Международный союз электросвязи

МСЭ-Т X.1279

(09/2020)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность облачных вычислений – Управление определением идентичности

Система расширенной аутентификации с использованием телебиометрии с антиспуфинговыми механизмами обнаружения

Рекомендация МСЭ-Т X.1279

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности (1)	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	**X.1250–X.1279**
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность "умных" электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1360–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1389
Безопасность технологии распределенного реестра	X.1400–X.1429
Безопасность технологии распределенного реестра	X.1430–X.1449
Протоколы безопасности (2)	X.1450–X.1459
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699
КВАНТОВАЯ СВЯЗЬ	
Терминология	X.1700–X.1701
Квантовый генератор случайных чисел	X.1702–X.1709
Структура безопасности QKDN	X.1710–X.1711
Проектирование безопасности QKDN	X.1712–X.1719
Методы обеспечения безопасности QKDN	X.1720–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	
Безопасность больших данных	X.1750–X.1759
БЕЗОПАСНОСТЬ СЕТЕЙ 5G	X.1800–X.1819

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1279

Система расширенной аутентификации с использованием телебиометрии с антиспуфинговыми механизмами обнаружения

Резюме

В Рекомендации X.1279 представлена архитектурная основа системы расширенной аутентификации с использованием телебиометрии с антиспуфинговыми механизмами обнаружения. В настоящей Рекомендации проведен анализ угроз для традиционных решений телебиометрической аутентификации и представлены архитектурная основа системы и последовательность операций аутентификации, а также рассмотрены вопросы безопасности расширенной аутентификации с использованием телебиометрии с антиспуфинговыми механизмами обнаружения.

Хронологическая справка

Издание	Рекомендация	Утверждено	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1279	03.09.2020 г.	17-я	11.1002/1000/14261

Ключевые слова

Антиспуфинговое обнаружение, расширенная аутентификация, телебиометрия.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации. Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним в целях стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" (shall) или некоторые другие обязывающие выражения, такие как "обязан" (must), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу http://www.itu.int/ITU-T/ipr/.

Содержание

Введение

Технологии телебиометрической аутентификации часто используются в различных областях, требующих высокого уровня надежности, таких как электронный банкинг и услуги материально-технического снабжения. Для обеспечения безопасности телебиометрических данных необходимо принять меры по созданию системы безопасности, способной предотвращать потенциальные угрозы в этой области.

В настоящей Рекомендации анализируются угрозы для традиционных решений телебиометрической аутентификации и предлагается система расширенной аутентификации с использованием телебиометрии с антиспуфинговым обнаружением (ASD). Целью антиспуфингового обнаружения является установление того, что пользователь, отправляющий запрос на телебиометрическую аутентификацию, – реальное лицо, которому принадлежат биометрические данные. Для повышения безопасности и предотвращения использования поддельных биометрических данных антиспуфинговое обнаружение может использоваться вместе с телебиометрической проверкой. Функция антиспуфингового обнаружения может быть предназначена для повышения безопасности и предотвращения утечки биометрических данных.

Рекомендация МСЭ-Т X.1279

Система расширенной аутентификации с использованием телебиометрии с антиспуфинговыми механизмами обнаружения

1 Сфера применения

В настоящей Рекомендации представлена архитектурная основа системы усовершенствованной телебиометрической аутентификации с антиспуфинговыми механизмами обнаружения. В ней анализируются угрозы для традиционных решений телебиометрической аутентификации и приведено описание архитектурной основы системы и операций аутентификации, а также рассматриваются вопросы безопасности усовершенствованной телебиометрической аутентификации с антиспуфинговыми механизмами обнаружения.

Описанная в настоящей Рекомендации архитектурная основа системы может использоваться в качестве руководства при развертывании расширенных решений телебиометрической аутентификации с использованием функций антиспуфингового обнаружения.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[ITU-T X.1086] Recommendation ITU-T X.1086 (2008), *Telebiometrics protection procedures – Part 1: A guideline to technical and managerial countermeasures for biometric data security*

[ITU-T X.1087] Recommendation ITU-T X.1087 (2016), *Technical and operational countermeasures for telebiometric applications using mobile devices*

[ISO/IEC 24745] ISO/IEC 24745:2011, *Information technology – Security techniques – Biometric information protection*

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах:

3.1.1 аутентификация (authentication) [b-ISO/IEC 2382-37]: Действие, доказывающее или показывающее бесспорное происхождение или достоверность.

3.1.2 биометрический (biometric) [b-ISO/IEC 2382]: Имеющий отношение к биометрии.

3.1.3 сбор биометрических данных (biometric capture) [b-ISO/IEC 2382-37]: Получение и запись в воспроизводимой форме сигнала(ов) биометрической характеристики (биометрических характеристик) непосредственно от индивида(ов) или от представления(й) биометрической характеристики (биометрических характеристик).

3.1.4 биометрическая характеристика (biometric characteristic) [b-ISO/IEC 2382-37]: Биологические и поведенческие характеристики индивида, которые могут быть зарегистрированы и использованы в качестве отличительных повторяющихся биометрических признаков для автоматического распознавания индивидов.

3.1.5 биометрические данные (biometric data) [b-ISO/IEC 2382-37]: Биометрический образец или совокупность биометрических образцов на любой стадии обработки, например биометрический

контрольный шаблон, биометрическая проба**,** биометрический признак или биометрическое свойство.

3.1.6 биометрический признак (biometric feature) [b-ISO/IEC 2382-37]: Цифровое представление информации (числа или метки), извлеченное из биометрических образцов и используемое для сравнения.

3.1.7 биометрическое распознавание/биометрия (biometric recognition/biometrics) [b-ISO/IEC 2382-37]: Автоматическое распознавание индивидов, основанное на их поведенческих и биологических характеристиках.

3.1.8 база данных биометрических контрольных шаблонов (biometric reference database) [b-ISO/IEC 2382-37]: База данных записей данных биометрических контрольных шаблонов.

3.1.9 биометрический шаблон (biometric template) [b-ISO/IEC 19784-1]: Набор хранимых биометрических признаков, сравниваемых непосредственно с биометрическими признаками распознаваемого биометрического образца.

3.1.10 биометрическая верификация (biometric verification) [b-ISO/IEC 2382-37]: Процесс подтверждения биометрического заявления при сравнении.

3.1.11 сравнение (сопоставление) (comparison (match/matching)) [b-ISO/IEC 19784-1]: Оценка, вычисление или измерение степени схожести и различия между распознаваемым(и) биометрическим(и) образцом(ами)/биометрическими признаками/биометрическими моделями и биометрическим(и) контрольным(и) шаблоном(ами).

3.1.12 решение о сравнении (comparison decision) [b-ISO/IEC 19784-1]: Определение того, имеют ли биометрический образец и биометрический контрольный шаблон один и тот же биометрический источник на основании сравнительной(ых) оценки(ок), правил принятия решений, включая пороговое значение и, возможно, другие входные данные.

3.1.13 мобильное устройство (mobile device) [b-ISO 18461]: Портативное вычислительное устройство, обычно снабженное экраном с сенсорным, перьевым и/или клавиатурным вводом и интернет-соединением.

3.1.14 пользователь (user) [b-ISO/IEC 2382-37]: Любое физическое или юридическое лицо, взаимодействующие каким-либо образом с биометрической системой.

3.1.15 телебиометрия (telebiometrics) [b-ITU-T X.1081]: Применение биометрии в электросвязи.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины:

3.2.1 антиспуфинговое обнаружение (anti-spoofing detection): Процесс обнаружения и предотвращения спуфинга биометрической системы, осуществленного с помощью неправомерных действий.

3.2.2 обфускация (obfuscation): Акт преднамеренного создания трудного для понимания человеком исходного или машинного кода. Этот метод включает набор преобразований, изменяющих видимую функцию программного обеспечения без изменения результатов. Обфусцированная программа должна приводить к тем же результатам, что и необфусцированная.

ПРИМЕЧАНИЕ. – Обфускация – это метод, который обычно используется для сокрытия смысла программного обеспечения путем перестановки операций, но может использоваться и для добавления в код малозаметных меток. В обоих случаях алгоритмы предусматривают набор преобразований, изменяющих видимую функцию программного обеспечения без изменения результатов. Обфусцированная программа должна приводить к тем же результатам, что и необфусцированная [b-Disappearing Cryptography].

3.2.3 качество обнаружения (quality detection): Мера пригодности биометрического образца для получения или выполнения решения о биометрическом сравнении.

3.2.4 спуфинг (spoofing): Попытка объекта выдать себя за другой объект путем демонстрации записанного изображения, другого образца биометрических данных или искусственно полученной биометрической характеристики в целях имитации того или иного индивида.

ПРИМЕЧАНИЕ. – Это адаптированное определение взято из [b-ITU M.3016.0].

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

ASD	Anti-Spoofing Detection	Антиспуфинговое обнаружение
PII	Personally Identifiable Information	Информация, позволяющая установить личность
PKI	Public Key Infrastructure	Инфраструктура открытых ключей
SMS	Short Messaging Service	Служба коротких сообщений
SRP	Secure Remote Password	Безопасный удаленный пароль

5 Соглашения

Отсутствуют.

6 Угрозы безопасности для телебиометрической аутентификации и контрмеры

6.1 Базовая информация

С появлением интернет-услуг механизмы аутентификации, основанные на традиционном пароле, больше не могут удовлетворять требованиям удобства для пользователей и обеспечения безопасности; поэтому в целях большего удобства и большей безопасности в настоящее время чаще используются механизмы телебиометрической аутентификации.

Однако в механизмах биометрической аутентификации также существуют проблемы и риски, например, для аутентификации методом распознавания лиц злоумышленники могут использовать фотографию, компьютерное изображение или лицо на экране, а для телебиометрической аутентификации – копию телебиометрического образца (отпечатка пальца, радужной оболочки глаза или голосового отпечатка).

6.2 Эталонные режимы аутентификации

Существует два основных эталонных режима телебиометрической аутентификации на мобильных устройствах:

1) режим локальной аутентификации – биометрические данные хранятся на мобильном устройстве и телебиометрическая верификация выполняется на стороне мобильного устройства. Результат телебиометрической верификации передается на сервер;
2) режим удаленной аутентификации – биометрические данные хранятся на сервере и телебиометрическая верификация выполняется на стороне сервера.

В настоящей Рекомендации основное внимание уделяется режиму удаленной аутентификации.

6.3 Угрозы безопасности

6.3.1 Угрозы безопасности на стороне клиента

На стороне клиента телебиометрическая аутентификация сталкивается со следующими угрозами безопасности:

– клиентская программа (клиент) является фальсифицированным агентом или изменена путем ввода вредоносного кода;
– злоумышленники пытаются нарушить доступность и целостность клиента;
– злоумышленники пытаются похитить или изменить собранные биометрические данные клиента;
– для аутентификации методом распознавания лиц злоумышленники могут использовать фотографию, компьютерное изображение или лицо на экране;
– для телебиометрической аутентификации злоумышленники могут использовать копию биометрических данных (отпечатка пальца, радужной оболочки глаза или голосового отпечатка).

6.3.2 Угрозы безопасности на стороне сервера

На стороне сервера телебиометрическая аутентификация сталкивается со следующими угрозами безопасности:

– злоумышленники могут проникнуть на сервер, чтобы нарушить работу базы данных или прикладного программного обеспечения сервера;

– собранные биометрические данные или данные шаблона могут быть незаконно заменены или организована их утечка как измененных или похищенных данных;

– собранные биометрические данные или данные шаблона могут быть незаконно изменены при передаче;

– может использоваться незаконная программа сравнения.

6.3.3 Угрозы безопасности для канала связи между клиентом и сервером

Телебиометрическая аутентификация сталкивается со следующими угрозами безопасности для канала связи между клиентом и сервером:

– злоумышленники могут перехватить или изменить сообщения между клиентом и сервером;

– во время передачи от клиента к серверу биометрические данные могут быть украдены или изменены.

6.4 Меры противодействия

Для уменьшения этих угроз телебиометрической аутентификации наряду с верификацией телебиометрических данных при аутентификации обычно используются антиспуфинговые механизмы обнаружения (ASD).

ASD реализуется в рамках системы телебиометрической аутентификации. Функция ASD может использоваться для установления того, что пользователь, отправляющий запрос на телебиометрическую аутентификацию, – реальное лицо, которому принадлежат биометрические данные. Это позволяет избежать ситуации, когда злоумышленник использует для телебиометрической аутентификации поддельные или скопированные биометрические данные.

Для повышения безопасности и предотвращения ситуаций с использованием поддельных биометрических данных ASD может использоваться вместе с телебиометрической верификацией. Например, мобильное приложение может предложить пользователю кивнуть, покачать головой, моргнуть, открыть рот и т. д., чтобы подтвердить, что аутентификация запрошена реальным лицом.

Дополнительные угрозы безопасности и меры противодействия представлены в [ITU-T X.1086] и [ITU-T X.1087].

7 Архитектурная основа

7.1 Архитектурная схема

Архитектурная схема расширенной телебиометрической аутентификации с использованием механизмов ASD показана на рисунке 1.

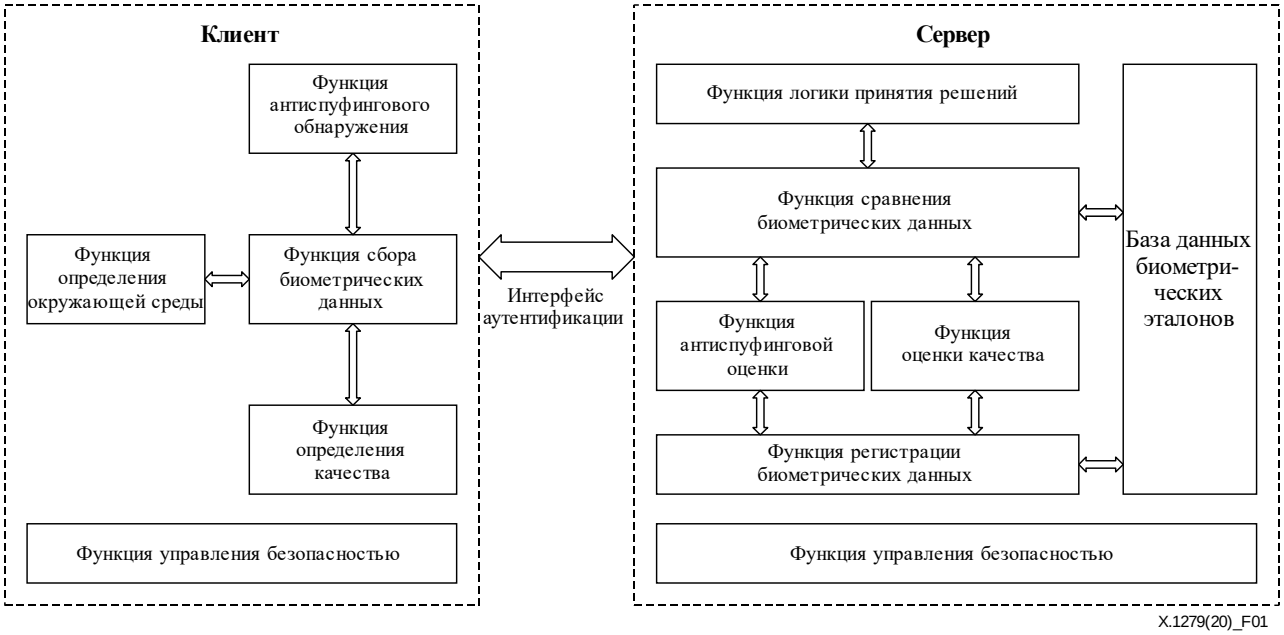

Рисунок 1 − Архитектурная схема расширенной телебиометрической аутентификации с использованием механизмов ASD

Подробное описание функций, показанных на этой схеме, приведено в пунктах 7.2 и 7.3.

7.2 Функции на стороне клиента

7.2.1 Функция определения окружающей среды

Эта функция отвечает за распознавание и обнаружение биометрических характеристик и условий окружающей среды. Например, она решает, удовлетворяют ли характеристики лица и окружающая среда условиям сбора данных.

7.2.2 Функция сбора биометрических данных

Эта функция используется для сбора биометрических данных конечных пользователей с последующей их передачей локальной функции определения качества и функции ASD для обработки, после чего биометрические данные передаются через интерфейс аутентификации на сервер для удаленной аутентификации.

7.2.3 Функция обнаружения ASD

Эта функция используется для обнаружения ожидаемых движений в соответствии со стратегиями или политикой сервера, таких как кивок, покачивание головой, моргание, открывание рта и т. д.

Хотя ASD можно выполнять с помощью многих методов, для телебиометрической аутентификации на мобильных устройствах лучше всего подходит метод обнаружения реальности. В качестве инструмента определения того, может ли представляемый объект продемонстрировать подсистеме сбора биометрических данных признаки реальности, можно использовать процедуру вызов–ответ. Например, ожидается, что радужная оболочка глаза живого человека будет реагировать на изменения яркости видимого света (вызов) изменением размера зрачка (ожидаемый ответ живого человека).

Обнаружение реальности лица может состоять из следующих этапов, аналогичных процессам биометрического распознавания:

– сбор исходных данных для ASD от объекта с использованием подсистемы сбора биометрических данных;
– извлечение признаков из данных ASD; и
– сравнение признаков ASD с критериями.

7.2.4 Функция определения качества

Эта функция используется для предварительной оценки качества биометрических данных в соответствии со стратегиями или политикой сервера. Функция определения качества выполняет оценку качества собранных биометрических данных и извлекает биометрические характеристики. Обычно эта функция используется вместе с функцией ASD и функцией сбора биометрических данных в целях получения наилучших биометрических данных для моделирования и оценки.

7.2.5 Функция управления безопасностью

Функция управления безопасностью на стороне клиента отвечает за управление использованием регистрационных данных, безопасную среду и т. д.

7.3 Функции на стороне сервера

7.3.1 Функция регистрации биометрических данных

Эта функция отвечает за регистрацию биометрических данных. Записи регистрации биометрических данных могут поступать от клиента, импортироваться в пакетном режиме напрямую или извлекаться из других источников, таких как национальная база данных идентификаторов. Это можно делать с помощью шаблона регистрации биометрических данных.

7.3.2 Функция антиспуфинговой оценки

Эта функция используется для оценки того, являются ли биометрические данные поддельными или скопированными. Сервер выполняет глубокий антиспуфинговый анализ на основе предварительного результата обнаружения на стороне клиента и стратегий и политики сервера.

Сервер может подать клиенту команду на обнаружение ожидаемых движений в соответствии со своими стратегиями или политикой, таких как кивок, покачивание головой, моргание, открывание рта и т. д. Сервер получает от клиента искомые данные биометрических признаков и использует свой биометрический эталон и заранее определенную стратегию для оценки того, обладает ли представление объекта признаками реальности.

7.3.3 Функция оценки качества

Эта функция используется для оценки качества биометрических данных на основе предварительного результата обнаружения со стороны клиента и стратегий и политики сервера. Эта функция выполняет оценку качества полученных биометрических данных. Если качество не достигает требуемого порогового значения, то сервер отклоняет полученные биометрические данные и предлагает клиенту повторить их сбор. Если же качество соответствует требуемому пороговому значению, то биометрические данные передаются в функцию сравнения биометрических данных для выполнения сравнения.

Устройства разного типа могут обладать разными возможностями сбора биометрических данных. Качество биометрических данных можно улучшить, используя разные устройства. Для улучшения качества биометрических данных сервер может потребовать от пользователя применения нескольких устройств. Если биометрические эталоны получены от устройств разного типа, то сервер должен хранить и использовать разные биометрические эталоны для этих устройств.

7.3.4 Функция сравнения биометрических данных

Эта функция обеспечивает проверку биометрических признаков, полученных от клиента, и их сравнение с биометрическими эталонами, хранящимися на сервере. Биометрические эталоны, хранящиеся в базе данных биометрических эталонов, генерируются в процессе регистрации биометрических данных.

7.3.5 Функция логики принятия решений

Эта функция содержит логику принятия решений для запуска различных процессов аутентификации и направляет клиенту соответствующие инструкции для выполнения тех или иных процессов аутентификации. Решение принимается на основе данных управления рисками, включая информацию о программном и аппаратном обеспечении мобильного устройства и профиле пользователя. Например, если анализ данных показал, что конечный пользователь относится к группе повышенного риска, то

функция логики принятия решений потребует от клиента выполнить ASD в дополнение к основной процедуре сбора и сравнения биометрических данных.

7.3.6 База данных биометрических эталонов

База данных биометрических эталонов используется для хранения биометрических данных, данных управления рисками, имен пользователей, их идентификационных данных и т. д.

7.3.7 Функция управления безопасностью

Эта функция используется для обеспечения безопасного выполнения функций сервера и безопасного хранения базы данных биометрических эталонов во избежание искажения или хищения биометрических данных или шаблона.

8 Последовательность операций аутентификации

8.1 Типы сообщений

В стеке протоколов телебиометрической аутентификации на мобильных устройствах на разных этапах присутствуют сообщения как минимум трех типов:

– регистрация – сервер записывает регистрационную информацию пользователя и тип аутентификации, согласованный пользователем и сервером;

– аутентификация – сервер сравнивает полученные биометрические данные с зарегистрированным биометрическим эталоном;

– отмена регистрации – пользователь отменяет регистрацию на сервере. Сервер удаляет регистрационные данные пользователя.

ПРИМЕЧАНИЕ. – В настоящей Рекомендации основное внимание уделяется удаленной верификации. Клиент регистрирует биометрический эталон на сервере. Получив запрос на верификацию, сервер сравнивает полученные биометрические данные с зарегистрированным биометрическим эталоном.

8.2 Последовательность операций

8.2.1 Последовательность операций регистрации

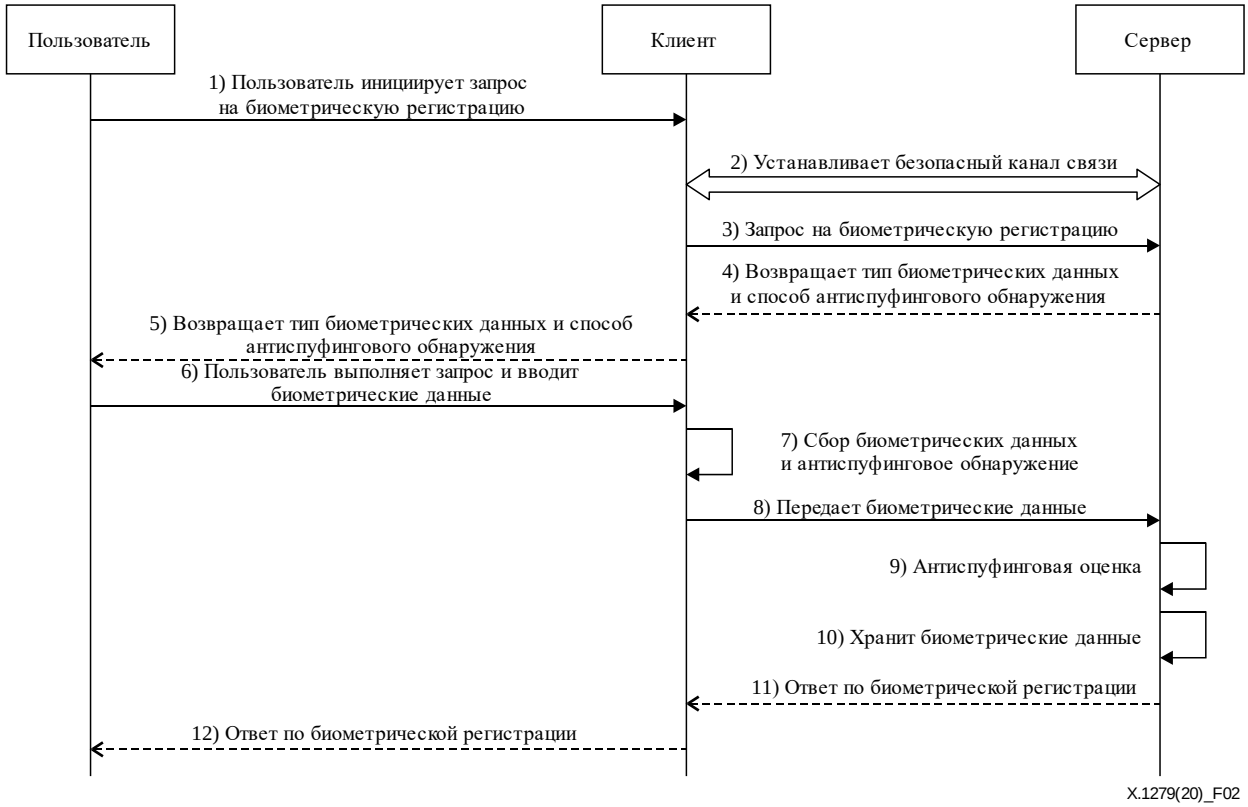

Рисунок 2 − Последовательность операций регистрации

На рисунке 2 показана последовательность операций регистрации. Ниже приводится подробное описание этих операций.

Подготовка: пользователь успешно проходит аутентификацию на сервере с помощью других механизмов аутентификации, например идентификатора учетной записи/пароля пользователя и кода подтверждения через службу коротких сообщений (SMS).

1) Пользователь применяет идентификатор учетной записи/пароль для входа в систему и инициирует запрос клиенту на биометрическую регистрацию.
2) Клиент устанавливает защищенный канал связи с сервером для защиты сеанса и передачи данных, например используя протокол безопасного удаленного пароля (SRP).
3) Клиент передает на сервер запрос биометрической регистрации вместе с идентификатором учетной записи пользователя и данными управления рисками.
4) Функция логики принятия решений на сервере возвращает клиенту надлежащий тип биометрической регистрации и способ ASD на основе анализа данных управления рисками и бизнес-логики.
5) Клиент просит пользователя выполнить указанные действия для сбора биометрических данных.
6) Пользователь выполняет требуемые действия и вводит биометрические данные в клиентскую программу.
7) Функция сбора биометрических данных клиентской программы собирает биометрические данные, а ASD опознает ожидаемые действия пользователя.
8) Клиент извлекает биометрические признаки и по установленному безопасному каналу связи отправляет их на сервер в качестве биометрического эталона.

9) Сервер связывает биометрические данные с идентификатором учетной записи пользователя и выполняет ASD.

10) Сервер сохраняет полученный биометрический эталон в базе данных биометрических эталонов.

11) Сервер возвращает результаты биометрической регистрации клиенту.

12) Клиент информирует пользователя о результате биометрической регистрации.

8.2.2 Последовательность операций аутентификации

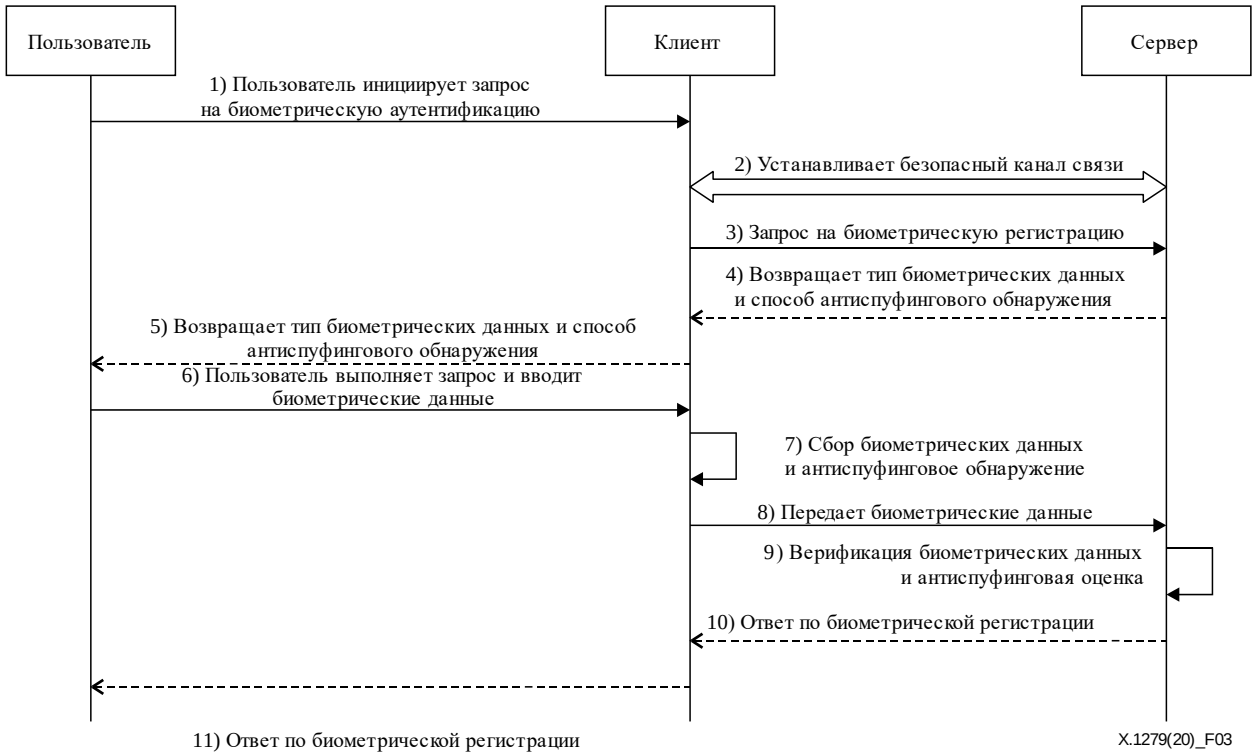

Рисунок 3 − Последовательность операций аутентификации

На рисунке 3 показана последовательность операций аутентификации. Ниже приводится подробное описание этих операций.

1) Пользователь инициирует запрос клиенту на биометрическую аутентификацию с указанием идентификатора своей учетной записи.

2) Клиент устанавливает защищенный канал связи с сервером для защиты сеанса и передачи данных, например используя протокол безопасного удаленного пароля (SRP).

3) Клиент передает на сервер запрос на биометрическую аутентификацию вместе с идентификатором учетной записи пользователя и данными управления рисками.

4) Функция логики принятия решений на сервере возвращает клиенту надлежащий тип биометрической регистрации и способ ASD на основе анализа данных управления рисками и бизнес-логики.

5) Клиент просит пользователя выполнить указанные действия для сбора биометрических данных.

6) Пользователь выполняет требуемые действия и вводит биометрические данные в клиентскую программу.

7) Функция сбора биометрических данных о клиенте собирает биометрические данные, а функция ASD опознает ожидаемые действия пользователя.

8) Клиент извлекает данные биометрических признаков и передает их на сервер по установленному безопасному каналу связи.

9) Сервер выполняет верификацию биометрических данных, сравнивая извлеченные биометрические признаки с биометрическим эталоном, и выполняет ASD.

10) Сервер возвращает результаты биометрической аутентификации клиенту.

11) Клиент информирует пользователя о результате биометрической аутентификации.

8.2.3 Последовательность операций отмены регистрации

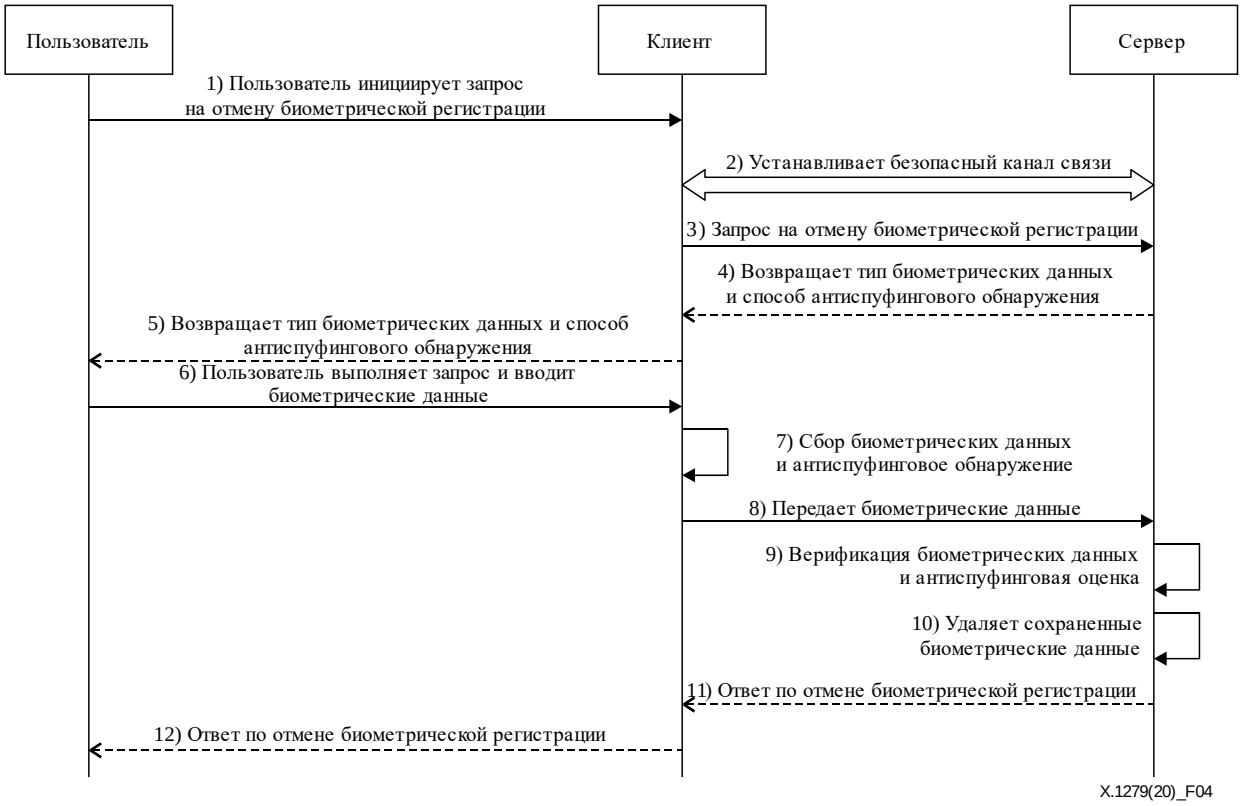

Рисунок 4 − Последовательность операций отмены регистрации

На рисунке 4 показана последовательность операций отмены регистрации. Ниже приводится подробное описание этих операций.

Подготовка: пользователь успешно проходит аутентификацию на сервере с помощью других механизмов аутентификации, например идентификатора учетной записи/пароля пользователя и SMS с кодом подтверждения.

1) Пользователь применяет идентификатор учетной записи/пароль для входа в систему и инициирует запрос клиенту на отмену биометрической регистрации.

2) Клиент устанавливает защищенный канал связи с сервером для защиты сеанса и передачи данных, например используя протокол SRP.

3) Клиент передает на сервер запрос на отмену биометрической регистрации вместе с идентификатором учетной записи пользователя и данными управления рисками.

4) Функция логики принятия решений на сервере возвращает клиенту надлежащий тип биометрической регистрации и способ ASD на основе анализа данных управления рисками и бизнес-логики.

5) Клиент просит пользователя выполнить указанные действия для сбора биометрических данных.

6) Пользователь выполняет требуемые действия и вводит биометрические данные в клиентскую программу.

7) Функция сбора биометрических данных о клиенте собирает биометрические данные, а функция ASD опознает ожидаемые действия пользователя.

8) Клиент извлекает данные биометрических признаков и передает их на сервер по установленному безопасному каналу связи.

9) Сервер выполняет верификацию биометрических данных, сравнивая извлеченные биометрические признаки с сохраненным биометрическим эталоном, и выполняет ASD.

10) Сервер удаляет биометрический эталон пользователя из базы данных биометрических эталонов.

11) Сервер возвращает результат отмены биометрической регистрации клиенту.

12) Клиент информирует пользователя о результате отмены биометрической регистрации.

9 Руководящие указания по безопасности

9.1 Безопасность клиента

Операционная система мобильного устройства должна своевременно обновляться до самой последней защищенной версии.

Клиент должен быть подписан, чтобы иметь возможность идентифицировать источник клиента.

Клиент должен быть защищен от несанкционированного изменения или обновления.

В клиентской программе должна быть усилена защита кода и данных от обратного инжиниринга, например, путем обфускации.

Сбор данных в клиентской программе должен осуществляться в безопасной среде, гарантирующей конфиденциальность и целостность собранных данных.

9.2 Безопасность сервера

На сервере должна соблюдаться политика строгого контроля доступа, любая операция на сервере должна быть предварительно аутентифицирована и авторизована.

Сервер должен быть способен устанавливать идентичность клиента.

От атаки с повторной передачей связь между сервером и клиентом должна быть защищена, например, путем использования в сообщениях динамических данных, таких как контрольное слово, вызов или метка времени.

Необходимо вести журналы операций на сервере, и целостность этих журналов должна быть защищена.

9.3 Безопасность хранения данных

Сертификаты МСЭ-Т X.509 и секретные ключи должны храниться в безопасном месте, и должна быть установлена строгая политика контроля доступа.

Секретные ключи должны храниться в зашифрованном тексте, а алгоритм шифрования должен иметь высокий уровень безопасности для предотвращения взлома.

Биометрические данные, хранящиеся на сервере, должны быть зашифрованы, и алгоритм шифрования должен иметь высокий уровень безопасности для предотвращения взлома.

Биометрические данные, хранящиеся на сервере, должны представлять собой извлеченный биометрический признак и не допускать возможности восстановления до исходных данных.

Остальные детали системы обеспечения безопасности хранения данных должны соответствовать требованиям [ISO/IEC 24745].

9.4 Безопасность связи

До начала любого сеанса связи между клиентом и сервером должен быть установлен безопасный канал связи, например, для этих целей подходит протокол https.

При аутентификации должен быть обеспечен механизм безопасного обмена ключами между клиентом и сервером, например, в качестве механизма безопасного обмена ключами может использоваться SRP.

Необходимо предотвратить возможность перехвата ключа, используемого для согласования безопасного канала связи, например, для согласования безопасного канала без передачи ключа можно использовать SRP.

При передаче информация, например обработанные биометрические данные и результат решения, должна быть зашифрована, а ее целостность должна верифицироваться односторонней функцией, такой как хеш-функция или инфраструктура открытых ключей (PKI), которая запрещает любое изменение данных во время передачи.

Обработанные биометрические данные должны быть десенсибилизированы и зашифрованы для передачи, а ключи шифрования должны быть разными для разных клиентов; для расшифровки сервер использует соответствующий ключ дешифрования.

Остальные детали системы обеспечения безопасности связи должны соответствовать требованиям [ISO/IEC 24745].

9.5 Другие аспекты безопасности

Помимо безопасности хранения данных и связи необходимо учитывать множество других аспектов безопасности, таких как безопасность обработки данных, защита информации, позволяющей установить личность (PII), и т. п. Другие детали системы защиты биометрической информации должны соответствовать требованиям [ISO/IEC 24745].

Дополнение I

Примеры и сценарии использования

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

I.1 Изучение сценариев использования услуг мобильных платежей

Алиса – пользователь приложения "мобильный кошелек", предназначенного для мобильных платежей. Процедура выглядит следующим образом.

1) В первый раз Алиса входит в приложение "мобильный кошелек", используя свое имя пользователя и пароль. Она не хочет вводить пароль при каждом платеже, а также боится забыть его. Поэтому в этом приложении она нажимает кнопку "Регистрация для осуществления платежей с распознаванием лица".
2) Приложение "мобильный кошелек" предлагает Алисе открыть камеру и кивнуть.
3) От приложения "мобильный кошелек" Алиса получает уведомление: "Вы успешно зарегистрированы".
4) Алиса покупает чашку кофе в кофейне "Старбакс" и для оплаты использует приложение "мобильный кошелек". Алиса открывает это приложение и готовится заплатить. Мобильное приложение просит Алису открыть камеру и кивнуть. Алиса вполне довольна результатом.
5) Алиса получает от приложения "мобильный кошелек" уведомление: "Вы успешно совершили платеж, спасибо!"
6) Через некоторое время Алиса решает больше не использовать эту функцию и, нажав кнопку, аннулирует данный способ оплаты.

I.2 Изучение сценариев использования услуг электронной коммерции

Боб – владелец магазина одежды; он хочет открыть интернет-магазин на платформе электронной коммерции. Процедура выглядит следующим образом.

1) Сначала Боб регистрируется на платформе электронной коммерции и подает заявку на открытие нового магазина. Боб устанавливает свое имя пользователя и пароль на платформе электронной коммерции через приложение электронной коммерции на своем мобильном устройстве.
2) Приложение электронной коммерции на мобильном устройстве предлагает Бобу открыть камеру и выполнить на камеру несколько последовательных действий, например открыть рот, покачать головой, моргнуть глазами и кивнуть.
3) Боб получает от мобильного приложения электронной коммерции уведомление: "Вы успешно зарегистрированы".
4) Через некоторое время Боб хочет разместить некоторые предметы одежды из своего магазина. Платформа электронной коммерции предлагает Бобу открыть камеру и выполнить на камеру несколько последовательных действий, например покачать головой, моргнуть глазами, открыть рот и кивнуть.
5) Боб получает от платформы электронной коммерции уведомление: "Вы успешно вошли в систему".
6) Через некоторое время Боб решает больше не использовать эту функцию и, нажав кнопку, аннулирует данный вариант аутентификации.

Дополнение II

Безопасный удаленный пароль (SRP)

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

SRP – это протокол аутентификации и обмена ключами на основе пароля. Преимущество SRP заключается в том, что в процессе аутентификации ключ не передается открытым текстом, пользователям достаточно помнить пароль. К тому же на сервере хранятся не пароли пользователей, а связанная с ними информация, так что даже в случае взлома сервера злоумышленник не сможет подменить законного клиента (так как не может получить пароль).

Подробная информация о протоколе SRP приведена в [b-RFC 2945].

Протокол SRP может использоваться для установления безопасных каналов связи между клиентом и сервером в процессе биометрической регистрации, биометрической аутентификации и отмены биометрической регистрации. Протокол SRP также может использоваться для согласования защищенных соединений с предъявлением пароля пользователя, при этом исключаются традиционные проблемы безопасности, связанные с паролями многократного действия. Протокол SRP может использоваться и для выполнения безопасного обмена ключами в процессе аутентификации, позволяя обеспечить требуемые уровни безопасности (защиту конфиденциальности и/или целостности) во время сеанса.

Дополнение III

Примеры выполнения сервером функции ASD при распознавании лиц

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

Примерами выполнения сервером функции ASD при распознавании лиц являются, в частности, следующие процедуры.

1) Получив от сервера некоторые подсказки или инструкции, пользователь выполняет указанное действие, и сервер опознает это действие по изображению лица.
2) Сервер должен быть способен определять угол наклона лица относительно камеры и распознавать живого человека по изменению угла наклона лица.
3) Сервер должен быть способен обнаруживать непрерывность мимики лица и предотвращать воспроизведение слайдов и подмену человека.
4) Сервер должен быть способен обнаруживать воспроизведение видеозаписи мимики лица.
5) Сервер должен быть способен предотвращать атаки с использованием изображения лица.
6) Сервер должен быть способен обнаруживать использование трехмерных моделей лица, созданных с помощью компьютерной графики.

Библиография

[b-ITU-T M.3016.0] Рекомендация МСЭ-Т M.3016.0 (2005 г.*), Безопасность для плоскости административного управления: обзор.*

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.1081] Recommendation ITU-T X.1081 (2011), *The telebiometric multimodal model – A framework for the specification of security and safety aspects of telebiometrics*.

[b-ITU-T X.1085] Recommendation ITU-T X.1085 (2016) | ISO/IEC 17922:2017, *Information technology - Security techniques − Telebiometric authentication framework using biometric hardware security module*.

[b-ITU-T X.1089] Recommendation ITU-T X.1089 (2008), *Telebiometrics authentication infrastructure (TAI).*

[b-ITU-T X.1252] Рекомендация МСЭ-Т X.1252 (2010 г.), *Базовые термины и определения в области управления определением идентичности*.

[b-ITU-T X.1254] Рекомендация МСЭ-Т X.1254 (2012 г.), *Структура гарантии аутентификации объекта.*

[b-ISO 18461] ISO 18461:2016, *International museum statistics*

[b- ISO/IEC 19784-1] ISO/IEC 19784-1:2018, *Information technology –Biometric application programming interface – Part 1: BioAPI specification.*

[b-ISO/IEC 19792] ISO/IEC 19792:2009, *Security evaluation of biometrics.*

[b-ISO/IEC 19989] ISO/IEC 19989, *Evaluation of presentation attack detection for biometrics*.

[b-ISO/IEC 2382] ISO/IEC 2382:2015, *Information technology – Vocabulary.*

[b-ISO/IEC 2382-37] ISO/IEC 2382-37:2017, *Information technology – Vocabulary – Part 37: Biometrics.*

[b-ISO/IEC 24761] ISO/IEC 24761:2009, *Information technology – Security techniques – Authentication context for biometrics*.

[b-ISO/IEC 30107] ISO/IEC 30107:2017, *Information technology – Biometric presentation attack detection.*

[b-ISO/IEC 30125] ISO/IEC 30125:2016, *Biometrics – Biometrics used with mobile devices.*

[b-RFC 2945] RFC 2945, *The SRP Authentication and Key Exchange System.*

[b-Disappearing Cryptography] Disappearing Cryptography (Third Edition), 2009, Pages 355–364.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии,
Женева, 2021 г.