6. *Barbosa E.* Detecting BluePill, 2007.
7. Hypersight Rootkit Detector. URL: http://northsecuritylabs.com.
8. *Nguyen A. M., Schear N., Jung H. D., Godiyal A., King S. T., Nguyen H. D.* MAVMM: Lightweight and Purpose Built VMM for Malware Analysis.
9. *Sharif M., Lee W., Cui W.* Secure In-VM Monitoring Using Hardware Virtualization, 2009.
10. *Becher M., Dornseif M., Klein C. N.* FireWire: all your memory are belong to us, 2005.
11. *Petroni N. L., Fraser T., Molina J., Arbaugh W. A.* Copilot — a Coprocessor-based Kernel Runtime Integrity Monitor, 2004.
12. *Rutkowska J.* Beyond The CPU: Defeating Hardware Based RAM Acquisition.
13. *Lawson N., Goldsmith D., Ptacek T.* Don't Tell Joanna the Virtualized Rootkit is Dead.
14. *Ramos, Jozo Carlos Carvalho dos Santos.* Security challenges with virtualization, 2009.
15. *Fritsch H.* Analysis and detection of virtualization-based rootkits, 2008.
16. *Коркин И. Ю., Петрова Т. В., Тихонов А. Ю.* Метод обнаружения аппаратной виртуализации в компьютерных системах // Бизнес и безопасность в России. 2010. № 56. С. 114–115.
17. Intel® 64 and IA-32 Architectures Application Note TLBs, Paging-Structure Caches, and Their Invalidation. URL: http://www.intel.com/products/processor/manuals.

Е. В. Котов, С. В. Ктитров

РАЗРАБОТКА ДОМЕНА ЗАЩИЩЕННОЙ ОС НА ОСНОВЕ LINUX

Основной особенностью мандатного разграничения доступа является ограничение передачи данных между субъектами доступа. При получении субъектом доступа к объекту доступа (например, процесса, выполняющегося от имени учетной записи некоторого пользователя, к объекту файловой системы) дальнейшие действия данного субъекта (в нашем случае процесса) в отношении к полученным данным от объекта (в нашем случае файла) методами дискреционного разграничения доступа никак не регламентируются. Таким образом, в рамках дискреционной модели пользователь, имеющий доступ к конфиденциальной информации, может ее дискредитировать, т. е. организовать утечку конфиденциальных данных, поместив эти данные в другой объект файловой системы, права на чтение которого имеет субъект, изначально не имеющий прав на доступ к конфиденциальной информации.

Мандатное разграничение доступа предназначено для ограничения информационных потоков между субъектами доступа.

Сетевая модель разграничения доступа защищенной модификации ОС Linux разрабатывалась с учетом локального разграничения доступа. Сокеты TCP/IP являются одним из средств передачи данных в рамках локальной системы (при взаимодействии через интерфейс обратной связи loopback). Реализация мандатной модели доступа в рамках сетевой подсистемы рассматриваемой ОС ограничивается исключительно добавлением маркеров доступа в сетевые пакеты и анализом их в ядре операционной системы.

Подсистема аутентификации также является локальной, так как задействует исключительно базы данных учетных атрибутов пользователей (в том числе и мандатных), располагающиеся в рамках локальной файловой системы. Для аутентификации в ОС МСВС используются следующие службы:
- PAM — служба загружаемых модулей аутентификации;
- nsswitch — служба доступа к учетной информации системы (кроме мандатного разграничения доступа);
- iss — служба доступа к учетной мандатной информации системы.

Всю информацию в конечном итоге службы получают из баз данных локальной файловой системы.

Мандатное управление доступом, реализованное в рассматриваемой ОС, позволяет осуществлять построение защищенных систем с повышенными требованиями к безопасности и

надежности. При этом использование возможностей мандатной модели в большинстве случаев ограничивается рамками операционной системы или доверенной вычислительной сети.

На сегодняшний день существует ряд задач, решение которых выходит за рамки локальной ЭВМ. Среди таких задач можно выделить реализацию следующих технологий:

- сетевые системы управления базами данных;
- безопасная виртуальная консолидация данных;
- защищенная электронная почта;
- службы каталогов (организация принципа Single-Sign-On);
- сетевая печать (маркировка документов в соответствии с мандатным уровнем пользователя);
- конференц-связь.

Для решения данных задач предлагается построение защищенного домена на базе модифицированной ОС Linux с учетом мандатного контроля доступа. В рамках создания домена подразумевается реализация следующих особенностей:

1. организация знания и доступа к сетевой базе учетных атрибутов пользователей (в том числе и мандатных);

2. организация распространения информации о доступных сетевых сервисах;

3. организация аутентификации на удаленных сетевых сервисах;

4. разграничение доступа маршрутизации сетевого трафика по признакам принадлежности информации, установленным ОС. Использование мультипротокольной коммутации по меткам (MPLS) [1, 2] позволяет гарантировать качество обслуживания при передаче больших потоков информации.

Поддержка реализации приведенных выше свойств домена требует расширения соответствующих протоколов передачи данных и маршрутизации, которая выполняется таким образом, чтобы сохранить совместимость с немодифицированными системами.

Создание домена защищенных операционных систем существенно расширяет область их применения по обработке информации, позволяя проводить распределенную обработку ресурсов при сохранении мандатного механизма доступа к данным.

СПИСОК ЛИТЕРАТУРЫ:

1. *Гольдштейн А. Б.* Исследование механизма туннелирования мультимедийного трафика в сети MPLS. Дисс. … канд. техн. наук. СПб., 2004.
2. *Гольдштейн А. Б, Гольдштейн Б. С.* Технология и протоколы MPLS. СПб.: БХВ-Санкт-Петербург, 2005.

А. А. Краснопевцев

О ЗАЩИТЕ ПРИЛОЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ВНЕШНЕГО АППАРАТНОГО МОДУЛЯ

В рамках работы проводилось исследование различных способов защиты программного обеспечения от несанкционированного копирования. В результате проведенного анализа для приложений, компилируемых в некоторое промежуточное представление, т. е. выполняемых на некоторой виртуальной машине, а не на реальном процессоре, было выявлено, что применение существующих