Информационная безопасность

УДК 004.056.2

С.Б. Вепрев[1]
П.И. Гончаров[2]

СКРЫТЫЙ МЕТОД ВЫЯВЛЕНИЯ УТЕЧЕК ИНСАЙДЕРСКОЙ ИНФОРМАЦИИ

S.B. Veprev
P.I. Goncharov

CONCEALED METHOD OF THE DETECTION OF LEAKS OF THE INSIDER INFORMATION

В статье описан скрытый метод идентификации пользователей на основе клавиатурной подписи.

Ключевые слова: *информационная безопасность, биометрические методы идентификации, клавиатурный почерк.*

The concealed method of the identification of users on the base of keyboard signature is described in the article.

Keywords: *information safety, the biometric methods of identification, keyboard handwriting.*

Анализируя статистику [1; 2; 3; 4] угроз информационной безопасности организаций, можно констатировать тот факт, что главное направление угроз – это угрозы внутренние. Наибольший вред организации наносится именно её работниками. На сегодняшний день внутренние угрозы примерно в четыре раза более «результативны», чем внешние.

Действия злонамеренного *инсайдера* (в дальнейшем в статье под словом инсайдер будем подразумевать именно злонамеренных инсайдеров) сложнее выявить. Для получения и передачи конфиденциальной информации зачастую не требуются усилия по сохранению её на отчуждаемые носители или передачи по каналам связи. Инсайдеру, как правило, требуется её просто запомнить или записать.

Одним из негативных факторов в проведении политики безопасности является халатность работников организации. Более 70% угроз были реализованы, когда в той или иной мере проявлялась халатность работников, которая позволяла инсайдеру узнать чужой пароль. В этом случае инсайдер получал соответствующий доступ и действовал под чужим именем.

В настоящее время используются комплексные методы защиты информации, которые в совокупности образуют единую систему защиты информации. Одновременное применение нескольких способов защиты является достаточно эффективным. В данной статье рассматривается один из таких способов, связанный с анализом клавиатурной подписи. Проведенный эксперимент связан именно с анализом клавиатурной подписи, а не клавиатурным почерком. Причинами проведения исследований именно в этом направлении стали следующие соображения:

• проведение процедур анализа клавиатурного почерка требует наличия текста доста-

[1] Доктор технических наук, доцент, профессор кафедры ИТиЕНД НОУ ВПО «Российский новый университет».

[2] Аспирант Финансового университета при Правительстве России.

точно большого объема (хотя бы нескольких словосочетаний). В современных условиях для получения конфиденциальной информации, как правило, нет необходимости набирать большие тексты;

• клавиатурный почерк подвержен изменениям во времени, и его устойчивость зависит от многих параметров (состояние здоровья, нервозность, торопливость и т. д.);

• парольная политика подразумевает как смену пароля, так и его случайный характер. Как правило, пароль состоит из букв и цифр, причем используется смена регистра. Пароль служит, прежде всего, для аутентификации пользователя, временные параметры его набора сравнительно неустойчивы;

• наиболее устойчивые временные параметры наблюдаются в том случае, когда осуществляется многократный периодический набор конкретного слова. Прежде всего это относится к набору **логина**.

Сразу следует отметить, что гипотеза об устойчивости временных интервалов при наборе логина тоже оказалась несостоятельной. Даже в этом случае временные интервалы между нажатиями клавиш носили случайный характер. Сравнение многократного набора одного и того же логина одним и тем же лицом показало такой разброс параметров, при котором невозможно достоверное определение респондента. В эксперименте имелся в виду не постоянный последовательный набор конкретного слова, а набор логина только при входе в систему.

Однако исследования показали, что общая динамика набора слова является достаточно устойчивой. При нормировании параметров набора логина соотнесение временных интервалов между собой определило некоторый образ – клавиатурную подпись. Такая подпись является характерной для индивидуума (рис. 1).

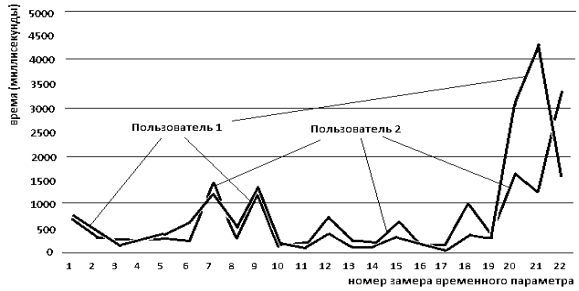

Рис. 1. Средние значения набора одного и того же логина для двух разных пользователей

Эксперимент показал следующие характерные особенности набора логина пользователем и инсайдером:

1) при нормировании временных параметров можно говорить о некотором устойчивом образе – клавиатурной подписи пользователя;

2) у пользователя периодически наблюдается выход временных параметров за пределы средних значений (отвлекся, задумался);

3) у инсайдера не наблюдается выхода временных параметров за пределы некоторых средних значений (сосредоточен);

4) чем меньше временной интервал между набором двух символов, тем более он характерен для конкретного пользователя;

5) у инсайдера «чужая» клавиатурная подпись размыта и не столь явно характеризуется некоторым образом (нет устойчивого навыка набора) (рис. 2).

Нормирование временных интервалов позволило создать некоторый образ клавиатурной подписи пользователя. Для инструментального анализа исходных данных использовалась нейронная сеть, реализованная на аналитической платформе DEDUCTOR.

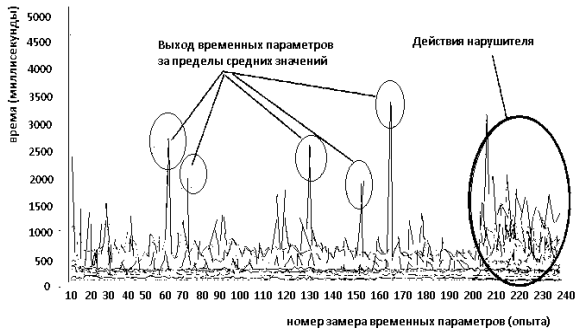

Рис. 2. Особенности набора логина пользователем и инсайдером

Последняя (пятая) особенность набора логина пользователем навела на мысль использовать не пару: (логин) – (пароль), а тройку: (общий для всех идентификатор) – (логин) – (пароль). Введение общего для всех идентификатора позволяет создать базу данных образов всех сотрудников. Таким образом, получается:

• *общий для всех идентификатор* – позволяет выявить, кто из респондентов осуществляет вход в систему;

• *логин* – уточняет образ пользователя (СВОЙ/ЧУЖОЙ) и определяет авторизацию пользователя;

• *пароль* – аутентифицирует пользователя.

Для того чтобы реализовать данный подход, разработан критерий легальности клавиатурной подписи, основанный на выявленных особенностях его набора.

Нормирование временных параметров:

$$\tau_i = \frac{t_i}{\sqrt{\sum_{i-1}^{n} t_i^2}} \cdot \quad (1)$$

Нормирование временных параметров позволяет сделать значение критерия, не имеющим размерности. Все дальнейшие вычисления осуществляются с «нормированным временем». Значение критерия обратно пропорционально разнице между вводом *i*-го символа в текущем замере и эталонным (математическим ожиданием времени перехода между нажатиями – τ^*):

$$\Omega = \exp\left(-\sum_{i=1}^{n} \left(\tau_i^* - \tau_i \right)^2 \right), \quad (2)$$

где τ_i^* – среднее время перехода $\prod_i$;

τ_i – текущее время перехода $\prod_i$;

n – количество всех параметров, фиксируемых для данного пользователя.

Эмпирически полученные данные показывают, что чем меньше время параметра, тем реже пользователь в нём ошибётся. Поскольку значимость конкретного параметра набора зависит от устойчивости его набора конкретным пользователем (индивидуальные навыки), требуется вывести весовые коэффициенты важности каждого параметра. Для эталонного значения он определяется статистическими параметрами устойчивости ввода данных. Чем меньше отклонений совершает пользователь при текущем наборе заданного параметра от среднестатистического, тем важнее будет его значение:

$$k_i^* = T^* / \tau_i^* . \quad (3)$$

Аналогично:

$$k_i = T / t_i . \quad (4)$$

В итоге получается значение критерия легальности клавиатурной подписи для конкретного набора:

$$W = \exp\left(-\sum_{i=1}^{n} k_i k_i^* \left(\tau_i^* - \tau_i \right)^2 \right). \quad (5)$$

В результате создания математической модели, её опытной апробации и подтверждения гипотезы был создан программный комплекс аутентификации пользователя на основе клавиатурной подписи. Модуль основан на клиент-серверной архитектуре и состоит из двух частей: клиентской, собирающей биометрические данные при вводе учётных данных с АРМ пользователей, и серверной, производящей их анализ.

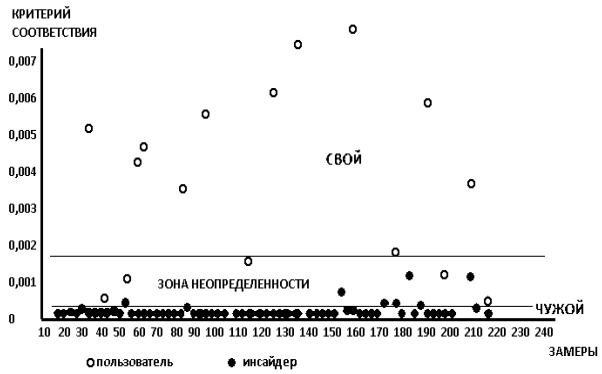

Рис. 3. Определение параметра СВОЙ/ЧУЖОЙ по критерию соответствия

Статистические данные показывают, что абсолютной точности определения параметра «пользователь – инсайдер» достичь не удается. Налицо некоторая «зона неопределенности» (см. рис. 3), для которой характерно наличие ошибок первого и второго рода. В том случае, если параметры ввода клавиатурной подписи попадают в эту зону, системе безопасности посылается соответствующий сигнал. В других случаях системе безопасности посылается сигнал СВОЙ или ЧУЖОЙ.

Полученные экспериментальные данные позволяют сделать вывод о достаточно точной аутентификации пользователя по его клавиатурной подписи. Полученный результат предоставляет возможность не только аутентификации пользователя, но и получение прогнозных данных об инсайдере. Для этого требуется наличие базы подписи всех пользователей системы. Введение помимо логина и пароля некоторого идентификатора, одинакового для всех, позволяет создать такую базу. Инсайдер в этом случае встречается с еще более сложной задачей – не только войти в систему под чужими параметрами, но и скрыть свои. Очевидно, что намеренное грубое искажение своей подписи приведет к идентификации инсайдера как такового. Если же инсайдер будет пытаться войти незаметно в систему, то неизбежно будет набирать свою подпись достаточно устойчиво, что по ранее полученным данным, отраженным в базе, позволит прогнозировать личность инсайдера.

Для данного, достаточно ограниченного, эксперимента, проведенного все-таки в «тепличных» условиях, параметры распознавания СВОЙ/ЧУЖОЙ оказались очень хорошими:

• однозначное определение пользователя более чем в 90%;

• однозначное определение инсайдера более чем в 80%.

Реальная картина, наверное, будет несколько хуже. Но главный вывод – данный метод с хорошей степенью точности позволяет определить возможное вхождение в систему инсайдера и позволяет спрогнозировать, кто именно осуществляет вход в систему. Наличие соответствующего программного комплекса либо позволит определить инсайдера, либо, в том случае если о подключении данных средств станет известно, может отпугнуть злоумышленника от проведения им незаконных действий.

Литература

1. CSO CERT Deloite, 2010 Cybersecurity watch survey Cybercyme increasing faster than some company expected, Framingham, Mass. – 2010. – Jan. 25.

2. Аналитический центр InfoWatch: исследование утечек информации и конфиденциальных данных из компаний и госучреждений России 2012. – М., 2012.

3. Аналитический центр InfoWatch: «Глобальное исследование утечек корпоративной информации и конфиденциальных данных 2012». – М., 2012.

4. Perimetrix, Инсайдерские угрозы в России 2008 г. – М., 2009.