Разработка централизованной системы разграничения прав доступа на основе избирательной многофакторной биометрической аутентификации

А.Н. Ручай
Челябинский государственный университет
e-mail: ruchai@pochta.ru

Данная работа направлена на разработку централизованной системы разграничения прав доступа на основе избирательной многофакторной биометрической аутентификации. Новизна работы заключается в разработке принципов избирательности и многофакторности аутентификации, так как на данный момент не существует подобных разработок. В зависимости от разных условий и факторов, в частности от доступности электронных средств, от удобства, от стойкости к атакам и уязвимостям, от болезней или увечий пользователей, может быть выбрана биометрическая аутентификация на основе любых таких биометрических характеристик, как ритм ввода пароля, голос, динамика подписи и графическое распознавание. Приведены результаты разработки программного обеспечения на основе нового подхода, кроме того, детально описывается архитектура системы и протоколы передачи биометрических данных. Проведен анализ возможных атак на разработанную систему, и сделаны выводы и рекомендации по методам защиты от них.

Введение

В настоящее время актуальной является разработка биометрических систем. Такие системы активно развиваются в течение последних 60 лет. Преимущества биометрических систем очевидны, они имеют большую практическую значимость, что обосновывает важность как теоретических исследований, так и практических разработок. Поэтому данная тема, без сомнения, является актуальной [1].

Разработчики и исследователи биометрических систем предлагают программные реализации на основе, как правило, одной биометрической характеристики без дополнительных инструментов и модулей, что создает проблемы при их использовании и эксплуатации [2]. Однако современные тенденции показывают стремление использовать системный подход для создания мультибиометрических систем аутентификации личности [1, 3, 4]. Здесь под мультибиометрической системой будем понимать систему с использованием нескольких биометрических характеристик человека, которые могут быть интегрированы на разных уровнях и использованы различными способами [1, 5]. Мультибиометрические системы принято разделять на два подкласса: мультимодальные и многофакторные системы аутентификации. В мультимодальных системах биометрические характеристики человека обрабатываются с помощью различных методов и принятие решение происходит по объединенному решающему правилу для повышения надежности. В многофакторных системах используют не только разные биометрические характеристики, но и другие методы аутентифкации, например, PIN–код, пароль, ритм ввода пароля, токены [6].

В зависимости от разных условий и факторов, в частности от доступности электронных средств, от удобства, от стойкости к атакам и уязвимостям, от болезней или увечий пользователей, может быть выбрана биометрическая аутентификация на основе любых таких биометрических характеристик, как ритм ввода пароля, голос, динамика подписи и графическое распознавание. Например, если необходимо разграничить права доступа в изолированном помещении без посторонних, то может быть использована аутентификация по голосу, по ритму ввода пароля или графическому распознаванию. Если помещение наоборот не обладает такими условиями, то аутентификация может быть осуществлена на основе ритма ввода пароля или по динамике подписи. Для осуществления аутентификации в мобильных или сенсорных устройствах может быть выбрана аутентификация по ритму ввода пароля, по динамике подписи или графическому распознаванию. На пропускных пунктах возможна аутентификация по динамике подписи. В настоящее время актуальной является задача разработки универсальных модулей, реализующих разграничение прав доступа на основе биометрической аутентификации [7].

Кроме того, системы разграничения доступа на основе биометрической аутентификации имеют большую практическую значимость и преимущества:

- уникальность, неотъемлемость и неотчуждаемость биометрической характеристики;
- затруднения при проведении атаки подбора по биометрической характеристике;
- независимость от операционной системы и кодировок символов;
- избирательность и многофакторность аутентификации;
- отсутствие ошибок третьего рода, когда невозможно аутентифицировать человека из-за болезней и увечий.

Целью данного проекта была разработка, исследование и реализация централизованной системы разграничения прав доступа на основе избирательной многофакторной биометрической аутентификации с клиент-серверной архитектурой. Для этого необходимо было решить следующие задачи:

- разработка принципов построения системы, архитектуры, протокола взаимодействия;
- разработка и реализация центра и модулей биометрической аутентификации;
- оценка надежности и тестирование работы модулей аутентификации по различным биометрическим характеристикам.

Архитектура системы

В работах [2, 7, 8] был описан разработанный комплекс модулей биометрической аутентификации для разграничения прав доступа в ОС Windows XP на примере текстозависимой верификации диктора [9, 10]. Данный комплекс модулей послужил основой для разработки и реализации централизированной системы разграничения прав доступа на основе избирательной многофакторной биометрической аутентификации. В

работе [11] были сформулированы основные принципы и был создан прототип централизированной системы разграничения прав доступа на основе избирательной многофакторной биометрической аутентификации.

В основу собственных разработок были положены работы [3, 4], в которых был предложен подход к созданию высокопроизводительных мультибиометрических технологий и систем на базе сервисно-ориентированной архитектуры, а также методы оптимизации и распараллеливания вычислений в задаче мультибиометрической идентификации.

С целью разработки и реализации централизированной системы разграничения прав доступа на основе избирательной многофакторной биометрической аутентификации были сформулированы требования к ее архитектуре [3]:

- возможность интеграции в рамках одной системы нескольких методов биометрической аутентифкации;
- возможность замены и модификации библиотек, в которых реализованы методы биометрической аутентифкации;
- гибкость в конфигурировании;
- обеспечение комплексной безопасности и защиты биометрических данных;
- поддержка сущестующих российских стандартов в сфере биометрических технологий.

Самым важным аспектом методологической разработки централизированной системы разграничения прав доступа на основе избирательной многофакторной биометрической аутентификации является требования отраслевых стандартов. Наиболее систематизированным документом является стандарт bioAPI (серия стандартов ГОСТ Р ИСО/МЭК 19784, 19795 и 24709). Согласно стандарту bioAPI, базовыми функциями произвольной биометрической системы являются регистрация (enroll) и сравнение (match). В ходе регистрации информация, полученная при помощи биометрических сканеров, преобразуется в цифровой шаблон. На этапе сравнения предъявляемые биометрические данные сравниваются с шаблоном регистрации. Результатом сравнения биометрических данных является число.

Современные разработки [3] изначально учитывают масштабируемость и распределенность архитектуры биометрической системы, в рамках которой используют концепцию сервисо-ориентированной архитектуры. Для такой архитектуры принято разделять внутреннюю логику биометрических приложений на элементарные сервисы [3]:

- вычислительные сервисы, отвечающие за выполнение функций биометрических библиотек, ядро системы;
- сервисы бизнес-логики приложения; сервисы хранилища;
- клиентские приложения, «тонкий» клиент терминальных станций;
- вспомогательные сервисы управления, мониторинга, диагностики;
- сервисы сообщений/предоставления интерфейса, отвечающие за обмен информацией между узлами системы;

• сервисы операционной системы, распределенная среда исполнения.

На рисунке 1 приведена схема взаимодействия перечисленных групп сервисов. Перечисленные сервисы с точки зрения аппаратных средств могут исполняться как на одном вычислительном сервере, так и на отдельных специализированных серверах или кластерах.

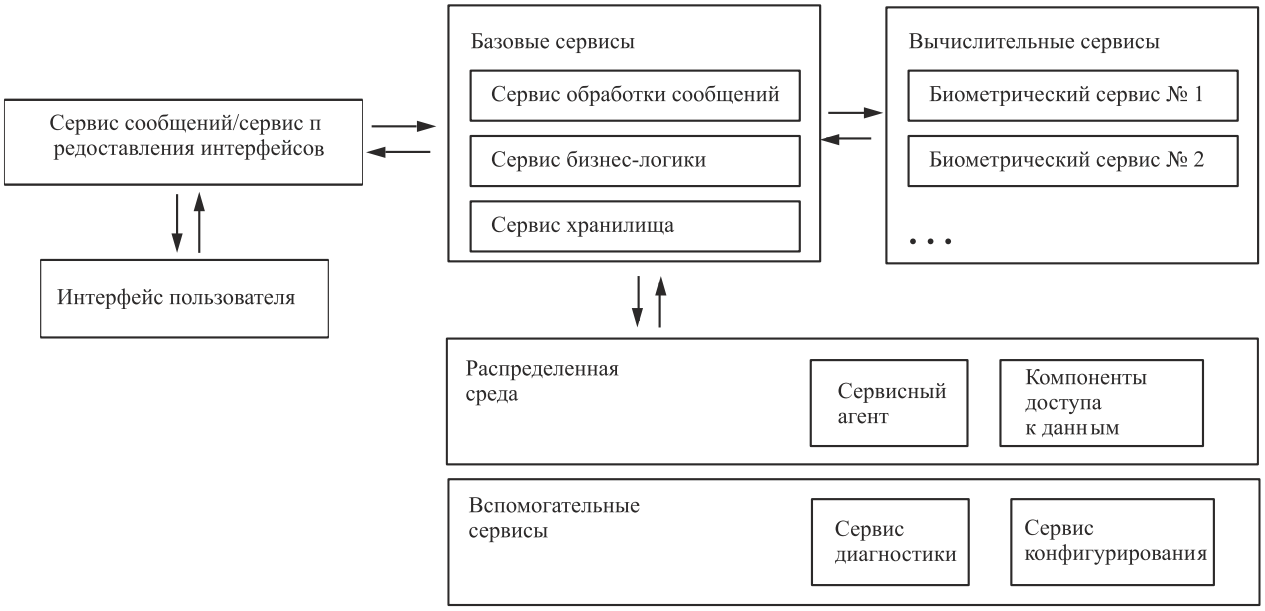

Рис. 1. Программная архитектура

Протоколы взаимодействия

Согласно bioAPI и российским стандартам по биометрии, реализация биометрической системы предполагает три типа данных [3]: исходные данные, полученные с терминальных устройств; данные, обработанные функциями специализированных библиотек (фильтрация, шумоочистка и т. д.); цифровой шаблон/модель биометрического образца. Кроме этого, функции биометрической системы [3]: регистрация, получение шаблона на основе исходных данных; сравнение двух шаблонов, определение меры сходства; нестандартные функции дополнительной обработки биометрической информации.

Основой для протокола передачи исходных биометрических данных являются стандарты по обмену биометрической информации. Стандарты серии ITL-1-200x предполагают следующий состав необходимой информации: заголовок; сопроводительная текстовая информация; биометрические образцы; сопроводительная информация по каждому биометрическому образцу.

Учитывая функциональное назначение компонентов, в работе [3] предлагается следующее базовое распределение сервисов и вычислительной нагрузки между клиентским и серверным компонентами системы (см. рисунок 2). В состав клиентского компонента включены: интерфейс пользователя; модуль управления запросами пользователя; биометрические сервисы; интерфейс администратора. В состав серверного компонента включены: сервис сообщений; сервис хранилища; биометрические сервисы.

Конечному пользователю основной функционал предоставляется посредством технологии «тонкого клиента», или специализированного ПО терминальных станций («тол-

стый клиент»). Пользовательские функции можно представить в виде комбинации следующих обращений [3]: Enroll, регистрация объекта учета в хранилище; Modify, изменение информации об объекте учета; Identify, биометрическая идентификация; Select, запросна выборку данныхиз хранилища.

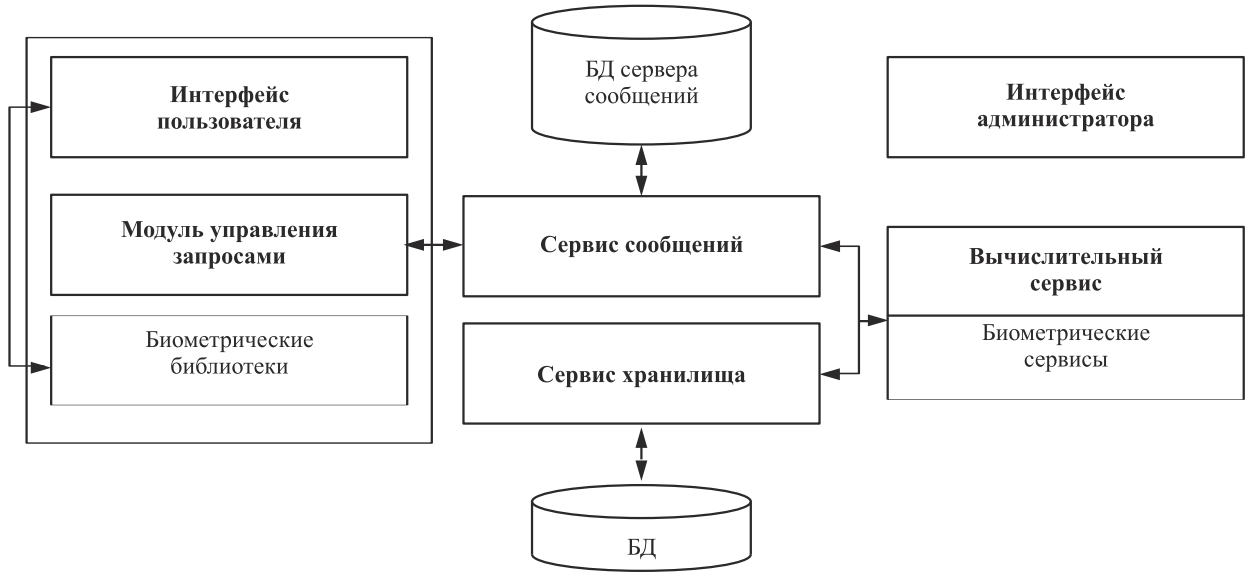

Рис. 2. Программная архитектура

Обмен данными между интерфейсом пользователя (A) и сервисом сообщений (B)

1. $A \to B$: Enroll, пакет данных
2. $B \to A$: Enroll, результат транзакции
3. $A \to B$: Modify, пакет данных
4. $B \to A$: Modify, результат транзакции
5. $A \to B$: Identify, пакет данных
6. $B \to A$: Identify, результат транзакции
7. $A \to B$: Selected, ID
8. $B \to A$: Selected, пакет данных

Обмен данными между интерфейсом пользователя (A) и биометрическими библиотеками клиентской части (B)

1. $A \to B$: Enroll, бинарные данные
2. $B \to A$: Enroll, ответы; шаблон регистрации; отказ в регистрации
3. $A \to B$: Process, бинарные данные
4. $B \to A$: Process, ответы; обработанные данные; дополнительная информация

Обмен данными между сервисом сообщений (A) и сервисом хранилища (B)

1. $A \to B$: Add, SQL запрос
2. $B \to A$: Add, результат транзакции
3. $A \to B$: Modify, SQL запрос
4. $B \to A$: Modify, результат транзакции
5. $A \to B$: Select, SQL запрос
6. $B \to A$: Select, пакет данных

Обмен данными между сервисом сообщений (A) и вычислительным сервисом (B)

1. $A \to B$: Enroll, пакет данных
2. $B \to A$: Enroll, результат транзакции
3. $A \to B$: Match, пакет данных
4. $B \to A$: Match, результат транзакции

Обмен данными между вычислительным сервером (A) и биометрическими библиотеками серверной части (B)

1. $A \to B$: Enroll, исходные данные
2. $B \to A$: Enroll, шаблон
3. $A \to B$: Match, шаблон
4. $B \to A$: Match, мера сходства

Атаки и защита биометрической системы

На основе анализа модели существующих атак и защиты можно сделать вывод, что многие проблемы и атаки предотвращаются с помощью цифрового кодирования, временных меток и шифрования открытого канала передачи данных [12, 13]. В связи с этим система разграничения прав доступа должна быть реализована с клиент-серверной архитектурой, что дает следующие преимущества:

- повышается общая безопасность системы;
- один мощный сервер сможет одновременно обслуживать множество клиентов;
- обеспечивается минимальная нагрузка на компьютер клиента;
- сводится к минимуму количество клиентских настроек;
- сервер можно переносить под любую ОС, а клиентские части останутся неизменными;
- клиентскую часть также можно написать под другую ОС, а сервер останется неизменным.

Клиент-серверная архитектура кроме этого позволяет отделить работу с внешними устройствами, чей интерфейс зачастую не стандартизирован, от основного вычислительного узла, который, в свою очередь, должен быть реализован с учетом требований российских и международных стандартов. На рисунке 3 изображена схема клиент-серверной архитектуры централизированной системы разграничения прав доступа на основе избирательной многофакторной биометрической аутентификации.

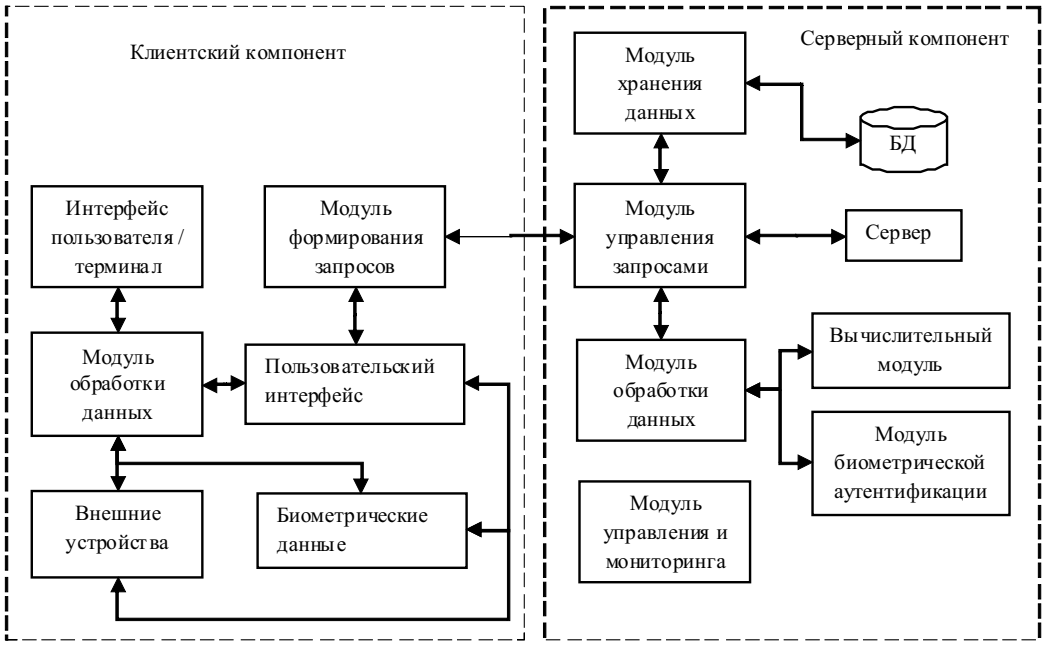

Рис. 3. Клиент-серверная архитектура

Заключение

В результате всей работы была разработана централизованная система разграничения прав доступа на основе избирательной многофакторной биометрической аутентификации. В зависимости от разных условий и факторов, в частности от доступности электронных средств, от удобства, от стойкости к атакам и уязвимостям, от болезней или увечий пользователей, может быть выбрана биометрическая аутентификация на основе любых таких биометрических характеристик, как ритм ввода пароля, голос, динамика подписи и графическое распознавание.

Важным этапом для реализации такой биометрической системы была разработка архитектуры системы и протокола передачи биометрических данных. Кроме того, был проведен анализ возможных атак на разработанную систему, и сделаны выводы и рекомендации по методам защиты от них.

Разработанная централизованная система разграничения прав доступа на основе избирательной многофакторной биометрической аутентификации успешно прошла тестирование на кафедре компьютерной безопасности и прикладной алгебры Челябинского государственного университета.

Однако, существуют направления для дальнейшего развития разработанной систе-

мы: обеспечение большей универсальности, применения других биометрических характеристик, увеличения производительности и надежности.

Список литературы

[1] Сесин Е.М. Системы идентификации личности, основанные на интеграции нескольких биометрических характеристик человека / Е.М. Сесин, В.М. Белов // Доклады ТУСУРа. №2(25), часть 2. 2012. С. 175-179.

[2] Ручай А.Н. Текстозависимая верификация диктора: математическая модель, статистические исследования, комплекс программ. Saarbrucken: LAP LAMBERT Academic Publishing, 2012. 144 с.

[3] Ушмаев О.С. Сервисно-ориентированный подход к разработке мультибиометрических технологий // Информатика и ее применения. Т. 2. Вып. 3. 2008. С. 41-53.

[4] Ушмаев О.С. Проблемы распараллеливания биометрических вычислителей в крупномасштабных идентификационных системах // Информатика и ее применения. Т. 3. Вып. 1. 2009. С. 8-18.

[5] Болл Р.М. Руководство по биометрии / Р. М. Болл, Дж. Х. Коннел, Ш. Панканти, Н. К. Ратха, Э. У. Сеньор. М. : Техносфера, 2007. 368 с.

[6] Ручай А.Н. Усиление парольной аутентификации с помощью проверки ритма ввода пароля / А.Н. Ручай, А.В. Волков // Современные проблемы математики. Екатеринбург: ИММ УрО РАН, 2013. С. 235 — 237.

[7] Ручай А.Н. Разработка комплекса модулей для разграничения прав доступа в ОС Windows XP на основе биометрической аутентификации // Информационные технологии и системы: материалы Первой междунар. конф. Челябинск: ЧелГУ, 2012. С. 75-76.

[8] Ручай А.Н. Разработка универсального комплекса модулей для разграничения прав доступа в ОС Windows XP на основе биометрической аутентификации // Безопасность информационных технологии. №3. 2013. (в печате).

[9] Ручай А.Н. Формантный метод текстозависимой верификации диктора // Вестник Челяб. гос. университета. Математика. Механика. Информатика. 2010. №23(204), вып. 12. С. 121-131.

[10] Ручай А.Н. Улучшение надежности формантного метода текстозависимой верификации диктора с помощью нового метода сегментации сигнала // Доклады ТУСУР. №2(24). 2011. С. 241-246.

[11] Ручай А.Н. Прототип централизованной системы разграничения прав доступа на основе избирательной многофакторной биометрической аутентификации // Безопасность информационных технологии. №1. 2013. (в печате).

[12] Ручай А.Н. Модель атак и защиты на биометрическую систему распознавания диктора // Доклады ТУСУРа. №1(23). 2011. С. 96-100.

[13] Dunstone T. Biometric system and data analysis: design, evaluation, and data mining / T. Dunstone, N. Yager. Boston, Ma: Springer, 2009. 268 p.