ПОЛУЧЕНИЕ И ОБРАБОТКА ДИНАМИЧЕСКИХ ПРИЗНАКОВ ОНЛАЙН-ПОДПИСИ

А.И. Митюхин

Одним из биометрических поведенческих признаков, используемых в аутентификационных системах является собственноручная подпись человеческой личности. Подписи можно считать уникальными изображениями со стабильными динамическими характеристиками. В отличие от статического (офлайнового) [1] метода получения сигнатурного эталона и образа подписи, когда верификация основывается на геометрических свойствах 2D-изображения $g(x,y), \{x,y\} \in \mathrm{Z}^+$, таких как плотности линий, скрещивания, ответвления линий и др., динамический (онлайновый) [1] способ формирования эталона и образа подписи использует значения 2D-пространственных координат $\{x,y\}$ и значения реального временного интервала написания подписи. Увеличение числа признаков распознавания усложняет фальсификацию, имитацию и подделку подписи. В работе рассматривается спектральный подход получения и обработки динамических признаков. Зная частоту дискретизации и спектральные характеристики изображения подписи, фиксируя координаты определенных критических и экстремальных точек, можно получить такие характеристики, как составляющие скорости (ускорения) электронного пера во время его движения на сенсорном экране устройства ввода (таблет-PC или др.) по осям x и y. Повышение эффективности обработки достигается применением быстрого алгоритма действительного дискретного ортогонального преобразования Хартли (ДПХ) на этапе вычисления скоростных составляющих признаков [2]. Для этого из изображения подписи формировались проекции сегментов на оси x и y в виде дискретных последовательностей $g^p(x)$ и $g^p(y)$ длиной $n = 100 - 200$ отсчетов. Диапазон значений n выбирался с учетом получения необходимых точностных характеристик системы контроля и длительности подписи 1–2 с.

Список литературы

1. Zhang H., Wang K.Y., Wang Y.A Survey of on-line signature verification // Proceedings of 6th Chinese Conference «Biometric Recognition». Beijing, 3–4 December 2011. P. 141–149.

2. Mitsiukhin A. Segmentation of dynamical images by means of discrete Hartley transform // Proceedings of 56 IWK. TU Ilmenau, DE, 12–16 September 2011. URN: urn:nbn:de:gbv:ilm1-2011iwk-011:5, id 1100. P. 1–4.

ИСПОЛЬЗОВАНИЕ РАСШИРЕНИЯ БРАУЗЕРА GHOSTERY ДЛЯ ПРОТИВОДЕЙСТВИЯ ОТСЛЕЖИВАНИЮ ПОЛЬЗОВАТЕЛЯ И КОНТЕКСТНОЙ РЕКЛАМЕ

Н.В. Михальков

В современном мире широко распространена проблема с утечкой конфиденциальной информации через веб-браузер. На многих сайтах работают трекинговые сервисы. Предназначены они для разного, например, для показа ориентированной на пользователя рекламы. И это только в лучшем случае. В худшем случае встроенный вредоносный код может похитить идентификационные данные, например номер карты, PIN-код и пр.

Для блокирования подобного рода слежки существует расширение для браузеров под названием Ghostery. Оно позволяет обеспечить анонимность пользователя в сети Интернет. Для оценки эффективности функционирования расширения проведен эксперимент. Для этого использовался персональный компьютер с операционной системой Windows, подключенный к сети интернет. Интеренет браузер Google Chrome с установленный расширением Ghostery.

На первом этапе исследования выполнялась настройка указанного расширения браузера, в частности такие параметры как аналитика, виджеты, конфиденциальность, маяки,

реклама. Расширение поддерживает технологию белых списков, позволяющих создать список исключений (доменов), для которых будет исключаться блокировка процедуры сбора информации о компьютере пользователя. На втором этапе исследования выполнялось тестирование расширения с предустановленными настройками. Необходимо отметить одно из преимуществ расширения – при блокировке процедур отслеживания со стороны интернет ресурса. Расширение демонстрирует, какие из процедур блокируются.

Таким образом, показано, что Ghostery позволяет просматривать и блокировать средства слежения на посещаемых веб-сайтах, позволяя контролировать сбор пользовательских данных. EnhancedAntiTracking (улучшенный антитрекинг) также обезличивает пользовательские данные для дополнительной конфиденциальности. Из недостатков расширения можно указать на более продолжительную загрузку веб-страниц [1, 2].

Список литературы

1. Расширение для браузеров Ghostery: отключение слежки за поведением посетителя. [Электронный ресурс]. URL: https://www.kv.by (дата обращения: 22.04.2019).

2. Ghostery – анонимность в сети Интернет. [Электронный ресурс]. URL: https://sys-team-admin.ru (дата обращения: 22.04.2019).

3. ОбзорприложенияGhostery Storage Server. [Электронный ресурс]. URL: https://geekon.media (дата обращения: 22.04.2019).

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ КОРПОРАТИВНОЙ СЕТИ С ПОМОЩЬЮ PARROT SECURITY OS

А.Д. Михейчик, О.А. Хацкевич

На сегодняшний день многие организации проводят мониторинг своей корпоративной сети для обнаружения уязвимостей, воспользовавшись которыми злоумышленники могут осуществить нелегитимные действия. Для проведения мониторинга сети могут закупаться специализированные программные или аппаратные средства, наниматься специалисты по информационной безопасности, использоваться online-инструменты и т.п.

В последнее время наибольшую популярность набирает тестирование на проникновение (пентестинг). Задача данной технологии заключается в осуществлении сетевых атак, которые не приводят к существенным последствиям работы сети, но с помощью которых можно обнаружить недостатки в корпоративной сети. К пентестингу можно отнести дистрибутив Linux – Parrot Security OS.

Parrot Security OS – дистрибутив Linux, основанный на операционной системе Debian. Основные задачи данного дистрибутива – проведение пентестинга, осуществление оценки уязвимостей и их устранение, анонимный просмотр веб-стариц.

Главные отличия представленного дистрибутива от известного Kali Linux следующее:

– в состав Parrot Security OS входит больше инструментов, с помощью которых можно осуществлять пентестинг;

– требует меньше ресурсов при установке, чем Kali;

– Parrot Security OS имеет более удобный графический интерфейс;

– направлен на большую анонимность при работе в сети Интернет, в отличие от дистрибутива Kali Linux.

ЦЕНТР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КАК СОСТАВЛЯЮЩАЯ СИСТЕМЫ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Е.В. Моженкова, А.И. Парамонов

В состав корпоративной вычислительной сети входят персональные компьютеры пользователей, и являются одним из источников угроз безопасности данных, обрабатываемых корпоративными информационными системами (КИС) [1]. Для снижения уровня угрозы безопасности на предприятиях вводятся ряд организационных и технических мер