Труды научно-технической конференции кластера пензенских предприятий,
обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.**
Том 9, Пенза-2014, с.73-75 (http://www.pniei.penza.ru/RV-conf/T9/C18)

СКРЫТАЯ ИДЕНТИФИКАЦИЯ СУБЪЕКТОВ ПО ОСОБЕННОСТЯМ ЛИЦА И КЛАВИАТУРНОГО ПОЧЕРКА С АЛЬТЕРНАТИВНЫМИ СЦЕНАРИЯМИ АВТОРИЗАЦИИ[1]

Ложников П.С., Сулавко А.Е., Еременко А.В. (г. Омск)

Вопросы защиты информации от неавторизованного доступа всегда были и остаются актуальными. Со временем изменяются лишь типы правонарушений, совершаемых в данной области. По мнению аналитического центра компании InfoWatch (одного из крупнейших производителей систем защиты от утечек конфиденциальной информации) перевод документооборота в электронную форму провоцирует в нашей стране распространение такого вида преступлений, как «кража личности» – использование чужих персональных данных в собственных целях. Об учащенных случаях нарушений такого рода свидетельствуют результаты глобальных исследований InfoWatch, проведенных в 2014 году. Отчасти такое положение вещей обусловлено несовершенством традиционных подходов к решению проблемы разграничения доступа. Использующиеся на практике процедуры аутентификации обычно основаны на проверке пароля, аппаратного идентификатора или биометрических данных пользователя. Пароли взламывают (для этого имеется множество методов - социальная инженерия, перебор паролей по словарю и без, подбор пароля на основе известных злоумышленнику данных о пользователе), аппаратный идентификатор можно украсть, а открытые биометрические данные (отпечаток пальца, радужка и т.д.) можно подделать. Несмотря на то, что последнее отнюдь не тривиальная задача, если злоумышленник обладает технологией изготовления муляжа, целевая система защиты (и любая аналогичная) будет скомпрометирована.

Недостатки традиционных средств защиты можно устранить, если сделать процедуру аутентификации скрытой от субъекта, а в качестве биометрических признаков использовать параметры его клавиатурного почерка и особенности лица. В представленной работе предлагается технология идентификации пользователей компьютерных систем, основанная на использовании данных признаков. При вводе пользователем пароля скрытая камера получает изображение лица субъекта, измеряются времена удержания клавиш и паузы между нажатием кнопок на клавиатуре. Если пароль верный, эти данные используются для скрытой идентификации личности, осуществляющей доступ к ресурсу. При точном совпадении данных с эталоном одного из зарегистрированных пользователей информационного ресурса – доступ разрешается. Если данные не соответствуют ни одному известному пользователю, то реализуется обманный сценарий авторизации – эмитируется возможность доступа к ресурсу с использованием фиктивных файлов, которых в действительности не существует[1]. При этом легальные пользователи получают сообщение (по SMS и/или электронной почте), информирующее об атаке.

1 - Работа выполнена в рамках проекта РФФИ № 15-37-21109

В спорных случаях (камера не работает, плохое освящение и др.) субъект получает доступ, но в процессе работы производится скрытый мониторинг его действий, анализ клавиатурного почерка и особенностей работы с мышью [2]. При несоответствии портрета работы субъекта в системе ни одному из известных – доступ к ресурсу будет ограничен.

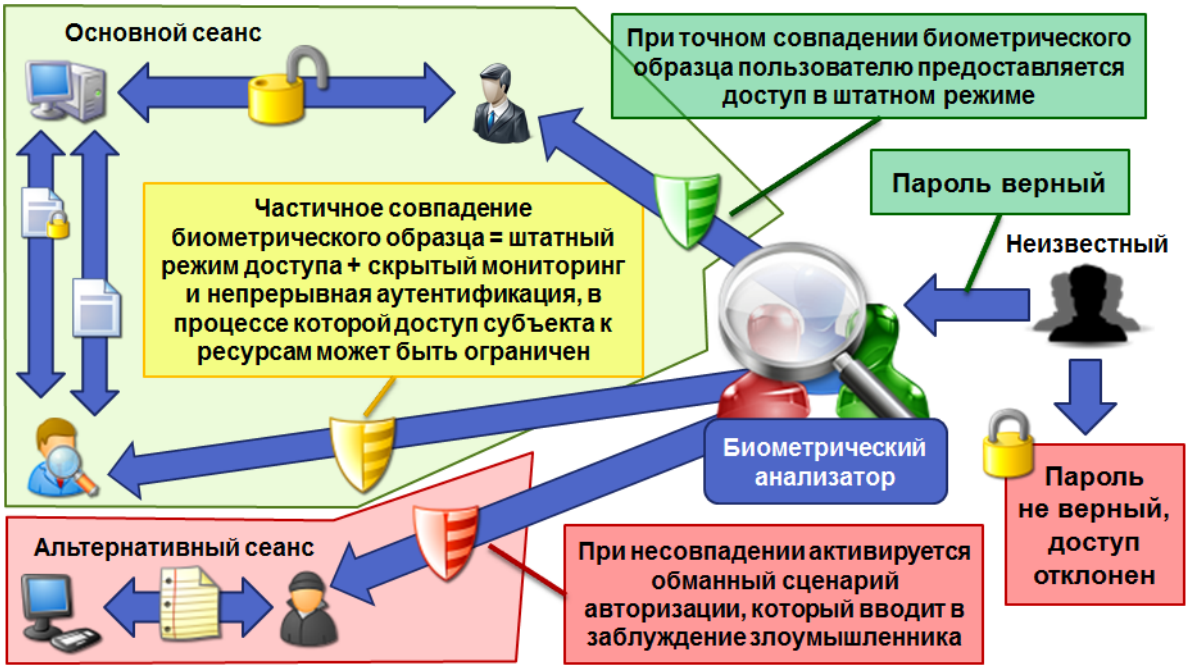

Рис.1. Принципы работы предлагаемой технологии

Чтобы избежать компрометации системы защиты посредством предъявления изображения лица зарегистрированного субъекта злоумышленником, используется методика обнаружения “живой” картинки, основанная на корреляционном анализе фрагментов изображений, распознавании мимики и движений лица, микроколебаний головы субъекта, а также за счет параллельного анализа его клавиатурного почерка.

Признаками клавиатурного почерка в данной работе являются времена удержания, паузы между нажатием клавиш, а также общее время ввода парольной фразы. В качестве признаков лица используются как статические (отношение расстояний между глазами, ушами, носом), так и динамические признаки (параметры движения краев губ, подбородка). Данные признаки являются случайными величинами для одного лица, поэтому при создании эталона производится многократное измерение данных характеристик. Процесс создания эталона сводится к следующему. Субъект многократно вводит парольную фразу (не менее 26 раз, при таком числе реализаций значений признаков клавиатурного почерка выборку значений можно считать репрезентативной [3]). Параллельно камера фиксирует параметры его лица, делая многократные измерения. Для признаков лица строится гистограмма относительных частот, исходя из параметров которой, можно судить о распределении признаков для каждого конкретного субъекта. Подделать все указанные признаки на практике не представляется возможным.

Для сравнения предъявляемых биометрических образов с эталонными планируется использовать аппарат Байесовских сетей, в частности алгоритм

последовательного применения модифицированной формулы гипотез Байеса (1) [4], которая дает достаточно высокие результаты при идентификации образов в пространстве малоинформативных признаков [4]. Суть алгоритма заключается в вычислении апостериорных вероятностей гипотез $P_j(H_i/A)$ за некоторое число шагов, равное количеству признаков, при помощи формулы (1). Каждая гипотеза подразумевает, что предъявляемые биометрические данные на этапе идентификации принадлежат определенному субъекту, т.е. каждая гипотеза ассоциируется с определенным эталоном субъекта. На каждом шаге на вход поступают данные об определенном идентификационном признаке в виде условных вероятностей гипотез, которые вычисляются исходя из закона распределения значений признака (в данном случае условная вероятность определяется, как относительная частота полученного на этапе идентификации значения признака), а также априорная вероятность. За априорную вероятность принимается апостериорная вероятность, вычисленная на предыдущем шаге. На первом шаге все гипотезы (субъекты) считаются равновероятными, т.е. $P_0(H_i/A)=1/n$, где n – количество гипотез (субъектов). Чтобы отличить известного пользователя компьютерной системы от неизвестного устанавливается пороговое значение апостериорных вероятностей гипотез [4]. Для принятия решений об активации одного из сценариев авторизации задаются пороговые интервалы. Подробнее данный процесс описан в [1].

$$P_j(H_i|A) = P_{j-1}(H_i|A) + \left(\frac{P_{j-1}(H_i|A)P(A_j|H_i)}{\sum_{i=1}^{n} P_{j-1}(H_i|A)P(A_j|H_i)} - P_{j-1}(H_i|A) \right) \times (W_j), \qquad (1)$$

где W_i вес j-го признака, $P(H_i/A_j)$ – апостериорная вероятность i-ой гипотезы, вычисляемая на j-ом шаге при поступлении j-ого признака, $P(A_j/H_i)$ – условная вероятность i-ой гипотезы при поступлении j-го признака. Вес признака W_i вычисляется исходя из его информативности, при $W_i = 1$ данная формула эквивалентна обычной (классической) формуле гипотез Байеса, подробно данный вопрос раскрывается в [4].

ЛИТЕРАТУРА:

1. Епифанцев Б.Н., Ложников П.С., Сулавко А.Е. Альтернативные сценарии авторизации при идентификации пользователей по динамике подсознательных движений // Вопросы защиты информации. – 2013. №2 (101). – С.28-35

2. Еременко А.В., Левитская Е.А., Сулавко А.Е., Самотуга А.Е. Разграничение доступа к информации на основе скрытого мониторинга действий пользователей в информационных системах: скрытая идентификация // Вестник СибАДИ. –2014, №6 (40).– С. 92-102.

3. Сулавко А.Е., Еременко А.В. Метод сжатия собственных областей классов образов в пространстве малоинформативных признаков // Искусственный интеллект и принятие решений – Москва: 2014, № 2. С. 95-102.

4. Епифанцев Б.Н., Ложников П.С., Сулавко А.Е. Алгоритм идентификации гипотез в пространстве малоинформативных признаков на основе последовательного применения формулы Байеса // Межотраслевая информационная служба. – 2013. №2 (163). – С.57-62.

Материал поступил 19.12.2015. Публикуется по положительной рецензии к.т.н. Безяева А.В.