УДК 004.056.53

М.Д. Кренцін
Л.М. Куперштейн

АНАЛІЗ ПРОТОКОЛІВ ПІРИНГОВИХ МЕРЕЖ

Вінницький національний технічний університет

Анотація

Розглянуто концепцію піринговоі мережі. Проаналізовано ряд поширених протоколів однорангових мереж. Виявлено особливості, переваги та сфери застосування кожного з протоколів. Проаналізовано основні вразливості кожного протоколу. Серед протоколів піринових мереж основними було взято BitTorrent, Gnutella, G2, Tox, Skype та Ethereum.

Ключові слова: пірингова мережа, Http, Ad-Hoc, веб-сервер, блокчейн, TCP, UDP, протокол, GNU, Tiger хеш, SHA-1, майнер, транзакція.

Abstract

The concept of peer-to-peer network is considered. Several common peer-to-peer protocols are analyzed. Features, advantages, and areas of application of each of the protocols are revealed. The main vulnerabilities of each protocol are analyzed. Among the peer-to-peer network protocols, the main ones were BitTorrent, Gnutella, G2, Tox, Skype and Ethereum.

Keywords: peer-to-peer network, Http, Ad-Hoc, webserver, blockchain, TCP, UDP, protocol, GNU, Tiger hash, SHA-1, miner, transaction.

Вступ

Нинішнє суспільство називають інформаційним, адже головним продуктом сьогодні є знання та інформація. Використання новітніх інформаційно-комунікаційних технологій, робота з різноманітними ґаджетами перекладається на якісно новий рівень. Але разом з тим, особливу увагу необхідно приділити безпеці цієї інформації, забезпеченню її цілісності та конфіденційності. Для цього було створено пірингові мережі.

Концепція однорангової (пірингової, peer-to-peer, P2P) мережі була вперше використана в 1969 р [1]. В свою чергу P2P розглядається як мережевий протокол, що забезпечує можливість створення мережі однорангових вузлів та їх взаємодію. У багатьох випадках мережі P2P використовують існуючі протоколи стеку TCP/IP для передачі, а саме TCP, UDP або їх обгортки [2]. Різні протоколи створюються для вирішення різних задач, у тому числі й захищеності самої мережі та даних. Також різні протоколи спрямовані на сторення вузькоспеціалізованих систем (обмін файлами, блокчейн тощо).

На сьогоднішній день не існує якогось універсального протоколу обміну даними в P2P мережі, адже неможливо передбачити всі потенційні вразливості та створити універсальний захист від усіх існуючих типів атак на однорангові мережі. Проте актуальним є аналіз існуючих протоколів, виявлення їх переваг та недоліків, а також певних особливостей реалізації. Це в свою чергу сприятиме забезпеченню в майбутньому цілісності, доступності та конфіденційності даних за рахунок вдосконалення існуючих рішень.

Результати дослідження

Пірингова мережа – це технологія, що реалізує об’єднання однорангових вузлів рівного статусу з собі подібними. Кожен вузол є і приймачем, і надавачем послуг. Такі вузли можуть обмінюватись інформацією безпосередньо [3]. Різні P2P мережі спрямовані на вирішення різного роду задач. Є як вузькоспеціалізовані системи (файлообмін), так і ті, що вирішують більш широкий спектр задач (месенджери, блокчейн). Однорангові мережі використовуються також у IP-телефонії, системах передачі потокового відео (P2PTV), для групової роботи, роботи з електронними гаманцями тощо [4].

Задля забезпечення надійного функціонування вищеописаних систем, при створенні піринговых мереж використовуються різні протоколи передачі та обміну даними. Кожен з них має свої особливості [5]. Тому розглянемо найбільш поширені:

1. BitTorrent — це комунікаційний протокол для однорангового обміну файлами (P2P), який дає змогу користувачам децентралізовано поширювати дані та електронні файли через Інтернет. Для надсилання або отримання файлів користувачі використовують клієнт BitTorrent на своєму комп'ютері, підключеному до Інтернету. Клієнт BitTorrent — це комп'ютерна програма, яка реалізує протокол BitTorrent. Популярні клієнти включають µTorrent, qBittorrent, BitComet та ін [6].

Однією з вразливостей цього протоколу є атака UDP-флуда. Реалізації BitTorrent часто використовують µTP для спілкування. У лабораторному середовищі P2P можна було проводити атаки «Відмова в обслуговуванні», де користувачі, які використовують клієнти BitTorrent, діють як підсилювачі атаки на іншу службу [7]. Кілька досліджень BitTorrent виявили файли, доступні для завантаження, що містять шкідливе програмне забезпечення. Зокрема, одна невелика вибірка вказала, що 18% усіх виконуваних програм, доступних для завантаження, містили шкідливе програмне забезпечення [8]. Інше дослідження стверджує, що аж 14,5% завантажень BitTorrent містять програмне забезпечення з вразливістю нульового дня, і що BitTorrent використовувався як механізм розповсюдження для 47% усіх знайдених програм з такою вразливістю [9].

2. Tox — це одноранговий протокол обміну миттєвими повідомленнями та відеодзвінками, який пропонує наскрізне шифрування. Заявлена мета проекту – забезпечити безпечне, але легкодоступне спілкування для кожного [10]. Використовує піринговий обмін інформацією для поліпшення пропускної здатності, але не вимагає реєстрації для використання, а ідентифікатор користувача створюється локально. Після установки клієнту Tox автоматично створюється пара ключів. Публічний ключ можна передавати кому завгодно — він служить як унікальний ідентифікатор для пошуку співрозмовника. Секретний ключ зберігається тільки у власника і підтверджує його справжність, не розкриваючи особисті дані.

Вразливим місцем даного протоколу є те, що IP-адреса вузла супроводжує кожен відправлений пакет даних [11]. Це в свою чергу дозволяє хакерам отримати особисту інформацію або місцезнаходження, якщо їх опублікувала третя сторона, або ж використати ці дані для різного роду атак на мережі.

3. Gnutella — це одноранговий мережевий протокол. На основі протоколу було реалізовано першу децентралізовану одноранговую на основі цього протоколу [12]. Протокол розроблений дуже відмовостійким. Виконуються всі пошуки через мережу Gnutella, поки всі файли обробляються в автономному режимі. Таким чином кожен вузол, який потребує файл запускає веб-сервер (міні HTTP 1.1) і спілкується із зацікавленими серверами через HTTP-команди. Відразу після того, як вузол отримав дійсну IP-адресу та порт сокета іншого сервера, він може виконати кілька запитів, надіславши дескриптори запиту та отримувати результати асинхронно.

Незважаючи на велику відмовостікість та переваги протоколу, мережі, що його реалізують вразливі до ряду атак [13]. У Gnutella немає положень для запобігання атак розподіленої відмови в обслуговуванні (DDoS). Ця атака стає можливою якщо вузол отримає якийсь спам-файл, що є активатором атаки. Даний протокол також вразливий до атаки «IP Harvesting». Оскільки для отримання наявних учасників мережі, IP-адреса повинна бути доступна для сканування, то це дає змогу хакерам здійснити атаку. Ще одна вразливість – це введення вірусів через Push-повідомлення. Протокол Gnutella побудований таким чином, що коли один вузол надсилає повідомлення іншому, то він його приймає без всякої перевірки, довіряючи контенту. А насправді там може бути небажаний вміст.

4. Gnutella2 (який часто називають G2) — це протокол однорангового зв'язку, розроблений в основному Майклом Стоксом і випущений у 2002 році. Незважаючи на те, що G2 був натхненний протоколом Gnutella, він мало поділяє свій дизайн, за винятком механізму рукостискання, з'єднання та завантаження [14]. G2 використовує розширюваний формат двійкових пакетів і абсолютно новий алгоритм пошуку. Крім того, G2 має споріднену (але істотно іншу) топологію мережі та покращену систему метаданих, яка допомагає ефективно зменшувати кількість підроблених файлів, таких як віруси, у мережі. Для ідентифікації файлів і безпечної перевірки цілісності файлів G2 використовує хеші SHA-1. Для забезпечення надійного паралельного завантаження файлу з кількох джерел, а також для надійного завантаження частин під час завантаження файлу, використовуються Tiger хеші. На основі цього протоколу були реалізовані ще кілька схожих, проте вони не набули поширення у сьогоденні.

Незважаючи на значні покращення протоколу Gnutella2, мережі, що його реалізують мають ті ж вразливості, що й Gnutella. Усі покращення спрямовані та покращення швидкодії та забезпечення цілісності даних.

5. Skype protocol – це протокол, що був створений 2003 року для мережі Skype, була першою одноранговою мережею IP-телефонії. Мережа містить три типи сутностей: супервузли, звичайні вузли та сервер входу [15]. Кожен клієнт підтримує кеш хоста з IP-адресою та номерами портів доступних супервузлів. Каталог користувачів Skype децентралізований і розподілений між супервузлами в мережі. Супервузли групуються в слоти (9–10 супервузлів), а слоти групуються в блоки (8 слотів). Супервузли ретранслюють зв'язок від імені двох інших клієнтів, обидва з яких знаходяться за брандмауерами або трансляцією мережевих адрес (NAT) «один до багатьох». Без ретрансляції через супервузли два клієнти з проблемами з брандмауером або NAT не зможуть здійснювати або отримувати дзвінки один від одного. Skype намагається змусити обидві сторони напряму узгодити деталі з'єднання, але іноді сума проблем на обох кінцях може перешкодити встановленню прямої розмови. Потік даних шифрується за допомогою RC4; однак метод лише обфускує трафік, оскільки ключ можна відновити з пакета. Голосові дані шифруються за допомогою AES.

Незважаючи на те, що Skype розвивається й до сьогоднішнього дня, він також має ряд вразливостей. Хоча Skype шифрує більшість своїх комунікацій, незашифровані пакети, що містять рекламу, витягуються з кількох місць. Цю рекламу можна легко захопити й замінити шкідливими даними. Skype також вразливий до фішингових атак [16].

6. Ethereum (ETH) – це протокол на основі блокчейну [17]. Суть протоколу полягає в тому, що це неієрархічна мережа комп'ютерів (вузлів), які будують і приходять до консенсусу щодо постійно зростаючого ряду «блоків» або пакетів транзакцій, відомих як блокчейн. Щоразу, коли вузол додає блок до свого ланцюжка, він виконує транзакції в блоці в тому порядку, в якому вони перераховані, тим самим змінюючи баланси ETH та інші значення для зберігання облікових записів Ethereum. Ці баланси та значення, відомі як «стан», підтримуються на вузлі окремо від блокчейну в дереві Меркла [18]. Кожен вузол зв'язується з відносно невеликою підмножиною мережі — її «рівними». Всякий раз, коли вузол бажає включити нову транзакцію в блокчейн, він надсилає копію транзакції кожному зі своїх однорангових партнерів, які потім надсилають копію кожному зі своїх однорангових і так далі.

Програмна реалізація протоколу Ethereum містить ряд вразливостей, що були зафіксовані різними дослідниками після здійснення кібератак на платформу, що реалізує цей протокол. Наприклад, виявлено проблему, яка дозволяє зловмисникам викликати відмову в обслуговуванні (DoS), надсилаючи до вузла надмірну кількість повідомлень [19]. Це викликано відсутністю пам'яті в одному з компонентів. Також була помічена вразливість, що могла призвести до розірвання ланцюжків, а це в свою чергу порушує істинне призначення блокчейну. Також у протоколі є вразливість переповнення/заниження цілого числа. При цьому виконується арифметична операція, яка вимагає змінної фіксованого розміру для зберігання даних, що виходить за межі діапазону типу даних. Ця вразливість може бути використана зловмисниками шляхом неправильного використання коду смарт-контракту та створенням несподіваних логічних потоків. Випадок експлуатації вразливості переповнення цілого числа – атака BECToken [20-21].

Висновки

Розглянуто концепцію пірингової мережі та її вплив на сучасний стан інформаційних технологій. Проаналізовано ряд поширених протоколів однорангових мереж, таких як BitTorrent, Gnutella, G2, Tox, Skype та Ethereum. Виявлено особливості, переваги та сфери застосування кожного з вищеперерахованих протоколів.

Проаналізовано основні вразливості кожного протоколу для подальшого їх аналізу. Основною атакою, яку можна здійснювати на платформи, що реалізують дані протоколи є відмова в обслуговуванні. Також можливі такі атаки, як флуд (для BitTorrent), фішинг (для Skype), викрадення IP (для Tox) тощо.

Виявлення та аналіз вразливостей протоколів P2P дозволить в подальшому уникати атак та створювати нові методи та протоколи для забезпечення цілісності, доступності та конфіденційності даних, що в свою чергу є основою пікринових мереж.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. The Social Forces Behind the Development of Usenet By Michael Hauben. [Електронний ресурс] – URL: http://www.columbia.edu/~hauben/book/ch106.x03.
2. P2P Networking. [Електронний ресурс] – URL: https://nakamoto.com/p2p-networking/.
3. Л.М. Куперштейн, М.Д. Кренцін. Аналіз тенденцій розвитку піринових мереж // Вісник Хмельницького національного університету. – 2021. – №4. – с.25-29.
4. Мартинюк Т.Б., Кожем'яко А.В., Куперштейн Л.М. Аналіз тенденцій розвитку сучасних комп'ютерних систем // Оптико-електронні інформаційно-енергетичні технології. – 2016. – № 2. – с. 5-13.
5. М.Д. Кренцін, Л.М. Куперштейн. Аналіз атак на моделі машинного навчання // L Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії. – 2021. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2021/paper/view/12746/10686.
6. BitTorrent Protocol 1.0 [Електронний ресурс] – URL: https://www.academia.edu/1032175/BitTorrent_Protocol_Specification_V_1_0.
7. P2P File-Sharing in Hell: Exploiting BitTorrent Vulnerabilities to Launch Distributed Reflective DoS Attacks [Електронний ресурс] – URL: https://www.usenix.org/system/files/conference/woot15/woot15-paper-adamsky.pdf.
8. Andrew D. Berns, Eunjin (EJ) Jung. Searching for Malware in BitTorrent // University of Iowa Computer Science Technical Report UICS-08-05. – 2008. – pp. 1-10.
9. Vegge, Håvard & Halvorsen, Finn & Nerg, Rune & Jaatun, Martin & Jensen, Jostein. Where Only Fools Dare to Tread: An Empirical Study on the Prevalence of Zero-Day Malware // Internet Monitoring and Protection, International Conference. – 2009. – pp. 66-71. DOI: 10.1109/ICIMP.2009.19.
10. A new kind of instant messaging [Електронний ресурс] – URL: https://tox.chat/.
11. Is Tox Chat Safe? A Detailed Review of This P2P Messaging App [Електронний ресурс] – URL: https://www.wizcase.com/blog/how-to-stay-safe-on-tox-chat/.
12. The World's Most Dangerous Geek [Електронний ресурс] – URL: http://www.davidkushner.com/article/the-worlds-most-dangerous-geek/.
13. Exploiting the Security Weaknesses of the Gnutella Protocol [Електронний ресурс] – URL: http://alumni.cs.ucr.edu/~csyiazti/courses/cs260-2/project/gnutella.pdf.
14. GTK-GNUTELLA [] – URL: http://gtk-gnutella.sourceforge.net/en/?page=news.
15. An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol [Електронний ресурс] – URL: https://arxiv.org/abs/cs/0412017.
16. Is Skype Safe and Secure? What are the Alternatives? [Електронний ресурс] – URL: https://www.comparitech.com/blog/information-security/is-skype-safe-and-secure-what-are-the-alternatives/.
17. Bhardwaj, Pushpit & Chandra, Yuvraj & Sagar, Deepesh. Ethereum Data Analytics: Exploring the Ethereum Blockchain. Department of Computer Science, Shaheed Sukhdev College of Business Studies, University of Delhi. – 2021.
18. A Survey of Security Vulnerabilities in Ethereum Smart Contracts [Електронний ресурс] – URL: https://arxiv.org/pdf/2105.06974.pdf.
19. The Ethereum network is currently undergoing a DoS attack [Електронний ресурс] – URL: https://blog.ethereum.org/2016/09/22/ethereum-network-currently-undergoing-dos-attack/.
20. A disastrous vulnerability found in smart contracts of BeautyChain (BEC) [Електронний ресурс] – URL: https://medium.com/secbit-media/a-disastrous-vulnerability-found-in-smart-contracts-of-beautychain-bec-dbf24ddbc30e.
21. New batchOverflow Bug in Multiple ERC20 Smart Contracts [Електронний ресурс] – URL: https://peckshield.medium.com/alert-new-batchoverflow-bug-in-multiple-erc20-smart-contracts-cve-2018-10299-511067db6536.

Кренцін Михайло Дмитрович – аспірант кафедри захисту інформації, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: mishatron98@gmail.com

Куперштейн Леонід Михайлович – к.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця email: kupershtein.lm@gmail.com

Krentsin Mykhailo D. – Postgraduate Student of the Department of Information Security, Faculty for Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: mishatron98@gmail.com

Kupershtein Leonid M. — PhD, Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Vinnytsia, email: kupershtein.lm@gmail.com