- VQ2 – приёмник;
- У – усилитель;
- ФНЧ – фильтр нижних частот;
- АЦП – аналогово-цифровой преобразователь;
- ЗУ – запоминающее устройство;
- ПК – персональный компьютер с оригинальным программным обеспечение;
- USB – интерфейс USB.

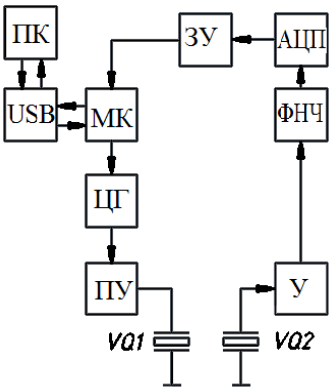

Рис. 2. Структурная схема системы контроля сварных соединений основанной на методе TOFD

Данная структура системы ультразвукового дефектоскопа отличается наличием прецизионного цифрового генератора для возбуждения колебаний в излучателе, что необходимо для корректного применения фазового метода обработки сигналов. Кроме того это позволяет реализовать прецизионный многошкальный фазовый метод измерения времени задержки сигналов. Последний основан на определении задержки в соответствии с выражением $\tau=(2\pi\nu+\varphi)/\omega$, где n – количество целых фазовых циклов, φ – фазовый сдвиг сигналов в интервале $(0, 2\pi)$, ω – круговая частота гармонической несущей.

Проведенное моделирование процесса обработки сигналов УЗД подтвердило возможность их обнаружения на фоне аддитивных шумов для соотношения сигнал/шум меньше единицы. Показано, что повышение точности определения временного положения импульсов может быть достигнуто путем увеличения получаемой измерительной информации за счет увеличения частоты дискретизации сигналов в АЦП, либо применением специальных методов определения энергетических центров импульсов.

Использование методов статистической фазометрии для обработки сигналов в методе TOFD позволяет расширить функциональные возможности и область применения последнего, а также уменьшить погрешность определения временных задержек сигналов и за счет этого повысить достоверность контроля размеров дефектов.

1. R. Halmshaw. Introduction to the Non-Destructive Testing of Welded Joints. – Printed by Lightning source, Milton Keynes, England. – 2006. – 84 с.
2. Ультразвуковой дифракционно-временной метод контроля (TOFD) стыковых сварных соединений труб из полиэтилена высокой плотности (ПЭВП) [электронный ресурс]. -Режим доступа: https://www.olympus-ims.com/ru/applications/ultrasonic-tofd-butt-fusion/
3. An overview TOFD method and its Mathematical Model [электронный ресурс]. –Режим доступа: http:// www.ndt.net/article/v05n04/mondal/mondal.htm.
4. Куц Ю. В. Статистическая фазометрия / Ю.В. Куц, Л.М. Щербак – Тернополь: Изд-во Тернополь. технического ун-та имени Ивана Пулюя, 2009. – 383с.
5. Бендат Дж., Пирсол А. Прикладной анализ случайных данных: пер. с англ. – М.: Мир, 1989. – 540 с.

УДК 681

MOTION IMPRINT КАК ОДИН ИЗ ФАКТОРОВ СТРОГОЙ АУТЕНТИФИКАЦИИ

Лебедев А.Н., Степанов Б.А., Нестеров М.С., Онуфриев С.В.
Москвоский государственный технический университет им. Н.Э. Баумана
Москва, Россия

Современные реалии формируют новые требования к системам безопасности. Развитие методов взлома требует постоянной актуализации средств противодействия новым угрозам. Сейчас проступает проблема, когда стандартная (парольная) аутентификация пользователя не всегда в силах обеспечить защиту от несанкционированного доступа. В таких случаях пользуются дополнительными мерами по аутентификации пользователей. Вводят усиленную аутентификацию или строгую, которая включает в себя сразу несколько факторов.

Нами была поставлена задача разработать многофакторную систему аутентификации с использованием комбинации трех факторов: уникальная информация, уникальный предмет, биометрические данные (motion data). Данная статья посвящена одному из факторов – отпечаток движений (motion imprint).

Под отпечатком движений (motion imprint) понимается совокупность индивидуальных особенностей движений рук во время набора символов на клавиатуре.

Мы предположили, что такие отпечатки имеют достаточную вариативность, чтобы можно было сделать однозначное утверждение о принадлежности отпечатка данному человеку.

Для того, чтобы сделать первоначальные выводы, мы разработали ряд программ и провели несколько экспериментов.

В качестве источника motion data служат умные часы Huawei Watch (1st gen) на базе операционной системы Android Wear. Для них была написана программа, опрашивающая сенсор движения и записывающая полученные данные в текстовый файл с содержанием времени, и соответствующие мгновенные значения осей акселерометра и гироскопа. Параллельно с этим написан простейший кейлоггер на библиотеке jQuery. Кейлогер ведет запись текущего времени, событий нажатия и отжатий кнопок клавиатуры.

В самом эксперименте участвовало четыре человека. Каждый из них надевал умные часы и вводил одну и ту же парольную фразу на компьютере по 20 раз. По окончании проведения экспериментов были получены логи с умных часов и кейлоггера. Синхронизировав время между показаниями, мы смогли отрезать показания, не относящиеся к эксперименту.

Таким образом, суммируя, было получено 480 дискретных функций для всех осей сенсора. Их них были отфильтрованы неудачные попытки ввода пароля.

Каждая из функций содержит 250-350 отсчетов, что зависит от времени набора парольной фразы.

Далее был проведен краткий анализ полученных данных. Для проведения анализа использовалась функция взаимной корреляции.

Так мы рассчитали максимум взаимной корреляции между попытками ввода парольной фразы одного человека и между попытками ввода пароля разных людей.

На рисунке 3 показаны результаты взаимной корреляции двух попыток одного человека. Здесь каждой из осей акселерометра и гироскопа соответствует 6 функций взаимной корреляции. Максимумы функций имеют следующие значения:

max (cor) A_x = 0,92;
max (cor) A_y = 0,63;
max (cor) A_z = 0,71;
max (cor) G_x = 0,55;
max (cor) G_y = 0,76;
max (cor) G_z = 0,96.

Коэффициенты, которые наиболее близки к единице – это сигнал акселерометра по оси X и сигнал гироскопа по оси Z.

На рисунке 4 показаны результаты взаимной корреляции двух попыток ввода одного пароля разными людьми. Максимумы функций имеют следующие значения:

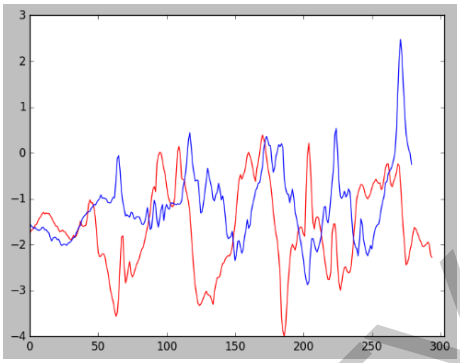

Рисунок 1 – Сигнал по оси X акселерометра попыток ввода одного пароля двумя людьми

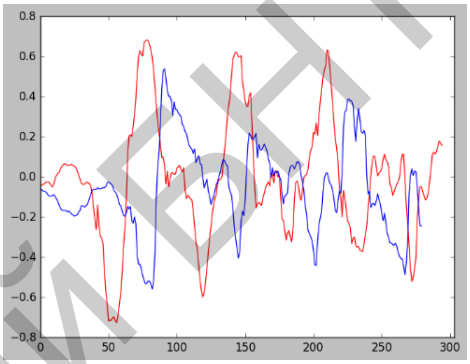

Рисунок 2 – Сигнал по оси Z гироскопа попыток ввода одного пароля двумя людьми

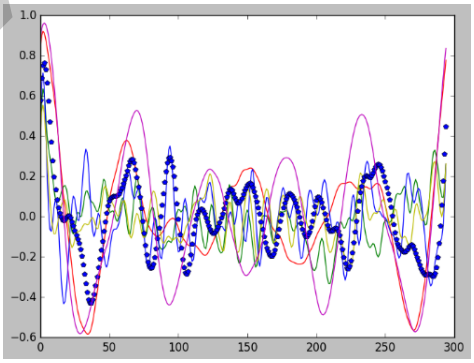

Рисунок 3 – Корреляция сигналов акселерометра и гироскопа попыток ввода одного пароля одним человеком

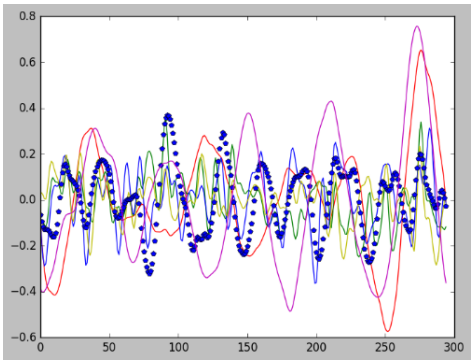

Рисунок 4 – Корреляция сигналов акселерометра и гироскопа попыток ввода одного пароля двумя людьми

max (cor) A_x = 0,65;
max (cor) A_y = 0,35;
max (cor) A_z = 0,31;
max (cor) G_x = 0,23;
max (cor) G_y = 0,37;
max (cor) G_z = 0,76.

Можно заметить, что некоторые коэффициенты уменьшились более в чем два раза. Также примечательно, что в некоторых случаях оси A_x и G_z также показывали значения корреляции порядка 0.7, что близко к значениям, полученным при сравнении попыток одного человека. Однако остальные оси A_y, A_z, G_x G_y также продолжали сохранять двукратную разницу значений.

1. Лебедев А.Н., Онуфриев С.В., Степанов Б.А., Способ строгой многофакторной аутентификации. // «Безопасные информационные технологии». Сборник трудов Седьмой всероссийской научно-технической конференции / под ред. Матвеева В.А. – М.: НУК «Информатика и системы управления» МГТУ им. Н. Э. Баумана, 2017. – С. 194–196.

УДК 004.021

ЗАЩИТА КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОТ АТАК JACKPOTTING

Максимов Р.Л., Рафиков А.Г.
Московский государственный технический университет имени Н. Э. Баумана
Москва, Российская Федерация

Введение. Классическими примерами автоматизированных систем, которые стали неотъемлемой частью жизни каждого современного человека и требующие защиты от злоумышленников, являются банкоматы, платежные терминалы, терминалы самообслуживания, билетопечатающие автоматы.

Несмотря на постоянный интерес к банковскому сектору со стороны злоумышленников, представители этого бизнеса неохотно тратят дополнительные средства на дорогостоящие решения по защите банковских автоматов от атак на информацию. Если раньше практически всегда объектами атак становились клиенты банков, то в последнее время зачастую такими объектами становятся непосредственно системы банковского обслуживания и банковские автоматы (банкоматы, платежные терминалы).

Банкомат представляет особенный интерес для злоумышленников как хранилище денежных средств. Несмотря на то, что деньги хранятся в защищенном сейфе, злоумышленники находят способы добраться и до них.

Помимо радикальных методов, например, подрыва газом или кражи банкомата, имеют место и более высокотехнологичные атаки на уровне аппаратного и программного обеспечений, сетевого взаимодействия, подсистемы управления периферийным оборудованием. К ним относятся, так называемые, атаки jackpotting, одна из реализаций которых заключается в скрытом размещении внутри банкомата некоторого устройства (black box) и его непосредственном подключении к шинам или портам банковского автомата, что позволяет злоумышленнику удаленно контролировать все периферийные устройства. Это приводит к возможности анализа, перехвата и изменения команд при работе с диспенсером, что, в конечном счете, обеспечивает беспрепятственный несанкционированный вывод денежных средств из сейфа атакуемого объекта.

Основными проблемами, при этом, являются: использование стандартных интерфейсов (USB, RS232, SDC) и незащищенных коммуникационных каналов, в частности, для связи «хост-диспенсер», отсутствие механизмов аутентификации, авторизации и регистрации действий злоумышленников во время проведения jackpotting-атаки.

Широкому распространению атак на информацию банкоматов также способствует доступная злоумышленнику документация банкоматов с описанием протоколов и формата команд управления.

Относительно простым и недорогим решением по защите банкоматов от jackpotting-атак с использованием black box, может стать устройство на базе криптоконтроллера, имеющего нановаттное энергопотребление, возможность подключения батареи резервного питания, аппаратную поддержку криптографических алгоритмов для защиты каналов информационного обмена и реализующего функции блокирования наиболее критических периферийных устройств при обнаружении кибератаки. Таким образом, «блокиратор» использует алгоритмы взаимной аутентификации модулей устройства и шифрования потока управляющих команд для обнаружения атак, защиты и снижения ущерба от них путем блокирования соответствующего модуля.

К критическим (с точки зрения безопасности) периферийным устройствам банкоматов относятся: защищенная EPP-клавиатура (encrypting PIN pad), устройство для чтения карт (card reader), диспенсер (dispenser) и устройство для внесения наличных денег (cash-in).

Однако разработать высокоэффективный, быстродействующий, надежный криптографический алгоритм для решения поставленной