АНАЛІЗ ДЕЦЕНТРАЛІЗОВАНОГО ПРОТОКОЛУ ОБМІНУ ПОВІДОМЛЕННЯМИ BITMESSAGE

Гріненко Т.О., Мандич Д.Р.
Науковий керівник – д.т.н., проф. Олійников Р.В.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. БІТ, тел. +38 (057) 702-14-25)
e-mail: madr0310@gmail.com

In the work will been represented an idea of peer-to-peer decentralized message protocol, its properties, characteristics, need for the modern world and possible ways to use.

Після повідомлення Едварда Сноудена про те, що за більш ніж мільярдом людей в 60 країнах ведеться глобальне стеження, виникла необхідність створення дійсно конфіденційного засобу комунікації. Вже через рік, а саме 21 березня 2013 року, вийшла перша бета-версія клієнта BitMessage [1,2]. Ключовою інновацією протоколу BitMessage стала відсутність центральних серверів або будь-якого центру, який обробляє дані. Протокол працює за схемою peer-to-peer, тобто кожен вузол є і клієнтом, і сервером одночасно, а єдиний сервер відсутній [1,2].

Протокол підтримує обмін зашифрованими повідомленнями, використовуючи end-to-end шифрування. Це означає, що повідомлення може прочитати тільки відправник і одержувач, а жодна проміжна ланка не має такої можливості.

Варто зазначити, що для кожного повідомлення, яке передається по мережі BitMessage, використовується алгоритм доказу виконання роботи proof-of-work. Щоб відправити повідомлення, автор повинен виконати деяку ресурсномістку роботу. Складність proof-of-work залежить від обсягу повідомлення і обсягу вкладень, що входять в нього.

BitMessage використовує модель анонімності, яку можна охарактеризувати як «всі отримують все», що є формою приватного пошуку інформації, яка, як відомо, є теоретично безпечною, але також неефективною. Ця модель ускладнює, якщо не унеможливлює, визначення повідомлень, призначених для користувачів. У поєднанні з відсутністю метаданих BitMessage здається близьким до досягнення цієї властивості в практичному сенсі. Протокол приховує відправника і одержувача. Ця властивість досягається за рахунок того, що ні відправник, ні одержувач не розголошують ніякі ідентифікатори (наприклад, відкриті ключі, BitMessage-адреси або мережеві адреси користувачів). Крім цього, будь-який користувач може використовувати Tor для підключення до інших учасників мережі. Підключення через Tor дозволяє приховати сам факт використання BitMessage с точки зору зовнішнього спостерігача. У протоколі також є можливість підпису повідомлення для підтвердження авторства тексту повідомлення і для забезпечення цілісності. Передбачена

підтримка відкритих каналів, наприклад, для новинних або інформаційних ресурсів. Тобто, існує адреса, яку може прослуховувати будь-який бажаючий користувач. Ця функція працює аналогічно каналам в Telegram або розсилкам в звичайній пошті. Також є підтримка закритих групових чатів. Тобто серед бажаючих користувачів створюється загальний секрет, за допомогою якого шифруються повідомлення в цьому чаті. Причому, для цього необов'язково вказувати одну зі своїх адрес. Закритий чат неможливо цензурувати, видалити або заблокувати.

У протоколі Bitmessage для зашифрування даних використовується алгоритм AES з довжиною блоку 256 біт, який працює в режимі CBC (Cipher Block Chaining) [3]. В даному випадку ключ розраховується як загальний секрет між відправником і отримувачем за схемою ECDH (Elliptic-curve Diffie-Hellman). Такий секрет відправник може отримати автономно без взаємодії з одержувачем. Для цього йому необхідно використовувати свій особистий ключ і відкритий ключ одержувача. Одержувач, використовуючи свій особистий ключ і відкритий ключ відправника, зможе отримати аналогічний секрет. Таким чином, обидва учасники мають однаковий секрет для зашифрування повідомлень. Також, для підвищення рівня безпеки алгоритму ECDH може використовуватися рандомізатор для генерації нового ключа шифрування для кожного нового повідомлення. Реалізація шифрування в BitMessage заснована на бібліотеках з відкритим вихідним кодом, що вважається гарною практикою. BitMessage використовує бібліотеки OpenSSL для реалізації генерації випадкових чисел, шифрування і гешування.

Протокол BitMessage може використовуватися в додатках, в яких необхідно забезпечувати анонімність і конфіденційність. Протокол також є можливою гарною альтернативою звичайній електронній пошті. BitMessage представляє систему, яка об'єднує електронну пошту і безпеку PGP.

Протокол BitMessage забезпечує високий рівень безпеки та анонімності, але є специфічним в роботі: відсутня миттєва відправка повідомлень, також необхідна стабільна робота ПК та інтернету.

Список джерел:

1. BitMessage Wiki [Електронний ресурс] – Режим доступу до ресурсу: https://bitmessage.org/wiki/Main_Page.

2. Jonathan Warren, Bitmessage: A Peer-to-Peer Message Authentication and Delivery System, 2012.

3. Fips 197 «Advanced Encryption Standard», 2001.