УДК 004.75

РОЗВИТОК КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ АНОНІМНОЇ МАРШРУТИЗАЦІЇ В ІНТЕРНЕТ

Людмила Ковальчук[1], Роман Олійников[2], Юрій Беспалов[3], Ганна Неласа [4]

[1]Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, lusi.kovalchuk@gmail.com,
[2]Харківський національний університет ім. В.Н. Каразіна, roliynykov@gmail.com,
[3]Інститут теоретичної фізики ім. М.М. Боголюбова Національної академії наук України, yu.n.bespalov@gmail.com,
[4]Національний університет "Запорізька політехніка" annanelasa@gmail.com

Із розвитком сучасного суспільства базові послуги безпеки інформації при користуванні Інтернет стають дедалі важливішими. При цьому важливим є не тільки забезпечення цілісності та конфіденційності передачі критичної інформації по телекомунікаційним каналам, а й збереження анонімності абонентів, які є учасниками взаємодії. Стрімкий розвиток децентралізованих систем в останні роки приділяє особливу увагу наявності властивості анонімності суб'єктів криптографічних протоколів.

Метою даної роботи є розробка алгоритму децентралізованого сліпого порогового перешифрування для створення криптографічного протоколу анонімної маршрутизації в Інтернет.

Порівняння технологій Proxy, VPN та Tor приводить до висновку, що Proxy-сервер зручно використовувати для захисту локальної мережі від зовнішнього доступу, в роботі VPN головне – приватність, а при використанні Tor головне – анонімність. Tor зашифровує трафік тричі, ніби створюючи три шари цибулини. Щоразу користувач потрапляєте до Інтернету за допомогою випадкового комп'ютера-волонтера, шлях постійно змінюється, а сам браузер за замовчуванням не зберігає історію.

В [1] було представлено методи аналізу трафіку, які дозволяють зловмисникам, які лише частково бачать мережу, визначати, які вузли використовуються для ретрансляції анонімних потоків, і в такий спосіб створюють загрози анонімності користувачів мережі Tor. До того ж, якщо зловмисник контролює достатньо велику частину вузлів Tor мережі, існує не нульова ймовірність, того, що трафік саме того учасника, який цікавить атакуючого, пройде через ці вузли.

Ми пропонуємо підхід, який дозволяє для переадресації між мережами використовувати порогове сліпе перешифрування, яке базується на схемі шифрування Ель-Гамаля в групі точок еліптичної кривої, зокрема на її властивостях гомоморфності. Також для побудови протоколу ми використовуємо порогову схему генерації ключів [2] і децентралізовану схему використання шар відкритого ключа

та (NIZK) доведення без розголошення рівності дискретних логарифмів. Також ми вважаємо, що існує деякий децентралізований *комітет*, який виконує певні дії у цьому протоколі. Зазначимо, що існування такого комітету не порушує децентралізацію протоколу, оскільки всі дії комітету є децентралізованими і єдиною вимогою до нього є наявність чесної більшості.

Цей протокол працює коректно з будь-якою кількістю децентралізованих учасників за єдиною умовою, що кількість учасників більша за певний поріг. Алгоритм сліпого перешифрування подібно до алгоритму сліпого підпису працює наступним чином: той, кому адресоване зашифроване повідомлення, використовуючи децентралізовану схему генерації ключа і інші вказані нами протоколи, комітет [3] перешифровує повідомлення з використанням відкритого ключа іншого абонента, не розшифровучи його і не читаючи його вміст. Тобто тут суть в тому, що він перешифровує на іншому відкритому ключі, не розшифровуючи, тобто не бачачи вміста цього повідомлення.

Для підгрупи E великого простого порядку q групи точок еліптичної кривої та фіксованої базової точки $G \in \mathbf{E}$, визначимо *ElGamal* перетворення:

$$E_{r,H} : \mathbf{E} \times \mathbf{E} \to \mathbf{E} \times \mathbf{E},$$

в залежності від параметра $r \in \{2,...,q-2\}$ та $H \in \mathbf{E}$, як зсув на елемент $(rG, rH) \in \mathbf{E} \times \mathbf{E}$:

$$E_{r,H}(V_1, V_2) = (V_1 + rG, V_2 + rH) = \left(E_r^{(1)}(V_1), E_{r,H}^{(2)}(V_2)\right). \quad (1)$$

При використанні Tor-браузера анонімність забезпечується наявністю трьох шарів маршрутизації, тобто є лише один проміжний вузол, який розділяє вхід і вихід. Відповідно, якщо злочинець контролює цей проміжний вузол, він може деанонімізувати абонентів на вході та виході.

Основна ідея протоколу, що пропонується, полягає в заміні цього проміжного вузла комітетом, який і виконує сліпе порогове перешифрування з використанням порогової схеми. В цьому випадку для того, щоб зв'язати конкретного користувача з конкретним виходом, зловмиснику необхідно контролювати більшість вузлів мережі. Ця схема дійсно буде працювати повільніше, ніж Tor-браузер, та не може бути використаною для взаємодії реального масштабу часу (відео, аудіо). Але вона є ефективною саме для маршрутизації приватних повідомлень, якщо потрібен високий рівень анонімності.

Література

1. Steven J. Murdoch and George Danezis Low-Cost Traffic Analysis of Tor, 2006, https://murdoch.is/papers/oakland05torta.pdf.

2. Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, Tal Rabin, Secure Distributed Key Generation for Discrete-Log Based Cryptosystems, 2006, https://link.springer.com/article/10.1007/s00145-006-0347-3.

3. Bingsheng Zhang, Roman Oliynykov, Hamed Balogun A Treasury System for Cryptocurrencies: Enabling Better Collaborative Intelligence, Network and Distributed // System Security (NDSS) Symposium 2019, https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_02A-2_Zhang_paper.pdf.

УДК 004.056

THE STATE OF CYBER SECURITY OF UKRAINE DURING A FULL-SCALE INTRUSION

Dora Sabov[1], Pavlo Mulesa[2], Marianna Sharkadi[3]
[1] Uzhhorod National University, szabodora20@outlook.hu
[2] Uzhhorod National University, pavlo.mulesa@uzhnu.edu.ua
[3] Uzhhorod National University, marianna.sharkadi@uzhnu.edu.ua

Over the course of the past decade, Ukraine has unfortunately been subjected to a persistent and alarming pattern of cyberattacks, with a significant number of these incidents being attributed to Russia. In fact, recent statistics indicate that the Ukrainian state has endured a staggering total of 397,000 separate attacks in the year 2020 alone, with a similarly high number of approximately 280,000 attacks occurring within the first 10 months of 2021.

It is important to recognize that the impact of these cyberattacks extends far beyond the immediate security implications for the Ukrainian state itself. The use of digital means to target critical infrastructure, financial institutions, and government entities in Ukraine represents a serious threat to regional and global stability, with the potential to inflict harm and disrupt operations far beyond Ukraine's borders.

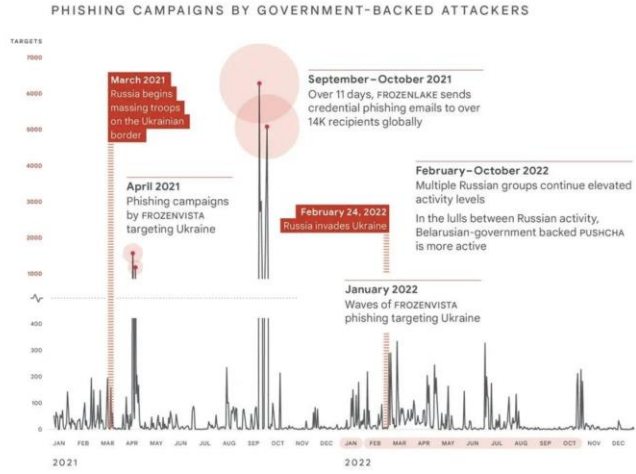

Figure 1. Phishing campaigns by government-backed attackers