Другим способом снижения пропускной способности рассматриваемого информационного потока является контроль частоты создания слушающих сокетов. Однако введение в ОС таких изменений может значительно снизить скорость взаимодействия процессов между собой с использованием интерфейса сокетов.

ЛИТЕРАТУРА

1. ГОСТ Р 53113-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Ч. 1. Общие положения. М.: Стандарты, 2008.
2. *Efstathopoulos P. O. and Krohn И. O.* Labels and Event Processes in the Asbestos Operating System // Proceedings of the SOOP'05. ACM, 2005.
3. *Девянин П. Н.* Анализ безопасности управления доступом и информационными потоками в компьютерных системах. М.: Радио, 2006. 176 с.

УДК 004.94

## О ПОСТРОЕНИИ ИЕРАРХИЧЕСКОГО РОЛЕВОГО УПРАВЛЕНИЯ ДОСТУПОМ

Д. Н. Колегов

Рассматривается подход к построению ролевого управления доступом для компьютерных систем (КС) с иерархией сущностей, отражающей организационно-управленческие отношения.

В моделях ролевого управления доступом семейства *RBAC* [1], как и в других известных ролевых моделях и их расширениях [2, 3], не используются механизмы задания и проверки разрешённых прав доступов субъекта к сущности, учитывающие уровни иерархии сущностей КС.

В реальных КС, в которых одновременно могут работать сотни пользователей, структура ролей может быть очень сложной, а количество различных прав доступа значительным — проблема реализации и администрирования системы управления доступом является чрезвычайно важной задачей [4].

Для решения этой задачи строится расширение базовой модели *RBAC*, содержащее в дополнение к последней следующие положения:

— задана решётка уровней иерархии КС и для каждой сущности указан уровень иерархии;
— определено множество типов сущностей КС и для каждой сущности указан её тип;
— задано множество ролей, каждая из которых представляет собой некоторое множество прав доступа к сущностям определённого типа;
— каждый субъект обладает некоторым множеством разрешённых для данного субъекта ролей;
— субъект обладает правом доступа к сущности КС в том и только в том случае, если субъект обладает ролью, в множестве прав доступа которой имеется данное право доступа к сущности данного типа и уровень иерархии субъекта не меньше уровня иерархии сущности.

Использование введённых положений позволяет значительно эффективнее и гибче реализовать механизм ролевого управления доступом по сравнению с моделями *RBAC*.

На основе [4] опишем формальную структуру предлагаемой модели.

Основными элементами модели иерархического ролевого управления доступом, обозначаемой *RBAC-H*, являются:

— $E = O \cup C$ — множество сущностей, где $O$ — множество объектов, $C$ — множество контейнеров и $O \cap C = \varnothing$;
— $U$ — множество пользователей, при этом пользователи по определению не являются сущностями ($U \cap E = \varnothing$);
— $S \subseteq E$ — множество субъект-сессий пользователей;
— $T$ — множество типов сущностей;
— $L$ — множество уровней иерархии сущностей;
— $R_r$ — множество видов прав доступа;
— $R$ — множество ролей;
— $P \subseteq (R_r \times T) \cup (R_r \times E)$ — множество прав доступа ко всем сущностям одного типа и сущностям;
— $PA : R \to 2^P$ — функция прав доступа ролей, задающая для каждой роли множество прав доступа к сущностям, при этом для каждого права доступа $p \in P$ существует роль $r \in R$, такая, что выполняется условие $p \in PA(r)$;
— $UA : U \to 2^R$ — функция авторизованных ролей пользователей, задающая для каждого пользователя множество ролей, на которые он может быть авторизован;
— $type : E \to T$ — функция типов сущностей;
— $f_e : E \to L$ — функция, задающая уровень иерархии каждой сущности;
— $user : S \to U$ — функция принадлежности субъект-сессии пользователю, задающая для каждой субъект-сессии пользователя, от имени которого она активизирована;
— $roles : S \to 2^R$ — функция текущих ролей субъект-сессий, задающая для пользователя роли, на которые авторизован активизированный от его имени данный субъект в текущей сессии, при этом в каждом состоянии системы для каждой субъект-сессии $s \in S$ выполняется включение $roles(s) \subseteq UA(user(s))$.

Пусть $X$ — заданное разбиение множества $E$. Доменом $d$ сущностей множества $E$ называется всякий класс из $X$.

Иерархией доменов называется заданное на множестве $X$ отношение частичного порядка «$\leqslant$», удовлетворяющее следующим условиям:

— если для $d \in X$ существуют $d_1, d_2 \in X$, такие, что $d \leqslant d_1, d \leqslant d_2$, то $d_1 \leqslant d_2$ или $d_2 \leqslant d_1$;
— в $X$ существует наибольший элемент.

Описанная иерархия доменов соответствует КС с иерархической древовидной структурой, отражающей организационно-управленческие отношения, и задаёт верхнюю полурешётку $(X, \leqslant)$.

Пусть $L$ — множество уровней иерархии сущностей, такое, что $|L| = |X|$ и существует биективное отображение $X$ на $L$. Определим на множестве $L$ отношение частичного порядка «$\leqslant$», где для любых $l_1, l_2 \in L$ верно $l_1 \leqslant l_2$ тогда и только тогда, когда $d_1 \leqslant d_2$ для соответствующих $d_1, d_2 \in X$. Тогда $(L, \leqslant)$ — верхняя полурешётка уровней иерархии сущностей.

Аналогично модели *RBAC*, предполагается, что множества $U$, $X$, $T$, $L$ $P$, $R$, $R_r$ и функции $UA$, $PA$, $type$ не изменяются с течением времени.

Пусть заданы множества $E$, $S$, $X$, $U$, $T$, $P$, $R$, $R_r$, функции $PA$, $UA$, $type$, $user$, $roles$ и полурешетка $(L, \leqslant)$. Определим предикат $can\_access(s, e, p)$, истинный тогда и только тогда, когда выполняются следующие условия:

— $f_e(e) \leqslant f_e(s)$;
— $(p, type(e)) \in PA(roles(s))$.

Говорят, что в КС реализовано иерархическое ролевое управление доступом *RBAC-H*, если любая субъект-сессия $s \in S$ пользователя $user(s) \in U$ может обладать правом доступа $p \in R_r$ к сущности $e \in E$ тогда и только тогда, когда истинен предикат $can\_access(s, e, p)$ .

Таким образом, модель *RBAC-H* ориентирована на КС, в которых уровень иерархии сущностей является существенным при определении политики управления доступом. Добавление атрибутов иерархии и типов сущностей к элементам моделей *RBAC* позволяет адаптировать последние к условиям функционирования реальных КС, а также существенно упростить реализацию и администрирование политики ролевого управления доступом.

ЛИТЕРАТУРА

1. National Institute of Standards and Technology. Role Based Access Control (RBAC) and Role Based Security. [Электронный ресурс]. Режим доступа: `http://csrc.nist.gov/groups/SNS/rbac`.
2. *Kuhn D. R., Coyne E. J., and Weil T. R.* Adding attributes to role-based access control // IEEE Computer. 2010. No. 43(6). P. 79–81.
3. *Sandhu R. S. and Mohammad A. A.* A Model for Attribute-Based User-Role Assignment // Proc. 18th Annual Computer Security Applications Conf. San Diego, California, USA, December 09–13. IEEE Computer Society Washington, 2002. P. 353.
4. *Девянин П. Н.* Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учеб. пособие для вузов. М.: Горячая линия-Телеком, 2011. 320 с.

УДК 681.322

## ЛАБОРАТОРНЫЙ ПРАКТИКУМ «ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ» НА ПЛАТФОРМЕ CISCO PACKET TRACER

Д. Н. Колегов, Б. Ш. Хасанов

Рассматриваются вопросы организации и проведения лабораторного практикума «Основы построения защищённых компьютерных сетей» на кафедре защиты информации и криптографии Национального исследовательского Томского государственного университета [1]. Практикум представляет собой набор лабораторных работ, которые могут использоваться в рамках одноимённого курса, курса «Вычислительные сети» или курсов смежной тематики. Актуальность данного практикума определяется тем фактом, что в настоящее время компьютерные сети являются ключевой составляющей современных информационно-телекоммуникационных систем. Среди всех задач по построению компьютерных сетей важнейшей является обеспечение защищённости от угроз конфиденциальности, целостности и доступности. При этом подсистема защиты должна являться частью компьютерной сети, обеспечивающей её безопасность, как одно из возможных свойств. При таком подходе к разработке архитектуры компьютерных сетей говорят о защищённых компьютерных сетях.

Целью лабораторного практикума является получение знаний, необходимых при проведении работ по проектированию защищённых компьютерных сетей, а также навыков настройки механизмов безопасности и средств функционирования сетевой инфраструктуры.