УДК 343.1+004

Віталій Вікторович НОСОВ,
кандидат технічних наук, доцент,
професор кафедри інформаційних технологій та кібербезпеки
факультету № 4 Харківського національного університету внутрішніх справ

РОЗПОДІЛЕНИЙ КРИПТОАНАЛІЗ ПРИ ОБМЕЖЕНИХ РЕСУРСАХ ДЛЯ ПОТРЕБ ПРАВООХОРОННИХ ОРГАНІВ

Перед оперативними підрозділами правоохоронних органів при здійсненні досудового розслідування деяких кримінальних правопорушень виникає задача розшифрування вилучених у підозрюваного в скоєнні злочину зашифрованих симетричними криптосистемами даних, які можуть стати доказом у скоєнні злочину.

На практиці, при очевидній відсутності спеціалізованих обчислювальних ресурсів, підвищити обчислювальну ефективність криптоаналізу зашифрованих симетричними криптосистемами даних можна тільки за рахунок паралельної розподіленої клієнт-серверної атаки на базі локальної мережі персональних комп'ютерів, де сервер здійснює періодичний розподіл виділених підмножин простору можливих ключів шифрування між клієнтами, які в свою чергу передають задачу локальній програмі перебору ключів (ЛППК).

З точки зору застосовності системи розподіленого криптоаналізу (СРК) в оперативних підрозділах правоохоронних органів можна сформулювати вимоги до її компонентів:

1) максимальна універсальність до типів зашифрованих даних;

2) відкриті вихідні коди і ліцензія вільного програмного забезпечення;

3) функціонування на різних платформах;

4) обчислення як на центральних, так і на графічних процесорах клієнтських персональних комп'ютерів;

5) операційна система Windows на клієнтських персональних комп'ютерах;

6) необмежена кількість клієнтів.

Максимальну універсальність до типів зашифрованих даних забезпечує вилучення гешу ключа шифрування із різних об'єктів зашифрованих даних (*.docx, *.pdf, *.zip, *.7z, *.rar, та ін.) і обчислення гешу від імовірних ключів для порівняння із вилученим.

ЛППК, що відповідають вище зазначеним вимогам, можуть бути або *Hashcat*[3], або *John the Ripper jumbo release (JtR)*[4]. Для них існують взаємно сумісні програмні рішення вилучення гешу ключа із багатьох типів зашифрованих даних [5,6]. У якості СРК, які використовують Hashcat або JtR і задовольняють встановленим вимогам, можуть бути: *Hashtopolis*[7], *Fitcrack*[8], *Cracklord*[9], *GoCrack*[10].Розробники Fitcrack в [1] навели результати експериментального дослідження ефективності свого рішення у порівнянні із Hashtopolis, де для кожного типу перебору ключів (повний перебір, за шаблоном, за словником, гібридний) запропонували різну стратегію розподілу завдань. Fitcrack в цілому показав більшу ефективність і більш високий рівень абстракції та автоматизації розподіленого криптоаналізу. Результати подібних досліджень ефективності та застосовності рішень Cracklord та GoCrack не знайдені.

Для оцінки застосовності СРК в локальної мережі із 21 ПК під управлінням ОС Windows 7 Professional у зв'язці з Hashcat був інстальований та перевірений на працездатність Hashtopolis. Серверна частина була розгорнута в ОС Kali Linux Light на віртуальній машині Oracle VM VirtualBox, а клієнтська в середовищі Python 3.7.2 ОС Windows. Результати тестування розподіленого перебору ключів для гешів, обчислених за різними алгоритмами, підтвердили працездатність Hashtopolis та показали, що зростання швидкості паралельних обчислень не є прямо пропорційним до кількості агентів із-за витрат часу на формування підмножин простору ключів, їх доставки агентам і отриманням результатів перебору.

З урахуванням [1] та проведеного тестування була ідентифікована задача із оптимального визначення для клієнтів розміру підмножини простору можливих ключів (chunk) в залежності від кількості агентів, їх

3 https://hashcat.net/
4 https://www.openwall.com/john/
5 https://github.com/stricture/hashstack-server-plugin-hashcat/tree/master/scrapers
6 https://github.com/magnumripper/JohnTheRipper/tree/bleeding-jumbo/run
7 https://github.com/s3inlc/hashtopolis
8 https://github.com/nesfit/fitcrack
9 https://github.com/jmmcatee/cracklord
10 https://github.com/fireeye/gocrack

поточної швидкості перебору, алгоритму гешу, типу перебору (повний перебір, за шаблоном, за словником, гібридний).

В подальшому, після порівняльної оцінки вище зазначених СРК, доцільна розробка набору різних конфігурацій найбільш ефективної СРК із методикою їх оптимального застосування оперативними підрозділами правоохоронних органів.

Список бібліографічних посилань

1. Hranický R., Zobal L., Ryšavý O., Kolář D. Distributed password cracking with BOINC and hashcat. *Digital Investigation*. 2019. Vol. 30, No. 1. Pp. 161–172. URL: https://www.fit.vut.cz/research/publication-file/11961/Distributed_password_cracking_with_BOINC_and_hashcat.pdf (дата звернення: 25.04.2020).

Одержано 26.04.2020