Державна служба України з надзвичайних ситуацій
Національний університет цивільного захисту України

ЗВД

ЗАПОБІГТИ
ВРЯТУВАТИ
ДОПОМОГТИ

Матеріали міжнародної науково-практичної конференції молодих учених «Проблеми та перспективи забезпечення цивільного захисту»

ХАРКІВ 2024

ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

МАТЕРІАЛИ

міжнародної науково-практичної конференції молодих учених

«Проблеми та перспективи забезпечення цивільного захисту»

Харків – 2024

УДК 614.8

Проблеми та перспективи забезпечення цивільного захисту: матеріали міжнародної науково-практичної конференції молодих учених. Харків: НУЦЗУ, 2024. 558 с. Українською та англійською.

Включено матеріали, які доповідались на міжнародній науково-практичній конференції молодих учених на базі Національного університету цивільного захисту України.

Розглядаються аспекти вдосконалення цивільного захисту держави.

Матеріали розраховані на інженерно-технічних працівників Державної служби України з надзвичайних ситуацій, науково-педагогічний склад, ад'юнктів, слухачів, студентів та курсантів закладів вищої освіти України та інших країн світу.

СКЛАД ОРГКОМІТЕТУ КОНФЕРЕНЦІЇ

УДК 004.5

ПОРІВНЯННЯ ШВИДКОДІЇ HMAC АЛГОРИТМІВ

Малярова Д.М., ХНУРЕ
НК – Маляров М.В., к.т.н., доцент, НУЦЗУ

На сьогоднішній день інформаційні технології стали невід'ємною частиною суспільства, забезпечуючи збір, зберігання та обмін даними. Розвиток криптографії та програмного захисту інформації набуває все більшого значення, але викликом залишається постійне покращення їхньої надійності.

Автентифікація (англ. authentication) – процедура перевірки відповідності пред'явленого ідентифікатора об'єкта комп'ютерної системи на предмет належності його цьому об'єкту; встановлення або підтвердження автентичності [1].

Коди автентифікації, або MAC-коди (англ. message authentication code) – криптографічні геш-функції, для обчислення яких необхідно знати секретний ключ, використання якого дозволяє гарантує неможливість підміни захищених об'єктів. MAC-коди дуже корисні для перевірки автентичності без порушення безпеки [2].

HMAC (ISO/IEC 9797-1) – MAC-код на основі геш-функції, що має таку перевагу, що дозволяє повторне використання існуючих реалізацій геш-функції. MAC-коди на основі геш-функції та секретного ключа найбільш загальні методи, оскільки вони звичайно швидше, ніж коди на основі блокового шифру [3].

При реалізації HMAC можуть використовуватися різні функції гешування, такі як Whirlpool, MD4, MD5, RIPEMD, SHA-0, SHA-1, SHA-2 (SHA-256, SHA-384, SHA-512), Tiger та інші. Швидкість обчислень визначається кількістю циклів процесора, затрачуваних на один байт оброблюваного повідомлення [3]:

- Алгоритм HMAC-Whirlpool, HMAC-SHA-512 мають найбільшу довжину коду та довжину ключа. А найбільшу довжину ключа, але найкоротшу довжину коду мають алгоритми HMAC-MD4 та HMAC-MD5.
- Найшвидшим алгоритмом на усіх типах процесора (Pentium2, PIII/Linux, Pentium4, Xeon, AMD) є HMAC-MD4, а другим за швидкодією є HMAC-MD5. Найповільнішими є алгоритми HMAC-SHA-384 і HMAC-SHA-512.

Довжина коду та довжина ключа можуть змінюватися залежно від алгоритму гешування та типу процесора. Загалом, алгоритми з більшою довжиною коду більш безпечні, але вимагають більше обчислювальних ресурсів.

Таким чином, автентифікація, шифрування даних та використання кодів автентифікації (MAC-кодів) забезпечують безпеку під час обробки та передачі даних, дозволяючи перевіряти автентичність та запобігати підробкам. Алгоритми HMAC, базовані на різних функціях гешування, є ефективними та універсальними методами для створення кодів автентифікації, дозволяючи забезпечити безпеку інформації у сучасних інформаційних системах.

ЛІТЕРАТУРА

1. Захарченко М. В. Асиметричні методи шифрування в телекомунікаціях: навч. посіб. М. В. Захарченко, О. В. Онацький, Л. Г. Йона, Т. М. Шинкарчук. Одеса: ОНАЗ ім. О. С. Попова, 2011. 184 с.

2. Шнаер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. Б. Шнаер. 2-е изд. М.: ТРИУМФ, 2001. 308 с.

3. Євсеєв С. П. Гешування даних в інформаційних системах: монографія. С. П. Євсеєв, О. Ю. Йохов, О. Г. Король. Х.: Вид. ХНЕУ, 2013. 312 с.

Секція 6. Психологічне та гуманітарне забезпечення оперативно-рятувальних підрозділів