УДК 004.4

Круглікова А.Д.
Полтавський національний технічний університет
імені Юрія Кондратюка

АНАЛІЗ АЛГОРИТМІВ ДЛЯ ОЦІНКИ СТІЙКОСТІ ПАРОЛІВ

У статті розглянуті особливості алгоритмів оцінки стійкості паролів до взломів на основі аналізу сучасних методів хакерських атак на системи авторизації.

Ключові слова: *пароль, взлом, ентропія інформації, алгоритми оцінки стійкості пароля до взлому.*

Вступ

Ні для кого не є секретом, що сьогодні на переважній більшості систем для аутентифікації користувачів використовується парольний захист. Це стосується персональних комп'ютерів, корпоративних комп'ютерів, веб-аплікацій, ssh/pgp ключів.

Пароль - це набір символів, призначений для підтвердження особи користувача системи. Використовуються паролі для захисту інформації від несанкціонованого доступу. Для користувачів це є один з найзручніших варіантів, який не вимагає спеціальних знань.

З погляду інформаційної безпеки таку аутентифікацію не можна вважати повністю безпечною. Існує дві проблеми: людський чинник і технічна недосконалість. Більшість користувачів не хочуть або не можуть запам’ятати складні паролі і не усвідомлюють наскільки легко зламати їх пароль. Так, наприклад, використання в якості паролю осмислених фраз робить можливим їх підбір по словнику. А якщо користувач встановлює в багатьох системах однаковий пароль і ніколи не міняє його, то зловмисники можуть зламати одну систему і отримати доступ до всіх інших.

Отже, необхідно перевіряти стійкість паролю до взлому на етапі його створення користувачем і забороняти вводити слабкі комбінації.

Мета цієї роботи полягає в аналізі і розробці ефективного алгоритму оцінки стійкості паролю до взлому.

Для досягнення поставленої мети було поставлено і вирішено наступні завдання:

• Аналіз методів хакерських атак на парольні системи.

• Дослідження даних про нестійкі до взлому паролі.

• Розробка алгоритму для оцінки стійкості паролів на основі всіх проаналізованих даних.

Багато вчених проводили дослідження в цій області раніше. Була виведена формула Андерсена для кількісної оцінки стійкості паролю. Дослідження також проводив Мещеряков Р.В. і розробив методи оцінки просторів паролів в залежності від алфавіту для паролів. [4]

Аналіз методів хакерських атак

Злом парольних систем є дуже поширеною хакерською атакою. В разі успіху такої атаки, зловмисник отримує повний доступ до функцій і даних системи, що зумовлює популярність такого методу і важливість дослідження методів захисту від нього.

Для того, щоб створити алгоритм перевірки паролю на стійкість від злому треба проаналізувати існуючи методи злому:

1. Прямий перебір (brute force (англ.) - груба сила, рішення «в лоб») - перебір всіх можливих поєднань допустимих в паролі символів.

2. Підбір по словнику - метод заснований на припущенні, що в паролі використовуються існуючі слова якої-небудь мови або їх поєднання, повторення слів (*sunsun*); зворотного порядку символів слова (*esirnus*); транслітерації букв (*parol*); заміну букв кирилиці латинською розкладкою (*gfhjkm*).

3. Метод соціальної інженерії - заснований на припущенні, що користувач використовував в якості паролю особисті відомості, такі як його ім'я або прізвище, дата народження і т. п.

4. Перевірка по словнику найпопулярніших паролів

5. Перевірка послідовностей символів (12345, qwerty і т.д.)

Який пароль можна однозначно назвати не стійким до злому?

Для досліження були взяті дані з 967 паролів одного із зламаних поштових серверів мережі Інтернет.

Пароль з невеликої кількості (до 5) символів/цифр є однозначно слабким. 335 паролів (майже третина) складалася виключно з цифр.

Всього 2 паролі містили спецсимволи. У 33 випадках ім'я і пароль користувача співпадали. Найпопулярнішим виявився пароль 123 (зустрічався 35 разів, майже кожен 27 пароль). На другому місці пароль qwerty (20 паролів). Далі слідують: 777 (18 разів), 12 (17 разів), hacker (14 разів) і 1, 11111111, 9128 (по 10 разів). 16 паролів складалися з одного символу / цифри.

Ентропія, як міра стійкості паролю

Мірою стійкості паролів традиційно є ентропія - міра невизначеності, вимірювана звичайно в бітах [7].

Ентропія інформації в 1 біт відповідає невизначеності вибору з двох паролів, в 2 біта - з 4 паролів, в 3 біта - з 8 паролів і т.д.

Ентропія в N біт відповідає невизначеності вибору з 2^8 паролів. У разі використання випадкових паролів (наприклад, випадкових чисел, що згенеровані за допомогою генератора) ентропія обчислюється досить просто: вона залежить від кількості можливих паролів для заданих параметрів. Так, для випадкового пароля завдовжки N символів, складеного з алфавіту, що містить M букв, ентропія буде рівна:

$$E=log_2 M^8$$

Але для обрахунку ентропії паролю який був придуманий людиною така формула не підходить.

Найпоширенішим підходом до підрахунку ентропії в цьому випадку є підхід, який був запропонований американським інститутом NIST:

• ентропія першого символу пароля складає 4 біта;

• ентропія наступних семи символів пароля складає 2 біта на символ;

• ентропія символів з 9-го по 20-го складає 1,5 біта на символ;

• всі подальші символи мають ентропію 1 біт на символ;

• якщо пароль містить символи верхнього регістра і неалфавітні символи, то його ентропія збільшується на 6 біт.

Така формула дає кращі результати, але все одно порахує велику ентропію для довгого паролю, хоча той наприклад співпадає з ім'ям користувача. Час злому такого паролю буде мінімальний, отже ця формула все ще потребує покращення.

Для кількосної оцінки сили паролю також використовують формулу Андерсона:

$$4.35 \cdot 10^4 \cdot (\mathrm{k}) \frac{M}{P} \leq A^1, \text{ де}$$

k - кількість спрою підбору пароля в хвилину;

M - час дії паролю в місяцях;

P - вірогідність підбору паролю;

A^l - потужність простору паролів (A - потужність алфавіту паролів, l - довжина паролів).

Якщо крім розрахунку ентропії, додати ще перевірку по словнику, по списку популярних паролів, наявність послідовностей символів і звіряння з даними користувача, то результат буде відповідати дійсності і забезпечить використання користувачами стійких до злому паролів.

Алгоритм для оцінки стійкості пароля

Отже, на основі проаналізованих даних про можливі способи хакерських атак, а також на основі досліджених даних про завідомо слабкі паролі отримуємо наступний алгоритм:

1. На вхід отримуємо пароль для аналізу.

2. Розроховуємо ентропію за допомогою.

• алгоритму brute force (повний перебір всіх можливих комбінацій із всіх можливих символів)

• алгоритму перевірки по словнику (словники різних мов, назв фільмів, імен)

• перевірка паролів з повтореннями (повторення однакових символів, цифр, слів)

• перевірка алфавітник та числових послідовностей (наприклад, 12345, qwerty, abcdef)

• перевірка по регулярному виразу (кількість символів в верхньому і нижньому регістрі, цифр і спеціальних сииволів)

• перевірка дат і років (часто в паролях використовую роки народження, дати свят і визначних паролів)

3. Рахуємо мінімальну кількість часу необхідну для взлому даного пароля.

Основним результатом роботи алгоритму є ентропія паролю. Для того, щоб розрахувати час злому треба задати наступні конфігураційні опції:

• T- Час відповіді парольної системи на один запит

• N -Кількість ядер, які використовуються хакерами

Час злому паролю розраховується по наступній формулі [6]:

$$t = \frac{2^{E-1} \cdot T}{N}, \text{ де}$$

E - ентропія паролю;

t - час на підбір паролю.

В наступній таблиці наведені результати роботи програми, в якій реалізований даний алгоритм. Час обробки одного запиту (T) було задано в 10 мілісекунд (підходить для таких хеш функцій: Bcrypt, Scrypt, PBKDF2). Кількість одночасних спроб хакерів (N) - 100.

Таблиця 1

Пароль	Час взлому	Ентропія	Найслабше місце
12345	0.0	2.585	Популярний пароль
nastya1993	21 хвилина	24.479	словник + рік
Zbr)3Yq&	>10000 років	52.559	повний перебір
qwerty123	0.001 секунди	4.907	популярний пароль
appleskyhomeworksunday	8 місяців	38.315	підбір по словнику

Висновки

В результаті цієї роботи були виконані поставлені завдання:

• проаналізовано сучасні методи хакерських атак на парольні системи

• досліджено дані про нестійкі до взлому паролі

• на основі цього розроблено алгоритм для оцінки стійкості паролів.

Даний алгоритм можна використовувати для перевірки паролю на етапі його створення користувачем і забороняти вводити слабкі комбінації. Алгоритм може бути сконфігурований для потреб різних систем.

Список літератури:

1. Жуков И.Ю., Иванов М.А., Осмоловский С.А. Принципы построения криптостойких генераторов псевдослучайных кодов // Проблемы информационной безопасности. Компьютерные системы. 2001, №1.

2. Зензин О.С., Иванов М.А. Стандарт криптографической защиты - AES. Конечные поля. Серия СКБ (специалисту по компьютерной безопасности). Книга 1. М.: КУДИЦ-ОБРАЗ, 2002.

3. Немнюгин С.А. Программирование - СПб.: Питер, 2000.

4. Мещеряков Р.В. Теоретические основы информационной безопасности автоматизированных систем / Мещеряков Р.В., Праскурин Г.А. – Томск: Из-во Томск. межвуз.центр дист. образ., 2005. – 243 с.

5. Fluhrer S.R. Statistical analysis of the alleged RC4 keystream generator / S.R. Fluhrer, D.A. McGrew // Fast Software Encryption, Cambridge Security Workshop Proceedings. - 2000.

6. William E. Burr, Donna F. DodsonW. Timothy Polk, Information Security, April 2006, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-63ver1.0.2.pdf

7. Password strength https://en.wikipedia.org/wiki/Password_strength

Kruglikova Anastasiya Dmytrivna
Poltava National Technical University
named after Yuri Kondratyuk, Ukraine, Poltava

ANALYSIS ALGORITHMS TO ESTIMATE THE STABILITY OF PASSWORDS

The present article deals with the features of algorithms for password strength estimation based on the analysis of contemporary methods of hacker attacks on the systems of authorization.

Keywords: *password, hacking, information entropy, algorithms for password strength estimation.*