УДК 681.3.07

А.В. Головин, В.В. Поляков, В.П. Каракулин

Частично контролируемая компьютерная система для критических приложений

Одной из наиболее серьезных проблем, затрудняющих широкое применение современных информационных технологий, является обеспечение их безопасности [1–3]. Особенно важна безопасность информации в так называемых критических приложениях, к числу которых относятся системы государственного и военного управления, объекты атомной энергетики, ракетно-космическая техника, а также финансовая сфера, нарушение нормального функционирования которых может привести к тяжелым последствиям для окружающей среды, экономики и безопасности государства.

Критические приложения современных информационных технологий представлены аттестованными полностью контролируемыми компьютерными системами (КС) с программной реализацией их функций. Однако поддержание целостности программ в процессе запуска и, особенно, в процессе функционирования КС является трудной задачей [4].

Для построения надежной защиты КС ее разработчик должен владеть наиболее полными знаниями о конкретной операционной системе (ОС), под управлением которой будет работать полностью контролируемая КС. К таким ОС, распространяемым на правах свободных лицензий в виде исходного кода, транслируемого в исполняемый код аттестованным компилятором, относят Linux. Linux является одним из стандартов для файловых серверов и серверов приложений. Структура этой ОС и применяемые политики безопасности делают Linux уязвимой лишь из-за ошибок, присутствующих в ее коде. Однако отсутствие развернутой системы управления безопасностью в Linux вынуждает предоставлять пользователям и процессам права существенно большие, чем наименьшие необходимые. Некоторые действия могут потребовать даже прав суперпользователя, что крайне опасно из-за уязвимости КС.

Одной из основных проблем всякой ОС является большое количество строк ее кода, что практически исключает полный контроль исходных текстов ОС. По данным, приведенным в работе [5], ядро Linux содержит примерно 15000 ошибок, Windows XP – как минимум в два раза больше, количество ошибок в коде драйверов устройств – еще больше. Вследствие этого злоумышленники могут пытаться внедрить в исходный код тщательно замаскированные закладки, что позволит получить контроль над КС.

Поэтому представляет интерес разработка частично контролируемой КС на основе Linux.

Безопасность в таких КС может быть обеспечена:

– использованием специальных аттестованных (полностью контролируемых) аппаратно-программных средств, выполняющих ряд защищенных операций и играющих роль специализированных модулей безопасности;

– изоляцией от злоумышленника ненадежной компьютерной среды, отдельного ее компонента или отдельного процесса с помощью полностью контролируемых средств.

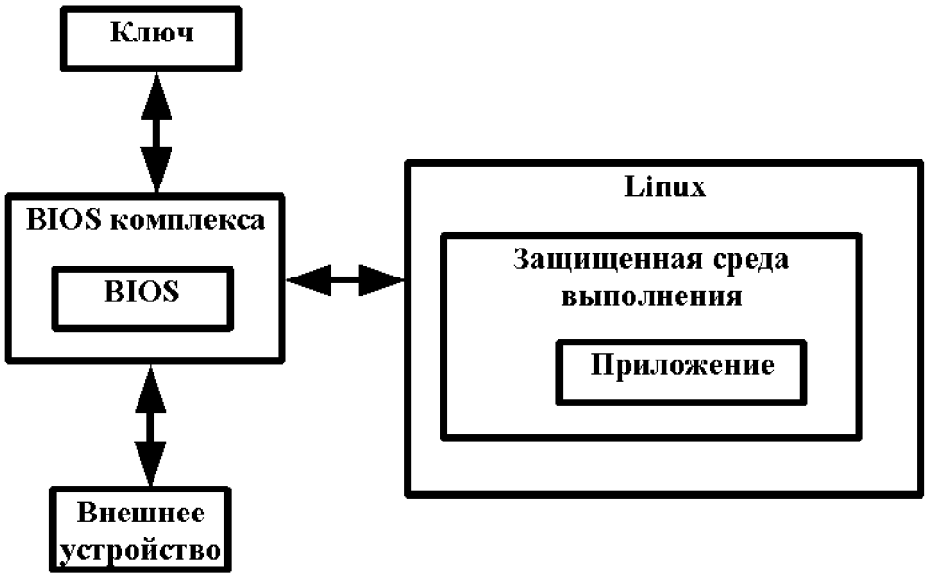
Часть этих требований может быть выполнена штатными расширениями Linux. Прежде всего, это Hardened Linux – набор политик отбора безопасного кода приложений в среде Linux, и Security-Enhanced Linux (SELinux), добавляющий в систему новые элементы защиты.

SELinux представляет собой набор технологий расширения системы безопасности Linux – это три новые технологии: мандатный контроль доступа (МКД), ролевой доступ и система типов [6].

МКД реализует принцип «наименьших необходимых привилегий» – один из основных принципов безопасности SELinux. Важно, что МКД предоставляет разные наборы прав разным процессам, и, что очень важно, не позволяет пользователю (случайно или намеренно) изменить эти права.

Роли представляют собой наборы привилегий. В любой момент времени каждый пользователь может выступать в одной из доступных ему ролей. Роли позволяют предоставлять пользователям дополнительные привилегии без утраты идентичности пользователя. Политика безопасности SELinux определяет правила перехода из одной роли в другую. Не всякий переход из одной роли в другую допустим.

Типы объединяют группы субъектов и объектов, предоставляя им определенные права. Основной функцией типов является ограничение возможных действий субъекта над объектом. В SELinux действует механизм принудитель-



Структурная схема защищенной компьютерной системы

ного присвоения типов, в соответствии с которым каждый процесс принадлежит к определенному типу, определяющему права этого процесса.

Современная КС, подлежащая аттестации по требованиям безопасности и удовлетворяющая требованиям адекватности, унификации, инвариантности и абсолютности защиты, должна разрабатываться на основе программно-аппаратных решений [7–8].

Для выполнения критических приложений предлагается КС на основе SELinux, дополненная программно-аппаратными средствами защиты. Принципиально важным является то, что разработанная программно-аппаратная компонента является самостоятельным программным продуктом, внешним по отношению к ОС, что сохраняет возможность независимо обновлять версии ОС и приложений.

Структурная схема такой КС изображена на рисунке. Эта КС включает программно-аппаратную поддержку:

– идентификации и аутентификации пользователя, с использованием персональных данных и ключа на этапе идентификации;

– разграничения доступа пользователей и приложений к внешним устройствам и ресурсам КС, с использованием как дискреционного, так и мандатного метода разграничения доступа;

– контроля целостности программ, данных и системных областей дисков;

– организации функционально замкнутого пространства выполнения приложений.

Критичные для безопасности части кода и данных КС хранятся на флэш-компоненте, что, с одной стороны, облегчает обновление, а с другой – повышает степень защиты от перезаписи вирусами или от атак хакеров. КС такого типа могут быть уязвимыми из-за допущенных во время конфигурации ошибок. Такие уязвимости быстро устраняются путем обновления программного обеспечения.

Основой рассматриваемой КС является Gentoo Linux с расширением SELinux. Особое внимание уделяется конфигурации и контролю за драйверами. Основной контроль осуществляется при помощи защищенной среды выполнения – типов (доменов) SELinux. Контроль обмена информацией с внешними устройствами производит программно-аппаратная компонента.

При включении КС, до загрузки ОС, производится идентификация и аутентификация пользователя аппаратными средствами. Современные требования к системам контроля и управления доступом (СКУД) требуют установки повышенной защиты. Наибольшее применение нашли алгоритмы многофакторной идентификации и аутентификации [9]. В рассматриваемой КС реализован алгоритм, являющийся модификацией алгоритма прохода по двум ключам – алгоритм «код + брелок» с возможностью ввода модифицированного кода [10].

Контроль целостности программ и данных производится через заданный интервал времени программой контроля на предмет совпадения размера, даты модификации и контрольной суммы заданных файлов, и при изменении контролируемых параметров происходит восстановление испорченного файла из резерва.

Основным механизмом противодействия скрытым угрозам может служить обеспечение замкнутости программной среды [8]. Корректно настроенная замкнутая программная среда КС эффективно противодействует запуску злоумышленником собственных программ, являясь основной защитой от вирусных атак.

Для удобной и корректной настройки эксплуатационных параметров КС администратором безопасности (с правами, отличными от прав суперпользователя) разработана графическая программа – Центр управления безопасностью КС.

Разработанная КС предлагается в качестве частично контролируемой компьютерной системы с повышенными требованиями к безопасности, в частности, как основа автоматизированных рабочих мест обслуживания защищенного документооборота.

Литература

1. Ярочкин В.И. Информационная безопасность. – М., 2003.

2. Лосев С. Информационная безопасность снаружи и изнутри // Сетевой журнал. – 2005. – №3.

3. Черняк Л. Новые задачи информационной безопасности // Открытые системы. – 2005. – №5–6.

4. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. – М., 1999.

5. Таненбаум Э. Надежные и защищенные операционные системы? / Э. Таненбаум, Д. Хердер, Х. Бос // Открытые системы. – 2006. – №6.

6. Боровский А. SELinux — система повышенной безопасности // Открытые системы. – 2005. – №4.

7. Онучин С. Устройства защиты информации. Критерии выбора // Мир связи: Connect! – 1999. – №9.

8. Трубников А.Н. Оценка эффективности систем защиты от НСД // Информационное противодействие угрозам терроризма. – 2005. – №5.

9. Шрамко В.Н. Комбинированные системы идентификации и аутентификации // PCWeek/RE. – 2004. – №45.

10. Омельянчук А.М. Усиленные алгоритмы в системах доступа особо важных объектов. // Системы безопасности. – 2005. – №2.