5. Співпраця з іншими джерелами - для збору інформації можна звертатися до джерел, таких як люди, експерти, співробітники організацій, які можуть надати корисну інформацію.

Ці методи можуть бути використані окремо або в комбінації з іншими методами для здійснення OSINT. Важливо також враховувати законодавство та етичний кодекс.

УДК 004.056.5

МЕТОД ДВІЙНОГО ХЕШУВАННЯ SHA З ДОДАТКОВИМ ПЕРЕБОРОМ

Денис Іванов
Київський національний університет будівництва і архітектури
denys.ivanov20@gmail.com

Метод двійного хешування SHA з додатковим перебором є ефективним і безпечним способом захисту інформації від несанкціонованого доступу. Даний метод використовує два послідовних хешування з використанням різних алгоритмів SHA, що дозволяє збільшити безпеку процесу.

Для підвищення безпеки методу, можна застосовувати додатковий перебір, який полягає у генерації випадкових значень та їх використанні у якості солі для хешування. Це дозволяє змінювати вихідний результат хешування для однакових даних, що унеможливлює зловмисникам відновлення вхідних даних.

Ще однією перевагою методу двійного хешування SHA з додатковим перебором є його швидкість та простота використання. Даний метод може бути використаний для захисту даних на різних рівнях, включаючи зберігання паролів та інших конфіденційних даних. Незважаючи на всі його переваги, метод двійного хешування SHA з додатковим перебором не є бездоганним. Існує можливість атаки методу шляхом зламування хеш-функцій, тому важливо регулярно оновлювати алгоритми хешування та солі для максимальної безпеки.

На сьогоднішній день методами локально чутливого-хешування (LSH) використовують майже у всіх сферах IT воно є досить актуальними. LSH – це метод, який знижую розмір багатомірних даних. Уявити апаратний або технічний засіб без використання LSH досить складно. Вони допомагають, знаходити дублікати, задіяні у кластеризації та конізації даних, знаходження найближчого сусіда, особливим представлення хешування є те що можна шифрувати в особистому коді інформацію. Для створення рекомендацій можуть використовуватися дані про дії користувача або його характеристики. У роботі розглядається задача кодування текстової інформації у хеш представлення та конізації даних. Представлення набору даних у вигляді LSH дуже важлива тому що саме цю методику використовують у збережені важливої інформації у базах даних, саме метод чутливого-хешування захищає нашу особисту інформацію від зловмисників.

Захист та конфіденційність даних у базах даних одна із головних умов успішного підприємства. Захист паролів та тексту представленого та записаного в базах даних потрібна особливого догляду да контролю. У випадку атаки на систему та втрати даних потягне за собою колосальні збитки та втрати клієнтського базису. Запорукою надійності є повторне хешування даних з використанням солей та повторних алгоритмів cost для надійності та затримання циклу. Швидкість не завжди є добре на живому прикладі з хешуванням даних, можна сказити, що чим швидша хеш функція, тим більш вона вразлива для повного перебору. Всі приклади паролів хешу за алгоритмом MD5 та SHA і зберігаються у вигляді хеш-значень у базі даних.

MD5 – це 128-бітний алгоритм хешування, розроблений професором Рональдом Л. Призначений для створення «відбитків» або дайджестів повідомлення довільної довжини і подальшої перевірки їх достовірності. Широко застосовувався для перевірки цілісності інформації та зберігання хеш паролів у базах даних.

SHA (Secure Hash Algorithm) - це сімейство криптографічних алгоритмів хешування, розроблених Національним інститутом стандартів і технологій (NIST) США. Він використовується для створення унікальних «відбитків» даних, які мають фіксовану довжину. SHA є більш безпечним алгоритмом, ніж MD5, оскільки він використовує більш складні математичні операції та має більшу довжину хешу. Однак, з появою нових технологій і збільшенням обчислювальної потужності комп'ютерів, деякі версії SHA також можуть бути вразливими до атак. Ці алгоритми широко використовуються для перевірки цілісності даних, створення цифрових підписів та збереження хеш паролів у базах даних. У разі крадіжки бази вихідні паролі можуть бути відновлені за допомогою заздалегідь підготовлених райдужних таблиць , так як часто користувачі використовують ненадійні паролі, що легко підбираються за словниками. Якщо ж пароль "посолити", тобто при обчисленні хеш-значень приєднати до вхідних даних рядок з декількох випадкових символів, які будуть значенням солі, то результуючі значення не співпадатимуть з поширеними словниками хеш-значень.

Знання солі дозволяє згенерувати нові словники для перебору, тому значення солі має зберігатись у таємниці. Для солі вірні ті ж рекомендації до складності, що і для складності пароля, тобто значення солі має мати хорошу ентропію і довжину. Використання методу хешування SHA з додатковим перебором та використанням прикладних солей. Аналіз останніх дослідження показали, що із швидким рухом розвитку комп’ютерної індустрії росте потужність апаратної одиниці і постала проблема захищеності даних представлених у хеш значені, завдяки перебору по алгоритму не постане проблема знайти відповідну колізію до вже отриманого хеш значення.

Алгоритм SHA по собі вже застарілий, але його продовжують активно використовувати і по цей час і саме для нас постає головне питання у використанні алгоритму хешування з додатковим перебором та використання адаптивних солей для надійного шифрування даних, які представляються у базах даних.

Література

1. Next Generation Firewall. URL:https://www.fortinet.com/ru/products/next - ge neration-firewall
2. Top 5 best NGFW vendors of 2021. URL: https://www.nomios.com/news-blog/top-5-next-generation-firewall-vendors-ngfw-2022/
3. Finding SHA-1 Характеристики: General Results and Applications (англ.). Дата звернення: 4 жовтня 2017 року. Архівовано 26 липня 2008 року.
4. SHA-1 Collision Search Graz (англ.). - Дослідницький проект технолог ічного університету Граца . Архівовано з оригіналу 7 листопада 2008 року.

УДК 004.056

КЛАСИФІКАЦІЯ ТА АНАЛІЗ ЗАГРОЗ В ІНТЕЛЕКТУАЛЬНИХ ТРАНСПОРТНИХ СИСТЕМАХ

Павло Ігнатоля[1], Ярослав Сивохоп[2], Василь Різак[3]
Ужгородський національний університет
[1]pavlo.ihnatolia@uzhnu.edu.ua, [2]syvockhop@gmail.com,
[3]editor@physics.uz.ua

Урбанізація та технологічна революція з початку 1990 року спричинила появу концепцій “розумних міст” - населених пунктів, що використовують передові технології та керовані даними рішення для покращення якості життя своїх мешканців, підвищення їх безпеки та оптимізації міських послуг.

Основою функціонування будь-якого міста є його транспортна інфраструктура - це і фізична інфраструктура, така як дороги, мости та тунелі, а також транспортні системи, як-от громадський транспорт, системи спільного використання велосипедів та самокатів та інші автономні транспортні засоби.

Метою даної роботи є встановлення, класифікація та аналіз загроз в інтелектуальних транспортних системах для подальшої розробки комплексної системи захисту (КСЗІ) для інтелектуальних транспортних систем.

Розумна транспортна інфраструктура використовує технології та дані для створення ефективної, безпечної та зручної транспортної системи для жителів міста. Це відбувається шляхом впровадження широкого спектру технологій:

- обладнання для збору інформації - це різні IoT-пристрої, камери відеонагляду, GPS датчики та інші пристрої, що збирають інформацію про поточну завантаженість доріг та транспортних вузлів.
- Технологій для передачі даних (мобільні мережі, WiFi та провідне підключення) та протоколів комунікації (HTTPS, MQTT, LoRa/ZigBee) для доставки зібраних даних до центрів їх обробки.
- Центрів обробки інформації та прийняття рішень, де проводиться аналіз великих об'ємів даних в режимі реального часу та прийняття рішень про оптимізацію трафіку.

Разом з цим виникають нові загрози та виклики, притаманні розумній транспортній інфраструктурі та необхідність впровадження захисту від них.

Виділимо наступні типи загроз для розумної транспортної інфраструктури: