МОДЕЛЮВАННЯ СУЧАСНИХ АТАК НА МЕРЕЖУ БЛОКЧЕЙН

Фесенко Д.
Науковий керівник – Петренко О.Є.
Харківський национальный университет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. БІТ)
e-mail: dmytro.fesenko@nure.ua

The paper deals with the design and implementation attacks on different systems based on blockchain technology. Intruder model and threat model for blockchain networks created. Blockchain network attacks are analyzed and methods of defense against these attacks are proposed. Recommendations were made regarding the use of blockchain technologies, taking into account all the factors considered.

Блокчейн – це система регістрів, які являють собою розподілену систему та не мають центрального органу, що складаються з реєстрів обліку криптографічно підписаних транзакцій, згруповані в блоки, де кожен блок пов'язується з попереднім після перевірки.

Розглянемо можливості застосування імітаційного моделювання для ефективної роботи мережі блокчейн.

Блокчейн, як і кожна система має потенційні вразливості, що можуть стати на заваді роботи системи, наприклад, при створенні системи на основі технології блокчейн з нуля одна невелика помилка може стати фатальною. Команда проекту, що створюється на основі системи блокчейн або займається його розробкою та підтриманням дієздатності, має бути дуже досвідченою, бо вірогідність допустити помилку у такій складній системі підвищується.

Атака 51%. Якщо один або декілька учасників мережі володіють більшою частиною вузлів/потужності мережі, тоді це надає їм можливість контролювати загальний консенсус і включати в блокчейн необхідні тільки їм дані.

Розглянемо можливість проведення атаки типу «людина по середині» (MITM). В загальному випадку розглянемо «Вузол 1», на який буде здійснено атаку, якому ми привласнимо ім’я Аліси (A). Вузол, який буде працювати з Алісою, тобто «Вузол 2» буде мати ім’я Боб (B). Зловмисник, який поставив собі за мету скомпрометувати повідомлення, будемо називати Мелорі (E).

Аліса відправляє Бобу повідомлення про запит на отримання блоку для синхронізації, яке перехоплює Мэлорі:

$$A \overset{E}{\rightarrow} B : \text{BLOCK REQ}$$

Розглянемо випадок, коли не буде використовуватися шифрування, а лише гешування блоків в вузлах, таким чином не потрібно отримувати ключі шифрування.

Мелорі передає повідомлення Бобу, при чому Боб на даному етапі не розуміє, що це повідомлення не від Аліси:

$$E \rightarrow B : \text{mod data}$$

Мэлори перехоплює блок Боба та модифікує його:

$$A \overset{E}{\leftarrow} B : \text{BLOCK DATA}$$

Мэлорі відправляє Алісі модифікований блок:

$$A \leftarrow E : \text{MOD BLOCK}$$

Аліса, отримавши повідомлення намагається додати дані до ланцюгу блоків, але через використання механізму зберігання попередніх блоків виявляється факт підміни геш-значення пов'язаного блоку і атака стає неможливою. Атака може бути реалізована, якщо цей блок ще не фігурував в блокчейні. Для унеможливлення цієї атаки необхідно використовувати захищене з'єднання. На рисунку 2 наведено статистику використання захищених з'єднань.

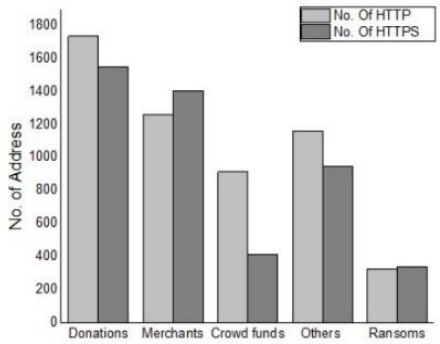

Рисунок 1 – Статистика використання захищеного з'єднання користувачами

Отже, імітаційне моделювання роботи системи блокчейн дозволяє розглянути всі етапи роботи мережі блокчейн та механізм генерації блоків, їх синхронізації між собою, перевірки валідності блоків та можливостей з їх модифікації.

Список використаних джерел:

1. NISTIR 8202. Блокчейн Technology Overview, 2017. – С. 7 – 20.
2. Don Tapscott, Alex Tapscott Блокчейн Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World / Don Tapscott, Alex Tapscott Блокчейн – К. : Information Systems, 2016 – С. 65 – 102.
3. Andreas M. Antonopoulos Mastering Bitcoin: Unlocking Digital Cryptocurrencies / Andreas M. Antonopoulos – К. : NGITS, 2014. – С. 10 – 150.
4. Блокчейн: атаки, безопасность и криптография [Електронний ресурс]. – Режим доступу: www/ URL: https://www.securitylab .ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/343072.php – 26.08.2018 р.