УДК 004.62+004.77

**А.О. Аносов, А.В. Платоненко**

# ГЕНЕРУВАННЯ УНІКАЛЬНОГО ПАРОЛЮ ЗІ ЗМІННИМ ПРАВИЛОМ УСКЛАДНЕННЯ

Розглянуто метод підвищення захисту бездротових мереж від перехоплення інформації та впливу на неї, шляхом створення надійного паролю зі змінним правилом ускладнення. Даний метод дає змогу його використання для програмних та апаратних засобів захисту, а також можливість застосовувати його для підвищення захисту облікових записів користувачів та інших систем захисту, де необхідне використання надійного паролю.

***Ключові слова:*** інформаційна безпека, загрози інформаційної безпеки, бездротові мережі, захист мереж від несанкціонованого доступу, захист мобільних пристроїв.

## Вступ

Ненадійні паролі зазвичай стають причиною хакерських атак [1]. Після того як зловмисник підключиться до мережі, він отримує доступ до підключених пристроїв. Крім того, якщо ненадійний або стандартний пароль використовується для панелі налаштувань, то всі підключені пристрої також піддаються ризику хакерської атаки, яка вже може здійснюватися віддалено [2].

Більшість атак направлена на підбір паролю, стійкість якого залежить від можливої швидкості підбору. Для сучасного комп'ютера, при стандартних режимах роботи, з використанням центральних процесорів (CPU), швидкість підбору може становити 6000-7000 паролів за секунду, в залежності від моделі та режиму роботи.

Існує можливість збільшити ці значення в тисячі разів, завдяки використанню графічних процесорів у відео-картах (GPU). На прикладі однієї із відео-карт, що використовується для перебору хешів паролів, швидкість підбору може становити до 15 млрд. за секунду, а з використанням GPU-ферм (наприклад 12 відео-карт, об'єднаних для спільної роботи) може досягати 200 млрд. за секунду. Спеціалізовані ферми можуть досягати значення в 350 млрд. переборів за секунду, та не обмежуються цим значенням.

Таким чином кількість часу необхідного на перебір може значно зменшитись, саме тому постає необхідність в ускладненні паролю, для зменшення ймовірності його злому.

## Основна частина

Завдання пошуку надійного паролю для захисту інформації в бездротових мережах потребує перевірки на стійкість до підбору. Множина паролів складається з комбінацій символів, які можуть складати пароль, ймовірність підбору якого може здаватись досить малою (при використанні CPU), але враховуючи використання спеціального обладнання (об'єднаних GPU), час на підбір може значно зменшитись, а відповідно, ймовірність підбору паролю буде більшою, ніж могло здаватись.

Враховуючи статистику [2] та проведені розрахунки [3], можна вважати, що використання методу генерування унікального паролю зі змінним правилом ускладнення дасть змогу підвищити рівень захищеності бездротової мережі, шляхом зменшення ймовірності підбору пароля.

Складовими частинами, що покладені в основу методу є використання інтегрованого підходу до аналізу та генерації паролів:

- за показниками довжини,
- набору символів з різних множин,
- на можливу/часткову наявність у різних за типами словниках паролів.

Оскільки паролі з часто вживаних слів є значною проблемою в захисті користувачів, то множина паролів заздалегідь обрана з символів, що не мають повторення, з метою уникнення простоти їх підбору [4].

Враховуючи ймовірність генерування паролю (які хоч і складаються з букв, що не повторюються) з можливою наявністю в ньому слів, або поєднання символів, що можуть значити слова, набрані на розкладці іншою мовою, постає необхідність у введені правила ускладнення для таких паролів, де кількість цих слів у паролі буде переважати [5, 6, 7].

Для того, щоб збільшити ймовірний час підбору пропонується ввести певні правила ускладнення.

Із загальної множини паролів відбирається множина $U_z$ (рис. 1), що складається з паролів, які мають в собі малі літери англійського алфавіту. До підмножини ускладнення $U_z$ потрапляють паролі, якщо в них є 3, або більше простих слів англійською мовою, або комбінацій набору символів, що може бути в словниках.

В залежності від кількості та довжини слів виділяються підмножини $U_l$, кожна з яких має певну кількість слів, а саме: для англомовних слів, або комбінацій набору символів з 26 букв отримаємо 16 варіантів (слова від 3 до 6 букв), що вказані у таблиці 1.

Отже в даному випадку $U_z$ буде складатись з 16 підмножин $U_l$. В свою чергу кожна підмножина $U_l$ має порядкове значення $d$, що означає номер правила ускладнення.

$$d = \{d_1 \dots d_{16}\} \tag{1}$$

де $d$ – правило ускладнення з різними значенням кількості букв у слові,
$d_1 \dots d_{16}$ – порядкове значення правила, що визначає ускладнення в таблиці 1.

Відповідно до обраного номеру правила $d$ обираються паролі з підмножини $U_l$ , які додаються до множини ($C_p$ - $U_z$), що в свою чергу створює множину $C_k$.

Отже, при додаванні паролів, обираються ті, які складаються з певної кількості букв (відповідно до певного правила $d$), що робить даний метод генерування унікального паролю універсальним та ускладнює можливість зловмисника в спробі створення такого ж самого алгоритму генерування, оскільки правило $d$ може також бути змінним, відповідно до певної множини паролів, що несе за собою вже три рівня ускладнення для унікального паролю.

$$L_d \in U_z \tag{2}$$

де $L_d$ – випадковий пароль з множини $U_z$,
$U_z$ – множина ускладнення, зі слів або набору символів.

Кожне значення правила $d$ розраховується для кожного варіанту за формулою комбінацій де:

- довжина паролю становить 26 символів,
- пароль може складатись з декількох слів (від 4 до 8 слів довжиною від 3 до 6 букв).

Оскільки можливе поєднання різних слів з різною кількістю букв у слові, то для розрахунку довелось використовувати добуток та додавання комбінацій, відповідно до правил комбінаторики для «і» та «або».

Таким чином добуток комбінацій означає поєднання кількості значень паролів, кількість букв у яких, сумарно складають довжину алфавіту. Для кожної довжини слова та поєднання слів різної довжини отримаємо певне значення комбінацій, що можна буде використати для розрахунку.

Таблиця 1

Кількість слів, або набору символів, що може бути частиною паролю

| $d_n$ | Кількість слів у паролі | Кількість букв у слові | | | | | | | | | Кількість комбінацій |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 4 | **6** | **6** | **6** | **6** | 2 | | | | | $7{,}50\cdot10^{14}$ |
| 2 | 5 | **6** | **6** | **6** | **5** | **3** | | | | | $1{,}50\cdot10^{15}$ |
| 3 | 5 | **6** | **6** | **5** | **5** | **4** | | | | | $2{,}25\cdot10^{15}$ |
| 4 | 5 | **6** | **5** | **5** | **5** | **5** | | | | | $2{,}70\cdot10^{15}$ |
| 5 | 5 | **5** | **5** | **5** | **5** | **5** | 1 | | | | $1{,}62\cdot10^{16}$ |
| 6 | 5 | **5** | **5** | **5** | **5** | **4** | 2 | | | | $4{,}05\cdot10^{16}$ |
| 7 | 6 | **5** | **5** | **5** | **4** | **4** | **3** | | | | $6{,}75\cdot10^{16}$ |
| 8 | 6 | **5** | **5** | **4** | **4** | **4** | **4** | | | | $8{,}44\cdot10^{16}$ |
| 9 | 6 | **5** | **4** | **4** | **4** | **4** | **4** | 1 | | | $4{,}22\cdot10^{17}$ |
| 10 | 6 | **4** | **4** | **4** | **4** | **4** | **4** | 2 | | | $1{,}05\cdot10^{18}$ |
| 11 | 7 | **4** | **4** | **4** | **4** | **4** | **3** | **3** | | | $1{,}40\cdot10^{18}$ |
| 12 | 7 | **4** | **4** | **4** | **4** | **3** | **3** | **3** | 1 | | $5{,}62\cdot10^{18}$ |
| 13 | 7 | **4** | **4** | **4** | **3** | **3** | **3** | **3** | 2 | | $1{,}12\cdot10^{19}$ |
| 14 | 7 | **4** | **4** | **3** | **3** | **3** | **3** | **3** | **3** | | $1{,}50\cdot10^{19}$ |
| 15 | 8 | **4** | **3** | **3** | **3** | **3** | **3** | **3** | **3** | 1 | $6{,}00\cdot10^{19}$ |
| 16 | 8 | **3** | **3** | **3** | **3** | **3** | **3** | **3** | **3** | 2 | $1{,}20\cdot10^{20}$ |
| | | | | | | | | | **Всього** | | **$2{,}15\cdot10^{20}$** |

Формула розрахунку кількості можливих комбінацій паролів має вигляд:

$$U_l = C_l^m \cdot C_{l-m}^m \cdot C_{l-2m}^m \cdot \ldots \cdot C_{l-(p-1)m}^m \cdot C_{l-pm}^m \quad (3)$$

де:
*l*-кількість літер алфавіту,
*m* –кількість букв у слові (3…6),
*p* = 1…*m*, при умові: $m<pm<l$.

Отже для кожного рядка таблиці буде певне значення, що розраховується за формулою (3), а загальне значення кількості паролів множини $U_z$ буде сумою значень, що розраховані за формулою (3).

$$U_z = U_{l1}+\ldots+U_{l16} \quad (4)$$

Графічно множини паролів, умовно, можна зобразити так:

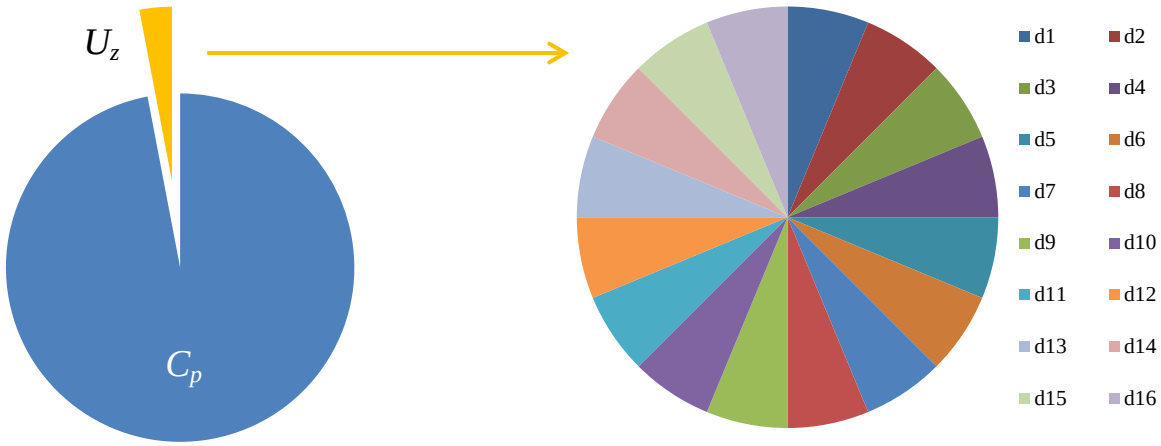


Рис. 1. Кількість слів, або набору символів, що може бути частиною паролю

Можливе використання ($C_p$ - $U_z$) та d1 або ($C_p$ - $U_z$) та d2 або ($C_p$ - $U_z$) та d3 і т.д., тому загальна кількість комбінацій можливих слів з 6, 5, 4, або 3 букв англійської мови складає $2{,}15 \cdot 10^{20}$ ($U_z$), а кількість можливих комбінацій паролів без даної комбінації слів становитиме $5{,}82 \cdot 10^{21}$ ($C_p$-$U_z$), на перебір яких потрібно на 681 млн. років менше (при умові підбору в 10 тисяч паролі за секунду), ніж у випадку комбінацій всіх можливих значень паролів ($C_p$), які описані вище, але за рахунок введення правила ускладненя $d$ та вибірковому додаванню паролів, вже маємо значення $1{,}25 \cdot 10^{42}$ ($C_k$), що розраховується за формулою (5):

$$C_k = (C_p - U_z) \cdot U_z \quad (5)$$

де $C_k$ - кінцева ускладнена комбінація,
$C_p$ – початкове значення комбінації,
$U_z$ – значення комбінацій слів з різної кількості букв, з формули (4)

Формула (5) отримана з суми добутків початкової комбінації $C_p$ без множини $U_z$ та значень $d$, що в результаті дає кінцеве, ускладнене значення.

**Висновки**

Розроблений метод генерування паролів, з введенням змінного правила ускладнення, значно зменшує ймовірність можливого підбору паролів, оскільки кінцеве значення ($C_k$) у $2{,}07 \cdot 10^{20}$ разів більше за початкове значення ($C_p$).

Розроблений метод підвищення захисту бездротових мереж може бути складовою для програмних та апаратних засобів захисту, а також може забезпечити використання для підвищення захисту облікових записів користувачів та інших систем захисту інформації, де необхідне використання надійних паролів.

Перспективним напрямком подальших досліджень є створення та підтримка в актуальному стані бази словників паролів для аналізу та подальша повна автоматизація запропонованого методу.

**Список використаної літератури**

1. Платоненко А. В. Сучасні загрози інформаційної безпеки для державних та приватних установ України / А. В. Платоненко. // Сучасний захист інформації. – 2015. – №4. – С. 86–90.

2. Платоненко А. В. Загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв та засоби їх захисту / А. В. Платоненко. // Сучасний захист інформації. – 2017. – №1. – С. 128–132.

3. Аносов А. О. Модель перехоплення та захист інформації в бездротових мережах / А. О. Аносов, А. В. Платоненко. // Сучасний захист інформації. – 2017. – №2. – С. 90–94.

4. Платоненко А.В. Средства защиты современных мобильных устройств в сетях нового поколения / А. В. Платоненко, А. А. Аносов. // Региональная конференция «Перспективы предоставления услуг на основе сетей пост-NGN, 4G и 5G. Организационные и технические решения по их построению и защите» – Київ: ДУТ, 2017.

5. Программы для создания словарей. [Електронний ресурс] – Режим доступу: https://hackware.ru/?p=2661

6. Взлом пароля методом грубой силы. Изучаем bruteforce атаку. [Електронний ресурс] – Режим доступу: https://geekmaze.ru/2016/03/04/izuchaem-bruteforce-ataku/

7. Грубая сила против паролей. [Електронний ресурс] – Режим доступу: https://geektimes.ru/company/amd/blog/277068/

Надійшла 05.08.2017 р. Рецензент: д.т.н., проф. Хорошко В.О.