УДК 004.056:519.21

А.Р. Караван
І.А.Клєопа

МОДЕЛЮВАННЯ АТАКИ ГРУБОЇ СИЛИ З ВИКОРИСТАННЯМ ТЕОРІЇ ЙМОВІРНОСТЕЙ ТА ОЦІНКОЮ МАТЕМАТИЧНОГО СПОДІВАННЯ ЧАСУ ВЗЛАМУ

Вінницький національний технічний університет

Анотація

Метою даної статті є застосування методів теорії ймовірностей для моделювання атак грубої сили та обчислення математичного сподівання часу взламу систем автентифікації. Зі зростанням обчислювальних можливостей зловмисників дедалі більшого значення набуває застосування математичних методів для аналізу атак грубої сили, що дозволяє обґрунтовано оцінювати очікуваний час взламу систем автентифікації. Безпека інформаційних систем значною мірою визначається стійкістю паролів, аналіз якої ґрунтується на методах теорії ймовірностей. Попри свою простоту, атаки грубої сили залишаються ефективним способом несанкціонованого доступу, що зумовлює актуальність їх дослідження.

Ключові слова: математичне сподівання, теорія ймовірностей, математичні методи.

Abstract

The purpose of this article is to apply methods of probability theory to model brute force attacks and calculate the expected time of hacking authentication systems. With the growth of computing capabilities of attackers, the use of mathematical methods for analyzing brute force attacks is becoming increasingly important, which allows for a reasonable assessment of the expected time of hacking authentication systems. The security of information systems is largely determined by the strength of passwords, the analysis of which is based on methods of probability theory. Despite their simplicity, brute force attacks remain an effective method of unauthorized access, which makes their research relevant.

Keywords: mathematical expectation, probability theory, mathematical methods.

Вступ

У сучасному цифровому середовищі проблема захисту інформації набуває особливої актуальності у зв'язку зі зростанням кількості кіберзагроз та обсягів конфіденційних даних. Однією з базових і водночас найпоширеніших загроз є атака грубої сили (brute force), що полягає у послідовному переборі всіх можливих варіантів ключа або пароля до моменту знаходження правильного.

Математичне моделювання такої атаки дозволяє оцінити її ефективність і часові витрати на реалізацію залежно від довжини ключа, потужності алфавіту та обчислювальних ресурсів. Використання апарату теорії ймовірностей дає змогу визначити ймовірність успішного підбору за певну кількість спроб, а також обчислити математичне сподівання часу взлому. Такий підхід забезпечує обґрунтовану оцінку криптографічної стійкості систем захисту та дозволяє формулювати рекомендації щодо вибору безпечних параметрів аутентифікації.

Результати дослідження

Стійкість криптографічних систем автентифікації до атак повного перебору (brute-force) є прогнозованою величиною, яку можна кількісно оцінити через математичне сподівання часу зламу. За умови рівноймовірного вибору паролів, середній час успішної атаки прямо пропорційний потужності простору ключів та обернено пропорційний швидкості перебору, що дозволяє використовувати ймовірнісні моделі для точного налаштування параметрів безпеки. Розглянемо основні з них.

1. Залежність часу взламу від ентропії (довжини пароля)

Математичне сподівання часу взламу атаки грубої сили експоненціально залежить від довжини пароля. За умови фіксованого алфавіту з потужністю A загальна кількість можливих комбінацій

зростає як A^L, де L — довжина пароля. Таким чином, додавання лише одного символу до пароля збільшує середній час взламу в A разів, що свідчить про нелінійний, експоненціальний характер цієї залежності. Це робить збільшення довжини пароля одним із найефективніших способів підвищення криптографічної стійкості.

- Аргумент 1: Загальна кількість можливих паролів визначається формулою

$$N = A^L$$

де A— потужність алфавіту, L— довжина пароля.

- Аргумент 2: Математичне сподівання кількості спроб до успіху:

$$E[X] = \frac{N+1}{2}$$

- Аргумент 3: Додавання одного символу до пароля збільшує середній час взламу в A разів, що підтверджує експоненціальний характер залежності.

Висновок: Збільшення довжини пароля — один із найефективніших способів підвищити стійкість системи.

2. Вплив потужності алфавіту

Розширення алфавіту безпосередньо впливає на ймовірнісний простір атаки грубої сили. Зі збільшенням кількості допустимих символів зростає загальна кількість можливих комбінацій, що призводить до зменшення ймовірності успіху кожної окремої спроби. Використання комбінованих алфавітів (літери, цифри, спеціальні символи) суттєво ускладнює перебір, оскільки рівномірний розподіл імовірності «розмивається» на значно більшому просторі можливих паролів.

- Ймовірність вгадати пароль за одну спробу:

$$p = \frac{1}{N}$$

- Якщо N збільшується через більший алфавіт, то p стає меншим.
- Тобто шанс вгадати пароль з першої спроби або з невеликої кількості спроб падає.

Аргумент 1: Збільшення кількості символів в алфавіті A збільшує загальну кількість комбінацій:

$$N = A^L.$$

- Аргумент 2: Ймовірність успіху однієї спроби зменшується:

$$p = \frac{1}{A^L}$$

- Аргумент 3: Використання комбінованих алфавітів (цифри, літери, спецсимволи) значно ускладнює перебір, оскільки кожна спроба стає менш імовірною.

Висновок: Розширення алфавіту — важливий метод підвищення криптографічної стійкості.

3. Обчислювальна швидкість як критичний чинник

Математичне сподівання часу взламу є обернено пропорційним швидкості перебору v, що напряму пов’язує теоретичну модель із реальними обчислювальними ресурсами зловмисника. Зростання швидкості перебору в декілька разів відповідно зменшує очікуваний час успішної атаки, що дозволяє кількісно оцінити, за яких умов криптографічна система стає вразливою. Таким чином, модель дає змогу співвіднести параметри пароля з можливостями сучасного апаратного забезпечення.

Пароль розглядається як випадкова величина, що рівномірно розподілена на множині всіх можливих комбінацій.

Загальна кількість можливих паролів визначається формулою

$$N = A^L,$$

де A — потужність алфавіту, а L — довжина пароля. Це показує, що простір пошуку зростає експоненціально, а отже навіть незначне збільшення L або A суттєво ускладнює атаку.

За умови рівномірного перебору математичне сподівання кількості спроб до успішного взламу обчислюється як

$$E[X] = \frac{N+1}{2},$$

що дозволяє отримати середню кількість перевірок, необхідних зловмиснику.

Перехід від кількості спроб до реального часу здійснюється з урахуванням швидкості перебору v(спроб за секунду):

$$E[T] = \frac{E[X]}{v}.$$

Це безпосередньо пов'язує теоретичну модель з практичними обчислювальними можливостями атакуючої сторони.

Чим швидше обладнання атакуючого, тим менше часу потрібно для успішного перебору. Модель дозволяє кількісно оцінити, за яких умов система стає вразливою (наприклад, при сучасних GPU атака на короткі паролі може зайняти секунди).

Безпека пароля повинна оцінюватися не лише за довжиною та алфавітом, а й з урахуванням реальних обчислювальних можливостей зловмисника.

Для підтвердження аналітичних результатів у роботі використано комп'ютерне моделювання мовою C++, що дозволяє експериментально перевірити отримані формули та продемонструвати вплив параметрів пароля на очікуваний час взламу.

Код програми:

C++ реалізація

```
#include <iostream>
#include <cmath>
#include <cstdlib>
#include <ctime>
using namespace std;
int main() {
int A;
int L;
double v;
int trials = 100000;
cout << "Enter alphabet size A: ";
cin >> A;
cout << "Enter password length L: ";
cin >> L;
cout << "Enter brute-force speed v (attempts per second): ";
cin >> v;
cout << "\n--- THEORETICAL MODEL ---\n";
double N = pow(A, L);
double expectedAttempts = (N + 1) / 2;
double expectedTime = expectedAttempts / v;
cout << "Total number of combinations N = " << N << endl;
cout << "Expected number of attempts E[X] = "         << expectedAttempts << endl;
cout << "Expected cracking time E[T] = "         << expectedTime << " seconds\n";
cout << "\n--- EMPIRICAL SIMULATION ---\n";
srand(time(0));
double sumAttempts = 0;
for (int i = 0; i < trials; i++) {
      int position = rand() % (int)N + 1;
      sumAttempts += position;
}
double empiricalEX = sumAttempts / trials;
cout << "Empirical expected value E[X] = "         << empiricalEX << endl;
cout << "Theoretical expected value E[X] = "         << expectedAttempts << endl;
cout << "\n--- EFFECT OF PASSWORD LENGTH ---\n";
cout << "L\tExpected time (seconds)\n";
```

```
cout << "------------------------------\n";
for (int length = 1; length <= L; length++) {
        double combinations = pow(A, length);
        double time = ((combinations + 1) / 2) / v;
        cout << length << "\t" << time << endl;
}
return 0;
}
```

Висновки

Проведене дослідження демонструє, що застосування методів теорії ймовірностей та математичного моделювання дозволяє кількісно оцінити стійкість паролів до атак грубої сили та передбачити очікуваний час взламу. Аналіз показав, що збільшення довжини пароля та потужності алфавіту експоненціально підвищує криптографічну стійкість, а обчислювальні можливості атакуючого визначають практичну вразливість системи.

Отже, поєднання теоретичних розрахунків і емпіричних симуляцій є ефективним інструментом для прогнозування безпеки інформаційних систем і прийняття обґрунтованих рішень щодо захисту даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Математичні методи криптології: Навчальний посібник [Електронний ресурс] (Для студентів техн. спец. вищ. навч. закл.) / [А.Д. Кожухівський, І.Д. Горбенко, Г.І. Гайдур, О.А. Кожухівська, В.В. Марченко]; М-во освіти і науки України, Державний університет телекомунікацій. Київ: ДУТ, 2021 – 244 с.
2. Ігнатович А.О. Критерій ефективності для визначення стійкості блокових шифрівна основі внесених змін статистичних характеристик шифрованого тексту / Ігнатович А.О., Глухова О.В., Лозинський А.Я., Яремчук Р.І. // ACIT'5 "Сучасні комп'ютерні інформаційні технології". ТНЕУ. – Тернопіль. 22-23 травня 2015. – С. 167-168.

Караван Анастасія Русланівна – студентка групи 1ЕХКБ – 25б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: nastykaravan@gmail.com

Науковий керівник: ***Клєопа Ірина Анатоліївна*** – pHd, доцент, кафедра вищої математики, Вінницький національний технічний університет, м. Вінниця, Хмельницьке шосе, 95, e-mail: paceka08@vntu.edu.ua

Caravan Anastasia Ruslinivna – student of group 1EHKB – 25b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: nastykaravan@gmail.com

Scientific supervisor: ***Klieopa Iryna Anatoliivna*** – PhD, Associate Professor, Department of Higher Mathematics, Vinnytsia National Technical University, Vinnytsia, Khmelnytske Shosse, 95, e-mail: paceka08@vntu.edu.ua