ются всевозможные имена вида *доменное_имя|доменная_зона2.доменная_зона1*, где операция | — операция конкатенации, *доменная зона2* принимает все значения из списка возможных доменных зон для доменного имени *доменное_имя*. Такая мера целесообразна, поскольку при разработке фишинговых ресурсов злоумышленники часто используют «двойные» доменные зоны.

Система защиты от фишинговых атак

На основе полученных результатов может быть создана полноценная система защиты от фишинговых атак. Предлагается следующая схема функционирования такой системы защиты для каждого информационного ресурса:

1) генерация списка потенциально опасных доменных имен;
2) получение списка зарегистрированных и доступных потенциально опасных информационных ресурсов;
3) определение степени опасности каждого из потенциально опасных информационных ресурсов;
4) пополнение антифишинговых баз вновь обнаруженными опасными ресурсами.

Для обеспечения высокой степени защиты ресурса необходимо регулярно повторять последовательность действий 2 — 4 и проводить непрерывное обучение системы.

ЛИТЕРАТУРА

1. *Lininger R. and Vines D.* Phishing: Cutting the Identity Theft Line. Wiley, 2005. 334 p.
2. *Bay H., Ess A., and Tuytelaars T.* SURF: Speeded Up Robust Features // Computer Vision and Image Understanding (CVIU). 2008. V. 110. No. 3. P. 346–359.
3. *Зеленков Ю. Г., Сегалович И. В.* Сравнительный анализ методов определения нечетких дубликатов для Web-документов // Труды 9 Всерос. науч. конф. «Электронные библиотеки: перспективные методы и технологии, электронные коллекции» — RCDL'2007. Переславль-Залесский, Россия, 2007. С. 166–174.

УДК 004.94

ПОДХОДЫ К РАЗРАБОТКЕ ДИСКРЕЦИОННОЙ ДП-МОДЕЛИ СОВРЕМЕННЫХ ЗАЩИЩЕННЫХ ОПЕРАЦИОННЫХ СИСТЕМ[1]

В. Г. Проскурин

Рассматривается дискреционная ДП-модель, развивающая и конкретизирующая существующие ДП-модели для случая, когда моделируемая компьютерная система является защищенной операционной системой (ОС). Далее будем называть предлагаемую модель ЗОС ДП-моделью. Она основывается на базовой ДП-модели [1], ФПАС ДП-модели [2] и ФС ДП-модели [3], а также отчасти на модели мандатной политики целостности информации Биба [1]. Будем использовать систему обозначений [1].

Предлагаемая модель характеризуется следующими основными отличиями от ранее разработанных ДП-моделей.

1. В модель вводится новый элемент — множество учетных записей пользователей U. Права доступа к сущностям назначаются не напрямую субъектам, как в других ДП-моделях, а учетным записям пользователей, которые делегируют права доступа субъектам, выполняющимся от имени соответствующей учетной записи. Другими словами, множество разрешенных прав доступа R определяется как подмножество множества $U \times (E \cup U) \times R_r$. Задается отображение $user : S \to U$, определяющее для каждого

[1]Работа выполнена при поддержке Министерства образования и науки Российской Федерации.

субъекта, от имени какой учетной записи он выполняется. Для каждой учетной записи $u \in U$ задается множество параметрически ассоциированных с ней сущностей $]u[$, реализация от каждой из которых информационного потока по памяти к субъекту позволяет породить нового субъекта от имени учетной записи u. При этом сущности, параметрически ассоциированные с учетной записью, не обязательно являются параметрически ассоциированными с субъектом, порожденным от имени данной учетной записи. По аналогии с множеством доверенных субъектов L_S среди учетных записей выделяется подмножество доверенных учетных записей L_U.

2. В дополнение к правам доступа $read_r$, $write_r$, $execute_r$, own_r, традиционно рассматриваемым в дискреционных ДП-моделях, вводится право доступа $grant_r$, позволяющее формализовать ситуацию, когда субъект-владелец предоставляет к сущности ограниченный доступ субъектам, выполняющимся от имени других учетных записей.

3. В модель вводятся новые элементы: множество видов совместного доступа $Share = \{read_a, write_a\} \subset R_a$ и две функции — $sa : E \setminus S \to 2^{Share}$, задающая текущие доступы к сущностям, не являющимся субъектами, и $sm : E \setminus S \to 2^{Share}$, задающая разрешенные совместные доступы к сущностям, не являющимся субъектами. При формальном описании доступа субъекта к объекту учитывается совместный доступ, т. е. множество доступов A определяется как подмножество множества $S \times E \times R_a \times 2^{Share}$. Перечисленные новые элементы модели позволяют формализовать ситуацию, когда субъект s_1, имеющий право $read_r$ или $write_r$ на доступ к некоторой сущности e, не может реально осуществить доступ $read_a$ или соответственно $write_a$, поскольку другой субъект s_2 уже осуществляет к сущности e доступ, не допускающий совместного использования данной сущности более чем одним субъектом. Рассматриваются совместные доступы $read_a$ и $write_a$, по определению устанавливается, что доступы $read_a$ совместимы между собой, но несовместимы с доступами $write_a$, а доступ $write_a$ к сущности может осуществляться субъектом только в монопольном режиме. Данное допущение описывает наиболее типичный сценарий организации совместного доступа к объектам; другие сценарии (например, комбинация параметров $GENERIC\_READ$ и $FILE\_SHARE\_WRITE$ в терминах $Windows$) реализуются крайне редко, в основном при обращениях к файлам баз данных, формализация доступа к которым далеко выходит за рамки предлагаемой модели.

4. Для каждого права доступа $r \in R$ к сущности $e \in E$ вводится множество (возможно, пустое) сущностей-параметров $](e, r)[$, не являющихся субъектами. Если для некоторой конкретной пары (e, r) множество $](e, r)[$ непусто, то для реализации доступа к сущности субъекту необходимо реализовать к себе информационные потоки по памяти от всех сущностей из $](e, r)[$. Введение в ДП-модель сущностей-параметров позволяет формализовать непрямые доступы субъектов к сущностям, требующие временной смены эффективного идентификатора учетной записи, от имени которой выполняется субъект (*su*, *sudo*, $SUID/SGID$ в $UNIX$, олицетворение учетной записи в $Windows$ и т. п.), либо других, более сложных взаимодействий субъекта со специальными сущностями ОС (UAC в Windows и т. п.).

5. В модель вводятся новые элементы, позволяющие формально описать систему мандатного контроля целостности (MIC), входящую в ОС семейства $Windows$ начиная с версии $WindowsVista$. К этим элементам относятся линейная шкала $(LI, \leqslant)$ поддерживаемых уровней целостности, функция $i_u : U \to LI$, устанавливающая максимально допустимый уровень целостности для субъектов, выполняющихся от имени заданной учетной записи, функция $i_s : S \to LI$, задающая текущий уровень целостности субъекта, и функция $i_e : E \setminus S \to LI$, задающая уровень целостности для сущ-

ностей, не являющихся субъектами. Без ограничения общности можно рассматривать случай, когда в моделируемой системе заданы только два уровня мандатной целостности — низкий и высокий.

6. В правила преобразования состояний ЗОС ДП-модели добавлены два новых правила: $create\_first\_subject$, формализующее порождение первого субъекта в сеансе работы пользователя с моделируемой системой, и $delete\_access$, формализующее прекращение доступа субъекта к сущности и обусловленное этим снятие ограничений по совместному доступу к данной сущности.

Предлагаемая ЗОС ДП-модель позволяет применять научный аппарат ДП-моделей к задачам формального описания и научного обоснования различных практических решений, реализуемых в современных защищенных ОС. В частности, предполагается использовать ЗОС ДП-модель в рамках работ по повышению защищенности отечественных ОС.

ЛИТЕРАТУРА

1. *Девянин П. Н.* Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учеб. пособие для вузов. М.: Горячая линия-Телеком, 2011. 320 с.
2. *Колегов П. Н.* ДП-модель компьютерной системы с функционально и параметрически ассоциированными с субъектами сущностями // Вестник Сибирского государственного аэрокосмического университета им. акад. М. Ф. Решетнева. 2009. Вып. 1(22). Ч. 1. С. 49–54.
3. *Буренин П. Н.* Подходы к построению ДП-модели файловых систем // Прикладная дискретная математика. 2009. № 1(3). С. 93–112.