

ПЕРСПЕКТИВНЫЕ ОБЛАСТИ ПРИМЕНЕНИЯ ИДЕНТИФИКАЦИИ

*Софийский Алексей Владимирович
ведущий системный архитектор, компания ЦРТ*

Задачи идентификации (определения) личности нам приходится решать на каждом шагу. Мы даже не всегда обращаем внимание на то, что проходим или проводим эту проверку. А ведь когда мы открываем ключом замок в квартиру, осуществляем авторизацию на компьютере или принимаем вызов по телефону – мы каждый раз сталкиваемся с идентификацией. Данная процедура осуществляется с целью контроля и управления различными ресурсами: доступом к информации или денежным счетам, управлением устройствами, доступом к рабочим помещениям. Развитие новых сервисов и систем, требующих обеспечения безопасности доступа к их ресурсам, приводит к необходимости разработки новых методов и подходов к идентификации пользователей этих сервисов и систем. Давайте рассмотрим наиболее актуальные направления развития систем идентификации.

СПОРТИВНЫЕ И КУЛЬТУРНЫЕ МЕРОПРИЯТИЯ

Спортивные хулиганы, особенно футбольные, на протяжении долгого времени являются головной болью для организаторов спортивных мероприятий и владельцев стадионов. Многие крупные мероприятия не обходятся без актов вандализма, а порой и погромов на спортивных аренах и стадионах. Помимо непосредственного материального ущерба организаторам мероприятий грозят чувствительные штрафы со стороны международных регулирующих организаций. Основным методом борьбы для владельцев спортивных объектов является недопущение хулиганов на свою территорию, т. е. фактически стандартная задача ограничения доступа по «черному списку».

В 2005 году государство ввело необходимую нормативную базу, ограничивающую возможность посещения спортивных объектов лицами, в отношении которых будет вынесено соответствующее постановление суда. Ведение списков хулиганов, чье присутствие на территории спортивных объектов запрещено судом, для футбольных стадионов осуществляется централизованно РФПЛ – в соответствии с постановлениями УЕФА. Эта же

организация поставила перед собой задачу определения наиболее подходящей технологии выявления хулиганов при попытке пройти через входные турникеты. В партнерстве с несколькими компаниями была выработана технология идентификации болельщиков на основе метода биометрического распознавания лица человека. Внедрение данной технологии на стадионе Петровский позволило отработать все этапы контроля доступа. В настоящий момент внедрение технологии биометрической идентификации болельщиков планируется осуществить на всех крупных стадионах ко времени проведения Чемпионата мира по футболу 2018 года.

Аналогичный подход может применяться при проведении различных мероприятий, где требуется предварительная аккредитация. К таким мероприятиям можно отнести также проведение кинофестивалей, деловых форумов и любых иных мероприятий, подразумевающих частичную или полную аккредитацию посетителей. Аккредитация позволяет сформировать некоторый «белый список», по которому в дальнейшем будет осуществляться допуск. Упомянутый выше метод идентификации по изображению лица позволяет проводить в автоматизированном режиме проверку листа аккредитации, осуществляя, например, выявление «акционистов» (хулиганов, способных осуществить провокацию), при попытке выдать себя за журналистов. Тот же метод применяется при регистрации участников непосредственно на мероприятии – для проверки права присутствия в соответствии с «белым списком». Данный подход к идентификации посетителей на мероприятиях с ограниченным доступом стал встречаться несколько чаще, например, применялся в рамках проведения мероприятий на Петербургском международном экономическом форуме в 2016 году.

ИНТЕРНЕТ ВЕЩЕЙ И УМНЫЙ ДОМ

Современные концепции развития технологий описывают появление в ближайшем будущем «интернета вещей». Эта концепция подразумевает появление локальных и глобальных сетей передачи данных, используемых множеством устройств для технического вза-

имодействия между собой. Межмашинное взаимодействие позволит человеку автоматизировать множество процессов, занимающих его время. В то же время, увеличение уровня информационного взаимодействия устройств, автоматизации получения информации и принятия решений ведет к увеличению требований к аутентификации владельца.

Одну из областей применения интернета вещей описывает концепция «умный дом». Умный дом – это высокотехнологичная система, позволяющая объединить все коммуникации в одну и поставить ее под управление искусственного интеллекта, программируемого и настраиваемого под все потребности и пожелания хозяина. «Умный дом» послужит вам, если вы хотите, чтобы по вечерам в гостиной зажегся верхний свет, а днем горела только настольная лампа в кабинете, чтобы вы смогли зимой греть ноги в кресле на кухне, а по осени не мерзнуть в спальне, чтобы иметь возможность включить через интернет обогреватель на даче и помещение прогреется к вашему приезду. А вот при использовании биометрии «умный дом» может сделать ваше жилище не только более удобным, но и гораздо более безопасным: за сохранность имущества и конфиденциальных данных можно будет больше не беспокоиться, потому что их будут защищать ваши физические характеристики: голос, лицо, отпечатки пальцев, рисунок сетчатки – все, что нельзя ни подделать, ни украсть. На сегодняшний день наибольшее распространение получили биометрические замки: с их помощью контролируется доступ в дома, квартиры, хранилища, сейфы и прочие помещения, которые нужно дополнительно защищать от проникновения.

ПЛАТЕЖНЫЕ СИСТЕМЫ И БАНКОВСКОЕ ОБСЛУЖИВАНИЕ

Наверное, наиболее заинтересованным в идентификации пользователей участником рынка является банковский сектор. Практически ни одна сторона банковского обслуживания не обходится без идентификации пользователя. Давайте рассмотрим некоторые из них.

Важной составляющей современной жизни является возможность моментальной оплаты товаров и услуг в любое время и из любого места. Для того чтобы получить доступ к своему банковскому счету и провести платеж через одну из платежных систем в настоящее время необходимо использовать данные своей банковской карточки, указав данные вручную или считав их специальным устройством, и пройти парольную идентификацию, и пройти альтернативу многие банки начинают предлагать использование биометрических данных для получения возможности управления счетом.

Уже сейчас можно встретить реализацию биометрической идентификации для этой цели. В настоящий момент Сбербанк в пилотном режиме внедрил проект доступа к электронному кошельку для учащихся школ. Списание средств производится после прохождения идентификации школьника по изображению венозного русла, при этом деньги со счета можно потратить только в столовой учебного заведения. Данное решение позволяет обеспечить доступ к электронному кошельку вне зависимости от наличия каких-либо идентификаторов (карт и паролей), обеспечить целевое расходование средств и мониторинг времени и факта приобретения обеда со стороны родителей. Та же технология получила распространение в Японии для получения доступа к счету клиентов банка в банкоматах. Другим знаковым пилотным проектом стал проект по интеграции сканера отпечатков пальцев в POS-терминал для оплаты покупок в одном из магазинов «Азбуки Вкуса». В то же время необходимо отметить некоторую настороженность пользователей систем биометрии, связанную с особенностями их применения – отпечатки пальцев являются контактным методом и ассоциируются у многих с правоохранительными органами, а устройства считывания изображения венозного русла используют дополнительную подсветку в ближнем ИК спектре.

Нередки случаи, когда при проведении подозрительных по мнению банка операций, например, снятии денежных средств за границей, операции по банковской карте блокируются. Чтобы разблокировать счет, необходимо позвонить в банк и пройти парольную авторизацию. Данный метод разблокировки содержит ряд неудобств, прежде всего связанных с использованием контрольного слова, которое большинство пользователей используют крайне редко. Дополнительным минусом данного метода является возможность ложной верификации в случае предварительного сбора информации о клиенте со стороны мошенников. Некоторые банки рассматривают возможность проведения биометрической идентификации по голосу при обращении на горячую линию, что позволит нивелировать оба недостатка. При этом идентификация по голосу может являться не только заменой парольной верификации, но и дополнительным фактором проверки. В случае же, если регламенты банка не подразумевают возможности разблокировки через звонок на горячую линию, то возможна видеоидентификация пользователя через специальные приложения. Это позволяет оператору помимо верификации данных пользователя провести сравнение образов голоса и изображения лица человека.

Не менее важной задачей является обеспечение безопасности оплаты това-

ров и услуг с помощью банковских карт. Одной из ключевых технологий, используемых для обеспечения безопасности платежей через интернет-банкинг, является технология 3D Secure. Протокол 3D Secure добавляет дополнительный шаг авторизации – пароль, предоставляемый банком-эмитентом карты. В то же время национальный институт стандартизации США (NIST) не рекомендует для задач авторизации в будущем использовать пароли, рассылаемые сетями операторов связи через SMS, для задач аутентификации, в связи с возможностью их дискредитации. Одним из вариантов дополнительного идентификатора для обеспечения банковских платежей может быть формируемый биометрический шаблон. Крупнейшие платежные сервисы – в том числе Visa и Mastercard – заявляют о применении различных стандартов биометрической аутентификации для обеспечения доступа к биометрическим сервисам финансовых услуг.

Несмотря на несомненный интерес финансового сектора к биометрическим методам идентификации на пути их широкого внедрения существует ряд серьезных препятствий. Одним из них является сложность формирования баз данных биометрических признаков, разработки единых протоколов биометрической идентификации и стандартизации в этой области. Внедрения в России в первую очередь несут локальный характер в рамках партнерских инициатив игроков финансового сектора и технологических лидеров в области биометрических технологий. Для дальнейшего развития и внедрения биометрических технологий в финансовом секторе необходима выработка единого подхода к процедурам биометрической идентификации и аутентификации.

НАЦИОНАЛЬНАЯ БИОМЕТРИЧЕСКАЯ ПЛАТФОРМА. ГОСУДАРСТВЕННЫЕ СЕРВИСЫ, ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Вопросы разработки единых технологических подходов в настоящий момент реализуются различными государственными и межгосударственными институтами. Данный уровень позволяет обеспечить как научно-технологическую поддержку этой инициативы, так и нормативное обеспечение. Одновременно с этим работа с задачами идентификации и верификации пользователей на государственном уровне позволяет проводить всесторонний анализ предлагаемых решений, привлекая необходимых экспертов. Наиболее известной инициативой в данной области является индийская программа Aadhaar.

В январе 2009 года правительством Индии было учреждено государственное агентство UIDAI, целью которого яв-

ляется создание национального идентификационного проекта – выдача каждому жителю Индии 12-значного идентификационного номера (Aadhaar), привязанного к его персональным и биометрическим данным (фотография, десять отпечатков пальцев, изображения радужной оболочки обоих глаз). Хранение данных производится централизованно. По имеющимся данным в настоящий момент Aadhaar выданы около 850 млн жителям Индии. С марта 2015 года был запущен облачный сервис хранения документов пользователей для предоставления государственным служащим по номеру Aadhaar.

С марта 2015 года в рамках пилотного проекта при поддержке Департамента электроники и информационных технологий ведется продажа SIM-карт с привязкой к Aadhaar. Данная работа ведется в рамках программы Digital India – программы предоставления государственных услуг гражданам через интернет-инфраструктуру. Программа запущена в 2015 году. NPCI (Национальная платежная корпорация Индии) по инициативе Резервного банка Индии разработала и опубликовала API унифицированного платежного интерфейса, предполагающего проведение платежей после двухфакторной аутентификации по данным Aadhaar. Данная инициатива предназначена для стимулирования страны к переходу к электронным транзакциям с помощью смартфона и биометрической технологии. К настоящему моменту платежный сервис Paytm получил лицензию и начал работать с использованием указанного API.

Это лишь часть наиболее знаковых шагов по развитию биометрических систем идентификации в рамках указанной

программы. Благодаря этим инициативам множество коммерческих компаний из разных стран развивают и проводят внедрение своих систем для нужд целевых государственных и коммерческих программ Республики Индия.

Другой крупнейшей программой по идентификации является международная программа ID4Africa. Реализация программы ID4Africa, объединяющей 26 стран Африки, посвящена разработке универсальной ID-карты граждан для проведения процедуры online и offline идентификации с целью повышения эффективности программ социального обеспечения, сбора налогов и контроля пересечения границ, а также выявления мошенничества в этих сферах. Также программа призвана в будущем обеспечить прозрачность банковских услуг и мобильных платежей. Данная программа реализуется в рамках плана ООН по устойчивому развитию на Африканском континенте к 2030 году. Данный подход обеспечивает возможность применения единых стандартов и правил идентификации на международном уровне.

В настоящий момент Российская Федерация не принимает участия в подобных международных инициативах. В то же время стоит обратить внимание на активность Минкомсвязи по разработке концепций и планов в этой области. В системном проекте электронного правительства до 2020 года, подготовленном Минкомсвязи, предусмотрено развитие биометрических технологий для идентификации граждан. Задача создания единой базы биометрических данных граждан элегантно решается путем расширения функционала уже работающей Единой системы иденти-

фикации и аутентификации. Это позволяет решить задачи обеспечения инженерной инфраструктуры, логической проработки системы, обеспечения информационной безопасности с наименьшими затратами, используя существующий задел системы. В перспективе многофакторная аутентификация ЕСИА позволит значительно облегчить процедуры по оказанию различных сервисов компаниям и населению. В настоящее же время проводится оценка реальных возможностей технологий, анализ бизнес-процессов, выработка норм и правил. Надеюсь, в ближайшее время у нас появится возможность оценить результаты этого труда, попробовав на практике испытать преимущества биометрии.

Что же касается наиболее нестандартных вариантов применения биометрических технологий, то это может быть идентификация для неграмотных людей. Например, в рамках специальной программы, известной под названием «финансовое включение», технологическая компания NCR выпустила банкоматы для неграмотных, которые считывают не цифровые, а биометрические данные. Таким образом, ими могут пользоваться даже те обитатели развивающихся государств, которые не знают цифр и не могут читать.

Также биометрию можно использовать в детских игрушках. Игрушка может узнавать ребенка, его родителей и друзей, вести с ним интерактивный диалог с учетом контекста присутствия его или других персон, которых она «знает».

И последний пример, который я приведу, – использование биометрии для подсчета статистики: учета посещаемости школ, подсчетов при голосовании и так далее.



■ Линейка периферийных модулей Fastwel, выполненных в стандарте PCI-S.03U, пополнилась модулем аудио/видео захвата VIM554. Данный модуль предназначен для приема аналоговых видеосигналов стандартного разрешения (SDTV) и речевых аудиосигналов, преобразования их в цифровую форму и ввода в системную память компьютера. Модуль использует скоростной интерфейс ввода/вывода (PCI Express x4) и рассчитан на применение в системах PCI-S.03U совместно с вычислительными модулями Fastwel различных архитектур. Поставляется как с обычным ребристым радиатором, так и в кондуктивном исполнении. Рабочие температуры от -40 до +85°С. VIM554 обеспечивает программную совместимость с ОС Windows Embedded Standard 7, 32/64 разряда, а также Linux 3.2.0.

■ В ассортименте компании Hanwha Techwin появились мониторы

Samsung SMT-4933. Экономичная LED-подсветка 49» экрана, разрешение 4K Ultra HD, HDMI-интерфейсы. При эксплуатации в режиме 24/7 новинка проработает не менее 50000 часов. Широкие углы обзора – 178° по горизонтали и по вертикали, время отклика пикселя 8 мс, контрастность 4700:1, яркость 500 кд/м².

■ Теперь в портфеле решений Office Anatomy доступно оборудование компании Ruckus, которая является лидером на рынке решений для инфраструктуры мобильного интернета и беспроводных корпоративных систем WLAN. Специалисты Office Anatomy прошли обучение в Ruckus Wireless, подтвердив свою квалификацию для работы с оборудованием данного поставщика.

■ Компания Lantech выпустила коммутаторы IPGS-3204MGSFP уровня 2+. 4 порта 10/100/1000T для периферии и 2 слота SFP для передачи данных по волоконно-оптическим линиям связи. Модификации с блоком питания на 12 или 48 В, полоса пропускания 18 Гбит/с, организация высокоскоростной отказоустойчивой сети. LED-индикаторы состояния портов, все современные сетевые протоколы, поддерживается система обнаружения и устранения возможных сбоев и неисправностей, а также основные инструменты управления, включая SNMP, Telnet и CLI. IPGS-3204MGSFP совмещены с PoE-инжекторами.

■ Линейку AHD-видеорегистраторов DIVITEC пополнили модели DT-iDVR04400 и DT-iDVR08400, на 4 и 8 каналов соответственно. Запись с разрешением AHD-N (1080N)/AHD-M при скорости 25 к/с. Отображение в Full HD 1080p. 2 видеовыхода. Жесткий диск SATA 3,5” (до 6 Тб). Обе модели на базе ОС Linux, кодек H.264. Поддержка работы в «облачном» сервисе.