ЗАЩИТА ВИРТУАЛИЗАЦИИ С ИСПОЛЬЗОВАНИЕМ СИСТЕМ ПРИНУДИТЕЛЬНОГО КОНТРОЛЯ ДОСТУПА

УДК 004.056.53

Исаков Д.А., аспирант
кафедра мультимедиа технологий
Уральский федеральный университет, ВШЭМ

Аннотация. В статье описывается, как системы принудительного контроля доступа могут быть развернуты на ОС Linux для гипервизора KVM. Большое внимание уделяется двум системам с открытым исходным кодом: SELinux и AppArmor. Проводится анализ уровня безопасности этих систем поумолчанию. Особое внимание уделяется sVirt-технологии, реализованной для SELinux и AppArmor. Приводятся преимущества и недостатки SELinux и AppArmor, а также показывается необходимость развертывания системы принудительного контроля доступа в облачных инфраструктурах.

Ключевые слова: безопасность, виртуализация, принудительный контроль доступа.

Abstract. As the title implies the article describes how mandatory access control (MAC) systems can be deployed in Linux-based hypervisor KVM. Much attention is given to two open-source MAC systems: SELinux and AppArmor. Attempts are made to analyze basic security level of these MAC systems. It is spoken in detail about sVirt realization for SELinux and AppArmor. Conclusions are drawn about advantages and disadvantages of SELinux and AppArmor and recommendations are given to deploy MAC systems in cloud infrastructure.

Keywords: virtualization, sVirt, SELinux, KVM, AppArmor, policy, security, isolation.

Введение

Бурное развитие облачных технологий не изменило требований к обеспечению информационной безопасности: конфиденциальность, целостность и доступность. Пользуясь услугами облачных провайдеров, нельзя быть до конца уверенным в полной защищенности данных. Многие компании принимают альтернативное решение — создают собственное частное облако. Одним из ключевых этапов проектирования частного облака является выбор платформы виртуализации. При принятии данного решения компании руководствуются требованиями к функциональности гипервизора, его стоимостью, а также лицензией, по которой он распространяется. Кроме признанных лидеров таких, как Vmware и Microsoft, существует ряд решений, распространяемых под лицензией General Public License (GPL), например, Kernel-based Virtual Machine (KVM). Базовой операционной системой (ОС) для развертывания KVM является Debian. Данная ОС поддерживает две системы принудительного контроля доступа - Security-Enhanced Linux (SELinux) и AppArmor. В статье будет проведен анализ вышеуказанных систем

принудительного контроля доступа в разрезе обеспечения безопасности хостовой и гостевых ОС.

Системы принудительного контроля доступа

В современных ОС семейства Linux основной является дискреционная система контроля доступа, которая состоит из 3 групп (владелец, группа-владелец и остальные), а также из 3 возможных действий для этих групп: чтение, запись и выполнение. К сожалению, данная система контроля имеет несколько весьма ощутимых недостатков:

2. отсутствие централизованного контроля за информационными потоками;
3. пользователь определяет доступ к своим данным вне зависимости от глобальных политик;
4. в случае компрометации системы, права могут быть изменены без ведома самого владельца[1].

Системы принудительного контроля доступа также называют системами мандатного управления доступом. Информации, содержащейся в системе, присваиваются метки конфиденциальности. При доступе к информации происходит проверка разрешения субъекта на доступ к информации такого уровня конфиденциальности[2].

В ОС семейства Linux самыми распространенными являются 2 системы принудительного контроля доступа: SELinux и AppArmor. В обеих системах защита строится на политиках безопасности или профилях. За исполнение политик отвечает ядро. Обе системы работают поверх дискреционной модели доступа, дополняя ее. Существуют предустановленные политики, в которых определено соответствие между процессом и файлом. Главным различие между SELinux и AppArmor является способ определения объектов файловой системы. В случае SELinux используется жесткая ссылка, тогда как AppArmor использует полный путь.

Использование SELinux для защиты гипервизора KVM

Основным разработчиком SELinux сегодня является компания RedHat. В целях продвижения использования SELinux компания осуществляет активную доработку политик под программное обеспечение, например: веб-серверы, базы данных, почтовые серверы. Существует ряд булевых переменных, которые можно указать при создании собственной политики, отключив, например, сетевой доступ к гостевой ОС или доступ к USB устройствам[3]. По умолчанию, существует политика, которая защищает хостовую ОС от скомпрометированной виртуальной машины. Все запускаемые виртуальные машины по умолчанию имеют домен qemu_t. А любой образ диска виртуальной машины имеет тип virt_image_t. Все чаще производитель по умолчанию запрещает загрузку виртуальных машин, использующих образа, находящиеся не в /var/lib/libvirt/images. Таким образом, в случае компрометации виртуальной машины получение доступа к директориям типа /etc, /usr, / хостовой ОС невозможно, если на них не установлен домен qemu_t, что является грубым нарушением принципа наименьших привилегий.

Существует дополнительная модель безопасности - проект sVirt, который позволяет обеспечить защиту гостевых операционных систем друг от друга. Если система была скомпилирована с поддержкой sVirt, то она будет всегда включена, когда включен SELinux. При использовании данной модели безопасности каждая виртуальная машина использует тип svirt_t, но с разными номерами категорий. Например, метка может выглядеть так: system_u:system_r:svirt_t:s0:c12,c23, где 12 и 23 — категории.

Существует 2 способа приписывания меток виртуальным машинам: вручную и динамически. При ручном приписывании меток на этапе создания виртуальной машины необходимо их приписать гостевой ОС и образам дисков. Динамическое приписывание меток осуществляется при каждой загрузке виртуальной машины демоном libvirtd. Если диск является общим для нескольких гостевых ОС, то он получит общую метку system_u:system_r:svirt_image_t:s0. Диски, помеченные «только для чтения», получат метку system_u:system_r:svirt_content_t:s0.

Таким образом, применение расширения sVirt для SELinux существенно увеличивает безопасность, позволяя ограничить не только доступ к хостовой ОС из скомпрометированной виртуальной машины, но и не позволяет получить доступ к ресурсам других виртуальных машин.

Использование AppArmor для защиты гипервизора KVM

Система AppArmor была разработана компанией Novell. Сейчас разработку продолжает компания Canonical, которая начиная с версии Ubuntu 7.04 включила данную систему в официальный репозиторий, а с версии Ubuntu 8.04 идет вместе с дистрибутивом и запускается по умолчанию. Для каждой программы в системе, контроль исполнения которой необходим, нужно создать профиль безопасности, определив в нем доступ к каталогам, другим программам и ресурсам ОС. Существует две серьезные проблемы, которые пока не решены. Возможность выхода из-под контроля, используя жесткую символическую ссылку, т.к. контроль осуществляется с использованием в профиле полного пути до файла, а не его функционала или возможностей. Причиной второй проблемы также являются пути к файлам. Общеизвестно, что атакующие очень часто используют папку с временными файлами для начала атаки, а также генерируют случайные имена для своего вредоносного программного обеспечения. Таким образом, если программе нужен доступ в каталог /tmp для создания временного файла со случайным именем, то придется расширить права программы, что может привести к увеличению площади атаки[4].

Базовые настройки AppArmor позволяют защитить хостовую ОС от скомпрометированной гостевой ОС. Расширение sVirt позволяет защитить гостевые ОС друг от друга. Если на хостовой ОС в AppArmor создан профиль для демона libvirtd, то для каждой гостевой машины при старте будет также создан уникальный профиль, если администратор не создал его раньше вручную. Имя для профиля берется из UUID виртуальной машины, сам профиль содержит все необходимые правила для доступа к дискам и другим

ресурсам. Невозможность доступа к ресурсам других гостевых ОС обеспечивается созданием уникального профиля перед стартом виртуальной машины. По умолчанию в профиль копируются настройки, которые используются для /usr/sbin/libvirtd. Профиль для демона libvirtd должен быть загружен до запуска самого демона на хостовой ОС.

Заключение

Сравнивая SELinux и AppArmor, нельзя не отметить тот факт, что SELinux является более продвинутым средством обеспечения безопасности. Во-первых, при его настройке не требуется создавать профили для всех контролируемых программ, можно использовать одну политику для нескольких приложений. Во-вторых, динамическое присвоение категорий ускоряет развертывание виртуальных машин. В-третьих, SELinux развивается очень активно, возможно через некоторое время он де-факто станет стандартом для систем принудительного контроля доступа ОС семейства Linux.

Использование систем принудительного контроля доступа существенно повышает безопасность гипервизора, а при внедрении расширения sVirt позволяет дополнительно изолировать гостевые виртуальные машины друг от друга. Однако данные системы требуют квалифицированного обслуживающего персонала, существенно удлиняют время ввода систем в эксплуатацию, особенно в случае, если конфигурация является сложной и не стандартной.

Список литературных источников

1. Безопасный Linux: Часть первая. AppArmor – песочница для приложений // developerWorks Россия URL: http://www.ibm.com/developerworks/ru/library/l-apparmor-1/index.html (дата обращения: 20.12.2014).

2. Mandatory access control // wikipedia.org

URL: http://en.wikipedia.org/wiki/Mandatory_access_control (дата обращения: 23.12.2014).

3. SELinux // redhat.com URL: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/5/html/Virtualization/sect-Virtualization-Security_for_virtualization-SELinux_considerations.html (дата обращения: 24.12.2014).

4. Безопасный Linux: Часть третья. Архитектура безопасности // developerWorks Россия

URL: http://www.ibm.com/developerworks/ru/library/l-apparmor-3/index.html (дата обращения: 24.12.2014).