УДК 681.3

Дослідження/

Євген Завальнюк
Заступник начальника відділу інформаційних технологій центру інформатизації управління Національного банку у Вінницькій області, кандидат технічних наук

Простота і захищеність графічного пароля для користувача

У наш час більшість громадян має паролі. Вони застосовуються для ідентифікації користувача в різних комп'ютерних системах та мережах. Паролями послуговуються як звичайні користувачі, так і адміністратори зі спеціальними правами доступу. Захищеність пароля в кожній організації чи установі визначена політикою інформаційної безпеки. Проте жодна політика безпеки в застосуванні паролів не має на меті зменшення впливу людського чинника, тобто не пропонує самому користувачеві методику збереження персонального пароля не будь-де, а лише у власній пам'яті. Тому є проблема сумісності двох складових цього процесу. З одного боку – легкості запам'ятовування пароля, а з другого – необхідності високого рівня його захищеності від перехоплення і достатньої складності для запобігання його відтворення.

Nowadays, the majority of users have got passwords. The ones are used to identify a user in various computer systems and networks. Both common users and administrators with special access rights use passwords. Password protection in each organization or institution is determined by the information security policy. But, none of password security policies is aimed at diminution of the human factor influence i.e. it makes no provision for the procedure of personal password saving somewhere but in one's own mind. That is why there is a problem of compatibility of both components of the process viz. on the one hand, a password should be easy kept in mind, and on the other hand, it should be highly protected from interception and replay attack.

Ключові слова: пароль, політика безпеки, захист, символьний пароль, графічний пароль, стереограма.
Key words: password, security policy, protection, character password, graphical password, stereogram.

Оскільки рівень захищеності пароля в кожній організації чи установі визначений політикою інформаційної безпеки, детальні складові цих персональних електронних ключів доступу можуть бути різними, але всі вони зазвичай мусять відповідати таким вимогам:

– пароль має складатися як мінімум із восьми знаків;

– пароль не повинен відтворювати загальновідомі персональні дані самого користувача – бути схожим на його ім'я та прізвище, дату народження тощо;

– пароль не може бути словом, яке міститься в будь-якому словнику;

– пароль необхідно створювати на основі комбінації верхніх та нижніх регістрів літер і спеціальних символів;

– упродовж певного періоду шість останніх паролів не повинні повторюватися.

СИМВОЛЬНИЙ ПАРОЛЬ: ВАРІАНТИ ЗАХИСТУ

Багато років тому користувачі персональних комп'ютерів (ПК) винайшли методи створення псевдовипадкового пароля. Найпростіший із них створюється так: необхідно взяти слово і виконати з ним певні дії. Розглянемо слово "Android" як приклад. Користувачі можуть створити на його основі такі паролі: "AnDrOiD" (верхні і нижні регістри, що чергуються), "diordnA" (змінити напрямок написання, використавши зворотний варіант), "roidAnd" (перетасовувати склади), "A2d4o6d8" (поєднати цифри і літери). Проте надмірне ускладнення пароля призводить до проблем із його запам'ятовуванням самим користувачем.

Користувачі, які мають на своєму комп'ютері клавіатуру з кириличним або латинським шрифтом, використовують паролі на рідній мові з посимвольною заміною на латинські символи. Наприклад пароль "Пролісок" латинським шрифтом буде таким: "Ghjkbcjr". Цей спосіб дещо збільшує захищеність пароля, але він фактично безпорадний проти атаки з використанням розширеного словника, який має спеціальні правила транслітерації. Адже пари букв "кирилиця/латинь" на клавіатурах однотипні: "й/q", "я/z" тощо. Отже, цей метод створення пароля не становитиме великих проблем для злому електронного ключа у процесі підбору слова із словника зі зміною алфавіту. Практика застосування складних паролів користувачами свідчить про те, що останні, як правило, або просто забувають такі паролі, або прагнуть їх зберегти "на пам'ять" у записниках, настільних календарях,

мобільних телефонах. Ясно, що захищеність паролів після таких записів зводиться нанівець.

Спробою допомогти користувачеві була ідея створювати пароль за першими літерами слів із будь-якого знайомого речення. Наприклад, пароль із речення "Еней був парубок моторний і хлопець хоч куди козак" буде набір букв "Ебпміххкк". Звісно, такого "слова" немає в жодному словнику. Але цьому способу притаманні й певні недоліки: в пам'яті необхідно тримати все речення, а при зміні кількох паролів, котрі не повинні повторюватися протягом певного часу, необхідно мати неабиякі літературні здібності.

Зважаючи на всі недоліки таких електронних ключів, постала необхідність вирішити проблему поєднання високого рівня захищеності пароля (убезпечення від перехоплення та складності відтворення) і простоти його запам'ятовування користувачем.

ГРАФІЧНИЙ ПАРОЛЬ: ЧИ ТАКЕ МОЖЛИВЕ?

У більшості комп'ютерних операційних систем багато років тому відбувся перехід на графічний інтерфейс. А принцип введення паролів у цих системах досі залишається символьним! Користувачі навіть не уявляють собі, що пароль може бути не алфавітно-цифровим. Оскільки люди живуть і працюють у сучасному інформаційно-технологічному середовищі, в якому сенс і значення людського зору є домінуючим для більшості дій, наш мозок спроможний до обробки і зберігання великої кількості графічної інформації. Більшість користувачів вважає, що дуже важко запам'ятати послідовність пароля з десяти літер. Водночас кожен із нас легко запам'ятовує обличчя багатьох людей, місця, які ми відвідали, або об'єкти, які ми бачили. Ці графічні дані в електронному вигляді мають мільйони байтів інформації та забезпечують великий потенціал для унікальності вибору пароля. Саме тому так звані графічні паролі є практичнішими для людини, водночас вони значно підвищують рівень інформаційної безпеки та захищеності даних користувача персонального комп'ютера [1].

Розгадати графічний пароль за допомогою будь-якого словника нереально – частково завдяки великій кількості можливих варіантів пароля, але переважно тому, що немає жодних доступних для пошуку словників для графічної інформації. Також важко реалізувати автоматизацію морфологічного розгадування. І це при тому, що ми можемо впізнати обличчя знайомої людини менш як за одну секунду. Комп'ютеру для обробки мільйонів байтів інформації у процесі підбору варіантів графічного відповідника до оригінального зображення (пароля) необхідна значна кількість часу.

На основі цих фактів інженери-програмісти винайшли варіант захисної системи для надійної та відносно простої аутентифікації (перевірки на відповідність) користувача. Найцікавіше і найкорисніше в ній те, що запам'ятати і відтворити пароль не зможе навіть той, хто перебуває безпосередньо поряд із монітором користувача. Новий спосіб введення графічного пароля надзвичайно надійний – хакерам не допоможе навіть клавіатурний перехоплювач (сніфер).

ПАРОЛЬ У НОВИХ СИСТЕМАХ – ЦЕ НЕ НАБІР СИМВОЛІВ, А ГРАФІЧНЕ ЗОБРАЖЕННЯ

Наприклад, користувач повинен за допомогою комп'ютерної мишки позначити чотири точки (в межах десяти пікселів зображення) на великій фотографії пейзажу. Ви можете завантажити в програму будь-яку фотографію. Найголовніше – така особливість: це має бути звичний на вигляд (стандартний) пейзаж із безліччю потенційно цікавих місць. Коли користувач створює пароль, він обирає чотири (або більше) точки, які йому дуже легко запам'ятати, наприклад, конкретне дерево, човен, будівля, надувна куля (див. схему 1).

Такий пароль, що зберігається в пам'яті людини, навіть описати простими словами буде складно. Це графічний пароль, який ґрунтується на спогадах і зорових асоціаціях. Але ці спогади дуже надійні. Тим паче, що зображення може бути місцем або пейзажем, знайомим лише для конкретного користувача. Підібрати "відмичку" для такого пароля вельми складно. Навіть важко уявити, скільки може бути на зображенні робочого стола комп'ютера варіантів комбінацій із набору лише в чотири точки! Також чудово й те, що самому користувачеві незручно записувати чи відтворювати такий графічний пароль у записнику.

Є спосіб введення пароля, який

Схема 1. **Графічний пароль, створений за допомогою кількох точок на зображенні заставки робочого стола комп'ютера користувача**

Схема 2. **Графічний пароль, створений за допомогою трьох точок і трикутника з переліку випадкових "іконок" на зображенні заставки робочого стола комп'ютера користувача**

має ще цікавіші властивості. Навіть якщо при введенні цього пароля за вашою спиною стоятиме інша особа, "випадково" запам'ятати і відтворити всі "кліки" вона ніколи не зможе. Аналогічна ситуація – якщо користувач перебуває в зоні дії камери системи відеоспостереження. Переглянувши відеозапис, ніхто не зможе відновити такий пароль. Особливість цього пароля полягає в тому, що при його створенні необхідно вибрати і запам'ятати десять "іконок" щонайменше із сотні можливих. Ці "іконки" вельми різноманітні. Уявіть – за необхідності введення пароля система видає на екран одразу величезне панно з "іконок", перемішаних випадковим чином. Серед них обов'язково будуть три "ваші". Їх необхідно подумки з'єднати лініями (таким чином користувач вибудує трикутник) і "клікнути" мишкою в будь-якій точці усередині цієї фігури – див. схему 2.

При цьому "іконки" одразу ж перебудовуються, перемішуються. Деякі з них зникають, інші – додаються. І серед усього цього хаосу користувач за допомогою зорової пам'яті одразу бачить "свої" значки з тих десяти, які він попередньо обрав (не обов'язково ті, котрі були на екрані щойно). Знову користувач подумки з'єднує їх у геометричну фігуру і натискає курсор у будь-якому місці, але лише в межах цієї геометричної фігури. І так десять разів поспіль. Лише після десяти таких етапів машина однозначно ідентифікує "іконки", які користувач тримає в пам'яті, обираючи місце для натискання курсором підтвердження пароля. Будь-який спостерігач за жодних умов не зможе запам'ятати чи вгадати ваш графічний пароль, навіть безпосередньо контролюючи ваші дії. При цьому забезпечується високий рівень секретності. Як наголошують дослідники, "якщо ви маєте чимало різних зображень, і якщо ви повинні пройти такий тест кілька разів поспіль, усі можливі комбінації "іконок" становитимуть мільярди варіантів" [2].

На жаль, ці два методи є дещо складними для використання, адже:

– не кожен користувач зможе візуально на екрані з'єднати лініями "іконки", особливо якщо вони будуть розташовані далеко одна від одної;

– якщо пропонувати користувачеві до десяти разів обирати варіанти в новому зображенні, то за наявності за спиною камери відеоспостереження це не збільшує захищеність пароля, а, навпаки, зменшує його. Адже в цьому випадку при перегляді відеозапису виникає можливість провести аналіз статистики розташування і наявності певних "іконок" на екрані. Звісно, якщо у хакера для цього є достатньо часу.

СТЕРЕОПАРОЛЬ – НЕТРАДИЦІЙНИЙ І НАДІЙНИЙ ЗАХИСТ

Оскільки описані вище графічні "ключі" мають деякі недоліки, фахівці розробили ще один оригінальний метод введення графічного пароля, який не має таких вад, але при цьому потребує від користувача певної уваги.

Даний спосіб полягає у використанні стереограми як базового зображення для графічного пароля. Як відомо, стереограма побудована таким чином, що користувач, аби побачити її без спотворень, повинен перебувати прямо перед екраном монітора. При цьому його очі повинні знаходитися на певній фокусній відстані від поверхні екрана монітора [3]. Сама стереограма як базис для графічного пароля створюється заздалегідь за участі самого користувача, тобто в ролі тривимірних орієнтирів для створення "ключа" необхідно обрати відомі лише цьому працівникові об'єкти. Схема введення такого пароля може бути будь-якою з описаних вище, але з меншим числом точок на екрані (див. схему 3).

Маємо стереопароль. Основна його перевага така: перебуваючи під непрямим кутом і на певній відстані від екрана монітора, сторонній спостерігач – чи то колега користувача, чи оператор камери відеоспостереження – не зможе побачити на екрані нічого, крім яскравого візерунка.

Можливим недоліком стереопароля є той факт, що користувач повинен буде навчитися фокусувати свій погляд на стереозображенні. Але високий рівень захищеності такого особистого пароля для персонального комп'ютера нівелює всі його незначні недоліки.

ГРАФІЧНИЙ ПАРОЛЬ – У КОЖЕН ДІМ

Ідея запровадження графічного пароля набула нового практичного значення після виходу нової операційної системи "Майкрософт Віндовз 8" (Microsoft Windows 8) у 2012 році. Інтерфейс цієї операційної системи насамперед орієнтований на планшетні персональні комп'ютери, тому гра-

Схема 3. **Графічний пароль, створений за допомогою трьох точок на стереограмі зображення заставки робочого стола комп'ютера користувача**

Схема 4. **Послідовність дій користувача на зображенні заставки робочого стола комп'ютера в операційній системі "Віндовз 8"**

фічні паролі в них пропонуються користувачам уже як штатна опція. Насамперед вона призначена для власників сенсорних екранів і забезпечує зручне використання графічного пароля для доступу до пристрою, адже зробити це вони можуть значно швидше, ніж шляхом введення довгих символьних паролів. Проте власники стаціонарних ПК і ноутбуків, оснащених мишкою, також можуть скористатися цією цікавою функцією.

Перш ніж її використовувати, необхідно знайти відповідне зображення і завантажити його в систему. Наступний крок – обрати панель "Користувачі", а потім панель "Створити графічний пароль". Для вашого облікового запису завчасно має бути створений звичайний символьний пароль, якщо його немає – необхідно створити, відтак з'явиться посилання на створення графічного "ключа".

Після цього користувач має створити три комбінації рухів – дій на обраному зображенні. Зробити це потрібно двічі, як і з символьним паролем – один раз для завантаження і другий – для підтвердження пароля. Дуже важливо при цьому запам'ятати напрям і послідовність рухів (маніпуляцій мишкою), – чи це лінія або круговий рух, а також їх позиційне розташування на екрані монітора і місця "кліків" (див. схему 4).

Після того, як користувач обрав і завантажив зображення для створення на його основі пароля, на ньому система формує сітку координат. Довша сторона зображення розбивається на 100 сегментів, потім розбивається коротка сторона і також створюється сітка, на якій фіксуються комбінації рухів. Окремі точки маніпуляцій визначаються їх координатами на сітці. Для лінії запам'ятовуються початкові та кінцеві координати і їх порядок, використаний для визначення напряму малювання лінії. Для кола система запам'ятовує координати його центра, радіус та напрямок руху по колу. Для простого "кліка" запам'ятовуються координати місця дотику курсором. При спробі виконання реєстрації за допомогою графічного пароля введені на екрані маніпуляції порівнюються з еталонним зразком, збереженим при налаштуванні графічного пароля. При цьому аналізується різниця між кожним рухом і автоматично приймається рішення про успішність перевірки достовірності на основі сумісності з еталоном або виявленої кількості помилок. Якщо маніпуляція неправильна (наприклад, має бути коло, а замість нього вводиться лінія), перевірка достовірності ключа буде заблокована. Якщо ж види таких рухів, їх порядок введення і напрями збігаються, то система аналізує, наскільки вони відповідають еталонним, і надає доступ користувачу до ПК.

Аби визначити необхідну кількість маніпуляцій для гарантування високого рівня безпеки графічного пароля, необхідно порівняти його з іншими способами перевірки достовірності. Наприклад, із ПІН-кодом і символьним паролем. Аналіз кількості унікальних комбінацій ПІН-коду простий. У ПІН-коді, який має чотири розряди (із десятьма незалежними можливими значеннями в кожному з них), може бути 10 000 унікальних комбінацій. Аналіз текстових паролів може бути спрощений, якщо передбачити, що паролі – це послідовність знаків, яка складається з рядкових літер (їх 26), прописних літер (ще 26), цифр (10) і символів (10). У простому випадку, коли пароль складається лише з n строкових літер, можливі 26n перестановок. Якщо пароль може мати довжину від 1 до n знаків, кількість перестановок буде такою: пароль, що складається з восьми літер, має 208 млрд. можливих комбінацій, що для більшості користувачів здається достатньою кількістю. Кількість комбінацій пароля лише з декількох маніпуляцій курсором і знаків наведено в таблиці.

Як бачимо, використання лише трьох маніпуляцій забезпечує значну кількість унікальних комбінацій і таку ж надійність, яку має пароль із п'яти – шести випадково обраних знаків. Слід пам'ятати, що графічний пароль є додатковим способом ідентифікації або реєстрації в системі, тобто він лише доповнює символьний пароль, а не замінює його! Тому якщо користувач усе-таки забуде графічну комбінацію, то завжди матимете резервну можливість увійти до свого ПК, ввівши символьний пароль. Водночас варто врахувати, що аутентифікація в операційній системі "Віндовз 8" можлива і за допомогою облікового запису сервісу авторизації Майкрософт Лів Ай.Ді. (Live ID) [5], біометричної аутентифікації, а також ПІН-коду.

У попередніх версіях операційних систем пароль на персональних комп'ютерах зберігався у файлі Ес.Ей. Ем. (SAM). Відповідно для зламу цього пароля зловмисникові потрібний був фізичний доступ до системи та привілею "Систем" (SYSTEM). Що ж маємо нині? Операційна система "Віндовз 8" не є цілком безпечною – потенційному зловмисникові буде нескладно зламати систему, тому що в механізмі аутентифікації з'явилися нові слабкі ланки. Природно, хакерові необхідно буде просто знайти найвразливішу з них. Наприклад, реєстрація в системі за допомогою сервісу авторизації Майкрософт. Для кінцевого користувача це, безперечно, зручно: якщо він забув пароль, то може зайти на сайт Live ID з іншого комп'ютера, скористатися послугою зміни пароля – і зареєструватися на своєму комп'ютері з новим паролем.

Але, поза всяким сумнівом, ця функція створює нові "шпарини" для дій зловмисників. Доки користувач працюватиме за іншим комп'ютером, пароль до сервісу авторизації Майкрософт може зберігатися разом з останніми паролями в браузері тощо. І що найцікавіше, пароль Live ID, ПІН-код, графічний і біометричний паролі – всі вони використовуються для

Таблиця. **Порівняння можливих комбінацій пароля з різних наборів – комбінацій знаків і маніпуляцій курсором**

Складність	10-розрядний ПІН-код	Пароль із набору знаків a-z	Пароль зі складнішого набору знаків	Графічний пароль із декількох маніпуляцій
1	10	26	–	2 554
2	100	676	–	1 581 773
3	1 000	17 576	81 120	1 155 509 083
4	10 000	456 976	4 218 240	612 157 353 732
5	100 000	11 881 376	182 790 400	398 046 621 309 172
6	1 000 000	308 915 776	7 128 825 600	
7	10 000 000	8 031 810 176	259 489 251 840	
8	100 000 000	208 827 064 576	8 995 627 397 120	

Джерело: [4].

додаткового зберігання і шифрування звичайного пароля для реєстрації в системі. Ці ланки пов'язані зі звичайним паролем. Якщо користувач вибрав аутентифікацію за графічним паролем, то, по суті, сам графічний пароль застосовується як "ключ" для зберігання і шифрування звичайного пароля. Таким чином, окрім файла Ec.Ай.Ем., звичайний пароль зберігатиметься ще в одному місці. Якщо користувач вибрав реєстрацію з Live ID, то звичайний пароль (символьний, але зашифрований за допомогою цього сервісу авторизації Майкрософт) зберігатиметься в іншому місці. Тобто дізнавшись пароль Live ID, зловмисник зможе відновити і оригінальний текстовий пароль.

Вочевидь, що на планшетних ПК зручно малювати лінії й окреслювати кола пальцем. Але ці графічні елементи буде значно важче повторити комп'ютерною мишкою. Користувач матиме десятки варіантів з'єднання прямою лінією двох відомих йому точок на екрані монітора. Лише тому, що він не зможе провести відносно пряму лінію мишкою, введення графічного пароля ускладнюється. У більшості випадків ця лінія виходитиме кривою, яка кожного разу буде різною. Аналогічна ситуація з колами та іншими фігурами. Тому для стаціонарного ПК у графічному паролі доцільно використовувати лише декілька точок, "клікнувши" по них курсором мишки в необхідній послідовності, як описано вище.

ВИСНОВКИ

У наш час одна з інноваційних можливостей комп'ютера – новий спосіб виконання авторизації та входу до операційної системи. Більшість користувачів ПК не хоче ускладнювати цю процедуру при запуску системи, проте для працівників банків такий легковажний підхід до інформаційної безпеки просто неприпустимий! Отже, необхідно надати користувачу швидкий і зручний механізм доступу до системи ПК, який водночас був би безпечним і надійним.

Описаний спосіб введення графічного пароля буде корисним для співробітників банків із підвищеною функціональною відповідальністю, тобто для адміністраторів, аудиторів, менеджерів, співробітників служб безпеки та на тих робочих місцях, де наявність камери відеоспостереження передбачена технологічними вимогами – тобто для касирів, охоронців. Також доцільне використання такого пароля для клієнтів банкоматів із вбудованим тачпадом (touchpad), де присутність сторонніх осіб є постійною.

При використанні графічного пароля у користувача формуватиметься сучасний погляд на проблему інформаційної безпеки, а людський чинник у методиці його запам'ятовування і використання буде зведено до мінімуму. Нові способи аутентифікації насамперед мають сприяти зростанню зручності роботи користувача з ПК. ❑

Література

1. Blonder G. Graphical Passwords. – US patent №5 559 961. – 1996.

2. Leonardo Sobrano. Jean-Camille Birget. Graphical passwords // The Rutgers Scholar. – An Electronic Bulletin of Undergraduate Research. – 2002. – vol. 4.

3. Завальнюк Е. А. Нарисуй мне пароль // PC World. – 2006. – № 6. – С. 110–113.

4. Steven Sinofsky. Выполнение входа с помощью графического пароля. – [Електронний ресурс]. – Режим доступу: http://blogs.msdn.com/b/b8_ru/archive/2011/12/22/signing-picture-password.aspx.

5. Безмалый В., Нефедов Д. Применение графического пароля в Windows 8 // Windows IT Pro/RE. – 2012. – № 10. – С. 45–47.

Нотатки з дискусійного клубу/

Чи може бізнес бути чесним?

В Університеті банківської справи Національного банку України відбулося засідання дискусійного клубу на тему "Справедливий бізнес: чи може бізнес бути чесним?" Науковці, викладачі, студенти Львівського, Черкаського та Харківського інститутів банківської справи УБС НБУ, банкіри-практики, експерти і представники духовенства в гарячих дискусіях висловили свої погляди на проблему та підходи до її розв'язання.

The round table meeting "Fair business: can business be honest?" was held in the NBU Banking University. During the discussion, scientists, teachers, students of the Lviv, Cherkasy and Kharkiv banking institutes of the NBU Banking University, bankers-practitioners, experts and clergy representatives exchanged their views on the question and discussed approaches to its solving.

Чесність, порядність і справедливість є основними категоріями моральності й людяності. Проте для отримання прибутку і розвитку бізнесу необхідно також бути освіченим, цілеспрямованим, наполегливим, винахідливим, комунікабельним. Як поєднати всі ці чесноти і досягти успіху? Чи діють у сучасних умовах принципи етичного бізнесу та чи може бути він справедливим?

Студентки Інституту магістерської та післядипломної освіти УБС НБУ ***Ірина Дрозд*** і ***Юлія Шубіна***, представляючи доповідь "*Справедливий бізнес є чесним бізнесом*", наголосили, що в Кодексі етики Європейської бізнес-асоціації визначено принципи ведення чесного бізнесу. Компанії мають сприяти поширенню правил чесної та прозорої конкуренції, некорупційних форм ведення бізнесу, дотримуватися чинного законодавства, поважати права інтелектуальної та інших форм власності, права працівників, намагатися розвивати конструктивні взаємозв'язки між місцевими та центральними органами влади, поважати інтереси місцевих громад і визнавати важливість захисту навколишнього середовища. Тобто, іншими словами, бізнес необхідно здійснювати без хабарів, виплат заробітної плати у конвертах,