Tugas Minggu 5

Fajri Nurfauazan | 1103180184 | TK-42-PIL

Dalam makalah ini, kami memperluas ruang strategi penambangan untuk memasukkan strategi "stubborn" baru yang digunakan untuk berbagai parameter dan menghasilkan lebih banyak pendapatan bagi penambang. Akibatnya, hasil menunjukkan bahwa selfish mining attack (serangan penambangan egois) tidak (secara umum) optimal. Selanjutnya, hasil menunjukkan bagaimana penambang dapat lebih meningkatkan keuntungannya dengan menyusun serangan penambangan yang tidak sepele dengan *network-level eclipse attacks* atau serangan gerhana ditingkat jaringan. Selanjutnya akan menunjukkan, bahwa dengan strategi terbaik untuk penyerang, khususnya dalam beberapa kasus, korban dengan *eclipse attacks* (serangan gerhana) sebenarnya bisa mendapatkan keuntungan dari *eclipse* (gerhana)!

Analisis awal keamanan di Bitcoin bergantung pada asumsi bahwa sebagian besar jaringan, yang akan diukur dengan sumber daya komputasi, maka secara jujur akan menjalankan klien referensi secara default. Secara intuitif mata uang kripto yang dirancang dengan aman dan penyerang yang mengendalikan sebagian kecil dari sumber daya komputasi jaringan seharusnya hanya dapat memperoleh sebagian kecil dari hadiah penambangan.

Namun, penyerang berbahaya dan jahat dapat menggunakan berbagai jenis serangan untuk mendapatkan bagian yang tidak adil dari hadiah penambangan. istilah penyebut serangan seperti itu secara umum sebagai serangan penambangan, dan serangan tingkat jaringan yang berusaha membuat partisi jaringan antara kekuatan penambangan, disebut sebagai " *eclipse attack*". Terkait ini penyelidikan strategi yang meningkatkan pendapatan penyerang. Akan memperkenalkan keluarga baru dari strategi alternatif "*stubborn mining* " yang menggeneralisasi dan mengungguli serangan penambangan secara egois.

Untuk sebagian besar ruang parameter yang menarik dan strategi baru, secara signifikan meningkatkan pendapatan penyerang. Tergantung pada parameter lingkungan dan strategi penambangan yang *stubborn* (Keras kepala) dapat mengalahkan penambangan yang egois hingga 25% (bahkan tanpa memanfaatkan serangan tingkat jaringan apa pun).

Dalam salah satu strategi penambangan yang disebut *trail-stubbornness*, penyerang terus menambang di garpu pribadinya bahkan jika garpu publik di depan, sehingga melanggar aturan rantai terpanjang. Pendapatan penyerang meningkat dengan kombinasi non-sepele dari penambangan keras kepala dan serangan tingkat jaringan. Seorang penambang yang keras kepala juga dapat mengeksploitasi serangan tingkat jaringan untuk lebih meningkatkan keuntungannya. Khususnya, dengan serangan *Eclipse* yang berhasil, penyerang mengisolasi korban dari rekan-rekannya yang lain di tingkat jaringan, dengan mengontrol koneksi masuk dan keluarnya.

Hasil menunjukkan bahwa ruang strategi non-sepele ada saat menggabungkan penambangan keras kepala dengan *eclipse attack* (serangan gerhana). Tergantung pada parameternya, strategi ini terkadang dapat menghasilkan 30% keuntungan dibandingkan dengan penggunaan naif dari node yang di- *Eclipse*. Selain itu hasil menunjukkan bahwa secara mengejutkan, dalam beberapa rentang parameter, strategi terbaik penyerang benar-benar membantu node yang hilang, sehingga korban mungkin memiliki sedikit insentif untuk mencegah, mendeteksi, atau bereaksi terhadap serangan semacam itu.

Eksplorasi sistematis ruang strategi, Secara sistematis mengeksplorasi ruang strategi yang akan menggabungkan *elfish-mining-style attacks* atau serangan gaya penambangan egois dengan serangan *eclipse* (gerhana) tingkat jaringan, dan menunjukkan bahwa tidak ada strategi tunggal yang merupakan strategi optimal " *one-size-fitsall* ". Sebaliknya, penyerang harus memilih strateginya berdasarkan perkiraan parameter termasuk jumlah daya komputasi yang dapat digunakannya, fraksi jaringan yang berpotensi dikalahkan, dan fraksi jaringan tersisa yang dapat dipengaruhinya.

Di bawah ruang strategi yang telah dipertimbangkan, akan menunjukkan strategi dominan untuk berbagai wilayah ruang parameter. Namun, tidak menutup kemungkinan strategi lain di luar ruang strategi yang akan berkinerja lebih baik. Setelah itu, menunjukkan bahwa kemungkinan menggabungkan serangan penambangan dengan serangan tingkat jaringan semakin memperumit ruang kemungkinan strategi.

Implementasi referensi Bitcoin mengamanatkan bahwa, setiap kali beberapa penambang menghasilkan blok yang valid, ia mendistribusikannya ke seluruh jaringan. Penambangan *elfish* (egois) berhasil karena

penambang jujur terpaksa menghabiskan (sebagian) siklus komputasi mereka pada blok yang ditakdirkan untuk tidak berada di rantai publik.

Berbagai serangan lain telah dipelajari, Pada lapisan jaringan, setiap node Bitcoin (total sekitar 7000, hari ini) terhubung melalui TCP ke banyak rekan, dengan maksimum default 125. mendemonstrasikan serangan *Eclipse* tingkat jaringan di mana satu node memonopoli semua kemungkinan koneksi ke korban dan menghilangkannya dari jaringan. Dengan cara ini node *Eclipse* (gerhana) dapat memfilter pandangan node yang terhalang dari blockchain. Penjelasan teknik yang rumit untuk mencapai serangan *Eclipse* (gerhana) pada jaringan Bitcoin itu disebutkan dimakalah lain. Meskipun beberapa tindakan balasan yang diusulkan telah diterapkan yang mengurangi kelayakan melakukan serangan gerhana oleh satu node, beberapa node dapat berkolusi dan masih berhasil dalam gerhana - khususnya, kami berpendapat bahwa itu mungkin sebenarnya menjadi insentif yang cocok untuk pemain egois untuk berkolusi dalam meluncurkan serangan gerhana.

Selanjutnya, memberikan dasar untuk memahami bagaimana penyerang dapat mengeksploitasi node yang hilang untuk mendapatkan keuntungan dan menganalisis keuntungan yang dapat dicapai. Pengetahuan tentang jaringan Bitcoin selanjutnya dapat membantu penyerang tingkat jaringan. Misalnya, Coinscope mengusulkan teknik non-sepele untuk memetakan topologi jaringan Bitcoin serta kekuatan hash dari berbagai node. Pengetahuan seperti itu akan memungkinkan penyerang membuat serangan yang ditargetkan ke entitas penambangan *Eclipse* (gerhana). Mendefinisikan ruang strategi yang luas dan menggunakan kombinasi batas analitik dan pemecah numerik untuk menghitung strategi yang kira-kira optimal dari ruang ini. Ruang strategi mereka adalah generalisasi dari strategi penambangan yang *stubborn* (keras kepala); namun, tidak mempertimbangkan bagaimana menyusun serangan penambangan dengan serangan *Eclipse* (gerhana).