школи-семінару *«Питання оптимізації обчислень (ПОО-XLII)»* 21–25 вересня 2015 р. Україна, Закарпатська обл., Мукачівський р-н, смт. Чинадієво. С. 22.
4. Верлань А. Ф., Горошко И. О., Гушель Т. П. Способ регуляризации с усечением спектра ядра интегрального оператора в задаче восстановления сигналов. *Электронное моделирование.* 2004. 25, № 3. С. 3–11.

Рассмотрен один частный случай решения задачи интерпретации наблюдений, когда аппаратная функция измерительного преобразователя является чистым интегратором. При этом задача интерпретации сводится к дифференцированию выходного сигнала измерительного преобразователя.

Ключевые слова: *зашумленный сигнал, численное дифференцирование, интегростепенной ряд Вольтерра, регуляризация.*

Date received 21.03.2017

УДК 004.056.5

П. І. Стеценко, аспірант

Харківський національний університет радіоелектроніки, м. Харків

МАСШТАБНІ АТАКИ НА ДЕЦЕНТРАЛІЗОВАНІ СИСТЕМИ, ЩО ПОБУДОВАНІ НА ОДНОРАНГОВИХ ПІРИНГОВИХ МЕРЕЖАХ

Представлені сценарії масштабних атак на децентралізовані системи на прикладі криптовалюти Bitcoin, які основані на вразливостях протоколу BGP та надмірній централізації першого рівня архітектури даних систем.

Ключові слова: *децентралізована система, Bitcoin, BGP, одноранговa піринговa мережа, механізм досягнення консенсусу.*

Вступ. Найбільш популярною децентралізованою системою на даний момент є криптовалюта Bitcoin, ринкова капіталізація якої на початок 2017 року складала понад 18 мільярдів доларів США [1]. Популярність децентралізованих систем пояснюється відсутністю централізованого органа управління, відкритістю та можливістю збереження конфіденційності. Переважна більшість таких систем будується на єдиній архітектурі, яка показана на рис. 1.

Рис. 1. *Загальна архітектура децентралізованих систем*

Широке дослідження безпеки механізму досягнення консенсусу Proof-of-Work криптовалюти Bitcoin наведено в [2]. Можливість затримки або запобігання розповсюдженню блоків однорангoвою піринговою мережею представлена в [3]. Деанонімізація користувачів мережею наведена в [4].

Безпека протоколу BGP. Вимірювання та виявлення атак на таблиці маршрутизації широко досліджувалися у [5, 6], а атаки перехоплення — у [7]. Безпечні протоколи маршрутизації запропоновані в [8].

Концепції зловмисників AC-рівня були вивчені в контексті протоколу маршрутизації Tor [9]. У цих роботах також проілюстровані проблеми, викликані централізацією і атаки маршрутизації на розподілену систему. Проте, Tor і Bitcoin значно відрізняються у своїй поведінці: Tor маршрутизує повідомлення шляхом цибулевої маршрутизації, в той час як Bitcoin використовує випадкові з'єднання для флудингу повідомлень по всій мережі.

Безпека Bitcoin щодо мережевих атак була відносно більш дослідженою в порівнянні з іншими сценаріями атак. Атака на таблиці маршрутизації окремого вузла в контексті однорангової піринговой мережі Bitcoin розглядається у [10].

Таким чином, враховуючи єдину спільну архітектуру децентралізованих систем, вивчення масштабних атак на такі системи доцільно проводити на прикладі криптовалюти Bitcoin.

Дана робота присвячена масштабним атакам, які використовують вразливості протоколу BGP і централізацію Bitcoin на першому рівні архітектури.

Визначення 1. Протокол BGP (анг. Border Gateway Protocol) — протокол маршрутизації, що призначений для обміну інформацією о маршрутах між автономними системами. Протокол BGP є протоколом прикладного рівня моделі OSI та функціонує поверх протоколу транспортного рівня TCP (порт 179).

Визначення 2. Автономна система (AC) — це система IP-мереж та маршрутизаторів під управлінням одного або кількох операторів, які мають єдину політику маршрутизації [11].

Визначення 3. BGP-перехоплення — це оголошення автономною системою хибної інформації про те, як досягти одного або декількох IP-префіксів, що призводить до того, що інші автономні системи відправляють трафік в неправильні локації. Вразливість, що дозволяє реалізовувати BGP-перехоплення, полягає в тому, що протокол BGP не перевіряє достовірність інформації в оголошеннях.

Зловмисник, що перехоплює префікси, поглинає будь-який перехоплений трафік. Зловмисник може перетворити перехоплення префікса в атаку перехоплення, переконавшись, що залишив хоча б один шлях до пункту призначення недоторканим [7].

Від BGP-перехоплень складно як захиститися, так і уникнути їх. Розширення безпеки протоколу BGP (BGPSec або RPKI) використовуються рідко [12]. Тому оператори покладаються на системи моніторингу, які повідомляють про несанкціоновані оголошення (наприклад, BGPMon). Процес припинення перехоплення може зайняти кілька годин, тому що він керується людиною і складається з фільтрації або від'єднання зловмисника.

Надмірна централізація мережі Bitcoin. Централізація нижнього рівня архітектури Bitcoin полягає у тому, що дуже мала кількість АС розміщує більшість вузлів мережі. Графік залежності сумарної частки Bitcoin-вузлів від числа АС показано на рис. 2.

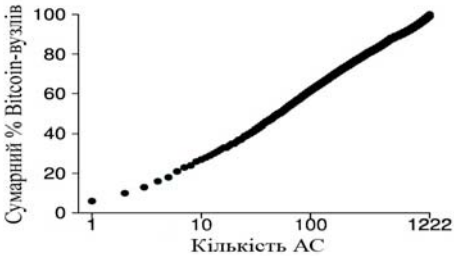

Рис. 2. *Графік залежності загальної кількості Bitcoin-вузлів від кількості АС, що їх розміщують*

З графіка можна зробити висновок, що лише 13 АС розміщують 30% всієї мережі, а менш ніж 100 АС — 50 % всіх вузлів мережі Bitcoin. Ці автономні системи відносяться до широкосмугових провайдерів, таких як Comcast (США), Verizon (США), CHINANET (CN), а також до хмарних провайдерів, таких як Hetzner (DE), OVH (FR) і Amazon (США). Аналогічна концентрація спостерігається при розподілі Bitcoin-вузлів IP-префіксам: лише 63 префікса (0,012 % Інтернету) утримують 20 % мережі.

Невелика кількість АС бачить значну частку Bitcoin-трафіку. Сумарний відсоток з'єднань, який може бути перехоплений зі збільшенням кількості АС, показаний на рис. 3.

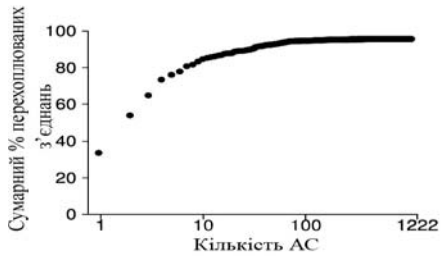

Рис. 3. *Графік залежності сумарного відсотка перехоплюваних Bitcoin-з'єднань від кількості АС*

Можна побачити, що тільки три АС, а саме: Hurricane Electric, Level3 і Telianet, можуть разом перехоплювати понад 60 % всіх Bitcoin-з'єднань. При цьому тільки Hurricane Electric знаходиться на шляху 35 % всіх підключень. В цілому, через великі транзитні провайдери (Tier-1) проходить велика частка всіх Bitcoin-з'єднань.

Наступною вразливістю є те, що більше 90 % мережі Bitcoin мають вразливість до перехоплень. Близько 93 % всіх префіксів, що розміщують Bitcoin-вузли, коротше, ніж /24, що робить їх вразливими для глобального IP-перехоплення з використанням більш специфічних оголошень [6]. Дійсно, префікси строго більше, ніж /24, як правило, одразу фільтруються багатьма інтернет-провайдерами. Слід зазначити, що інші 7 % вузлів, які знаходяться в /24 префіксах не обов'язково є безпечними. Вони можуть як і раніше бути перехоплені іншою АС, яка виконує атаку найкоротшого шляху. Зловмисник буде оголошувати /24, аналогічно вузли, що атакуються, вважатимуть за краще трафік від всіх АС, які знаходяться ближче до зловмисника, ніж до атакованого вузла (з точки зору числа переходів).

Сценарії масштабних атак. Зловмисники АС-рівня можуть впливати на Bitcoin-з'єднання шляхом довільного розриву з'єднань, їх затримування або модифікації системних повідомлень, якими обмінюються вузли на їх шляху. В залежності від спрямування атаки існує два сценарії — розділ мережі та затримка розповсюдження блоків. Обидва сценарії підривають механізм досягнення консенсусу.

1. Сценарій розділу мережі. Використовуючи BGP-перехоплення зловмисник може розділу мережі шляхом ізоляції окремих сегментів мережі, поглинаючи їх трафік. Схема розділу мережі показана на рис. 4.

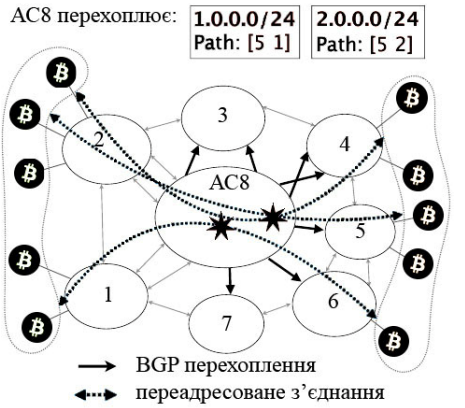

Рис. 4. *Розділ мережі з використанням BGP-перехоплення*

Наслідки. Операції з однієї сторони розділу можуть бути заблоковані і не доставлені іншій стороні. Це буде ефективно блокувати платежі. Транзакції, які додаються в блоки майнерами на стороні з меншою кількістю обчислювальної потужності майнінгу, в решті решт будуть видалені з регістру Blockchain, коли розділ відновиться. Вони можуть бути знову включені в нього, але це може зайняти деякий час, якщо виникне значне відставання. Це, в свою чергу, може привести до підвищення плати за транзакцію. Нарешті, зловмисник може використовувати той факт, що блоки по обидві сторони розподілу знаходяться в конфлікті, щоб відправити конфліктуючі транзакції з різних сторін. Це дозволить йому реалізувати подвійну витрату, не вимагаючи будь-якої власної обчислювальної потужності майнінгу. Ізолюючи частину мережі або затримуючи поширення блоків, зловмисники також можуть змусити вузли витрачати частину своєї обчислювальної потужності майнінгу.

2. Сценарій затримки розповсюдження блоків. Метою цієї атаки є послаблення механізму досягнення консенсусу Bitcoin. Затримка розповсюдження блоків є основною причиною розгалужень в регістрі Blockchain. Зловмисник використовує свою позицію і направляє блоки таким чином, щоб затримувати отримання вузлами інформації про останні додані блоки. Після запиту блоку від однорангового вузла вузол буде очікувати доставку цього блоку до 20 хвилин, перш ніж зробити такий запит з іншого однорангового вузла. Таким чином, мережевий атакуючий між відправником і отримувачем блоку може затримати його доставку, змушуючи одержувача залишатися необізнаним протягом 20 хвилин.

Наслідки. Значна затримка передачі блоків може бути використана для атак корисливого майнінгу, здійснюваних зловмисниками з потужністю майнінгу (атаки вимагають менше обчислювальної потужності майнінгу, ніж в ситуаціях без подібної затримки розповсюдження блоків [13]). Навіть без обчислювальної потужності майнінгу, блоки, що відкидаються, віднімаються з винагороди майнеру, тому що блоки, не включені в Blockchain, не приносять нагороду їх майнеру. Збільшення ступеня відкинутих блоків також полегшує подвійну витрату — Blockchain зростає з більш повільною швидкістю, і її можуть перегнати слабші атакуючі.

Висновки. В роботі розглянуто два сценарії масштабних атак на децентралізовані системи на прикладі криптовалюти Bitcoin — розділ мережі та затримка розповсюдження блоків.

Ключовими вразливостями, що дозволяють реалізувати такі атаки, є: надмірна централізація першого рівня архітектури, яка полягає в тому, що дуже мала кількість АС розміщує більшість вузлів мережі та бачить значну частку трафіку; вразливість протоколу BGP, яка

дозволяє зловмиснику AC-рівня шляхом BGP-перехоплення ізолювати окремі сегменти мережі; вразливість префіксів, що розміщують Bitcoin-вузли, для BGP-перехоплень.

Розглянуті в роботі наслідки будуть аналогічні для криптовалют, побудованих на подібній архітектурі. Що стосується децентралізованих систем в цілому, то наслідки можуть незначно відрізнятися в залежності від призначення системи і використовуваного механізму досягнення консенсусу.

Список використаних джерел:

1. Bitcoin market capitalization. Blockchain S.A.R.L. [Electronic resource]: https://blockchain.info/ru/charts/market-cap.
2. Bahack L. Theoretical Bitcoin attacks with less than half of the computational power. arXiv preprint: 1312.7013. 2013. 18 p.
3. Decker C., Wattenhofer R. Information propagation in the Bitcoin network. In IEEE Thirteenth International Conference on Peer-to-Peer Computing (P2P). IEEE. 2013. 10 p.
4. Biryukov A., Khovratovich D., Pustogarov I. Deanonymisation of clients in Bitcoin P2P network. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM. 2014. P. 15–29.
5. Shi X., Xiang Y., Wang Z. Detecting prefix hijackings in the Internet with Argus. IMC'12, ACM. 2012. P. 15–28.
6. Zhang Z., Zhang Y., Hu Y. C. Practical defenses against BGP prefix hijacking. CoNEXT'07, ACM. 2007. 12 p.
7. Ballani H., Francis P., Zhang X. A study of prefix hijacking and interception in the Internet. SIGCOMM '07, ACM. 2007. P. 265–276.
8. Boldyreva A., Lychev R. Provable Security of S-BGP and Other Path Vector Protocols: Model, Analysis and Extensions. CCS '12, ACM. 2012. P. 541–552.
9. Edman M., Syverson P. As-awareness in tor path selection. In Proceedings of the 16th ACM Conference on Computer and Communications Security. 2009. 10 p.
10. Stetsenko P., Perekopskiy A., Khalimov G. Attack on Bitcoin peer-to-peer network addressing mechanism. VI Międzynarodowa konferencja studentyw oraz doktorantyw «Inżynier XXI wieku». Bielsko-Biała. 2016. P. 393–402.
11. RFC 1930. Guidelines for creation, selection, and registration of an Autonomous System (AS). 1996. 10 p.
12. Lychev R., Goldberg S., Schapira M. BGP Security in Partial Deployment. In SIGCOMM. 2013. 12 p.
13. Sapirshtein A., Sompolinsky Y., and Zohar A. Optimal selfish mining strategies in bitcoin. CoRR. 2015. 31 p.

This paper presents the scenarios of large-scale attacks on the decentralized systems in the case of cryptocurrency Bitcoin, which are based on the vulnerability of the protocol BGP and excessive centralization of the first level of architecture of these systems.

Key words: *decentralized system, Bitcoin, BGP, peer-to-peer network, consensus mechanism.*

Одержано 10.02.2017