информационными рисками сложных систем//Информация и безопасность. – 2020. – Т. 23. №2(4). – С. 191-202.

4. *Калашников А.О.* Управление информационными рисками с использованием арбитражных схем//Системы управления и информационные технологии. – 2004. – № 4 (16). – С. 57-61.

5. *Калашников А.О.* Организационные механизмы управления информационными рисками корпораций. – М.: «ПМСОФТ», 2008. – 175 с.

6. *Ротарь В.И.* О принципе стимуляции в арбитражной схеме//Экономика и математические методы. – 1984. – Т. XVII. В. 4. – С. 751-764.

Асратян Р.Э.

Разграничение прав доступа к сервисным функциям в Службе защищенных сообщений на основе электронной подписи

Аннотация: Рассмотрены принципы авторизации и разграничения прав доступа в сетевой Службе защищенных сообщений, предназначенной для безопасной обработки информационных запросов в распределенных информационных системах. Отличительная особенность службы заключается в использовании реквизитов подписантов информационного запроса для определения возможности доступа к обрабатывающим сервисным функциям.

Ключевые слова: распределенные системы, Интернет-технологии, информационное взаимодействие, информационная безопасность, разграничение прав доступа

Современные Интернет-технологии являются важнейшей составной частью распределенных информационных систем, в значительной степени, определяющей эффективность и безопасность сетевых обменов. Сегодня в распоряжении разработчиков таких систем имеется целый ряд сетевых информационных технологий высокой степени универсальности и гибкости [1-3]. Достаточно упомянуть Web-технологии [3], покрывающие широчайший спектр применений от электронной

прессы до распределенных вычислений. Однако и сегодня разработчики информационных систем ощущают дефицит готовых решений в области организации защиты данных, авторизации и разграничения прав доступа к информационным ресурсам [4]. Это пробуждает интерес к созданию более специализированных сетевых технологий, более точно сфокусированных на поддержке распределенных информационных систем.

Новая сетевая службы PMS (Protected Message Service) была создана именно с этой целью. Ее главная особенность заключается в тесной интеграции функций сетевого информационного взаимодействия с функциями информационной защиты [5]. Внешне эта интеграция проявляется в том, что отмеченные функции входят в набор методов главного класса службы – класса «Защищенное сообщение» (PmsMessage), отображающего электронный документ (информационный запрос или ответ), снабженный одной или несколькими удостоверяющими электронными цифровыми подписями (ЭЦП). В отличие, например, от технологии Web-сервисов описываемая служба опирается не на модель вызова методов (функций-членов) удаленных объектов, а на модель обмена сообщениями. В данном случае это означает, что все сервисные обрабатывающие функции (методы) имеют одинаковую, жесткую спецификацию: они получают объект класса «Защищенное сообщение» в качестве параметра и возвращают объект того же класса.

Взаимодействие клиента и сервера PMS проиллюстрировано на рисунке 1. Здесь можно увидеть основные этапы организации обращения к сервисной функции MyFunc, размещенной на сервере MySrv в динамической библиотеке функций MyLib.dll, а также основные инструменты клиента, предоставляемые программным обеспечением PMS. Обращение включает следующие шаги.

Создание исходящего защищенного сообщения (конструктор PmsMessage) с одновременным наполнением его данными (например, информационным запросом в формате XML-документа).

Добавление к сообщению одной или нескольких удостоверяющих подписей (метод AddSignature).

- Создание объекта класса PmsConnection, отображающего защищенное сетевое соединение с сервером (конструктор PmsConnection.

- Передача исходящего сообщения на обработку в сервере MySrv и получение входящего защищенного сообщения, содержащего результат обработки (метод Process).
- Проверка электронной подписи у входящего сообщения (метод CheckSignature) и извлечение текстового документа, содержащего результат обработки (метод GetString).

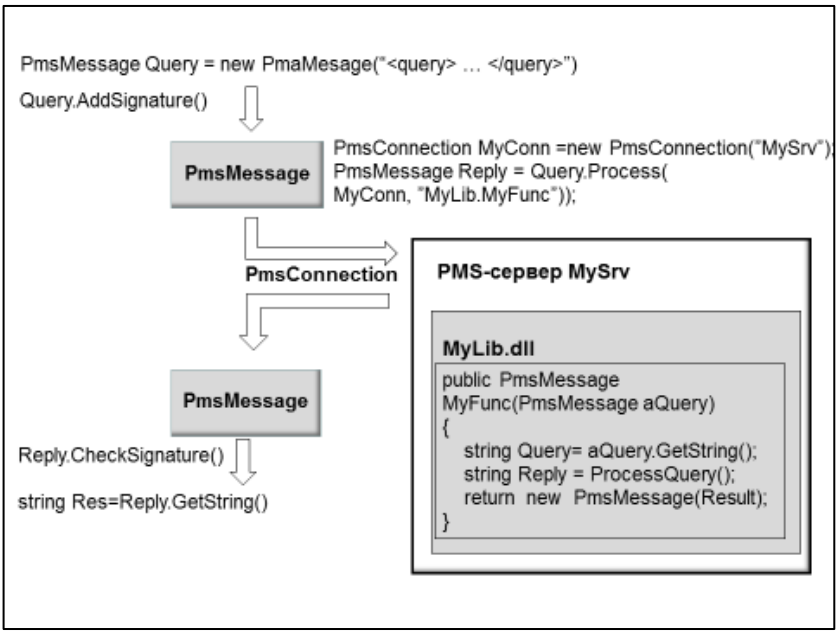

Рисунок 1 – Взаимодействие клиента и сервера PMS

К числу наиболее важных задач средств информационной безопасности в распределенных системах относится аутентификация и разграничение доступа пользователей к информационным ресурсам [6]. Традиционный подход к решению этой задачи основан на использовании той или иной формы централизованной регистрации пользователей с использованием специальных серверов или служб аутентификации и авторизации, ответственных за управление учетными записями пользователей и ассоциированными с ними правами. Однако в больших

распределенных системах реализация централизованного администрирования часто оказывается затруднительной.

PMS опирается на другой подход к решению этой задачи. Этот подход основан на использовании реквизитов подписантов информационного запроса, которые содержатся в удостоверяющих ЭЦП защищенного сообщения (точнее в сертификатах открытого ключа, встроенных в ЭЦП). Так как доступ к информационным ресурсам осуществляется через сервисные функции, рассматриваемая задача решается с помощью встроенных в PMS средств управления доступом к сервисным функциям.

Работа этих средств проиллюстрирована на рисунке 2. Как видно из рисунка, все сервисные функции сгруппированы в одну или несколько динамических библиотек функций, которые подключаются к серверу в момент его запуска. С каждой библиотекой связан собственный файл конфигурации, в котором заданы общие свойства библиотеки и/или отдельных сервисных функций. К числу этих свойств относятся и ограничения доступа к функциям. Эти ограничения задаются в форме требований к реквизитам подписантов: запрос к сервисной функции будет отклонен, если среди его подписантов нет ни одного, чьи реквизиты соответствуют этим требованиям.

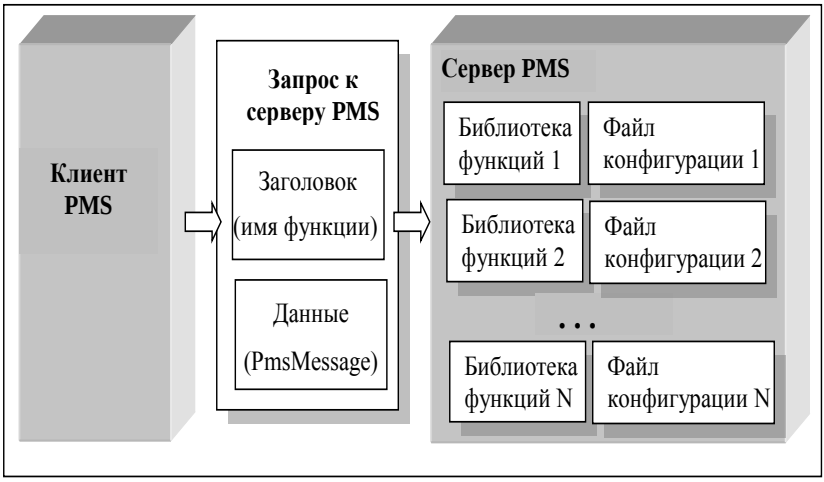

Рисунок 2 – Вызов сервисной функции в сервере PMS

Рассмотрим следующий пример. Предположим, что большая организация с названием «Гамма» имеет филиалы в областных центрах страны. Предположим также, что на PMS-серверах каждого филиала имеется библиотека сервисных функций, предназначенная для регистрации служащих этого филиала (рисунок 3). Эта библиотека содержит ряд относительно простых функций, обеспечивающих добавление, удаление и коррекцию записей о служащих в БД филиала (AddPerson, DeletePerson и CorrectPerson). Кроме того, библиотека включает функцию Report, которая предназначена для формирования отчета о кадровой статистике филиала за любой период времени (например, о динамике средней зарплаты служащих с группировкой по должностям и подразделениям).

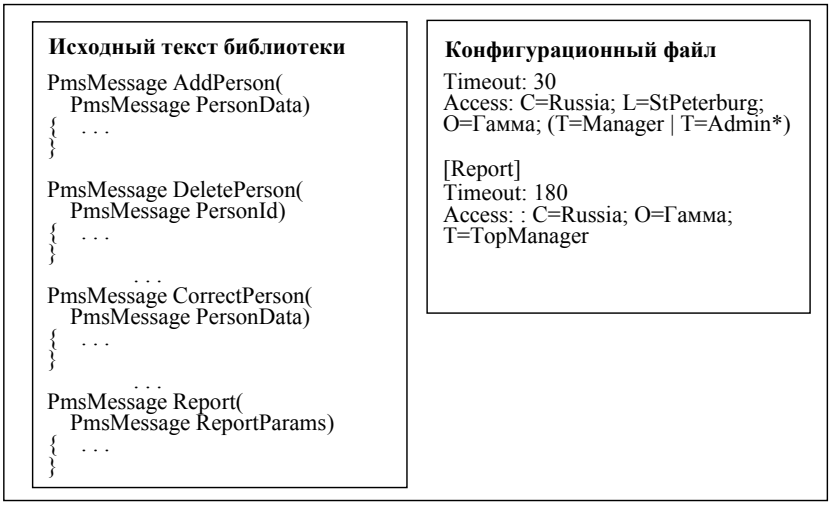

Рисунок 3 – Пример библиотеки сервисных функций и конфигурационного файла

На рисунке 3 приведен пример конфигурационного файла этой библиотеки, содержащего значения основных характеристик сервисных функций. Первые три строки этого файла задают значения «по умолчанию», которые относятся ко всем простым функциям библиотеки и задают предельно допустимое время

выполнения в секундах (Timeout) и ограничения доступа к ним (Access). Эти ограничения означают, что доступ к этим функциям разрешен только служащим данного филиала компании (L=StPeterburg; O=Гамма) в должности менеджера или администратора (T=Manager | T=Admin*). Последующие строки конфигурационного файла, размещенные после заголовка [Report], задают значения основных характеристик конкретной сервисной функции Report. Как видно из рисунка, доступ к этой функции разрешен всем топ-менеджерам компании «Гамма» (O=Гамма; T=TopManager), а предельно допустимое время выполнения (Timeout) составляет 180 секунд, т.е. значительно выше, чем у остальных функций (30). Поскольку эти характеристики заданы для конкретной сервисной функции, они имеют приоритет над характеристиками «по умолчанию», заданными в первых трех строках файла.

Легко видеть, что при описании ограничений на доступ к сервисной функции используется нотация стандарта X509 для описания реквизитов владельца сертификата открытого ключа [7].

Литература:

1. *Мак-Дональд М., Шпушта М.* Microsoft ASP.NET 3.5 с примерами на C# 2008 и Silverlight 2 для профессионалов. – М.: Вильямс, 2009. – 1408 с.

2. *Хант К.* TCP/IP. Сетевое администрирование. – СПб.: Питер, 2007. – 816 с.

3. *Jackson J.C.* Web Technologies: A Computer Science Perspective. – London: Pearson, 2011. – 574 p.

4. *Згоба А.И., Маркелов Д.В., Смирнов П.И.* Кибербезопасность: угрозы, вызовы, решения//Вопросы кибербезопасности. – 2014. – № 5. – С. 30-38.

5. *Асратян Р.*Э. Интернет-служба защищенной обработки информационных запросов в распределенных системах//Программная инженерия. – 2016. – № 11. – С. 490-497.

6. *Смит Р.Э.* Аутентификация: от паролей до открытых ключей. – М.: Вильямс, 2016. – 432 с.

7. *Полянская О.Ю., Горбатов В.С.* Инфраструктуры открытых ключей. – М.: Бином, 2013. – 368 с.