DOI: 10.17117/na.2015.07.656

Поступило в редакцию: 08.07.2015

<http://ucom.ru/doc/na.2015.07.656.pdf>

Евдокимов А.О., Грибин М.А., Смирнов Г.Ф. Модель реализации безопасности информации на основе изображений точечных отметок

Evdokimov A.O., Gribin M.A., Smirnov G.F.
The model implementation of information security
based on the image of point marks

В работе описана модель реализации безопасности информации на основе изображений точечных отметок на примере смартфонов с сенсорным экраном при использовании графических паролей. В качестве математической модели реализуемых программно-графических паролей использовать амплитудно-фазовую модель изображений групповых точечных объектов. Исследовано влияние разрешения сенсорного экрана и количество используемых отметок на устойчивость графического пароля

Ключевые слова: безопасность информационных систем, пароль, графически пароль, математическая модель, обработка изображений, групповые точечные объекты, амплитудно-фазовая модель

Евдокимов Алексей Олегович

Кандидат технических наук, доцент
Поволжский государственный технологический университет
г. Йошкар-Ола, пл. Ленина, 3

Грибин Максим Анатольевич

Студент
Поволжский государственный технологический университет
г. Йошкар-Ола, пл. Ленина, 3

Смирнов Григорий Фёдорович

Студент
Поволжский государственный технологический университет
г. Йошкар-Ола, пл. Ленина, 3

The article describes the implementation of information security model based on the image of point marks on the example of smart phones with touch screen which use graphical passwords. In use as a mathematical model implemented by software and graphical passwords is amplitude-phase model image group point objects. Researched the influence of resolution of the touch screen and the used number of marks on the stability of the graphical password

Key words: security of information systems, password, graphical password, mathematical model, image processing, group point objects, the amplitude-phase model

Evdokimov Aleksei Olegovich

Candidate of Engineering Sciences, Associate Professor
Volga state university of technology
Yoshkar-Ola, Lenin square, 3

Gribin Maxim Anatolyevich

Student
Volga state university of technology
Yoshkar-Ola, Lenin square, 3

Smirnov Gregory Fyodorovich

Student
Volga state university of technology
Yoshkar-Ola, Lenin square, 3

Изменение характеристик информационного продукта, позиционируемого как гибрид между результатом расчетно-аналитической работы и специфической услугой, предоставляемой индивидуальному пользователю ПЭВМ и ликвидация всех промежуточных звеньев на пути от источника информации к ее потребителю, например, становится возможным непосредственное общение автора и читателя, продавца и покупателя, певца и слушателя, ученых между собой, преподавателя и обучающегося, специалистов на предприятии через систему видеоконференций, электронный киоск, электронную почту дает возможность локализации угроз корпоративной информации, так как большая их часть связана с угрозой НСД, исходящей от самих сотрудников, имеющих доступ к информационным системам. При этом следует учитывать и сетевые ресурсы, прежде всего в составе локально-вычислительной сети (ЛВС), к которым сотрудник имеет доступ со своего компьютера в рамках своей служебной деятельности. Факты несанкционированного доступа к информации (НСД) показывают, что большинство современных информационных систем достаточно уязвимо с точки зрения безопасности [6].

В настоящее время выделяют два подхода к обеспечению компьютерной безопасности:

- использование только встроенных в ОС и приложения средств защиты. В данном подходе в основном приходится использовать более длинные и сложные для обычного перебора пароли;

- применение, наряду со встроенными, дополнительных механизмов защиты. Этот подход заключается в использовании так называемых технических средств добавочной защиты – программных, либо программно-аппаратных комплексов, устанавливаемых на защищаемые объекты.

Целью данной работы является описание модели реализации безопасности информации от несанкционированного доступа в компьютерных системах на основе изображений точечных отметок, представленных в виде графических паролей.

Таким образом, именно компьютер, находящийся в составе сети, следует в первую очередь рассматривать в качестве объекта защиты, а конечного пользователя – в качестве ее наиболее вероятного потенциального нарушителя. Как следствие, под сомнение ставится обоснованность концепции реализованной системы защиты в современных операционных системах (ОС), которая сводится к построению распределенной схемы администрирования механизмов защиты, элементами которой, помимо администратора, выступают пользователи, имеющие возможность назначать и изменять права доступа к создаваемым ими файловым объектам [4, 5].

Существующая статистика ошибок, обнаруженных в ОС, а также сведения о недостаточной эффективности встроенных в ОС и приложения механизмов защиты, заставляет специалистов сомневаться в достижении гарантированной защиты от НСД, при использовании встроенных механизмов, и все большее внимание уделять средствам добавочной защиты информации.

К добавочному средству защиты можно отнести криптографию [4]. Но не все могут использовать технологию, построенную на основе токенов и USB-

ключей по ряду причин таких, как проблема использования за пределами офиса, высокая цена на программное обеспечение и т.д.

Одним из наиболее перспективных методов обеспечения дополнительной безопасности компьютерных систем представляется использование систем графических паролей [3, 5], которые имеют ряд неоспоримых достоинств при обеспечении идентификации/аутентификации пользователей и разграничения доступа к информационным ресурсам.

Графический пароль – это новый способ получения доступа к устройству, который в данный момент запатентован компанией Microsoft и широко используется в – Windows Developer Preview. Как перспективный способ повышения степени защиты информации в компьютерных системах и мобильных устройствах.

Технология графического пароля основана на выборе пользователем определенных мест в графическом объекте (на изображении) и известна как графический пароль [1-3], или выборе определенной последовательности графических объектов [3] – динамический графический пароль. Эта технология позволит упростить авторизацию пользователя и дает определенные преимущества перед существующими методами идентификации и аутентификации.

Анализ существующих методы идентификации/аутентификации, такие как биометрические, парольные, системы одноразовых паролей и системы графических паролей показывает, что преимущества систем графического пароля перед другими видами систем аутентификации очевидны [4]:

- легкость запоминания;
- быстрая замена скомпрометированного пароля;
- высокая стойкость к методам взлома;
- сравнительно небольшая стоимость разработки.

Проблема легкости запоминания заключается в том, что пользователю предлагается запомнить не набор символов стойкого к простому перебору пароля, а некоторый набор графических объектов.

Есть несколько недостатков в существующих на сегодняшний день системах графических паролей. В большинстве случаев графические системы основываются на том, что в качестве пароля выступают либо координаты щелчков мыши, либо определенный набор символов, присвоенный графическим объектам. Как в первом, так и во втором случае знание реализации системы графического пароля дает возможность подобрать пароль методом перебора. В работе [4] обоснована необходимость использования методов стеганографии в системах графических паролей, что существенно усложняет взлом системы путем подбора и/или перехвата пароля при аутентификации пользователя.

В рамках представленной работы оценивалась эффективность работы системы графических паролей на базе математической модели изображения групповых точечных объектов.

Групповые точечные объекты как модель графических паролей

При выполнении обработки изображений в ряде областей (автоматическое чтение текста, дешифрование радиолокационных и аэрокосмических, медицинских снимков, извлечение информации из сюжетных изображений, по-

зиционирование геотеги́рование) возникает необходимость обработки не отдельных точечных объектов, а их совокупности, группы. В такие группы множество точечных объектов объединяется по определенному признаку, например, по признаку пространственной близости, яркостным характеристикам. После объединения каждое множество приобретает групповые признаки, становится групповым точечным объектом (ГТО) [8].

Примерами ГТО являются изображения созвездий на небесной сфере, символы матричной печати, отверстия и ключи печатных плат, локационные изображения, изображения реализаций случайных процессов. Очевидно, что совокупность отметок, задающих графический пароль как на матрице отметок, так и на сюжетном изображении также может быть отнесено к классу ГТО [7].

Групповые признаки более информативны при обработке изображений и обладают большей устойчивостью к действию мешающих факторов. Как показано в [8] одним из эффективных подходов к обработке изображений точечных объектов с целью обнаружения, распознавания и оценки их параметров является трактовка этих объектов как особого вида сигналов. Значительное количество работ, посвящено решению задачи обработки изображений плоских и пространственных групповых точечных объектов, основные результаты которых изложены в [8, 9]. Предложены быстродействующие алгоритмы, позволяющие эффективно формировать описание ГТО, хранить и выполнять операции упорядочения отметок, распознавания и оценки параметров и базирующиеся на строгих математических подходах теории сигналов.

Следовательно, задача идентификации/аутентификация пользователей на основе графического пароля может быть поставлена как задача распознавания и оценки параметров изображений групповых точечных объектов и сформулирована следующим образом: алфавит $A = \{A_l\}_{0,M-1}$ из M классов задан эталонными ГТО $A_l = \{\alpha_l(n)\}_{0,k-1}$ (храняемого в базе пароля пользователя) каждого класса, где k – число точек в составе ГТО (его размерность), Обрабатываемый (сигнальный) ГТО $B = \{\beta(n)\}_{0,k-1}$ (введенного пользователем графического пароля) получен вращением эталонного ГТО $A_j = \{\alpha_j(n)\}_{0,k-1}$ на неизвестный угол $\varphi\Delta$ (что позволяет учитывать дополнительные данные, например от встроенного гироскопа в мобильных устройствах), причем координаты точек измерены с некоторой ошибкой, позволяющей учитывать погрешность щелчка по сенсорному экрану или позиционирование курсора мыши в окрестностях некоторой заданной области.

Тогда задача идентификации пользователя по введенному ГТО может решаться путем нахождения меры схожести ω_l сигнального ГТО B с эталонными $A_l, l = 0, 1, \dots, M-1$, и принятием решения в пользу класса с максимальным значением данной меры [10]: $B \in A_j$ при $\omega_j \xrightarrow{l} \max$.

При этом данные получаемые при выполнении оценки параметров сигнального изображения ГТО B с эталонными изображением ГТО $A_l, l = 0, 1, \dots, M-1$, могут быть использованы при выполнении многофакторной процедуры иден-

тификации, что также приводит к повышению степени защиты информации от несанкционированного доступа.

Оценка устойчивости к несанкционированному доступу в компьютерных системах с графическим паролем

Для исследования устойчивости было взято два изображения мельниц, одно будем считать эталоном, второе введенным значением. На обоих изображениях нанесли точки в легко запоминающихся местах. Таким образом, такое изображения может трактоваться как изображения плоского группового точечного объекта. Соответственно для обработки графических паролей можно применить хорошо апробированный математический аппарат теории сигналов, позволяющий выполнять распознавание и оценку параметров изображений групповых точечных объектов.

Рис. 1. Пример графического пароля (изображения с нанесенными точками образуют групповой точечный объект)

Современные устройства имеют довольно большие экраны с высоким разрешением. Данный метод предполагает ввод значений не «точка в точку», т.е. не требуется нажимать каждый раз в определенных местах, ввод пароля предполагает введение значений с сохранением геометрических пропорций между точками. Это означает, что ввод может быть осуществлен как на всей площади экрана устройства, так и в верхней части или в нижней, в любой части экрана где угодно пользователю.

Докажем, что данный метод требует ввода пароля с соблюдением только геометрических пропорций между точками, проведя эксперимент на трех телефонах, имеющих разные разрешения экрана. Для эксперимента мы взяли телефоны средней и высокой ценовой категории: LG P-500 Optimus One с разрешающей способностью 320x480 пикселей, LG-D686 с разрешающей способностью экрана 540x960 пикселей, а также телефон Samsung NG-7100 с разрешающей способностью экрана 720x1280 пикселей. Для начала проведем эксперимент на телефоне с разрешением экрана 320x480 пикселей. Создадим два мас-

сива данных, включающие в себя значения координат точек обоих изображений. Отметим то, что значения эталона и введенные вручную, были взяты точно и с погрешностью соответственно. Используя несложное математическое преобразование, в частности формулу нахождения нормы вектора по заданным координатам $R_i = \sqrt{(x_i)^2 + (y_i)^2}$, формулу для нахождения угла между двумя

соответствующими векторами $\alpha_i = \arctg\left(\frac{y_i}{x_i}\right)$, формулу скалярного произведения сигналов $SP_j = ((S1_j)_0 \cdot (S2_j)_0) + ((S1_j)_1 \cdot (S2_j)_1)$, построим амплитудно-фазовую модель изображения (рис. 2).

Рис. 2. Плоская амплитудно-фазовая модель изображения графического пароля группового точечного объекта (R_i координаты точек, которые задают графический пароль, A_i координаты точек, которые введены пользователем)

Будем принимать введенный пароль за сигнал. Используя формулу для нахождения нормы сигнала, найдем их суммарную норму и разделим на их количество. $norma(signal) = \sum_{n=1}^N (S_n)_0^2 + (S_1)_1^2$ Таким образом, мы нашли две нормы сигнала.

a – разрешение экрана 320x480, b – разрешение экрана 540x960, c – разрешение экрана 720x1280

Рис. 3. Графики зависимости кол-ва точек n от коэффициента точности k

Далее проведем их сравнение, для этого используем ортонормированный базис векторов

$$sp(S_1, S_2) = \sum_{n=1}^N (S1_n)_0 \cdot (S2_n)_0 + (S1_n)_1 \cdot (S2_n)_1$$

Далее будем искать зависимость количества точек от точности введения. Запишем данные в массив и построим график зависимости количества точек от точности. Аналогичный эксперимент проведен с экранами больших разрешений, построен график зависимости количества точек от точности ввода. На рис. 3. представлено сравнение трех экспериментов, графики объединены в одной плоскости.

Видим, что на телефоне с малым разрешением кривая ярче выражена, это связано с тем, что погрешность ввода на маленьких экранах намного больше, чем на экранах средних размеров. Напомним, что мы имеем дело не с одинарными точками, а с множеством точек, т.е. каждая из восемнадцати точек представляет собой множество или, проще говоря, некую окружность. Чтобы избежать данной погрешности нужно масштабировать область точек для ввода пароля, чтобы зависимость оставалась постоянной. Так же отметим, что без масштабирования на телефонах с HD экраном и выше будет наблюдаться та же зависимость что и на экране 320x480.

Точность позиционирования у каждого устройства разная, во-первых, причиной этому способствует разное разрешение экрана и размер пикселя, во-вторых каждый производитель использует различные материалы для создания экрана, все эти критерии напрямую влияют на точность позиционирования. Несомненные плюсы данного метода заключаются в простоте ввода пароля, довольно надежной защиты устройства от несанкционированного доступа. Метод позволяет осуществлять ввод пароля как стилусом, так и пальцем. Так же данный метод не требует долгих и сложных вычислений, следовательно, не будет оказывать сильной нагрузки на процессор устройства пользователя. Так же данный алгоритм требует лишь геометрического соотношения между точками, т.е. пользователь сможет пользоваться вспомогательным изображением для ввода пароля, при этом, не снижая уровень защиты устройства.

Список литературы:

1. Sobrado Leonardo, J.C. Birget. Graphical passwords // The Rutgers Scholar. 2002. Vol. 4.
2. Wiedenbeck S., Waters J., Birget J.C., Brodskiy A., Memon N. Authentication using graphical passwords: Basic results // Human-Computer Interaction International, 2005.
3. Dirik A.E., Memon N., Birget J.C. Modeling user choice in the PassPoints graphical password scheme // Symposium on Usable Privacy and Security (SOUPS). July 2007. Carnegie-Mellon Univ., Pittsburgh.
4. Шокарев А.В., Шелупанов А.А. Использование компьютерной стеганографии для аутентификации пользователей // Материалы докладов Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых. Томск: Томский государственный университет систем управления и радиоэлектроники, 2006. С. 173-176.
5. Безмальный В.В., Нефедов Д.А. Применение графического пароля в Windows 8 // Windows IT Pro/RE. 2012. №10.
6. Евдокимов А.О., Лугов Д.Я., Грибин М.А., Смирнов Г.Ф. Исследование устойчивости графического пароля // Fundamental and applied sciences today V. Vol. 1. North Charleston, SC, USA 29406. 2015. Pp. 130-136.

7. Евдокимов А.О., Лугов Д.Я., Грибин М.А. Модель изображения групповых точечных объектов как основа реализации графических паролей для обеспечения безопасности компьютерных систем // Интеграция мировых научных процессов как основа общественного прогресса. №21. Ч. 2. Казань: Общество науки и творчества, 2015. С. 77-83.
8. Фурман Я.А., Кревецкий А.В., Передреев А.К. и др. Введение в контурный анализ и его приложения к обработке изображений и сигналов. М.: Физматлит, 2002.
9. Фурман Я.А., Кревецкий А.В., Роженцов А.А. и др. Комплекснозначные и гиперкомплексные системы в задачах обработки многомерных сигналов. М.: Физматлит, 2004.
10. Роженцов А.А., Евдокимов А.О., Григорьев А.В. Распознавание плоских изображений групповых точечных объектов при наличии ошибок обнаружения // Известия высших учебных заведений. Приборостроение. 2006. Т. 49. №4. С. 59-64.

© 2015, Евдокимов А.О., Грибин М.А., Смирнов Г.Ф.
 Модель реализации безопасности информации на
 основе изображений точечных отметок

© 2015, Evdokimov A.O., Gribin M.A., Smirnov G.F.
 The model implementation of information security
 based on the image of point marks