УДК 004

Формирование критериев сравнения модулей доверенной загрузки

Е. Г. Чепанова
ЗАО «ОКБ САПР», Москва, Россия

Рассмотрен вопрос выбора средств доверенной загрузки. Предложена методика формирования критериев сравнения, учитывающая реальные качества технических систем, в которых предполагается использование модулей доверенной загрузки, — их характеристики, уязвимости и цели нарушителей.

Ключевые слова: модуль доверенной загрузки, критерии сравнения, способы реализации атак, защитные меры, нарушитель информационной безопасности.

Под модулями доверенной загрузки (МДЗ) понимаются средства, предназначенные для обеспечения принудительной загрузки разрешенной операционной системы (ОС) с определенного носителя тем пользователем, которому разрешена работа на этом компьютере.

Количество существующих на рынке средств обеспечения доверенной загрузки достаточно велико. Чтобы не потеряться в их многообразии и иметь возможность сопоставлять их между собой, необходимы критерии сравнения. Критерии сравнения МДЗ могут быть полезны как разработчику МДЗ при определении функционала разрабатываемого средства защиты, так и конечным пользователям, перед которыми встал вопрос о выборе МДЗ.

Критерии формируются таким образом, что в них не навязывается конкретная реализация функций защиты.

Алгоритм формирования критериев изображен на рис. 1.

Рассмотрим подробнее этапы реализации представленного алгоритма.

Как правило, в типовой информационной системе используется разделение всех нарушителей на группы по признаку принадлежности к системе:

- внешние нарушители — физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование системы;
- внутренние нарушители — физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование системы.

Рис. 1. Алгоритм формирования критериев

К целям нарушителя информационной безопасности обычно относят:

- получение контроля над функционированием системы;
- получение контроля над ресурсами пользователей.

При этом предполагается, что все действия внешних нарушителей пресекаются организационными мерами.

Характеристики рассматриваемой типовой компьютерной системы:

- обеспечивается физическая защита средств вычислительной техники, доступ к которым кон-

Чепанова Екатерина Геннадьевна, аналитик.
E-mail: chepanova@okbsapr.ru

Статья поступила в редакцию 14 июня 2014 г.

тролируется с применением МДЗ, от внешних нарушителей;

- на компьютер с проверенным BIOS установлена проверенная (лицензионная) ОС;
- администратор безопасности является доверенным лицом;
- пользователям предоставляются различные права доступа к ресурсам системы;
- допускается загрузка ОС с внешнего носителя;
- аутентификация пользователя при входе в ОС осуществляется по паролю средствами ОС;
- данные о действиях пользователя записываются в системный журнал регистрации событий в соответствии с настроенными правилами аудита;
- к компьютеру подключено некоторое периферийное оборудование;
- оборудование компьютерной системы периодически подвергается модернизации.

Определены уязвимости защищаемой системы, которые потенциально может использовать нарушитель для достижения своих целей. Каждой уязвимости в соответствие поставлен свой набор способов реализации атак. После рассмотрения полученных сочетаний "уязвимость — способ реализации атаки" выбраны защитные меры (ЗМ), позволяющие блокировать выявленные уязвимости и обеспечивать минимально необходимый уровень защиты.

При этом выбор ЗМ, очевидно, оказывает влияние на исходное состояние системы, в общем случае связанное с изменением ее характеристик. Этим обусловлена необходимость рассмотрения аналогичным образом преобразованной системы. Таким образом, описанный процесс является циклическим. Предполагается, что в качестве условия прекращения поиска уязвимостей для преобразованной в результате прохождения очередной итерации системы может быть рассмотрена необходимость получения со стороны нарушителя неограниченного физического доступа к средству защиты (отключение средства защиты) для успешной реализации атаки (предполагается, что блокирование этой уязвимости должно выполняться с использованием комплекса организационно-технических мер).

В табл. 1 описаны уязвимости типовой системы: указаны способы реализации атак с использованием таких уязвимостей, характеристики системы, обуславливающие наличие уязвимостей, а также предложены ЗМ для блокирования каждой из них.

Описание уязвимостей после принятия первой группы ЗМ отображено в табл. 2. Некоторые ЗМ из табл. 2 являются конечными.

Описание уязвимостей системы после принятия второй группы ЗМ приведено в табл. 3.

Таблица 1

Описание уязвимостей системы

Уязвимость	Способы реализации атак	Характеристика системы, обуславливающая существование уязвимости	Принимаемая защитная мера
Штатная возможность загрузки ОС с внешнего носителя	Загрузка нештатной ОС с внешнего носителя	Допускается загрузка ОС с внешнего носителя	Блокировка загрузки ОС с внешнего носителя
Штатная возможность загрузки ОС любым пользователем, имеющим физический доступ к компьютеру	Загрузка ОС любым пользователем, имеющим физический доступ к компьютеру	Аутентификация осуществляется средствами ОС	Предъявление пароля до загрузки ОС
Возможность несанкционированной модификации программного обеспечения (ПО), системных файлов, конфигурации оборудования, реестра, файлов пользователя	Осуществление подмены системных файлов/ПО/файлов пользователя	Пользователям предоставляются различные права доступа к информационным ресурсам	Контроль целостности ПО, системных файлов, конфигурации оборудования, реестра, файлов пользователя
	Внедрение вредоносного ПО, осуществляющего модификацию программной среды/системных файлов/ реестра/файлов пользователя		
	Модификация программных средств/файлов пользователя с использованием штатных средств		
	Несанкционированное удаление программ/системных файлов/файлов пользователя		
	Подмена оборудования на оборудование с уязвимостями и недокументированными (недекларированными) возможностями		
	Несанкционированное изменение конфигурации оборудования		

Таблица 2

Описание уязвимостей системы после принятия первой группы защитных мер

Уязвимость	Способы реализации атак	Характеристика системы, обуславливающая существование уязвимости	Принимаемая защитная мера
При возникновении сбоев может быть необходима загрузка администратором с внешнего носителя	Выход/вывод системы из строя	Блокировка загрузки ОС с внешнего носителя	Запрет загрузки с внешнего носителя всем пользователям, кроме персонала, управляющего СЗИ
Использование нестойких паролей	Получение пароля методом перебора	Предъявление пароля до загрузки ОС	Предъявление аппаратного идентификатора
	Перехват пароля		
	Получение несанкционированного доступа к месту хранения паролей		
Хранение эталонных значений контрольных сумм (КС) ПО, системных файлов, конфигурации оборудования, реестра, файлов пользователя в открытом виде	Несанкционированное изменение ПО/системных файлов/конфигурации оборудования/реестра/файлов пользователя и (или) файла хранения КС	Контроль целостности ПО, системных файлов, конфигурации оборудования, реестра, файлов пользователя	Хранение эталонных значений КС в закрытой памяти
Хранение ПО МДЗ на жестком диске компьютера	Модификация процедур МДЗ	МДЗ обладает собственным ПО	Выполнение процедур контроля на аппаратном уровне
Несоответствие МДЗ изменяющимся требованиям по производительности, функциональности, совместимости и реализации интерфейса	Реализация атак, направленных на функции МДЗ, которые некорректно выполняются вследствие несоответствия развитой системе	Потребность в развитии (модернизации, расширении, обновлении) системы	Своевременное обновление ПО МДЗ
	Реализация атак, которые связаны с использованием новых возможностей системы		

Таблица 3

Описание уязвимостей системы после принятия второй группы защитных мер

Уязвимость	Способы реализации атак	Характеристика системы, обуславливающая существование уязвимости	Принимаемая защитная мера
Хранение идентификационных данных пользователя в открытом виде	Получение несанкционированного доступа к месту хранения идентификационных данных	Предъявление пароля и аппаратного идентификатора до загрузки ОС	Хранение идентификационных данных пользователя в закрытом виде (зашифрованными или в закрытой памяти)
Использование модифицированных пакетов обновления	Использование пакетов обновления с ошибками или закладками, способными привести к сбоям в работе МДЗ	Возможность своевременного обновления ПО МДЗ	Защищенное обновление МДЗ
Обновление ПО МДЗ любым пользователем, имеющим доступ к компьютеру	Несанкционированное обновление ПО с использованием вредоносных программ		
	Случайное обновление ПО МДЗ		
Обновление ПО МДЗ через ОС без вскрытия системного блока компьютера	Случайное обновление ПО МДЗ		

С учетом условия, на котором нужно остановиться в выявлении уязвимостей, предложенные в табл. 3 ЗМ являются конечными.

Сравниваемые МДЗ должны обеспечивать достижение конечных характеристик системы. Следовательно, в процессе анализа должно быть проверено наличие у рассматриваемых МДЗ функций, позволяющих достигнуть системы с такими характеристиками, а значит, критерии сравнения должны быть следующими:

- наличие возможности загрузки компьютера с внешнего носителя персоналом, управляющим

СЗИ, отсутствие такой возможности для всех остальных пользователей;

- наличие возможности и организация хранения идентификационных данных пользователя в закрытом виде;
- наличие предусмотренного порядка хранения эталонных значений КС в закрытой памяти;
- наличие возможности своевременного обновления ПО МДЗ;
- наличие процедур, обеспечивающих безопасность обновления ПО;
- обеспечение выполнения процедур контроля на аппаратном уровне.

Полученные критерии используются для проверки соответствия им сравниваемых МДЗ. Степень соответствия МДЗ критериям — показатель достижения системой с таким МДЗ необходимого уровня защищенности. Несоответствие МДЗ выдвинутым в этом документе требованиям не означает, что такое средство непригодно для использования, оно лишь означает, что для достижения необходимого уровня защищенности, возможно, понадобится применение дополнительных мер защиты.

Полученные результаты соответствия/несоответствия оцениваемого МДЗ приведенным критериям можно использовать двумя способами — для определения списка компенсирующих мер, которые будет необходимо принять в случае выбора намеченного МДЗ, либо для сравнения решений, обеспечивающих доверенную загрузку, и дальнейшего выбора оптимального решения на основе результатов этого сравнения.

Formation the comparison criteria of trusted startup hardware modules

E. G. Chepanova
OKB SAPR JSC, Moscow, Russia

The article is devoted to the choice of trusted startup tools. It is proposed a method of forming the comparison criteria, taking into account the real quality of the technical systems that include the use of trusted startup hardware modules – their characteristics, vulnerabilities and targets of attackers.

Keywords: trusted startup hardware module, the comparison criteria, the methods realization of attacks, protective measures, attackers of information security.

Received June 14, 2014