Сведения об авторах

Владимир Александрович Батура — аспирант; Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, кафедра вычислительной техники; E-mail: batu-vladimir@yandex.ru

Александр Ювенальевич Тропченко — д-р техн. наук, профессор; Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, кафедра вычислительной техники; E-mail: tau@d1.ifmo.ru

Рекомендована кафедрой вычислительной техники

Поступила в редакцию 23.12.13 г.

УДК 004.056.53

К. А. Щеглов, А. Ю. Щеглов

НЕПРОТИВОРЕЧИВАЯ МОДЕЛЬ МАНДАТНОГО КОНТРОЛЯ ДОСТУПА

Исследована модель мандатного контроля доступа, выявлены противоречия и недостатки, не позволяющие реализовать на ее основе безопасную систему. Разработаны и обоснованы модель целостности и доступности и „непротиворечивая модель мандатного контроля доступа“, применение которой позволяет предотвращать нарушение конфиденциальности информации, а также решать задачи обеспечения ее целостности и доступности в комплексе.

Ключевые слова: *защита информации, контроль доступа, правила доступа, мандат, категории информации, уровни конфиденциальности.*

Введение. Сегодня широкое практическое применение нашла модель мандатного контроля доступа, основанная на использовании меток безопасности (или мандатов) [1]. Эта предложенная Белла—ЛаПадулой [2] модель, согласно нормативному документу в области информационной безопасности [1], предназначена для использования в наиболее критичных приложениях с целью защиты обрабатываемой информации от нарушения конфиденциальности. Однако существует и альтернативная модель мандатного контроля доступа, предложенная Бибом [3], предназначенная для обеспечения целостности и доступности информации. Правила контроля доступа, определяемые этими моделями, полностью исключают друг друга. Вместе с тем задачи защиты конфиденциальности информации и обеспечения ее целостности и доступности системы должны решаться комплексно.

Альтернативные модели мандатного контроля доступа. Основу мандатного контроля доступа составляет возможность ранжирования (присвоения категории) обрабатываемой информации на основании какого-либо признака.

Практика секретного делопроизводства в компьютерной обработке информации, согласно модели Белла—ЛаПадулы [2], предполагает классификацию информации по уровням конфиденциальности.

Метки безопасности *объектов* отражают категорию конфиденциальности информации, которые могут быть сохранены в соответствующих объектах. Метки безопасности *субъектов* отображают полномочия или уровень допуска (по аналогии с формой допуска в секретном делопроизводстве) субъектов к информации различных уровней конфиденциальности.

Будем считать, что чем больше полномочия субъекта C и выше уровень конфиденциальности объекта O, тем меньше их порядковый номер в упорядоченных множествах:

$C = \{C_1, \ldots, C_l\}$ и $O = \{O_1, \ldots, O_l\}$ и тем меньшее значение метки безопасности M_i ($i = 1, \ldots, l$) им присваивается, т.е. $M_1 < M_2 < M_3 < \ldots < M_l$.

Таким образом, в качестве учетной информации каждому субъекту и объекту задаются метки безопасности из множества M. В общем случае метка присваивается группе равноправных (имеющих одинаковые полномочия) субъектов и группе объектов одного уровня конфиденциальности.

Обозначим метку безопасности субъекта (группы субъектов) и объекта (группы объектов) доступа как M_c и M_o.

Модель Белла—ЛаПадулы обеспечивает реализацию следующих правил, направленных на предотвращение понижения категории информации в процессе ее обработки:

1) субъект C имеет доступ к объекту O в режиме чтения, если выполняется условие: $M_c \le M_o$;

2) субъект C имеет доступ к объекту O в режиме записи, если выполняется условие: $M_c = M_o$.

Иногда также рассматривается возможность записи и при условии: $M_c > M_o$.

Чем ниже уровень конфиденциальности информации, тем более широкие возможности по ее обработке предоставляются, например, могут использоваться неконтролируемые внешние накопители, принтеры или сетевые ресурсы. Таким образом, несанкционированное понижение категории обрабатываемой информации напрямую связано с изменением режима ее обработки и, как следствие, с возникновением „каналов“ ее хищения.

Согласно „модели целостности Биба“ [3], в систему включается иерархический признак „целостность“, отображаемый мандатом, или меткой безопасности. Вводятся уровни целостности, сопоставляемые с субъектами и объектами доступа, последним присваиваются метки безопасности. Соответствующим образом изменяются и правила контроля доступа:

1) субъект C имеет доступ к объекту O в режиме чтения, если выполняется условие: $M_c \ge M_o$;

2) субъект C имеет доступ к объекту O в режиме записи, если выполняется условие: $M_c \le M_o$.

Практическое использование этой модели, инверсии модели Белла—ЛаПадулы, остается под большим вопросом. В частности, модель Биба критикуется специалистами за то, что она использует целостность как некую меру, в то время как целостность субъектов и объектов следует рассматривать как двоичный атрибут, который или есть, или нет. Кроме того, не понятен принцип классификации субъектов и объектов по параметру „целостность“.

Предлагаемая модель целостности и доступности. Непротиворечивая модель мандатного контроля доступа. Существует множество угроз, связанных с атаками со стороны приложений, наделяемых соответствующими функциями в результате прочтения ими вредоносного файла (не являющегося исполняемым), записанного на компьютер в процессе работы пользователя. К подобным приложениям, например, относятся офисные, которые могут приобрести вредоносные функции в результате прочтения системой документа, наделенного макровирусом, всевозможные командные интерпретаторы, наделяемые дополнительным функционалом, в результате прочтения ими „активного“ содержимого, в частности, скриптов и ActiveX-компонентов [4] и др. Приложение, наделенное вредоносными функциями, получает право записи (а также модификации и удаления) во все объекты, доступ к которым разрешен пользователю.

Построим модель мандатного контроля доступа. Будем считать, что вероятность записи (сохранения в процессе работы) вредоносного файла субъектом C_i (i=1, …, l) составляет $P_i(w)$ (i=1, …, l). Также будем считать, что чем меньше значение $P_i(w)$ для субъектов, соответственно объектов, в который разрешена запись субъекту, тем меньше их порядковый номер в упорядоченных множествах субъектов и объектов — $C = \{C_1, \ldots, C_l\}$ и $O = \{O_1, \ldots, O_l\}$, и тем

меньшее значение метки безопасности M_i (i = 1, …, l) им присваивается, т.е.: $M_1 < M_2 < < M_3 < \ldots < M_l$, при условии, что $P_1(w) << P_2(w) << \ldots << P_l(w)$.

Принцип мандатного контроля доступа — информация различных категорий обрабатывается в различных режимах, с использованием разных устройств и объектов, что полностью соответствует заданному условию $P_1(w) << P_2(w) << \ldots << P_l(w)$.

Между отношениями для меток безопасности M_i (i = 1, …, l): $M_1 < M_2 < M_3 < \ldots < M_l$, назначаемых при обработке ранжированной информации, и для вероятностей записи вредоносного файла $P_i(w)$: $P_1(w) << P_2(w) << \ldots << P_l(w)$, существует прямая связь.

Построим модель мандатного контроля доступа, позволяющую обеспечить целостность и доступность обрабатываемой информации. Эта модель регламентирует следующие правила доступа:

1) субъект C имеет доступ к объекту O в режиме чтения, если выполняется условие: $M_c \geq M_o$;

2) субъект C имеет доступ к объекту O в режиме записи, если выполняется условие: $M_c \leq M_o$.

Как видим, правила доступа для предложенной нами модели и модели Биба идентичны, однако различие этих моделей принципиально. Модель целостности Биба предполагает включение в систему иерархического признака „целостность“, отображаемого меткой безопасности, в то время как в представленной, так же как и в модели Белла—ЛаПадулы, вводится классификация (ранжирование) информации по уровням конфиденциальности — метки отражают категорию конфиденциальности информации.

Как следствие, именно эти модели можно рассматривать в качестве альтернативных решений, поскольку они основаны на использовании одного и того же ранжирующего признака, при этом предложенная модель является полной инверсией модели Белла—ЛаПадулы.

Исходя из сказанного можно сделать важнейший вывод о том, что безопасная обработка ранжированной по уровням конфиденциальности информации в общем случае достигается при реализации следующих непротиворечивых правил доступа:

1) субъект C имеет доступ к объекту O в режиме чтения и записи, если выполняется условие: $M_c = M_o$;

2) субъект C не имеет доступа к объекту O, если выполняется условие: $M_c \geq M_o$.

Именно эта модель, на наш взгляд, имеет все основания быть позиционирована как непротиворечивая модель мандатного контроля доступа, определяющая непротиворечивые правила доступа, поскольку ее применение позволяет решать задачи обеспечения конфиденциальности, целостности информации и доступности в комплексе, т.е. позволяет построить безопасную систему.

Заключение. В работе исследованы основные модели мандатного контроля доступа, в результате чего разработаны модель целостности и доступности и „непротиворечивая модель мандатного контроля доступа“, определяющая корректные правила доступа при обработке ранжированной по уровням конфиденциальности информации. Применение непротиворечивой модели позволяет решать задачи защиты конфиденциальности информации и обеспечения ее целостности и доступности в комплексе, что дает возможность построить безопасную систему.

Полученный результат имеет большое практическое значение, поскольку исследования продемонстрировали принципиальные недостатки применяемой модели контроля доступа, причем применяемой в наиболее критичных приложениях, что регламентируется соответствующим нормативным документом в области информационной безопасности [1].

СПИСОК ЛИТЕРАТУРЫ

1. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. М., 1992.
2. *Bell D. E., LaPadula L. J.* Security Computer Systems: Unified Exposition and MULTICS Interpretation, Revision 1, US Air Force ESD-TR-306, MITRE Corporation MTR-2997. Bedford MA, March 1976.
3. *Biba K. J* Integrity Consideration for Security Computer System. The MITRE Corp., Report MTR N3153 Revision 1, Electronic System Division, U.S. Air Force Systems Command, Technical Report ESD TR 76 372. Belford, Massachusetts, April 1977.
4. *Щеглов К. А., Щеглов А. Ю.* Защита от атак со стороны приложений, наделяемых вредоносными функциями. Модели контроля доступа // Вопросы защиты информации. 2012. Вып. 4 (99). С. 31—36.

Сведения об авторах

Константин Андреевич Щеглов — студент; Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, кафедра вычислительной техники; E-mail: schegl_70@mail.ru

Андрей Юрьевич Щеглов — д-р техн. наук, профессор; Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, кафедра вычислительной техники; E-mail: info@npp-itb.spb.ru

Рекомендована кафедрой вычислительной техники

Поступила в редакцию 23.12.13 г.

УДК 004.056

Т. А. МАРКИНА, А. Ю. ЩЕГЛОВ

МЕТОД ЗАЩИТЫ ОТ АТАК ТИПА DRIVE-BY-ЗАГРУЗКА

Рассмотрены атаки типа drive-by-загрузка, использующие скриптовые вредоносные программы. Предложен метод защиты от таких атак, заключающийся в запрете загрузки (установки) или запуска несанкционированных скриптов (программ), запрете запуска несанкционированных скриптов под видом санкционированных и запрете модификации санкционированных скриптов. Продемонстрирована реализация этого метода.

Ключевые слова: *вредоносные программы, скрипт, защита информации, drive-by-атака, антивирусная программа.*

Введение. Одним из наиболее распространенных методов заражения компьютеров вредоносными программами, по данным компании „Лаборатория Касперского“, являются drive-by-атаки [1]. Практически весь TOP 20 [1] детектируемых web-антивирусом объектов состоит из скриптовых вредоносных программ, которые принимают участие в таких атаках. Стоит отметить, что атаки типа drive-by используют только скриптовые вредоносные программы.

Общее количество сайтов, использующихся в данных атаках, к концу июня 2013 г., по данным лаборатории McAfee, превысило 74,7 млн, что соответствует 29 млн доменных имен. Наиболее критично то, что 96% вредоносных доменов используются для атак drive-by [2].

Описание атаки drive-by. Рассмотрим технологию атаки (рис. 1). Первое время злоумышленники, применявшие загрузки drive-by, создавали вредоносные сайты и, чтобы привлечь на них посетителей, использовали социальную инженерию. Такие web-страницы до сих пор остаются основным источником вредоносной сетевой активности. Однако в последнее время хакеры заражают вполне „законопослушные“ сайты, размещая на них скриптовые