Eclipse Attack

Penambangan Keras Kepala: Menggeneralisasi Penambangan Egois dan Menggabungkan dengan Serangan Gerhana

Mata uang kripto terdesentralisasi seperti bitcoin. Dan mana uang lainnya yang menarik minat public dan mungkin bias di bilang lebih sukses dari uang elektronik lainnya. Karena mana uang kripto membawa nilai moneter, secaara alami menjadi target serangan yang berharga, secara intuitif untuk mata uang kripto yang di rancang dengan aman, penyerang mengendalikan sebagian dari sumber daya komputasi jadringan seharusnya hanya dapat diperoleh sebiah hadiah dari penambangan. Namun, penyerang jahat dapat menggunakan berbagai jenis serangan untuk mendapatkan bagian yang tidak adil dari hadiah penambangan. Kami menyebut serangan seperti itu secara umum sebagaiserangan penambangan. Di antara yang paling terkenal adalah serangan gaya “penambangan egois” yang mengeksploitasi kelemahan dalam protokol konsensus terdistribusi.

Pada jurnal ini di jelaskan Serangan tingkat jaringan.Pada lapisan jaringan, setiap node Bitcoin (total sekitar 7000, hari ini) terhubung melalui TCP ke banyak rekan, dengan maksimum default 125. Koneksi peerto-peer antara node ini dapat disimpulkan melalui berbagai teknik.

Dimana pada jurnal memberikan penjelasan tentang pemodelan penamangan bitcoin yang di perluas serta menyertakan serangan eclipse juga. Pertama pada pemodelan penambangan bitcoin melakukan menentukan parameter kunci dan memiliki 3 parameter utama yaitu:

* Hashpower penyerang (yaitu, Alice)sebuah: bagian dari total hashpower jaringan yang dikendalikan oleh penyerang, selanjutnya disebut sebagai "Alice".
* Hashpower dari publik yang jujur (yaitu, Bob)b: bagian dari hashpower dari jaringan yang tersisa, selanjutnya disebut sebagai “Bob”. Perhatikan bahwab+sebuah=1.
* Pengaruh jaringan Alicec: sebagian kecil dari jaringan Bob (dalam hal kekuatan hash) yang akan menambang di blok Alice (yaitu, penyerang) ketika Alice dan Bob telah melepaskan blok pada (kurang lebih) pada waktu yang sama sehingga menghasilkan garpu dengan panjang yang sama.

Selanjutnya kedua model rantai markov dari penambangan. Kami memodelkan penambangan Bitcoin menggunakan proses keputusan Markov, di mana negara bagian menangkap aspek yang relevan dari informasi dari tersedia. Jika penambang jujur menemukan sebuah blok, iaakan segera menerbitkan blok tersebut.

Selanjutnya mengekspresikan penambangan jujur dan egois. Strategi penambangan di tentukan 2 keputusan kapan harus mengumkanpkan rantai pribadi ke public dan kapan harus menerima rantai public. Penambang jujur jika protocol dan menjalakankan klien referensi, maka dia mengungkapkan satu blok segera setelah nemambangnya.

Selanjutnya keuntungan pendapatan