УДК 681.3.

К. Г. Юденок, К. В. Кринкин

РАЗРАБОТКА МОДЕЛИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В РАСПРЕДЕЛЕННЫХ СЕРВИСНЫХ СРЕДАХ (ИНТЕЛЛЕКТУАЛЬНЫХ ПРОСТРАНСТВАХ)

Механизмы обеспечения контроля доступа играют ключевую роль во многих областях компьютерных наук, однако для информации, представленной на основе семантического веба, устоявшихся решений не существует. В данной статье описываются результаты исследований в этой области, направленных на обеспечение безопасности информации в распределенных сервисных средах (интеллектуальных пространствах), которые являются наиболее перспективным приложением стандартов и технологий семантического веб.

Интеллектуальные пространства, платформа Smart-M3, протокол идентификации хоста, безопасность, контроль доступа

Современные тенденции развития информационных и телекоммуникационных технологий ведут к необходимости разработки устойчивых и надежных инфраструктур для хранения и извлечения различного рода информации из широкого спектра участников информационного окружения. Такую инфраструктуру принято называть «интеллектуальным пространством» (ИП). Системы, реализующие функции интеллектуального окружения, предполагают присутствие нескольких устройств, использующих общее представление доступных ресурсов и сервисов. За счет использования интеллектуального окружения можно обеспечить более качественную поддержку пользователя, что предоставляет возможность гибкого использования и включения в интеллектуальное окружение различных новых устройств, а также доступа к информации и сервисам с любого устройства такого окружения вне зависимости от их физического расположения [1].

Контроль доступа в цифровых системах был глубоко изучен с момента возникновения информатики на всех уровнях абстракции компьютерных архитектур. Определение и обеспечение полной и общей модели контроля доступа, оптимизированной для информации, основанной на графах, является сложной задачей, рассмотрение которой выходит за рамки данной статьи [2].

Основное внимание в статье сосредоточено на описании предметной области, возможных решений по созданию механизмов безопасности, а также модели и механизмов обеспечения безопасности в составе платформы интеллектуальных пространств Smart-M3. С обзором платформы ИП Smart-M3 можно ознакомиться в [3].

Проблемы информационной безопасности платформы Smart-M3. Текущая версия платформы Smart-M3 имеет несколько механизмов контроля доступа для информации интеллектуального пространства, таких, как контроль доступа на уровне триплетов, политики контроля доступа, использующие шаблоны триплетов в качестве объектов безопасности [2]. Исследование данных механизмов позволит найти оптимальный способ для контроля доступа в ограниченных условиях (ширина канала, производительность вычислительных устройств и т. д.).

В качестве основных проблем безопасности в платформе Smart-M3 можно выделить следующие:

– отсутствие механизма идентификации и аутентификации пользователей пространства (подключение к пространству без подтверждения "личности пользователя"). Любой агент может в любой момент подключиться к пространству, зная только его параметры подключения;

– отсутствие механизма авторизации и контроля доступа пользователей пространства. В данный момент каждый пользователь имеет равные права во всем пространстве, все операции работы с данными пространства, такие, как вставка, обновление, удаление, запрос и подписка, доступны при первоначальном подключении;

– отсутствие конфиденциальности данных, так как вся информация хранится в открытом доступе.

Исходя из перечисленных проблем, можно сделать вывод, что платформа не имеет базовых механизмов обеспечения безопасности, что представляет большую угрозу не только данным, хранящимся в пространстве, но и всей платформе в целом.

Требования к методам защиты интеллектуального пространства. В области компьютерной безопасности существуют основные требования, которым должна отвечать каждая система для корректной работы в любых условиях своего жизненного цикла.

Выделим основные требования обеспечения безопасности для интеллектуального пространства, которые необходимо разработать:

– идентификация и аутентификация субъектов ИП (контроль доступа к ИП);

– авторизация субъектов ИП (контроль доступа к данным ИП);

– конфиденциальность данных системы безопасности ИП;

– целостность и доступность данных ИП;

– мониторинг системы безопасности ИП.

На данном этапе были проанализированы и исследованы различные методы и механизмы безопасности в рассматриваемой предметной области – от стандартных моделей обеспечения безопасности до сторонних решений, предлагаемых разработчикам систем безопасности.

Идентификация и аутентификация субъектов пространства. Для идентификации и аутентификации клиентов пространства было решено использовать HIP-протокол – протокол идентификации хоста. Данный протокол представляет определенные методы безопасности, такие, как аутентификация, шифрование и приватность [4], [5].

Авторизация и контроль доступа субъектов пространства. Механизм авторизации и контроля доступа субъектов пространства можно построить с помощью следующих решений: дискреционная модель безопасности, отображение RDF-графа пространства в виде виртуальной файловой системы, именованные графы, онтология ограничения доступа [6], [7], расширения контроля доступа для базы данных пространства. Отображение RDF-графа пространства в виде виртуальной файловой системы используется в описываемой работе как основной механизм обеспечения авторизации и контроля доступа.

Механизм отображения RDF-графа в виртуальную файловую систему очень похож на дискреционную модель безопасности из-за привязки к файловой системе. Модель отображения, как и дискреционная модель, будет иметь список контроля доступа (матрицу доступа), чтобы разделять права между субъектами системы. Можно сделать вывод, что модель отображения подобна дискреционной модели с добавлением алгоритмов представления данных в качестве сущностей файловой системы [8].

Дальнейшим шагом в развитии RDF-графов являются именованные графы, которые имеют свои собственные механизмы безопасности [9]. Онтология контроля доступа также может быть использована, но из-за постоянного доступа производительность всей системы будет под вопросом.

Рассмотрим механизм отображения RDF-графа пространства в виртуальную файловую систему более подробно.

Представление RDF-графа пространства в виде виртуальной файловой системы. Обеспечить механизм авторизации и контроля доступа в ИП можно отображением RDF-графа пространства на виртуальную файловую систему, где существуют собственные отработанные механизмы контроля доступа.

Будем рассматривать пространство, совокупность "SIB-DB" как файловую систему (определенную структуру каталогов), которая имеет определенные права доступа "RWX":

R – прочитать триплет, извлечь его составляющие (S, P, O);

W – записать (вставить) отношение в триплет;

X – получить список отношений объектов.

Рассматривая пространство в качестве виртуальной файловой системы, предполагаем, что RDF-граф будет подобием дерева каталогов и заключаем, что операции доступа к каталогам являются аналогами операций для RDF. Например, право файловой системы "выполнить" для RDF может быть представлено как "получить список всех субъектов (отношений) данного каталога" или "список отношений сущностей". Таким образом, проецируя операции (права) файловой системы на операции RDF, получаем новую область для решения проблемы контроля доступа к информации, содержащейся в интеллектуальном пространстве.

Реализация отображения графа на виртуальную файловую систему может быть реализована с помощью технологии FUSE (fusekit), которая позволяет разрабатывать собственные виртуальные файловые системы[1].

Механизм идентификации и аутентификации на основе протокола HIP. Для добавления поддержки HIP в платформу интеллектуальных пространств Smart-M3 был разработан специальный агент на серверной стороне платформы Smart-M3, задача которого –

[1] http://fuse.sourceforge.net/, http://sourceforge.net/projects/fuse/files/fuse-2.X/, http://code.google.com/p/fusekit/.

идентифицировать и аутентифицировать клиентов пространства, а также провести корректную настройку HIT-IP-отображения в системе для работы протокола HIP с платформой Smart-M3 [10].

Разработка HIP-агента. При подключении клиента к ИП активизируется HIP-агент, который идентифицирует и аутентифицирует клиента на основе протокола HIP. При соединении проверяется хеш-ключ клиента, на основании которого принимается решение по идентификации и аутентификации хоста пространства. Если хеш действителен, то агент соединяет клиента с пространством. Данное решение изображено на рис. 1, где *i*1 – интерфейс доступа (сокет) HIP-агента с семантическим информационным брокером (SIB), *i*2 – интерфейс доступа процессора знаний (КР) с HIP-агентом. Клиентская и серверная стороны должны быть настроены для работы по протоколу HIP.

Процедуру подключения клиента к пространству иллюстрирует диаграмма последовательностей (рис. 2).

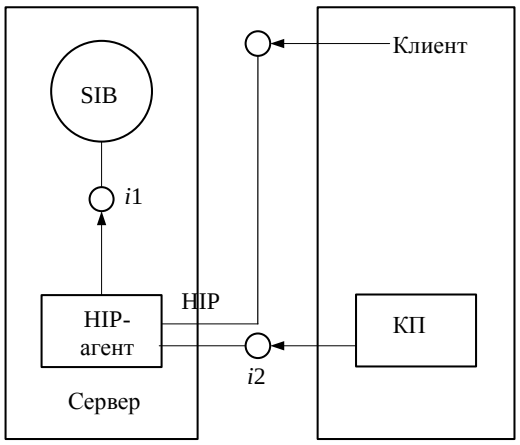

Рис. 1

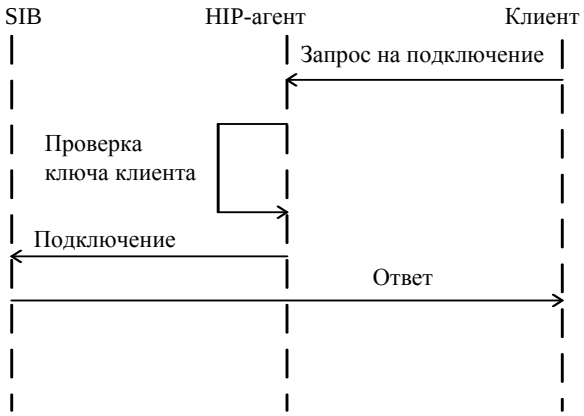

Рис. 2

Механизм отображения RDF-графа пространства в виде виртуальной файловой системы является основным механизмом обеспечения авторизации и контроля доступа для субъектов пространства.

Отображение RDF-графа пространства в виртуальную файловую систему. В данный момент платформа Smart-M3 работает следующим образом. На серверной стороне размещается семантический информационный брокер и база данных пространства. Для работы с клиентской стороной разработан специальный протокол SSAP, который предназначен для обмена данными между сторонами [3].

Вся информация интеллектуального пространства хранится в обычном хранилище данных – базе данных пространства. Информация ИП представлена в виде триплетов. Совокупность данных триплетов хранится в специально определенных таблицах БД платформы Smart-M3.

По результатам исследований в области авторизации и контроля доступа субъектов пространства, описанных ранее, было принято решение разработать виртуальную файловую систему (SIB FS), которая отображает информацию пространства в определенную структуру каталогов для последующих операций над ними.

Структура каталогов для отображаемой файловой системы имеет вид, представленный на рис. 3.

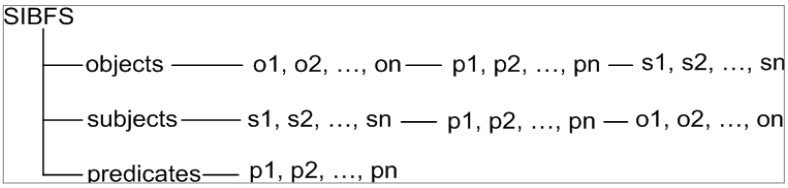

Рис. 3

Данная структура каталогов позволяет получать информацию в форме "субъект (s), предикат (p), объект (o)", наоборот и все предикаты (отношения).

Любая файловая система Linux предоставляет стандартные атрибуты управления доступом к файлам, каталогам и другим сущностям файловой системы. Таким образом, файловая система обеспечивает стандартные механизмы контроля доступа для пользователей системы.

Место отображения графа в составе платформы показано на рис. 4.

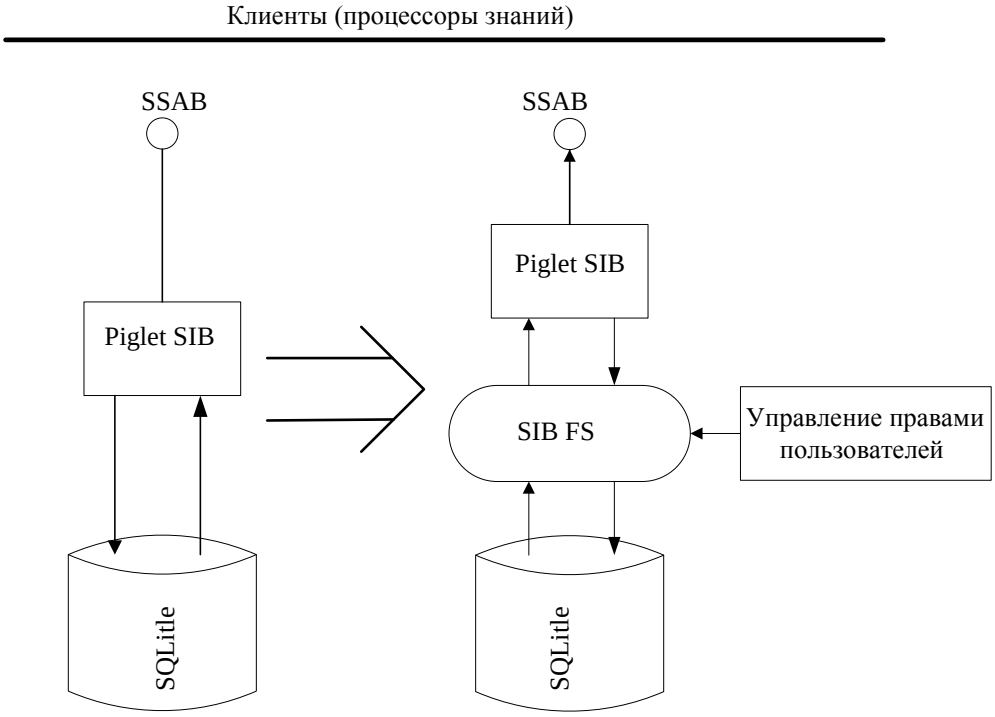

Рис. 4

Создание виртуальной файловой системы из данных пространства. RDF-граф может быть отображен в файловую систему, используя RDF-данные пространства, хранящиеся в базе данных ИП. Также данное отображение может быть реализовано с помощью SSAP-протокола. В качестве прототипа использовалось отображение графа пространства из RDF-данных интеллектуального пространства.

Общий алгоритм процесса отображения графа можно представить в следующем виде:

1. Реализация логики для работы с БД пространства. Данный шаг заключается в создании методов для работы с данными ИП. Таблица triple хранит все триплеты пространства в следующем виде: TABLE triple (s INTEGER, p INTEGER, o INTEGER, src INTEGER); таблица node в поле str хранит их значения в соответствии с полем id, номера s, p, o из таблицы triple. Необходимо извлечь все значения триплетов из таблицы node по ключам из таблицы triple и сохранить их в памяти либо в структуре данных.

2. Создание структуры каталогов виртуальной файловой системы на основе полученных данных. На данном этапе необходимо создать структуру виртуальной файловой системы (см. рис. 3).

Данный способ имеет недостаток, заключающийся в сложности администрирования, так как установка прав доступа на каждую таблицу или директорию таблиц требует тщательного контроля над процессом. Для его устранения планируется разработать специальную утилиту автоматической установки прав доступа.

Следующим этапом развития механизма авторизации является процесс внедрения модели отображения в платформу ИП Smart-M3 [10].

Тестирование разработанных механизмов. Тестирование разработанных механизмов безопасности проводилось в специально развернутой среде. В качестве основной операционной системы использовалась Ubuntu 10.04 с установленной платформой Smart-M3, реализацией протокола HIP-HIPL и другими компонентами, необходимыми для разработки.

Для проверки работы протокола HIP в составе ОС были развернуты две виртуальные машины (клиент и сервер) с установленной платформой Smart-M3, обмен данными между компонентами платформы осуществлялся по HIP-протоколу. Так как HIP-протокол полностью прозрачен для прикладного и транспортного уровней, любое IPv4-приложение может быть запущено поверх HIP-протокола при правильно настроенном отображении HIT-адресов в IP. При этом в данном эксперименте используются специальные LSI-адреса, предназначенные для поддержки IPv4-приложений, которые автоматически выдаются хостам при запуске протокола[2].

Первоначальная реализация механизма отображения графа пространства в виртуальную файловую систему позволяет создавать файловую систему на основе триплетов базы данных пространства, формируя заявленную структуру каталогов [10].

В результате исследования и разработки модели и механизмов обеспечения безопасности в распределенных сервисных средах (интеллектуальных пространствах) были достигнуты следующие результаты:

– проанализировано и смоделировано решение механизма идентификации и аутентификации на основе протокола HIP. Произведен тестовый запуск платформы Smart-M3 по протоколу HIP и проверена ее работоспособность;

– разработан прототип механизма авторизации и контроля доступа отображением RDF-графа в виртуальную файловую систему. Механизм протестирован в составе платформы Smart-M3, начат процесс внедрения механизма отображения в данную платформу.

Следующим этапом в усовершенствовании модели и механизмов обеспечения безопасности будет:

– внедрение модели отображения графа пространства в платформу Smart-M3;

– добавление разработанных механизмов в новую версию платформы Smart-M3 (Redland);

– разработка утилиты установки прав доступа для отображенной виртуальной ФС;

– разработка HIP-агента.

---

[2] http://osll.spb.ru/projects/kaspy/wiki/Hip_configuration_.

СПИСОК ЛИТЕРАТУРЫ

1. Шилов Н. Г., Кашевник А. М. Современные системы взаимодействия мобильных устройств в интеллектуальном окружении: требования и технологии // Тр. Всерос. конф. «Интегрированные модели, мягкие вычисления, вероятностные системы и комплексы программ в искусственном интеллекте», Коломна, 2009. Т. 2. С. 287–294.

2. Access Control at Triple Level: Specification and Enforcement of a Simple RDF Model to Support Concurrent Applications in Smart Environments / A. D'Elia, J. Honkola, D. Manzaroli, T. Salmon Cinotti // Smart Spaces and Next Generation Wired/Wireless Networking Lecture Notes in Computer Science. 2011. Vol. 6869. P. 63–74.

3. Smart-M3 Infmation Sharing Platform / J. Honkola , H. Laine, R. Brown, O. Tyrkkö // Proc. IEEE Symp. Computers and Communications, ser ISCC'10. IEEE Computer Society. 2010. P. 1041–1046.

4. Gurtov A. Host Identity Protocol (HIP): Toward the Secure Mobile Internet. Finland: John Wiley and Sons Ltd., 2008. P. 323.

5. Nikander P., Gurtov A., Henderson T. Host Identity Protocol (HIP): Connectivity, Mobility, Multi-homing, Security, and Privacy over IPv4 and IPv6 networks // IEEE Communications Surveys and Tutorials. 2010. Vol. 12. P. 186–204.

6. Ломов П. А., Шишаев М. Г. Разработка онтологии для семантического управления доступом // Инженерия знаний и технологии семантического веба. 2010. С. 82–91.

7. Andersen B., Neuhaus F. An ontological approach to information access control and provenance // Proc. of OIC 2009 (Ontology for Intelligence Community), Fairfax, VA, 2009. P. 51–57.

8. Devyanin P. N. Mathematical foundations of computer security. The application / Institute of Cryptography, Telecommunications and Computer Science. M., 2009. P. 40.

9. Named graphs / J. J. Carroll, C. Bizer, P. Hayes, P. Stickler // Web Semantics: Science, Services and Agents on the World Wide Web. 2005. Vol. 3. P. 247–267.

10. Yudenok K., Krinkin K. Distributed Service Environment (Smart Spaces) Security Model Development // FRUCT 12, Oulu. 2012. P. 172–184.

K. G. Yudenok, K. V. Krinkin

DISTRIBUTED SERVICE ENVIRONMENT (SMART SPACES) SECURITY MODEL DEVELOPMENT

Access control mechanisms play a key role in many areas of computer science, however, for the information provided on the basis of semantic web and established solutions don't exist. This work focuses on the research in this area, in particular to ensure the information security in distributed service environments (smart spaces), which are the most promising application of standards and technologies of semantic web.

Smart Spaces, Smart-M3, HIP, Security, Access control

УДК 007:681.512.2

Н. А. Жукова, А. И. Водяхо

АРХИТЕКТУРНЫЙ ПОДХОД К ПОСТРОЕНИЮ СИСТЕМ ОБРАБОТКИ МНОГОМЕРНЫХ ИЗМЕРЕНИЙ ПАРАМЕТРОВ ПРОСТРАНСТВЕННО РАСПРЕДЕЛЕННЫХ ОБЪЕКТОВ

Предлагается архитектурный подход к построению систем обработки многомерных измерений параметров пространственно распределенных объектов, в основу которого положена концептуальная модель, рассматриваемая как платформенно-независимое описание для данного класса систем.

Обработка сигналов, фреймворк, системная архитектура

Современный этап развития техники и технологий – это этап создания сложных многоуровневых систем, в которых все более значимую роль играет информационная составляющая. Для разработки сложных информационных систем (ИС) целесообразно применять архитектурный подход как средство повторного использования решений на всех уровнях – от повторного использования кода до повторного использования знаний. В основе архитектурного подхода лежит понятие фреймворка – лучшей практики (типового решения) [1].