ЗАХИСТ ТА ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

О.В.Курятник

Національний авіаційний університет

кафедра інженерії програмного забезпечення

Науковий керівник Радішевський М.Ф. (к.т.н., доцент)

Генератор паролів, що враховує механізми пам'яті людини

Аутентифікаця в системі

Аутентифікація - це процедура, що перевіряє, чи має користувач з пред'явленим ідентифікатором право на доступ до ресурсу. До технологій аутентифікації відносяться використання паролів, цифрових сертифікатів, біометричних показників, таких як відбитки пальців, райдужка чи геометрія обличчя [5].

Найнадійнішим засобом аутентифікації є біометричні показники. Однак біометрія знаходиться на самому початку довгого шляху і існує ряд проблем зв'язаних з відносною новизною даної технології.

Найбільш розповсюдженим є використання паролів. Паролі легко створити, зручно використовувати і вони не потребують ніяких додаткових пристроїв вводу. Саме з цим методом аутентифікації ми зустрічаємось кожного дня.

Існує кілька способів несанкціонованого доступу до ресурсів:

- обійти процедуру аутентифікації, скориставшись недосконалістю системи;
- дізнатися або підібрати пароль і вводячи правильний пароль, отримати відповідні повноваження.

Дізнавання - підглядання за набором паролю, застосування клавіатурних шпигунів, використання необережні користувача (папірець з паролем на видному місці). Протидія дізнаванню паролю – організаційні заході.

Підбір - повний перебір можливих комбінацій – BruteForce - метод Грубої Сили. Протидія підбору – збільшення довжини паролю.

Проблеми використання паролів

Отже, який же пароль зможе вчинити гідний опір спробам його підбору? Довгий, такий, що складається з букв різного регістра, цифр і спецсимволів. При цьому він має бути випадковим, тобто вибір символів здійснюється довільно (без якої б то не було системи) і більш ніде не використовуватися, при цьому єдиним місцем фіксації пароля має бути голова єдиної людини. Але твердження про те, що чим складніший пароль, тим безпечніший він, – це лише один із міфів комп'ютерної безпеки [2,6]. При виборі пароля необхідно враховувати і питання практичного використання пароля та людського фактору.

Коли як пароль використовується абракадабра з суміші великих і маленьких букв, цифр і спецсимволів, то такі паролі дуже важко запам'ятовуються, легко забуваються по витіканню короткого періоду "неактивності", особливо, якщо враховувати той факт, що користувачеві доводиться мати не один пароль. Тоді без знання мнемотехніки (яка зовсім не поширена серед користувачів) тут не обійтися. Вірогідність, що користувач потайки або явно запише такий пароль на листку, дуже висока. Дивно, як при цьому такий пароль може вважатися задовільним серед фахівців з інформаційної безпеки. Адже досить лише пройтися по будь-яким офісам в світі і ми можемо знайти стільки паролів, скільки нам потрібно: на листках в столах користувачів чи на вінчестері даного комп'ютера в файлах де містяться всі необхідні паролі.

Людський фактор залишається найслабшою ланкою в забезпеченні безпеки даних. Дослідження фірми SafeNet [1] показали, що працівники компаній не здатні впоратися з паролями доступу. Половина людей записують секретні коди на папері, а третя частина говорить їх колегам.

Людям потрібно пам'ятати все більше паролів. 80% опитаних використовують мінімум три пароля. Однак, 67% використовують один і

той же пароль для доступу до п’яти і більше сервісів, а 31% для доступу до дев’яти ресурсів і більше. Якщо компанії вимагають від співробітників вигадувати важкі паролі і часто їх змінювати, то збільшується ризик, що люди почнуть їх записувати. Така звичка знижує рівень безпеки і може дорого обійтися компанії.

Той варіант, коли як пароль використовується російське слово, набране на англійській клавіатурі також не є досить надійним. Запам'ятовується такий пароль легко, але і ламається дуже просто. Для злому не потрібно використовувати BruteForce пошук, досить тільки використовувати dictionary attack. Будь-яка нормальна програма для злому паролів може використовувати словник російських слів, набраних в англійському регістрі. Більше того, додатково перевіряються варіанти (якщо не вимагають занадто великих зусиль) із заміною одного-двох символів в слові. Також, приміром, перевіряються слова із заміненими O на 0, а S на 5. Частковим випадком є використання як пароль ненормативної лексики. Чомусь вважається, що зломщик посоромиться додати такі слова в словник для перевірки.

Особливості людської пам’яті

При виборі пароля потрібно враховувати властивості пам’яті людини. Довільно вибрані символи запам'ятаються, якщо їх вимовляння вголос має звукову форму (благозвучність) [4], що запам'ятовується і вони містять знайому нам граматику, інакше без шпаргалки не обійтися. Спецсимволи ж навпаки знижують благозвучність. Один з найнадійніших способів зберегти пароль в таємниці – це взагалі ніде його не записувати. З комп’ютера його може вкрасти програма-шпигун, яка проникла в ваш комп’ютер через мережу чи з флешкою колеги.

Перевіримо властивості людської пам’яті та мнемотехніки. Проаналізуємо чотири висловлювання [3]:

- «На столі лежить книга»
- «Стіл, книга»
- «Глокая куздра кудрячить бокра»
- «7ло*о_9е»

В першому випадку ми повністю розуміємо висловлювання, тому що слова нам знайомі, в нашій уяві автоматично виникають образи. До того ж це висловлювання містить знайому нам граматику, на основі якої наш мозок правильно розмістив образи в уяві.

В другому висловлюванні містяться лише знайомі нам слова. Під дією цих слів в нашій уяві також виникають образи, але граматики в цьому висловлюванні немає, тому наш мозок не знає як їх розташувати.

В третьому висловлюванні міститься знайома нам граматика і наш мозок готовий правильно розташувати образи, однак самі образи нам незнайомі. Відповідно до граматики нашої мови ми розуміємо, що хтось над кимось виконує якусь дію. Асоціації для слів «куздра» і «бокр» у кожного свої. За цим висловлюванням ми можемо сформувати певну зв’язку в пам’яті, адже це повідомлення несе для нас певний звуковий і візуальний образ. З точки зору нашого словникового запасу воно абсолютно безглузде.

В четвертому випадку немає ні знайомої нам граматики, ні звукової форми. В цьому випадку спостерігається повне нерозуміння почутого. Таке висловлювання ніяк не вплине на нашу уяву. Відповідно не будуть сформовані ніякі звукові або візуальні образи. Тому таке повідомлення не запам’ятається і буде лише «шумом» для нашого мозку. Саме такі висловлювання і є прикладом «безпечних» паролів.

Можливим рішенням проблеми використання паролів які складно запам’ятати є побудова та використання генератора безглуздих але вимовних паролів. Ці паролі схожі на третє висловлювання. Вони не є існуючими словами, але побудовані з урахуванням особливостей мови певного народу та людського організму вцілому.

Створення генератора таких паролів полягало в двох етапах:

1. Дослідницький етап – збір статистики звукових сполучень.
2. Створення генератора паролів.

Дослідження сполучуваності букв лексики

Послідовність букв будь-якого слова можна представити марковським ланцюжком k-го порядку. Були досліджені ланцюжки другого, третього та четвертого порядку.

Використовуючи ланцюжки 2-го порядку при виборі наступної букви враховувалася лише попередня буква. Тому паролі могли складатися з багатьох приголосних букв поспіль. Такі паролі важко промовляються і запам’ятовуються. При використанні ланцюжків 4-го порядку звужується простір кодових комбінацій, з’являються слова які входять до словника. Тому оптимальний варіант – це ланцюжки 3-го порядку.

На першому етапі був створений аналізатор текстів. В нього завантажувались тексти потрібної мови. Аналізатор рахував всі «трійки» букв які він зустрічав в словах цих текстів, а також їхню кількість. Паралельно підраховувалася і загальна кількість цих трійок. По закінченню обробки запропонованих текстів число знаходжень кожної «трійки» букв було поділене на загальну їх кількість. В результаті ми отримали імовірність зустрічі кожної «трійки». В подальшому аналізі враховувалася та особливість, що буквосполучення, які важко промовляються, використовуються в мові дуже рідко, а милозвучні – навпаки. Тому буквосполучення з найменшим відсотком зустрічання видалялися, а інші записувалися до бази даних. Імовірність зустрічі кожного буквосполучення різна ($P_1 \neq P_2 \neq ... \neq P_n$), але для збільшення кількості кодових комбінацій імовірність їх зустрічі вважалася рівною ($P_1 = P_2 = ... = P_n$). В результаті для одної мови ми отримали до 1000 унікальних «трійок» букв, які постійно використовуються в лексиці.

Генератор

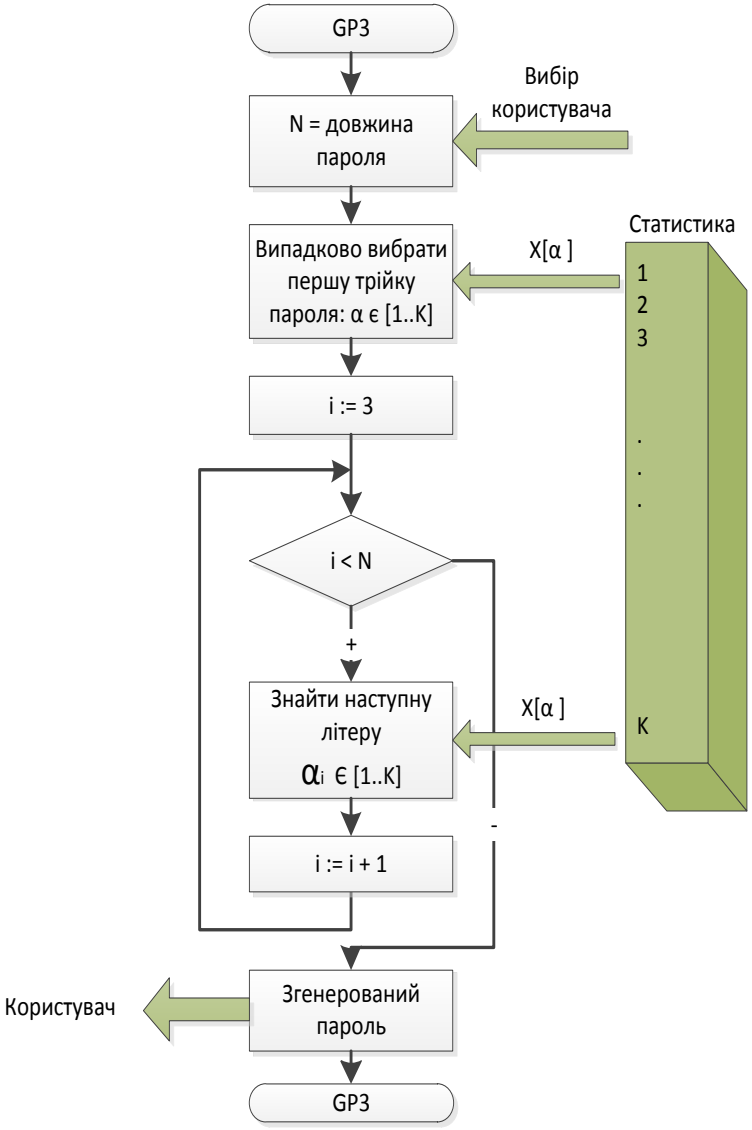

Рис. 6 - Алгоритм роботи генератора паролів

На другому етапі був створений генератор. Для його роботи потрібна база даних зі статистикою та датчик випадкових чисел. Початок пароля, за допомогою сгенерованого випадкового числа, береться довільно з усіх доступних трійок (див. Малюнок 1). Продовження відбувається на основі двох кінцевих літер пароля. В статистиці здійснюється пошук «трійок», які починаються с потрібних двох букв. За допомогою датчика випадкових чисел вибираємо довільну з них і

доповнюємо пароль 1 літерою. І так продовжуємо до потрібної довжини пароля. На малюнку 2 зображений інтерфейс програми. Користувач може вибрати потрібну йому довжину пароля та мову. Паролі генеруються після натискання на стилізовану кнопку.

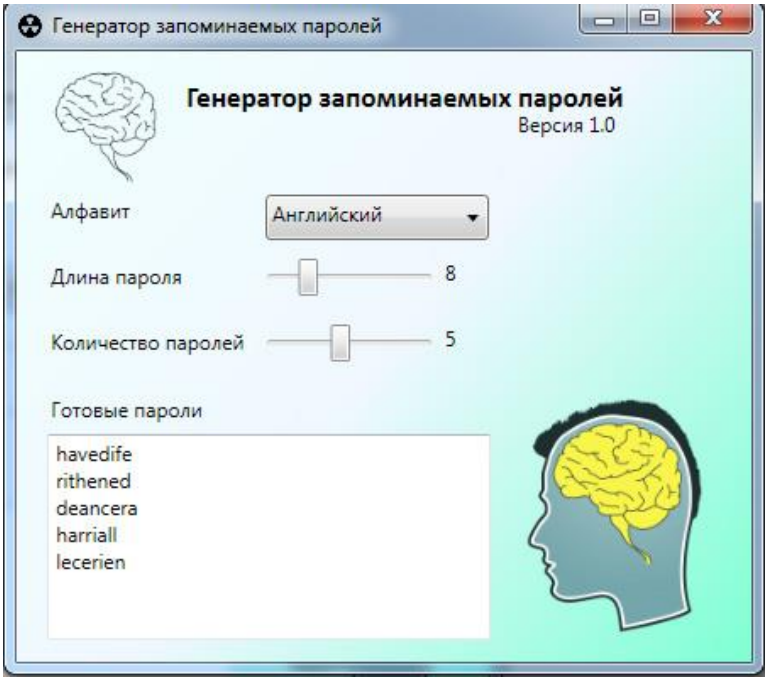

Рис.2 - Інтерфейс програми

Прикладами роботи генератора є такі паролі:

Паролі з застосуванням статистики англійської мови	**Паролі з застосуванням статистики російської мови**
fitespaicoo	ятиногласн
marlinage	вшивенейст
vinsider	скудоболн
hematedi	лалалейст
plesende	винакаточ
vendifeed	вечеиомин
comergene	уговолови
emationer	томилагор
sucharion	пятиновни
carantall	ничеселод

Звичайно, ці паролі дещо поступаються своєю милозвучністю реальним словам. Однак якщо порівнювати їх з тим набором символів, що видають звичні нам генератори, то вони запам'ятовуються "приємніше". Для їх запам’ятання також потрібно прикласти деяких зусиль, але, я думаю, не шкода витратити хвилину для запам’ятання потрібного пароля на все життя.

Специфіка використання паролів

Такі паролі потрібні не в усіх випадках, але сфера їх використання є досить широкою [2,7]. Наприклад, в локальних системах ці паролі будуть дуже зручними, адже парольні менеджери тут не допоможуть, а забутий пароль спричинить хоча і не критичні, але неприємні наслідки.

При аутентифікації до віддалених систем або веб-сервісів пароль може бути і складним для запам’ятовування, адже ми користуємося ними сидячи за локальними системами, тому в цьому випадку можна скористатися менеджерами паролів. Головна особливість віддалених систем в тому що вони погано ставляться до

перебору. Якщо ламати скачаний архів ви можете скільки завгодно, то з віддаленими системами все не так. Дуже часто система після 3-5 невдалих введень заблокує всі спроби на деякий час, а перебирати паролі з швидкістю декілька паролів в хвилину нереально. Вдалі зламування віддалених систем в більшості випадків зв'язані з дізнаванням паролів. Використовувати паролі, які легко запам'ятовуються, слід для тих сервісів які ви часто використовуєте, або використовуєте з чужих комп'ютерів.

Для доступу до парольних менеджерів та локальних програм також слід використовувати паролі, які добре запам'ятовуються. Адже дані в них зазвичай дуже добре шифруються, і зламати їх при надійному паролі майже неможливо.

Найбільш доцільним буде використовувати ці паролі в корпоративних системах. Адже там люди працюють в великих офісах, там же зберігаються їхні особисті речі. В цьому випадку дізнатися пароль методом дізнавання буде найпростіше. А наслідками такого злому можуть бути великі збитки для компанії.

Список використаних джерел

1. www.safenet-inc.com
2. www.bugtraq.ru
3. Зиганов М.А., Козаренко В.А., Семин А.Н. Техника запоминания иностранных слов. М.: Издательство «Образование», 2002.
4. Зиганов М.А., Козаренко В.А. Мнемотехника. Запоминание на основе визуального мышления. М.: Издательство: «Школа рационального чтения», 2001.
5. Ричард Э. Смит. Аутентификация: от паролей до открытых ключей. Пер. с англ. – М.: Издательский дом «Вильямс», 2002.
6. Петров В.П., Петров С.В. Информационная безопасность человека и общества. М.: Издательство «ЭНАС», 2007.
7. Корнеев И.К., Степанов Е.А. Защита информации в офисе. М.: ТК Велби, Издательство Проспект, 2008