ISSN 1991-346X

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

Х А Б А Р Л А Р Ы

ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

N E W S

OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

ФИЗИКА-МАТЕМАТИКА СЕРИЯСЫ

♦

СЕРИЯ ФИЗИКО-МАТЕМАТИЧЕСКАЯ

♦

PHYSICO-MATHEMATICAL SERIES

1 (305)

ҚАҢТАР – АҚПАН 2016 ж.
ЯНВАРЬ – ФЕВРАЛЬ 2016 г.
JANUARY – FEBRUARY 2016

1963 ЖЫЛДЫҢ ҚАҢТАР АЙЫНАН ШЫҒА БАСТАҒАН
ИЗДАЕТСЯ С ЯНВАРЯ 1963 ГОДА
PUBLISHED SINCE JANUARY 1963

ЖЫЛЫНА 6 РЕТ ШЫҒАДЫ
ВЫХОДИТ 6 РАЗ В ГОД
PUBLISHED 6 TIMES A YEAR

АЛМАТЫ, ҚР ҰҒА
АЛМАТЫ, НАН РК
ALMATY, NAS RK

«Известия НАН РК. Серия физико-математическая». ISSN 1991-346X
Собственник: РОО «Национальная академия наук Республики Казахстан» (г. Алматы)
Свидетельство о постановке на учет периодического печатного издания в Комитете информации и архивов Министерства культуры и информации Республики Казахстан **№5543-Ж**, выданное 01.06.2006 г.

Периодичность: 6 раз в год.
Тираж: 300 экземпляров.

Адрес редакции: 050010, г. Алматы, ул. Шевченко, 28, ком. 219, 220, тел.: 272-13-19, 272-13-18,
www:nauka-nanrk.kz / physics-mathematics.kz

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75.

News of the National Academy of Sciences of the Republic of Kazakhstan. Physical-mathematical series.
ISSN 1991-346X
Owner: RPA "National Academy of Sciences of the Republic of Kazakhstan" (Almaty)
The certificate of registration of a periodic printed publication in the Committee of information and archives of the Ministry of culture and information of the Republic of Kazakhstan N 5543-Ж, issued 01.06.2006

Periodicity: 6 times a year
Circulation: 300 copies

Editorial address: 28, Shevchenko str., of. 219, 220, Almaty, 050010, tel. 272-13-19, 272-13-18,
www:nauka-nanrk.kz / physics-mathematics.kz

Address of printing house: ST "Aruna", 75, Muratbayev str, Almaty

N E W S
OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 1, Number 305 (2016), 58 – 65

CONSTRAINTS REPRESENTATION IN ATTRIBUTE BASED ACCESS CONTROL MODELS

R. G. Bijashev, M. N. Kalimoldaev, O. A. Rog

Institute of information and computing technologies, Almaty, Kazakhstan.
E-mails: brg@ipic.kz, mnk@ipic.kz, olga@ipic.kz

Keywords: attribute access control, access control policy modeling, category of attributes, access control mechanism, constraints.

Abstract. Recently considerable research has been conducted on attribute based access control models (ABAC) which make authorization decisions based on various attributes of entities involved in the access.

In contrast to such widely used access control models as DAC (Discretionary Access Control), MAC (Mandatory Access Control), RBAC (Role Based Access Control), ABAC models provide flexible configuration of security policies and a dynamic decision-making capability. The ABAC-models are expected to overcome their shortcomings and take their advantages.

In this paper, we propose a generalized definition of the attribute based access control policy model, an important component of which are constraints. For the implementation of the constraints, the notion of attribute category of subjects and objects is introduced. Category encapsulates a structured set of all possible values of attributes and functions to manipulate them.

The structure of the set of the attributes enables to make access decision by comparing attribute values of subjects and objects, making, thus, the category the implementation mechanism of the attribute based access control policy.

Using parametric interpretation, the generalized model shows possibility of simulation of the DAC, MAC and RBAC models.

УДК 004.94

ПРЕДСТАВЛЕНИЕ ОГРАНИЧЕНИЙ МОДЕЛЕЙ АТРИБУТНОГО РАЗГРАНИЧЕНИЯ ДОСТУПА

Р. Г. Бияшев, М. Н. Калимолдаев, О. А. Рог

Институт информационных и вычислительных технологий КН МОН РК, Алматы, Казахстан

Ключевые слова: атрибутное разграничение доступа, моделирование политик разграничения доступа, категория атрибутов, механизм разграничения доступа, ограничения.

Аннотация. В последнее время активно разрабатываются модели атрибутного разграничения доступа (ABAC - attribute based access control), которые вырабатывают решение об авторизации на основе различных атрибутов сущностей – участников процесса разграничения доступа.

ABAC-модели, предоставляя, в частности, возможность гибкой настройки политик безопасности и обеспечивая динамичность принятия решений, призваны преодолеть недостатки и использовать преимущества таких широко используемых моделей разграничения доступа, как DAC - дискреционная, MAC - мандатная и RBAC - ролевая.

Разработано обобщенное определение модели политики атрибутного разграничения доступа, важным компонентом которой являются ограничения. Для реализации ограничений вводится понятие категории атрибутов субъектов и объектов. Категория инкапсулирует структурированное множество всех возможных значений атрибутов и функций для их обработки.

Структура множества атрибутов позволяет осуществлять выработку решений о предоставлении доступа путем сравнения значений атрибутов субъектов и объектов, делая, таким образом, категорию механизмом реализации политики атрибутного разграничения доступа.

С помощью параметрической интерпретации приведенной модели показана возможность моделирования DAC, MAC и RBAC.

1. Введение. Постановка задачи. Современные гетерогенные вычислительные среды характеризуются открытостью и динамичностью. Они состоят из автономных доменов, содержащих большое число пользователей, состав которых часто меняется, и которые синхронно обращаются ко многим ресурсам согласно правилам авторизации, характерным для конкретного домена.

Разграничение доступа является механизмом защиты информации, методы которого разрабатываются одновременно с развитием систем, содержащих конфиденциальные данные. Одними из первых, также широко применяющихся и в настоящее время моделей безопасности, являются модель дискреционного разграничения доступа (DAC-Discretionary Access Control), модель мандатного разграничения доступа (MAC - Mandatory Access Control) и модель ролевого разграничения доступа (RBAC - Role-based Access Control) [1]. Эти модели рассчитаны на применение в замкнутых и относительно стабильных распределенных системах, где субъекты и объекты идентифицированы уникальными именами, являющимися основой принятия решения о возможности авторизации.

Динамический характер систем делает затруднительным уникальную идентификацию большого количества объектов. Он также требует наличия гибкой настройки политик разграничения доступа с учетом характеристик областей, в которых осуществляются определенные виды вычислений, и специфики защиты информации в них.

Это приводит к дальнейшей разработке политик разграничения доступа и появлению новых методов авторизации. В создаваемых моделях в качестве средств выражения произвольных свойств и отношений субъектов и объектов разграничения доступа (сущностей) стали применяться

атрибуты. Атрибуты представляются в виде пар (имя, значение), они могут выражать идентификаторы и списки контроля доступа в моделях DAC, уровни классификации в моделях MAC, роли в моделях RBAC, а также служить параметрами других разрабатываемых моделей разграничения доступа.

В результате появился новый подход к реализации контроля доступа - Attribute based access control (ABAC) - как гибкий метод обеспечения доступа, основанный на оценке значений атрибутов в соответствии с правилами той или иной политики безопасности. При этом решение о предоставлении доступа запрашивающей стороне к информационному ресурсу принимается на основе значений их атрибутов, причем не обязательно, чтобы пользователи были заранее известны провайдеру.

Общепринятая модель атрибутного разграничения доступа включает следующие виды сущностей - пользователь, субъект (сервис), ресурс (объект), вычислительная среда. Сущности снабжены наборами атрибутов, характерными для каждого вида. Для обработки значений атрибутов применяются соответствующие правила. Это обеспечивает адаптацию модели к условиям ее функционирования.

Соответствующее определение ABAC предполагает, что запрос субъекта на осуществление определенных операций с объектом предоставляется или отвергается на основе значений атрибутов, присвоенных субъекту, значений атрибутов объекта, условий вычислительной среды и набора политик, определяемых в терминах этих атрибутов и условий.

В настоящий момент признано, что политика атрибутного разграничения доступа предоставляет достаточно свободы в формулировании правил защиты и обеспечивает необходимую безопасность ресурсов при применении ее в крупных неоднородных вычислительных системах.

С другой стороны, гибкость модели ABAC влечет за собой наличие разнообразных реализаций политик безопасности, и, как следствие, трудность их анализа, а также повышенную сложность инжиниринга атрибутов.

Хотя имеется значительное количество публикаций относительно ABAC, ее разработка не завершена. Множество фундаментальных вопросов относительно компонент ее базовой модели, в частности, таких как ограничения, еще требуют ответа [2-4].

В данной статье предлагается модификация модели системы атрибутного разграничения доступа (САРД) [5-7], обеспечивающая разграничение доступа по одному критерию.

Дано обобщенное определение политики и соответствующей ей модели атрибутного разграничения доступа, определяющей функционирование данной системы. В основу обобщенного определения положен разработанный принцип категоризации атрибутов. Предложен подход, позволяющий осуществлять унифицированное представление разнородных политик атрибутного разграничения доступа и позволяющий моделировать различные модели безопасности, в том числе DAC, MAC или RBAC.

В качестве области определения значений атрибутов рассматривается структурированный домен, представляющий собой множество всех возможных значений, на котором установлено отношение частичного порядка. Значения атрибутов домена присваиваются сущностям в качестве их меток безопасности. Полученное таким образом частично упорядоченное множество представлений сущностей дает возможность устанавливать факт доминирования метки безопасности субъекта над меткой безопасности объекта в процессе выдачи разрешения на доступ.

Исследованы различные виды структуры домена, которые, будучи используемыми как параметры интерпретации обобщенной модели, позволяют конструировать конкретные модели разграничения доступа.

Домен атрибутов вместе с заданным на нем набором функций, предназначенных для манипулирования его значениями, определяется как категория. Показано, что такая категория выполняет задачу ограничений – составной части разработанной модели – и является механизмом разграничения доступа для нее.

Преимуществом данного варианта модели ABAC является то, что он обеспечивает единую модель вычислений значений атрибутов, на основе которой возможно построение унифицированного представления различных моделей безопасности. Это влечет снижение сложности создания атрибутных представлений сущностей и, как результат, облегчает процесс настройки систем

атрибутного разграничения доступа в соответствии с требованиями к защите информации конкретных вычислительных сред.

2. Компоненты модели политики атрибутного разграничения доступа. Объектная модель E рассматриваемой системы разграничения доступа представлена в виде:

$$E=S \cup O,$$

где E={e} – множество сущностей, S={s} – множество субъектов, O={o} – множество объектов.

В большинстве случаев **субъект**, или запрашивающая сторона, рассматривается как кто-то или что-то, подающее запрос на доступ к единице информации с целью выполнения определенной операции над ней. Когда субъект является одушевленным, он рассматривается как пользователь, в противном случае субъект может быть автономным ресурсом или приложением, запускаемым от имени пользователя.

Объект, называемый также ресурсом, им, например, может быть информационный или аппаратный ресурс, а также системное или прикладное программное обеспечение, – это сущность, возможность доступа к которой определяется правилами политики разграничения доступа.

Сущности системы разграничения доступа представляются своими свойствами в виде атрибутов, или меток безопасности. Атрибут субъекта является свойством, которое выражает его возможность осуществить санкционированный доступ заданного вида к определенному кругу объектов. В свою очередь атрибут объекта обозначает круг субъектов, которые имеют доступ к нему.

Подразумевается, что система разграничения доступа использует централизованный метод управления полномочиями, что предполагает наличие выделенного субъекта – администратора, наделяющего пользователей правами доступа, причем пользователи лишены возможности изменения или передачи своих прав.

В связи с этим система проходит две стадии функционирования – стадию администрирования, во время которой производится настройка структуры и присвоения значений множества атрибутов, а также получения сущностями своих меток безопасности, и стадию, осуществляющую процесс собственно разграничения доступа, когда происходит выдача субъектами запросов на доступ к объектам и принятие решения о его разрешении или запрещении.

Обобщенная модель политики атрибутного разграничения доступа ABACM задается в виде:

$$ABACM = (Attr, Constr, AP), \quad (1)$$

где Attr – атрибутная модель сущности САРД; Constr – ограничения; AP - политика авторизации.

Атрибутная модель сущности системы Attr создается следующим образом. Введем понятие домена атрибутов:

$$Dom = (D_{POS} \cup \{\top, \bot\}), \quad (2)$$

где Dom - полная решетка;

$D_{POS} = (D_{Syn}, \sqsubseteq)$ – множество всевозможных значений атрибутов, упорядоченное отношением частичного порядка $\sqsubseteq$, т.е. такое частично упорядоченное множество, что каждое его подмножество $X \subset D_{POS}$ элементов вида $d_1 \sqsubseteq d_2 \sqsubseteq \ldots d_n \sqsubseteq d_{n+1} \ldots$ имеет наименьшую верхнюю грань нвг(X)=⊤ и наибольшую нижнюю грань ннг(X)=⊥ в Dom.

В зависимости от способа задания D_{POS}, подструктурами решетки Dom могут быть множество:

$$D_S=(D_{Syn}, \sqsubseteq_S), \quad (3)$$

линейно упорядоченное множество:

$$D_L=(D_{Syn}, \sqsubseteq_L), \quad (4)$$

или множество в виде дерева:

$$D_T=(D_{Syn}, \sqsubseteq_T). \quad (5)$$

Данные виды подструктур в дальнейшем служат параметрами интерпретации обобщенной модели ABACM, в результате которой получаются ее различные реализации, моделирующие модели безопасности, такие как DAC, MAC и RBAC;

$D_{Syn} = \{d_i\}$ - синтаксический домен, содержащий множество всех возможных значений атрибутов.

Дадим обобщенное определение функции SL, которая служит для присвоения меток безопасности сущностям в виде значений их атрибутов:

$$SL(e) = e_i. \tag{6}$$

Атрибут, или метка безопасности, сущности e может быть представлен как атомарным значением – элементом множества D_{Syn}:

$$e_i \in D_{POS}, \tag{7}$$

так и значением в виде структурированного подмножества элементов множества D_{POS}, предшествующих e_i:

$$e_i = Set(e) = \{e_j \mid e_j \sqsubseteq e_i,\ e_i \in D_{POS},\ e_j \in D_{POS}\}. \tag{8}$$

Ввиду того, что в процессе функционирования системы атрибутного разграничения доступа, метки безопасности субъектов и объектов получают значения из одного домена, можно считать, что, после присвоения меток безопасности администратором системы, множество субъектов входит в качестве подмножества во множество объектов:

$$S \subset O.$$

Рассмотрим компонент Constr – **ограничения модели политики атрибутного разграничения доступа.**

Ограничения Constr, являясь механизмом разграничения доступа модели политики атрибутного разграничения доступа, реализуют аспекты структуры, целостности и манипулирования данными матрицы доступа САРД, рассматриваемой в качестве базы данных атрибутов безопасности. Они представляются набором функций, работающих как на стадии администрирования, так и на стадии выдачи запросов на доступ во время функционирования системы.

Матрица доступа ACM представляет собой **предметную область** системы атрибутного разграничения доступа в момент времени t. Она определяется следующим образом:

$$ACM = (E, R),$$

где $E=S \cup O$ – множество сущностей системы, заданных своими метками безопасности; R – множество бинарных отношений между ними, определяемое структурой множества D_{POS}. Это множество отношений в свою очередь содержит подмножества:

$$R = (\preccurlyeq_{ss}, \preccurlyeq_{oo}, \succcurlyeq_{so}),$$

где $\preccurlyeq_{ss}$ – отношение предшествования, определенное на множестве субъектов $S=\{s\}$: $\preccurlyeq_{ss} = \preccurlyeq(s,s)=\{(s_i,s_j) \mid s_i \sqsubseteq s_j,\ s_i \in D_{POS},\ s_j \in D_{POS}\}$.

$\preccurlyeq_{oo}$ – отношение предшествования, определенное на множестве объектов $O=\{o\}$:

$$\preccurlyeq_{oo} = \preccurlyeq(o,o)=\{(o_i,o_j) \mid o_i \sqsubseteq o_j,\ o_i \in D_{POS},\ o_j \in D_{POS}\}.$$

$\succcurlyeq_{so}$ – отношение доминирования, обратное к отношению предшествования. На его основе в дальнейшем определяется отношение доступа. Отношение доминирования задается на декартовом произведении множеств меток безопасности субъектов и объектов $E=S \times O$:

$$\succcurlyeq_{so} = \succcurlyeq(s,o) = \{(s_i,o_i) \mid o_i \sqsubseteq s_i,\ s_i \in D_{POS},\ o_i \in D_{POS}\}.$$

Ограничения Constr являются набором функций:

$$Constr = (SL, Acc), \tag{9}$$

где SL – функция, присваивающая значения атрибутов сущностям, определенная в (6)-(8); Acc – функция доступа субъекта к объекту, основа обобщенного механизма атрибутного разграничения доступа, определенная на множествах

$$(D_{POS}, D_{POS}) \rightarrow Dom.$$

Функция Acc вычисляет значения наименьшей верхней грани значений атрибутов субъекта и объекта, сравнивая значения аргументов:

$$Acc(s, o) = нвг(s, o).$$

При этом

- Acc(s,o)=s, если метка безопасности субъекта доминирует над меткой безопасности объекта s⩾o;

- Acc(s,o)=o, если метка безопасности субъекта предшествует метке безопасности объекта s⩽o;

- Acc(s,o) = ⊤, если субъект и объект не связаны отношениями ⩾ или ⩽.

Исходя из вышесказанного, компонент модели **Политика авторизации** задается в виде булевой функции AP(s, o), которая выдает решение о возможности доступа субъекта s к объекту o на основе результата сравнения их меток безопасности функцией доступа Acc(s, o):

- доступ субъекта s к объекту o разрешен: AP(s,o) = TRUE, если Acc(s, o) = s.

- доступ субъекта s к объекту o запрещен: AP(s,o) = FALSE, если Acc(s, o) = o или Acc(s, o) = ⊤.

3. Категория атрибутов как механизм реализации различных политик атрибутного разграничения доступа. Для реализации политики атрибутного разграничения доступа в виде механизма разграничения доступа для нее, введем понятие категории.

Определим категорию как объект, состоящий из структурированного множества атрибутов, на котором заданы функции, предназначенные для манипулирования их значениями. Категория предназначена для:

1) представления обобщенной политики атрибутного разграничения доступа;

2) моделирования механизмов разграничения доступа, являющихся реализациями обобщенной модели, и соответствующих существующим, таким как DAC, MAC, RBAC, а также вновь разрабатываемым моделям безопасности. Полученные механизмы разграничения доступа входят в состав конструируемых САРД.

Приведем 2-х уровневую формулировку понятия категории.

Первый уровень представления категории, Cat^1, является обобщенной политикой атрибутного разграничения доступа ABACM, определенной в (1), он включает следующие компоненты:

$$Cat^1 = (Constr, CF, I),$$

где Constr – ограничения, задаваемые (9); CF –функции-конструкторы домена атрибутов; I – интерпретация, которая приписывает конкретный вид функциям множества функций Constr и функциям-конструкторам CF.

Интерпретация I – это пара (Dom, I_f), обладающая следующими свойствами:

Dom – структурированный домен всех возможных значений атрибутов, заданный в (2) – полная решетка, включающая множество D_{POS}, и служащая областью интерпретации;

I_f – функция интерпретации, которая, в зависимости от параметра интерпретации, а) строит подструктуру решетки Dom - домен D_{Str} в виде D_S, D_L или D_T, определяемых с помощью (3)-(5); б) создает наборы функций $Constr_{Str}$ и CF_{Str} следующим образом: каждому обобщенному определению функции из наборов Constr и CF сопоставляет некоторую функцию $f_{Str} \in Constr_{Str}$ или $f_{Str} \in CF_{Str}$, определяемую на домене D_{Str}:

$$I_f(f, Str) = f_{Str},$$

где f – функция, подлежащая интерпретации. Функция f определена на Dom, $f \in Constr$ или $f \in CF$; Str – параметр интерпретации, задающий вид результатов интерпретации - структуру решетки Dom_{Str} и функций, составляющие наборы $Constr_{Str}$ и CF_{Str}.

Str = S означает, что видом структуры является множество, Str = L – линейно упорядоченное множество, Str = T – множество в виде дерева;

f_{Str} – результат интерпретации функций наборов Constr и CF. Функция определена на Dom_{Str}, $f_{Str} \in Constr_{Str}$ или $f_{Str} \in CF_{Str}$.

Интерпретация дает второй уровень определения категории, или конкретную реализацию политики атрибутного разграничения доступа в виде ее механизма разграничения доступа Cat^2:

$$Cat^2(Str) = (Dom_{Str}, Constr_{Str}, CF_{Str}).$$

где Str – параметр интерпретации; Dom_{Str} – домен всевозможных значений атрибутов, структурированный, в зависимости от значения параметра интерпретации Str, в виде D_S, D_L или D_T;

$Constr_{Str}$ – преобразованное функцией интерпретации I_f множество Constr, содержащее конкретные представления функций SL и Acc;

CF_{Str} – множество функций для манипулирования значениями атрибутов домена Dom_{Str}, полученное в результате интерпретации CF - множества функций-конструкторов домена Dom.

В зависимости от значения параметра интерпретации могут быть получены следующие виды моделей разграничения доступа:

$$Cat^2(S) = (Dom_S, Constr_S, CF_S)$$

- модель DAC атрибутного разграничения доступа,

$$Cat^2(L) = (Dom_L, Constr_L, CF_L)$$

- модель MAC атрибутного разграничения доступа,

$$Cat^2(T) = (Dom_T, Constr_T, CF_T)$$

- модель RBAC атрибутного разграничения доступа.

Заключение. Дано определение политики и предложена обобщенная модель атрибутного разграничения доступа, основанная на сравнении значений атрибутов сущностей, принадлежащих структурированному домену.

Основным компонентом модели являются ограничения, задаваемые в виде набора функций, и реализующие различные аспекты матрицы доступа как базы данных атрибутов безопасности. На основе ограничений строится категория как объект, инкапсулирующий домен атрибутов и набор функций для манипулирования его значениями. Интерпретация функций категории с параметрами, отражающими различные виды подструктур домена, дает различные виды реализации конкретных моделей атрибутного разграничения доступа, в том числе DAC, MAC и RBAC.

ЛИТЕРАТУРА

[1] Гайдамакин Н.А. Теоретические основы компьютерной безопасности: учебное пособие. – Екатеринбург: Издательство Уральского университета, 2008. – 212 с.

[2] Hu V.-C., Ferraiolo D., Kuhn R., Schnitzer A., Sandlin K., Miller R., Scarfone K. NIST Special Publication 800-162. Guide to Attribute Based Access Control (ABAC). Definition and Considerations // NIST National Institute of Standards and Technology – http://dx.doi.org/10.6028/NIST.SP.800-162. – Jan 2014.

[3] Jin X., Krishnan R., Sandhu R. A unified attribute-based access control model covering DAC, MAC and RBAC // Proceedings of the 26th Annual IFIP WG 11.3 conference on Data and Applications Security and Privacy (DBSec'12). – 2012. – P. 41-45.

[4] Khalid Bijon, Ram Krishnan and Ravi Sandhu, Constraints Specification in Attribute Based Access Control, IEEE/ASE Science Journal, Vol 2, No. 3, 2013, P. 131-144.

[5] Калимолдаев М.Н., Бияшев Р.Г., Рог О.А. Формальное представление функциональной модели многокритериальной системы разграничения и контроля доступа к информационным ресурсам // Проблемы информатики. – 2014. – № 1(22). – С. 43-55.

[6] Rog O.A. Polymorphic typing of entities in the multi-criteria system of access control and a task of constructing types // Information Technologies, Management and Society. The 12 th International Scientific Conference Information Technologies and Management. 2014 April 16 – 17. Riga, 2014. - C. 66.

[7] Бияшев Р.Г., Калимолдаев М.Н., Рог О.А. Полиморфная типизация сущностей и задача конструирования механизма многокритериального разграничения доступа // Известия НАН РК. Серия физико-математическая. – 2014. – № 5. – С. 33-41.

REFERENCES

[1] Gaydamakin N.A. Theoretical Foundations of Computer Security: a tutorial. - Yekaterinburg: Ural University Publishing House, 2008. - 212 p. (in Russ.).

[2] Hu V.-C., Ferraiolo D., Kuhn R., Schnitzer A., Sandlin K., Miller R., Scarfone K. *NIST Special Publication 800-162. Guide to Attribute Based Access Control (ABAC). Definition and Considerations.* NIST National Institute of Standards and Technology, http://dx.doi.org/10.6028/NIST.SP.800-162, **Jan 2014** (in Eng.).

[3] Jin X., Krishnan R., Sandhu R. *A unified attribute-based access control model covering DAC, MAC and RBAC*. **2012**, Proceedings of the 26th Annual IFIP WG 11.3 conference on Data and Applications Security and Privacy (DBSec'12), 41-45 (in Eng.).

[4] Khalid Bijon, Ram Krishnan and Ravi Sandhu. *Constraints Specification in Attribute Based Access Control.* **2013**, IEEE/ASE Science Journal, Vol 2, No. 3, 131-144 (in Eng.).

[5] Kalimoldaev M.N., Bijashev R.G., Rog O.A. The formal presentation of the functional model of multicriteria system of differentiation and control access to information resources // Problems of Informatics. - 2014. - № 1 (22). - p. 43-55. (in Russ.).

[6] Rog O.A. *Polymorphic typing of entities in the multi-criteria system of access control and a task of constructing types.* **2014 April 16 – 17**, Information Technologies, Management and Society. The 12 th International Scientific Conference Information Technologies and Management. Riga, 2014, 66 (in Eng.).

[7] Bijashev R.G., Kalimoldaev M.N., Rog O.A. Polymorphic typing of entities and the task of constructing the mechanism of multi-criteria restricting access. // News of NAS RK. Series of physical and mathematical. - 2014. - № 5. - p. 33-41. (in Russ.).

АТРИБУТТЫ ҚОЛЖЕТІМДІЛІКТІ ШЕКТЕУ МОДЕЛДЕРІНІҢ ШЕКТЕУЛЕРІН ҰСЫНУ

Р. Г. Бияшев, М. Н. Қалимолдаев, О. А. Рог

Ақпараттық және есептеу технологиялар институты, Алматы, Қазақстан

Тірек сөздер: атрибуттық қолжетімділікті шектеу,қолжетімділікті шектеу саясатын моделдеу, атрибуттар санаты, қолжетімділікті шектеу механизмі, шектеу.

Аннотация. Соңғы жылдары атрибутты қолжетімділікті шектеу моделдерін жасау қарқынды даму үстінде (ABAC - attribute based access control), әр түрлі атрибуттарға негізделген - қолжетімділікті шектеу процесіндегі қатысушылардың авторизациялауға байланысты шешімдерін шығарады.

Қолжетімділікті шектеудегі кеңінен пайдаланылатын дискрециялық DAC, мандаттық MAC және рөлдік RBAC моделдерінің артықшылықтарын қолдану және кемшіліктерінен өтуге шақырылған жеке тұрғыда ұсынылған ABAC-моделдері арқылы қауіпсіздік саясатын икемді баптау мүмкіндігі мен динамикалық шешім қабылдауын қамтамасыздандыру.

Басты компонент шектеу қою болып табылатын атрибутты қолжетімділікті шектеу саясатындағы моделіне жалпылама анықтама берілді. Шектеулерді іске асыру үшін субъектілер мен объектілер атрибуттарының санаттары туралы ұғым енгізілді. Атрибуттардың барлық мүмкін мәндерін және олардың өңдеу функцияларын санат құрылымдық жиынтықта инкапсуляциялайды.

Субъектілер мен объектілер атрибуттарының мәндерін салыстыру арқылы атрибуттардың жиын құрылымы қолжеткізуде шешімдер жасауға мүмкіндік береді және осы арқылы атрибутты қолжетімділікті шектеу саясатын орындау механизмінің санатын қалыптастырады.

Ұсынылған моделді параметрлік талдау көмегімен DAC, MAC және RBAC-ты моделдеу мүмкіндігі көрсетілген.

Поступила 13.01.2016 г.

Publication Ethics and Publication Malpractice
in the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайте:

www:nauka-nanrk.kz

http://www.physics-mathematics.kz

Редактор *М. С. Ахметова*
Верстка на компьютере *Д. Н. Калкабековой*

Подписано в печать 16.01.2016.
Формат 60x881/8. Бумага офсетная. Печать – ризограф.
10,7 п.л. Тираж 300. Заказ 1.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-18, 272-13-19