РУХАНИ ЖАҢҒЫРУ

20 АСТАНА

ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2018»
XIII Халықаралық ғылыми конференциясы

СБОРНИК МАТЕРИАЛОВ

XIII Международная научная конференция
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ - 2018»

The XIII International Scientific Conference
for Students and Young Scientists
«SCIENCE AND EDUCATION - 2018»

12th April 2018, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2018» атты XIII Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XIII Международной научной конференции студентов и молодых ученых «Наука и образование - 2018»

PROCEEDINGS of the XIII International Scientific Conference for students and young scholars «Science and education - 2018»

2018 жыл 12 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96

«Ғылым және білім – 2018» атты студенттер мен жас ғалымдардың XIII Халықаралық ғылыми конференциясы = XIII Международная научная конференция студентов и молодых ученых «Наука и образование - 2018» = The XIII International Scientific Conference for students and young scholars «Science and education - 2018». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2018. – 7513 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-997-6

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-997-6

©Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2018

Conclusion

Continuous monitoring of the network is necessary for the high-quality operation of digital terrestrial broadcasting equipment. This allows to identify the critical state of equipment and restore the normal operation of digital terrestrial broadcasting in time.

Literature

1. Serov A.V. Digital terrestrial television DVB-T / H. St. Petersburg, 2010.
2. Kris Knox. DVB-T2: A new standard of broadcasting for high-definition television // TV Satellite: a magazine. № 11, 2008, (157Nick Wells).
3. Al - Matari Yahya, Nikitin OR. Criteria and methods for assessing technical indicators of TV images. Methods and devices of information transmission and processing: Interuniversity collection of scientific works - Issue 4. / Ed. Romashova V.V., Bulkina V.V. – St. Petersburg: St. Petersburg Gidrometeoizdat, 2004. P. 249-255.
4. Afanasyev A., Eremenko D. SECAM, PAL, NTSC // Stereo & Video, 2000. - T. VII.- № 6. P. 16-26.
5. Belikova T.P., Kronrod M.A., Chochia P.A., Yaroslavsky L.P. Digital processing of Mars surface photographs transmitted by AMC "Mars-4" and "Mars-6" // Space researches. – 1975.– T. XIII. - Issue 6. P. 898-906.
6. Berson B. Digital receiver NOKIA MEDIA MASTER. – Telesputnik, No. 7, 1997.
7. Bryce R. Reference book on digital television. – Moscow: Publishing house "Era", 1998.
8. Bykov R. Ye., Gurevich S. B. Analysis and processing of color and volumetric images. - M .: Radio and Communication, 1984. – 248.
9. Valentin Tikhonov. Digital games in Australia / / Journal "625", №6,1999.
10. Vargauzin V.A. Principles of digital television standard ATSC // Tele satellite, 1999, №9, P. 53-58.
11. Vargauzin V.A., Artamonov A. Comparative characteristics of the European and
12. American standards for digital terrestrial television / / Television satellite, 1999, No.11, P.52-56.

УДК 004.934

АРХИТЕКТУРА ДЛЯ СИНХРОННОЙ МНОГОСТОРОННЕЙ АУТЕНТИФИКАЦИИ С ИСПОЛЬЗОВАНИЕМ БИОМЕТРИИ

Абдиманов Абзал Асырханович

Магистрант Евразийского национального университета им. Л.Н. Гумилева

Научный руководитель – Ш. Ж.Сеилов

В последнее время широко распространена дистанционная индивидуальная аутентификация на основе биометрии. Однако несколько существующих бизнес-систем и процессов часто требуют одновременного участия нескольких сторон в режиме реального времени. Кроме того, новые процессы электронного бизнеса могут быть реализованы технологией, которая позволяет нескольким участникам проходить аутентификацию синхронно. В этой статье рассмотрено различие между традиционными процессами документооборота, которые требуют многосторонней аутентификации от синхронной многосторонней аутентификации, необходимой в бизнес-сценариях и потребительских сценариях. Предложена новая система и метод многосторонней аутентификации и авторизации с использованием биометрии в реальном времени.

Растущая индивидуальная идентификация с использованием биометрии становится широко распространенной. Однако несколько существующих бизнес-систем и процессов требуют синхронного участия и аутентификации нескольких сторон в режиме реального

времени. Кроме того, новые бизнес-процессы могут быть задействованы технологией, которая позволяет нескольким участникам удаленно аутентифицировать себя синхронно. Существующим решениям до сих пор не удалось синхронно аутентифицировать и разрешить несколько сторон, использующих биометрические данные, особенно в сетевой среде. При плотном росте Интернета многие коммерческие приложения изучаются с дистанционным управлением и, возможно, без присмотра. Например, система электронной коммерции может использовать отпечаток клиента для проверки транзакции через Интернет, например, покупку авиабилета. Другие примеры удаленной биометрической аутентификации включают авторизацию транзакции на продажу на основе отпечатков пальцев.

В настоящее время описаны несколько иллюстративных сценариев аутентификации, когда несколько сторон должны быть аутентифицированы одновременно (синхронно) или когда один или несколько идентификаторов должны быть аутентифицированы в течение определенного периода времени (постоянная синхронизация). Сценарии аутентификации включают (а) хранилище в банке, которое может быть открыто только двумя сотрудниками банка, где каждый сотрудник имеет отдельный ключ; (б) шкафчик или сейф в хранилище, который открывается в процессе работы сотрудника банка, открывающего хранилище ключом (или двумя сотрудниками с двумя отдельными ключами), и владелец сейфа, открывающий свою коробку с ключом в сочетании с ключом, используемым сотрудником банка; и (с) нотариус, свидетельствующий о выполнении документа путем проверки личности подписывающего лица с помощью обычных средств и аутентификации документа путем подписания нотариального штампа. Существуют и другие подобные приложения в военной и других подобных областях, где для совершения транзакции требуется несколько полномочий, например, выпуск оружия.

Если какая-либо транзакция выполняется во время многостороннего собрания (например, если участники голосуют по важному решению), и подлинность транзакции должна быть позже доказана, как правило, недостаточно аутентифицировать участников в начале собрания. Вместо этого может потребоваться доказать, что все стороны одновременно участвовали в транзакции. Эту проблему можно назвать одной из проблем синхронной биометрической аутентификации. Кроме того, когда транзакция охватывает значительную часть времени, часто необходимо доказать, что стороны не отсутствовали во время какой-либо части транзакции (например, никогда не покидали собрание). Эта проблема может упоминаться как одна из постоянных проблем биометрических аутентификаций.

Архитектура предлагаемой многосторонней системы аутентификации

На Рисунке 1 представлена схема архитектуры высокого уровня многосторонней системы аутентификации, в которой каждая сторона (например, инициирующая сторона, сторона 1, сторона 2, ..., сторона K) аутентифицируется на одном из многих серверов аутентификации, как сервер Synchronicity и Persistence Validation (SPV). Сервер SPV может считаться многокомпонентным сервером управления транзакциями. Сеть может быть общедоступной сетью, такой как Интернет, или может быть частной сетью. Двунаправленное подключение к сети - это несколько клиентских компьютерных устройств, таких как рабочая станция или ПК или карманное устройство, которое имеет пользовательский интерфейс, через который пользователь может взаимодействовать с другими устройствами в сети. Помимо традиционного пользовательского интерфейса имеются другие устройства ввода для получения биометрических сигналов. Полученные биометрические сигналы обрабатываются, например, путем сжатия, улучшения и/или анализа посредством подсистемы проверки подлинности (VCS). Биометрические сигналы, такие как те, которые представляют один или несколько отпечатков пальцев, голосовые отпечатки и/или изображения сетчатки, могут быть аутентифицированы через серверы аутентификации, которые являются компонентами серверов SPV. В системе на рисунке 1 могут использоваться несколько серверов аутентификации/пары баз данных. В этом случае

для идентификатора пользователя каждой стороны известно не только идентификатор пользователя, но и идентификатор для связанного с ним сервера аутентификации. Шаблоны биометрии, база данных и другие связанные компоненты могут составлять часть компонента биометрического процессора на сервере SPV.

Устройства ввода могут быть реализованы с использованием устройств захвата видео, например цифровые камеры. Они генерируют изображения части каждого пользователя на каждом устройстве ввода-вывода клиента, такие как изображение отпечатка пальца, изображение лица пользователя, изображение радужной оболочки пользователя или сетчатку или любую другую часть пользователя, которая подходит для использования при генерировании входных данных биометрии. Данные изображения могут передаваться как, например, 30 кадров в секунду (или меньше) видеоданных или при скорости супер-видео (более 30 кадров в секунду), или могут быть сжаты, например, с использованием методов MPEG. Использование сжатого изображения также полезно для скрытия ответов клиентов на вызовы, выпущенные сервером SPV.

По крайней мере один из серверов SPV подключен к сети и взаимодействует с различными клиентами через их соответствующие VCS. Биометрия, работающая в реальном времени, рассматривается здесь как включающая первые сертификаты, свидетельствующие об одновременном приобретении биометрических сигналов от нескольких сторон, а также вторых сертификатов, которые доказывают, что стороны непрерывно подавали сигналы биометрии в течение определенного интервала времени. Таким образом, бизнес-процессы, основанные на этой технологии, покрываются предлагаемой архитектурой.

Компоненты сервера проверки синхронности и стойкости

Сервер многостороней синхронизации: Пользователь (например, инициатор) инициирует синхронную многостороннюю транзакцию на клиенте. Клиент связывается с назначенным сервером SPV для транзакции.

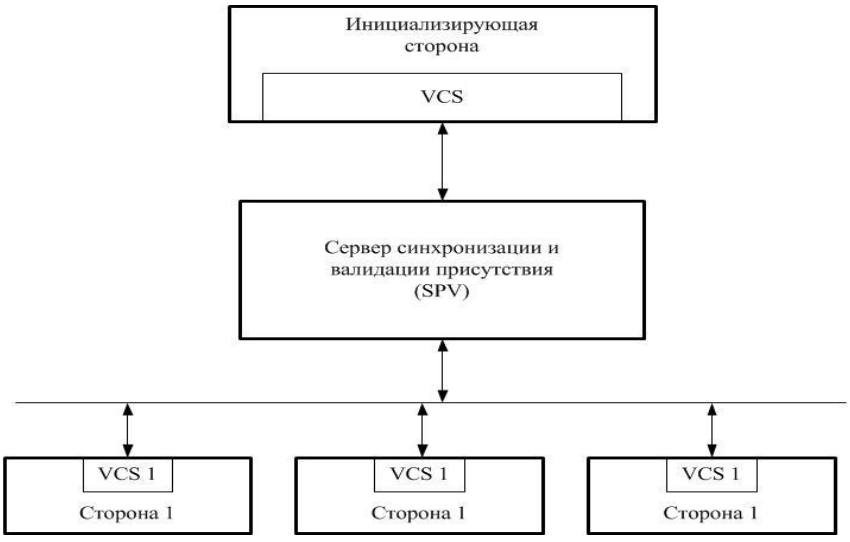

Рисунок 1 - Предлагаемая архитектура многосторонней системы аутентификации

Сервер SPV, основанный на политике, определенной для типа транзакции, поддерживаемой координатором политики, связывается с другими сторонами (например, Стороной 1, Стороной 2, ..., Стороной K), определенной политикой. Затем сервер SPV просит стороны предоставить свои биометрические сигналы, а также создает общие данные для всех вовлеченных сторон. На следующем шаге клиенты, получающие вызов, добавляют свой ответ на поток биометрических данных. В настоящей системе данные ответа клиента вставляются стеганографически в сжатый видеопоток. SPV-сервер отделяет сигналы биометрии и ответ от каждого из клиентов и передает ответ координатору синхронизации и

передает сигналы биометрии на сервер или верификатор биометрических данных. Временная метка клиентов и SPV-сервера является одним из примеров ответа на вызов, инициированный сервером SPV. Ответы, полученные от клиентов, используются для определения того, является ли получение сигнала биометрического сигнала синхронным, и сохраняются ли сигналы биометрии в течение, по меньшей мере, продолжительности времени, указанного политикой. Сервер SPV, основанный на результатах обработки валидатором ответа, координатором синхронизации и верификатором биометрии, затем удостоверяет (при необходимости) завершение многосторонней авторизации, запрошенную инициатором на клиенте.

Координатор синхронизации: синхронность реализуется и гарантируется с помощью протокола, управляемого сервером SPV. Время для проверки синхронности измеряется с помощью достаточно точных часов и не требует знания абсолютного времени, например, универсального скоординированного времени (UTC); сервер Trusted Time Server, настроенный на UTC, может быть использован для подтверждения того, что транзакция не только синхронно произошла между несколькими сторонами, но и транзакция также произошла в определенный абсолютный момент времени. Сервер Trusted Time Server может стать частью Координатора по синхронизации, или это может быть услуга третьей стороны.

Координатор политики: координатор политики содержит параметры политики, такие как задержка синхронизации, время сохранения, требуемый уровень безопасности, количество сторон, подлежащих аутентификации, и т.д.

В этой статье описывается новая система и метод многопартийной аутентификации. Процесс многопартийной аутентификации использует синхронные и постоянные сигналы биометрии, полученные от сторон транзакции на основе политики, для утверждения запроса транзакции. Сигналы биометрии предпочтительно выражаются в виде сжатых видеосигналов, имеющих статистически вставленные данные ответа на вызов.

Список использованных источников

1. Adolphs, R., D. Tranel, H. Damsio, and A.R. Damasio. Impaired recognition of emotion in facial expressions following bilateral damage to the human amygdala., 2014 // 440-450 с.

2. S. Narayanan. 2004. Analysis of emotion recognition using facial expressions, speech and multimodal information.,2008 // 331-338 с.

3. Ekman, P., W.V. Friesen, V. Wallace, and P. Ellsworth. Emotion in the human face: Guidelines for research and an integration of fi ndings. Oxford: Pergamon, 1998 // 201-218 с.

УДК 004.934

ВОЗМОЖНОСТИ БИОМЕТРИИ ДЛЯ АУТЕНТИФИКАЦИИ В БЕСПРОВОДНЫХ УСТРОЙСТВАХ

Абдиманов Абзал Асырханович
Магистрант Евразийского национального университета им. Л.Н. Гумилева
Научный руководитель – Ш. Сеилов

Надежная аутентификация личностей становится важной проблемой в контекстах электронного голосования, мобильной коммерции, контроля доступа и контроля пользовательского интерфейса. Традиционные системы аутентификации, например на основе PIN кода или пароля, имеют проблемы, связанные с безопасностью. Биометрические системы аутентификации используют физиологические и поведенческие черты человека, которые способны отличить авторизованного человека от мошенника. В этой статье рассмотрены биометрические технологий и ограничения беспроводных устройств, которые определяют осуществимость и производительность системы аутентификации. Даны короткие оценки самых распространенных биометрических систем.