УДК 378.14.014.13
М.І.Огурцов
Відкритий міжнародний університет розвитку людини «Україна»
Інститут персоналізації технічних систем та захисту інформації

ПЕРСОНАЛІЗАЦІЯ WEB-СЕРВІСІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ ДОСТУПНОСТІ У НАВЧАННІ

Робота присвячена задачі безпечного доступу студентів та викладачів до захищених Web-сервісів з незахищених комп'ютерів. Розглянуті основні можливості реалізації систем контролю доступу до захищених Web-сервісів в цьому випадку (онлайн-генератори паролів, менеджери паролів тощо). Сформульовано основні вимоги до систем парольного захисту. На основі проведених досліджень створено онлайн-генератор надійних паролів. Проведено порівняльний аналіз створеного генератору з іншими онлайн-генераторами паролів, виявлено, що жоден з конкуруючих продуктів не дає можливості створення повторюваного паролю для безпечної автентифікації користувача на небезпечному комп'ютері.

Ключові слова: *Web-сервіс, онлайн-генератор, автентифікація.*

Постановка проблеми. В процесі діяльності будь-якого студента чи викладача може виникнути ситуація, коли потрібен терміновий доступ до захищених web-сервісів наприклад, електронної пошти, що призводить до необхідності використання обладнання чужих комп'ютерів чи телекомунікаційних пристроїв, скажімо, у комп'ютерному клубі чи університетській аудиторії. В цьому випадку необхідні рішення проблеми безпечної ідентифікації та автентифікації користувача [1], засновані виключно на Web-сервісах і не пов'язані з якимись конкретними апаратними засобами. На жаль, на сьогоднішній день відсутні наукові дослідження можливих розв'язків даної проблеми, в багаточисельних публікаціях в галузі захисту інформації [2-6] просто рекомендують не використовувати чужі небезпечні комп'ютери для введення автентифікаційних даних для доступу до захищених ресурсів. Але що робити, якщо іншого вибору немає?

Постановка завдання. Яким чином користувачеві можна отримати доступ до потрібних ресурсів у цьому випадку? Без застосування апаратних засобів персоналізації єдиним доступним способом персоналізації доступу (науковий напрям по створенню комплексів захисту інформації від несанкціонованого доступу з гарантованою стійкістю [7]) до web-сервісів стає застосування парольного захисту. Але, як було доведено в [1-2], парольний метод персоналізації має ряд значних недоліків. Якщо захиститись від підглядання пароля зловмисниками можливо, виконуючи його введення з обережністю та контролем оточення, то складність пароля повинна залишатись високою, незважаючи на метод його введення. Складний пароль є важким для запам'ятовування, тому користувачі або намагаються не використовувати такі паролі, або зберігають їх у доступному місці у відкритому вигляді, що несе значний ризик компрометації пароля. Також часто обирають паролем своє ім'я, якесь слово чи комбінацію слів. Такі паролі легко підбираються зловмисниками. Для вирішення даної проблеми було розроблено генератор надійних паролів, який розміщено в мережі Інтернет у вільному доступі [8] (див. рис. 1). Будь-хто може застосовувати його просто в якості генератора надійних паролів. Також у даній роботі було визначено основні вимоги до надійності паролів, перевірено відповідність створеного генератора цим вимогам та проведено його порівняльній аналіз з іншими існуючими генераторами паролів.

Принцип роботи Web-генератору надійних паролів: в полі «Простий пароль» вводиться простий пароль користувача. Після цього на зображенні ключа, що розташоване нижче, слід набрати комбінацію ключа-ідентифікатора, натискаючи на його сегментах: при натисканні положення сегмента змінюватиметься на протилежне. Третє поле Web-генератора задає потрібну довжину створюваного пароля. Після того, як усі параметри задані, слід натиснути кнопку «Генерувати». В результаті буде згенеровано потрібний пароль. Слід мати на увазі, що це буде пароль без спеціальних символів, призначений саме для Web-сервісів. Web-генератор надійних паролів не орієнтований на застосування для локальних сервісів користувача, використовує при роботі мережеві стандарти передачі даних і тому при генерації складного пароля формує його лише на основі латинських букв та цифр. Значна частина Web-сервісів не підтримує паролів, що включають спецсимволи чи українські літери.

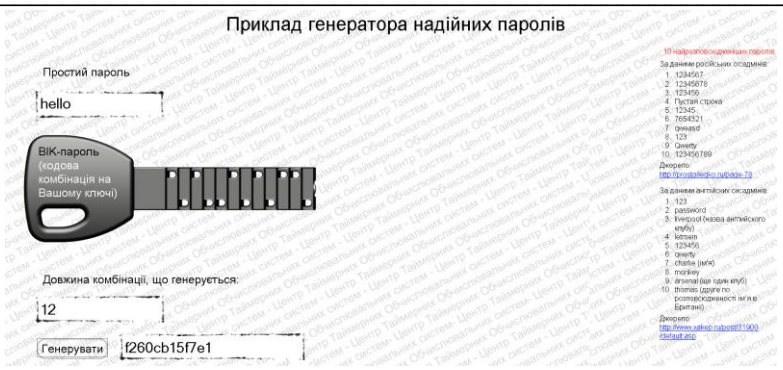

Рис. 1 – Web-генератор надійних паролів

В правій частині Web-генератора надійних паролів приведені найбільш часто застосовувані паролі, причому окремо наведені російські та англійські результати досліджень цього питання. Більшість паролів, які використовуються в світі, належать до списку з декількох десятків найбільш поширених паролів. Саме ці паролі в першу чергу випробовують зловмисники, коли хочуть отримати доступ до захищених паролем сервісів. Використовувати їх в якості свого пароля вкрай небезпечно і не рекомендується. Навіть при потужному алгоритмі шифрування пароль "мама" розкривається за 1 секунду. Також не варто ставити паролем свій день народження.

Скомпрометовані паролі слід змінювати відразу. Скомпрометованим паролем вважається пароль, який записаний на папірець на моніторі або носиться в портмоне, а також ті паролі, які, окрім вас знає хоча б ще одна людина. Більшість фахівців і адміністраторів регулярно радять або примушують змінювати паролі, бо паролі з часом компрометуються різними способами- від банальної крадіжки пароля, до помилки користувача, коли він використовує робочий пароль для входу у всі форуми і чати. Регулярна зміна паролів призводить до того, що користувачі записують їх на папірцях і телефонах, візитних картках і просто на моніторі, що також призводить до компрометації паролів.

Вимоги до парольного захисту:

1. Пароль не слід зберігати у відкритому вигляді (в текстовому файлі, в Інтернеті, або просто записаним на папірці).

2. Паролі не повинні складатись лише з цифр, простих комбінацій (наприклад, послідовного набору) цифр чи літер, зі словарних слів на будь-якій мові, навіть із доданою наприкінці цифрою чи спеціально внесеними помилками. Особливо не слід використовувати в якості пароля дати народження, імена та клички тварин.

3. Не слід дозволяти стороннім програмам діставати доступ до паролів. Якщо яка-небудь програма, сайт, поштове повідомлення і т.п. просить вас ввести або вислати пароль, то у жодному випадку не робіть цього. Доступ до паролів повинні мати тільки програми, для яких призначені ці паролі.

4. Не слід використовувати один пароль на всіх Інтернет сервісах. Якщо один пароль буде зламаний, то доступ до решти сервісів буде закритий іншими паролями.

5. Не слід використовувати "секретні питання", відповіді на які легко взнати або підібрати.

6. Використовуйте всі символи клавіатури, включаючи цифри і символи, що вводяться за допомогою клавіші Shift.

Якщо так трапилося, що біля вас виявилася людина, а вам необхідно набрати пароль на клавіатурі, то ви можете зробити так:

1. Спочатку наберіть явно невірний пароль.

2. Ще раз наберіть явно невірний пароль.

3. Наберіть вірний пароль.

Така послідовність збентежить людину, яка знаходиться поряд з вами, оскільки, якщо вона дійсно підглядає, що ви набираєте, то вперше вона буде дуже уважна, і добре запам'ятає набраний варіант. А ось далі її реакція і пам'ять ослабляться. Це дуже знизить її шанси підглянути і запам'ятати ваш пароль. У таких випадках також добре допомагає «сліпий» набір пароля. Це коли ви дуже швидко вводите досить складний пароль.

У будь-якому випадку є вірогідність, що ваш пароль буде перехоплений за допомогою клавіатурного шпигуна – спеціальної програми для перехоплення набраних символів. Ці програми записують все, що набрано на клавіатурі і в яких саме програмах це було набрано. Далі неважко

розібратися, який логін і пароль і для якої системи ви вводили. На цей випадок ось декілька рекомендацій, як заплутати клавіатурного шпигуна.

Перш ніж безпосередньо набрати пароль в потрібній програмі, слід в іншому вікні набрати і скопіювати в буфер частину вашого пароля. А потім вставити цей текст в потрібне поле і ввести частину пароля, що залишилася.

Не слід набирати логін і пароль водночас, а по частинах, перемикаючись в інші вікна і там залишаючи якісь натиснення на клавіатурі.

Такі маніпуляції буде важко розпізнати в файлах цих програм шпигунів. І зловмиснику буде важче за цими даними відновлювати ваш пароль. Дуже вірогідно, що він невірно відновить ваш пароль і після першої невдалої спроби його застосувати він кине цю справу.

Альтернативою застосування Web-генераторів надійних паролів може вважатися менеджери паролів [1]. Наприклад, менеджер паролів Password Commander генерує, зберігає паролі і може працювати із змінних носіїв, таких як USB flash диски і т.п. При використанні менеджерів паролів не забувайте: відходячи від комп'ютера (навіть на декілька хвилин), обов'язково завершіть програму або включіть хранитель екрана – в Windows натискайте [WIN]+[L] або використовуйте вбудоване блокування програми; забезпечте захист зовнішніх носіїв; не забувайте робити резервну копію бази даних паролів. Але повноцінною заміною Web-генераторів надійних паролів вони служити не можуть, бо по-перше, не завжди бувають при користувачеві у потрібний момент (за терміновою необхідністю немає часу їхати за флеш-носієм з менеджером паролів), а по-друге, багато комп’ютерів у місцях загального користування (комп’ютерні клуби, комп’ютерні бібліотеки тощо) задля підвищення рівня безпеки не підтримують підключення користувачами периферійних пристроїв, включаючи флеш-носії. Звичайно, можна просто розмістити свій складний пароль в мережі Інтернет, але у випадку вільного доступу будь-хто зможе скористатись цим паролем, якщо ж доступ обмежувати, то для отримання свого пароля слід знову ж таки ввести надійний пароль. Таким чином, можна зробити висновок, що єдиним надійним та універсальним засобом персоналізації користувача на потенційно небезпечному комп’ютері при отриманні доступу до захищених Web-сервісів є застосування онлайн-генератора паролів. Він відповідає усім вимогам, висунутим до систем парольного захисту. Проведемо порівняння роботи розробленого Web-генератора надійних паролів з іншими популярними українськими, російськими та зарубіжними онлайн-генераторами надійних паролів з урахуванням вимог до систем парольного захисту. Розглядати офлайн-генератори паролів ми не будемо через те, що вони також можуть бути недоступні під час ситуації, коли потрібен терміновий доступ до захищених web-сервісів, а засобів доступу до них немає і залишається використовувати, скажімо, апаратні ресурси Інтернет-клубу чи університетської лабораторії. Тому тестувати будемо лише онлайн-генератори. Основні результати тестування наведені в табл. 1.

Порівняння проводилось за наступними параметрами: включення до складу пароля цифр, великих літер, літер з мов, відмінних від англійської, спеціальних символів. Також враховувалась можливість самостійного формування набору літер та символів, зі складу яких буде згенерований пароль. Оцінювались розміри паролів, кількість генерованих паролів та можливість генерації повторюваного паролю, необхідна для вирішення поставленої в цій статті задачі. Більше інформації про конкретний генератор можна отримати, перейшовши за вказаним в таблиці посиланням на розміщення генератора в мережі Інтернет.

1 – вимкнення застосування даного набору символів неможливе;

2 – граничні дані не вказані, перевірка показала підтримку значень більше десяти тисяч;

3 – одразу генерується 20 варіантів кожного типу паролів;

4 – даний онлайн-генератор призначений для генерації паролів на основі ключових фраз. Він дозволяє створювати паролі з речення на російській (в 7 варіантах складності речення), причому в кожному варіанті перші три літери кожного слова речення використовуються в якості частинок пароля в англійській розкладці. Більше параметрів пароля задавати неможливо. Цей генератор є єдиним з розглянутих, який дає можливість створювати безпечний пароль, який можна було б легко запам’ятати. Але запропонований розробниками генератора метод у порівнянні з представленим в даній роботі є більш складним (бо ключові фрази генеруються автоматично, обирати їх самостійно не можна), та не захищений від підглядання та перехоплення введення з клавіатури;

5 – можливо формувати для генерації пароля лише набір спеціальних символів.

Таблиця 1.

Результати тестування онлайн-генераторів паролів

	Адреса генератора	Підтримка цифр	Підтримка великих літер	Підтримка різних мов	Підтримка спеціальних символів	Самостійне формування словника	Вибір довжини паролю	Кількість генерованих паролів	Створення повторюваного паролю
1	http://parol.org.ua/	+[1]	+[1]	-	-	-	-	1	-
2	http://mirage.net.ua/dev/passgen/	+	+	-	-	-	+	1-∞[2]	-
3	http://pass.rc-svit.com/	+	+	-	+	-	4-99	1-99	-
4	http://passwords.lance.com.ua/	+	+	-	+	-	5,6,8,10,12	20[3]	-
5	http://rassanov.ru/	+	+	-	+	-	6-32	32	-
6	http://exogens.ru	+	+	-	-	-	4-32	1-1000	-
7	http://www.genpas.ru/	+	+	+	+	+	1-∞[2]	1-∞[2]	-
8	http://pasw.ru/	+	+	+	+	+	1-99	1-99	-
9	http://passwd.ru/	-	+[4]		+[4]	-	6,9,12,15	5	-
10	http://www.pctools.com/	+	+	-	+	-	4-64	1-50	-
11	http://passwd.thebugs.ws/	+		-	+	-	1-255	6	-
12	http://maord.com/	+	+	-	+	-	4-64	1-2500	-
13	http://www.techzoom.net/	+	+	-	+	+[5]	4-64	4-32	-
14	http://tau-systems.org.ua/	+	-	-	-	-	1-48	1	+

Висновки. Таким чином, розглянувши найбільш популярні онлайн-генератори паролів, можна стверджувати, що функціональність їх є більш-менш схожою, просто лише частина розглянутих генераторів містить усю повноту можливих функцій. При їх застосуванні для формування паролів до web-сервісів значна частина функціональності є надмірною (web-сервіси часто не дозволяють застосування літер, відмінних від англійських, та спецсимволів). Крім того, значним загальним недоліком усіх розглянутих генераторів, окрім запропонованого, є неможливість генерації повторюваного пароля, тобто при однакових вхідних даних він видасть однакові вихідні. Це дає змогу застосування його в якості портабельної системи персоналізації користувачів при доступі до захищених Web-ресурсів. Жоден інший з розглянутих онлайн-генераторів не дає такої можливості. Крім того, запропонований Web-генератор надійних паролів є єдиним генератором, що емулює двохфакторну персоналізацію з використанням апаратних засобів, знижуючи ризик перехоплення пароля за допомогою клавіатурних шпигунів.

1. Ричард Э.Смит Аутентификация: От паролей до открытых ключей. – М.: Издательский дом Вильямс, 2002. – 424 с.
2. Афанасьев А., Веденьев Л., Воронцов А., Газизова Э. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. Под ред. А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева. – М.: Горячая линия-Телеком, 2009. – 552 с.
3. Бардаченко В.Ф., Кариман А.В., Колесницкий О.К., Василецкий С.А., Рашкевич А.А. Анализ современных средств аутентификации и защиты информации // УСиМ. — 2004. — №3. — С. 81 - 92.
4. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. — М.: Горячая линия — Телеком, 2000. — 452 с.
5. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд. Пер. с англ. — М.: Издательский дом "Вильямс", 2001. — 672 с.: ил.
6. Поліновський В.В., Герасименко В.А. Апаратно-програмні засоби ідентифікації та автентифікації користувачів на основі ВІК-ВАК технологій. Праці Міжнародної конференції «Розвиток інформаційно-комунікаційних технологій та Розбудова інформаційного суспільства в Україні» м. Ганновер, Німеччина, CeBIT-2007. – Київ: 2007. С. 107 – 113.
7. Бардаченко В.Ф., Поліновський В.В. Методи персоналізації складних технічних систем, у тому числі комп’ютерних та телекомунікаційних // Вісті академії інженерних наук України. — 2005. — №4 (27). — С. 7 - 11.