Р.В. Ермошин, М.В. Кузнецов

КОМБИНИРОВАННЫЙ МЕТОД АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ НА ОСНОВЕ КЛАВИАТУРНОГО ПОЧЕРКА

(Поволжский государственный университет
телекоммуникаций и информатики)

В настоящее время большую важность имеет проблема защиты информации и разграничение доступа к ней, а так же доступ к управлению информационных систем и их ресурсам.

Данная задача в наши дни решается несколькими методами аутентификации:

1. Парольный метод – используется уникальное знание (пароль, пин-код);
2. Атрибутный – используется уникальный предмет (ключ, смарт-карта);
3. Биометрические – используется уникальная характеристика пользователя (отпечатки пальцев, сетчатка глаза, голос, почерк).

Парольный и атрибутный методы имеют некоторые недостатки, главным из них является факт того, что имеется возможность обмана/взлома системы, кражи ключа, имитации уникального предмета, поэтому стремительно развиваются новые идеи по управлению доступом.

Методы аутентификации по биометрическим параметрам личности, ввиду неотъемлемости биометрических характеристик конкретного человека, способны обеспечить повышенную точность. К таким характеристикам относится и клавиатурный почерк.

При работе с клавиатурой потенциально могут быть задействованы сто сорок мышц, исходя из предположения, что наибольшее влияние оказывают около 20% от общего числа мышц, получим число равно 28, то есть примерно 28-мерную задачу управления. Задача большой размерности позволяет сделать предположение об уникальности клавиатурного почерка пользователя.

Клавиатурный почерк – поведенческая биометрическая характеристика, описываемая несколькими параметрами, такими как:

1. Скорость ввода – количество введенных символов, деленое на время печати;
2. Динамика ввода – время между нажатиями клавиш и время их удержания;
3. Частота возникновения ошибок при вводе и их род;
4. Использование функциональных клавиш;
5. Сила нажатия на клавиши.

Идентификация пользователя по клавиатурному почерку может осуществляться как по набору парольной фразы, так и по набору произвольного текста. Оба способа включают в себя 2 этапа – обучение и анализ/идентификация.

На этапе обучения пользователю нужно некоторое число раз ввести предлагаемые ему тестовые фразы, при этом рассчитываются его биометрические характеристики, и создается эталон. На этапе идентификации рассчитанные оценки сравниваются с эталонными, на их основании делается вывод о подлинности пользователя. Предлагаемые тестовые фразы следует выбирать таким образом, чтобы используемые в них символы равномерно располагались на рабочем поле клавиатуры.

Характерной особенностью аутентификации пользователя по клавиатурному почерку при вводе логина или пароля является краткость вводимой фразы, что упрощает работу при анализе вводимых данных, так как не приходится проверять такие данные, как частота возникновения ошибок и использованные клавиши, потому как логин или пароль – это заранее известная фраза. Еще одной не менее важной характеристикой при анализе ввода текста является число перекрытий между клавишами, т.е. нажатие на клавишу в то время, когда нажата другая.

Эталонные характеристики пользователя, полученные на этапе обучения системы, позволяют сделать выводы о степени стабильности клавиатурного почерка пользователя и определить доверительный интервал разброса для последующей идентификации пользователя. Во избежание дискредитации работы системы можно отсеивать пользователей, клавиатурный почерк которых не обладает необходимой стабильностью.

Таблица 1.Характеристики стабильности клавиатурного почерка пользователей

Ошибки, %	Аритмичность, %	Скорость, зн./мин.	Характеристика перекрытий	
			Число перекрытий, %	Используемое число пальцев
Менее 2	Менее 10	Более 200	Более 50	Все
Менее 4	Менее 15	Более 150	Более 30	Большинство
Менее 8	Менее 20	Более 100	Более 10	Несколько
Более 8	Более 20	Менее 100	Менее 10	По одному

Следует так же отметить, что не рекомендуется брать ключевые фразы длиннее 10 слов. Это объясняется тем, что короткие фразы пользователь вводит на подсознательном уровне. Подсознательные движения стабильны до тех пор, пока в них не вмешивается более высокий уровень мышления.

Надо сказать, что после продолжительного времени работы с такой системой система управления доступом должна вносить изменения в эталонные характеристики, поскольку клавиатурный почерк со временем имеет свойство меняться, особенно когда логин или пароль начинают вводиться на подсознательном уровне. Или же можно заставить систему раз от раза работать как в режиме настройки, так и в режиме анализа, т.е. при входе в систему пользователь вводит ключевую фразу, отклоняясь от эталона на допустимое значение,

происходит анализ биометрических характеристик и тут же корректировка эталона.

Недостаток такой системы анализа клавиатурного почерка заключается в том, что если пользователь находится в возбужденном состоянии, под воздействием психотропных препаратов, алкогольного опьянения или просто болен, то стабильность параметров работы нарушается, и процесс сквозной аутентификации может стать серьезной проблемой.

Таким образом, для повышения достоверности аутентификации пользователя не только при входе в систему, а так же в процессе работы, необходимо использовать комбинированный метод, сочетающий в себе стандартные процедуры ввода паролей на начальном этапе и анализа характерного поведения зарегистрированного пользователя на всём протяжении работы в защищённой системе.

И.Н. Ефимов, А.М. Косолапов

КЛАССИФИКАЦИЯ СПОСОБОВ ПОДТВЕРЖДЕНИЯ ПОДЛИННОСТИ РАСПОЗНАВАЕМОГО ОБЪЕКТА[2]

(Самарский государственный университет путей сообщения)

Системы автоматического распознавания лиц находят все большее применение в биометрических системах безопасности, контроля и управления доступом пользователей. Однако нельзя доверять системам, не использующим защиту от спуфинг (spoofing) атак. Для биометрических систем спуфинг — это обман путём предоставления биометрическому сенсору копий, муляжей, фотографий, видеозаписи, заранее записанных звуков и т. п. Цель атаки спуфинга при распознавании — представление незарегистрированного пользователя в системе как зарегистрированного. В [9] авторы продемонстрировали, успешный взлом коммерческих систем распознавания лиц, используя фотографию или видеозапись зарегистрированного пользователя с экрана устройства. Защита от спуфинг атак является трудоёмкой задачей, так как злоумышленник имеет непосредственный контакт с видеокамерой, поэтому невозможно использовать различные криптографические методы защиты. Наилучшие результаты, по данным разработчиков, продемонстрировали системы использующие специализированные сканеры или видеокамеры, позволяющие реконструировать 3D объект. Тем не менее, способы подтверждения подлинности объекта, не использующие специализированное оборудование и не требующие дополнительных действий, наиболее перспективны, т.к. удобнее для конечного пользователя и могут быть легко интегрированы в существующие системы распознавания лиц.

[2] Работа поддержана грантом фонда содействия развитию малых форм предприятий («У.М.Н.И.К.» I полугодие, Самара, 2014).

В работе предложена новая классификация известных способов подтверждения подлинности распознаваемого объекта в зависимости от реализации. Существующие классификации не отражают все многообразие известных способов подтверждения подлинности распознаваемого объекта (СППРО) и нуждаются в пересмотре и дополнении. СППРО разделяются в зависимости от вида воздействия на распознаваемый объект: способы с физическим воздействием (СФВ), с командным (СКВ) и без воздействия (СБВ). Оригинальная классификация СППРО представлена на рисунке 1.

Для функционирования способов, основанных на командном воздействии, пользователю необходимо произвести некоторые действия в указанный системой защиты момент: произнести сгенерированный случайный текст, моргнуть или открыть рот, продемонстрировать различные эмоции и т.д. Способы с физическим воздействием можно условно разделить на:

- способы, применяющие ИК излучение (ИКИ), с последующим анализом следующих характеристик: оптических свойств (ОС) человеческой кожи и зрачков, рельефной структуры (РС) объекта и т.д.;
- способы, применяющие видимый спектр света (ВСС), с последующим анализом следующих характеристик: оптических свойств (ОС) человеческой кожи, реакции зрачков (РЗ), рельефной структуры (РС) объекта и т.д.

Способы без воздействия на объект разделяют на:

- способы, анализирующие текстурные признаки (АТП): локальные бинарные шаблоны (ЛБШ), гистограммы ориентированных градиентов и т.д.;
- способы, использующие построение 3D модели объекта с помощью: карт глубин, аффинного преобразования, сканера или видеокамер и т.д.;
- способы, использующие обнаруженные биофизические признаки (ОБП): движение глаз, моргание, мимика, движение головы относительно фона, кровеносные сосуды, термограмма и т.д.

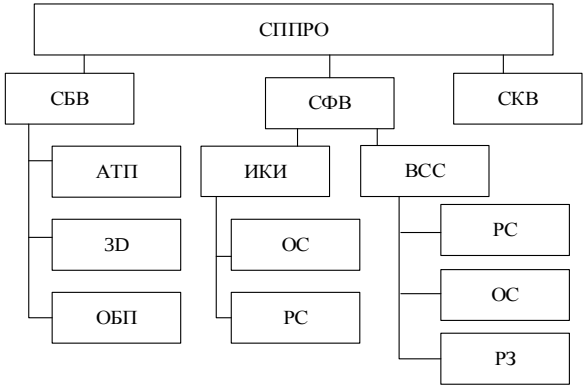

Рисунок 1 – Классификация СППРО

Ниже представлены различные примеры СППРО, не использующие воздействие на распознаваемый объект. Существует целый ряд работ, в которых