свидетельствуют многочисленные вирусы в документах Word и Excel, чего нет в документах Open Office, построенных на открытой модели.

Большое заблуждение — думать, что открытые стандарты и открытый исходный код опаснее закрытого, так как предоставляет возможность злоумышленникам исследовать его. На практике веб-сервер с открытым исходным кодом Apache гораздо популярнее и безопаснее веб-сервера Microsoft IIS. Исследование кода разными людьми позволяет не только найти уязвимости, но и оперативно устранить их.

Вирусы и трояны

И еще одно заблуждение: Windows, якобы, больше подвержена вирусам, троянам, атакам хакеров и т. д. Факты говорят об обратном: если сравнить количество заплаток Windows и Linux, то под Linux их выходит больше. Причиной этого заблуждения стала повсеместная распространенность Windows и, как следствие, больший интерес к ней злоумышленников.