이더리움 이클립스 공격 분석

황보규민* , 황선진*, 최윤호**

*부산대학교 (대학원생), **부산대학교 (교수)

Analysis of Ethereum Eclipse Attack

Gyu-Min Hwang-Bo*, Hwang Seon-Jin*, Yoon-Ho Choi**

*Pusan National University(Graduate student),

**Pusan National University(Professor)

요 약

블록체인은 최근 여러 어플리케이션에 적용되어 활용되고 있다. 퍼블릭 블록체인인 이더리움은 분산화 어플리케이션(DApps)을 최상위 계층에서 구동하며 다양한 서비스를 제공하고 있다. 이러한 서비스는 2016년 DAO 계약 해킹으로 전체 이더리움 화폐의 10%가 도난당한 사건이 있고 이에 따라 어플리케이션 계층의 보안연구가 활발히 이루어지고 있다. 하지만 대부분의 보안 연구는 어플리케이션 계층에서 많고 네트워크 계층의 연구는 아직 미비한 상황이다. 따라서 본 논문은 대표적인 이더리움 네트워크 공격인 이클립스의 개념과 공격 방식을 분석하고 현재 대응책이 적용된 부분과 이더리움이 가지고 있는 취약점을 설명한다. 이를 통해 네트워크 공격의 특징을 이해하고 클라이언트 구현 시 위협요소들을 보완한다면 더욱 안전한 플랫폼을 구축할 수 있다.

I. 서론

블록체인 기술은 분산 컴퓨팅 기반의 원장 관리 기술로써 최초의 블록체인인 비트코인을 사토시 나카모토가 제안했다. 이후 튜링 언어로 제작된 프로그래밍 가능한 스마트계약을 융합해 다양한 서비스를 가능하게 하는 이더리움이 등장한다. 퍼블릭 블록체인인 이더리움은 중앙기관 없이 합의 알고리즘[1]을 통해 불변성과 일관성을 인정받는다.

이더리움은 분산 어플리케이션(DApps)을 이용하여 개발자들의 필요와 목적에 따라 다양한 서비스 제공이 가능하다. 이러한 분산 기술의 발전에 따라 안정적인 서비스 제공을 위해 블록체인 기반 어플리케이션 계층의 보안 연구가 활발히 이루어지고 있다.

하지만 대부분 어플리케이션 계층의 보안 위협 대응 방안 연구가 이루어지고 있고 네트워크 계층에서는 아직 미비한 상황이다.

본 논문에서는 2장에서 이클립스 공격의 개념 및 공격 방식을 설명하고 3장에서는 결론을 서술한다.

II. 이클립스 공격

이클립스 공격은 단일 노드를 대상으로 하는 공격으로써 희생자 노드의 네트워크를 다수의 악의적인 노드들로 독점하는 공격이다. 다음은 대표적인 이클립스 공격 방식이다.

2.1 Permanent Eclipse Attack

Permanet Eclipse Attack[2]은 블록 전파 방식의 취약점을 이용한 공격으로 공격 방법은 아래와 같다.

1) 공격자 노드는 최초 블록부터 정상 체인보다 블록이 256개 많은 체인을 난이도를 낮추어 생성한다.
2) 희생자 노드는 공격자 노드에게 GetBlockHeaders를 전송한다.
3) 공격자 노드는 가장 높은 블록부터 제네

시스 블록까지 희생자 노드의 요청에 따라 헤더만 전송한다.

4) 희생자 노드가 모든 블록 헤더를 받으면 공격자 노드에게 블록 정보를 요청한다.
5) 공격자 노드는 블록을 한 번에 보내지 않고 하나씩 전송함으로써 블록 전파를 지연시킨다.

2.2 Synchronising to longer chain with lower total difficulty

블록체인이 자신보다 낮은 전체 난이도를 가지고 있는 체인과는 블록 전파 과정을 가지지 않음을 이용한 공격[2]이다. 공격 방법은 아래와 같다.

1) 공격자 노드는 최초 블록부터 정상 체인보다 블록이 256개 많은 체인을 난이도를 낮추어 생성한다.
2) 새롭게 참가한 노드와 연결된다.
3) 희생자 노드가 정상적인 다른 체인보다 256개 블록 이상 길다면 연결이 독점화된다.

2.3 Increasing the Minimum Difficulty Parameter in geth

공격자 노드가 최소 난이도로 채굴하여 희생자 노드에게 전송하면 희생자 노드의 최소 난이도가 높아진다. 이때, 정상 노드보다 최소 난이도가 높다면 희생자 노드가 정상 노드와 동기화를 하지 않는 취약점을 노린 공격[2]이다. 공격 방법은 아래와 같다.

1) 공격자 노드는 최소 난이도로 다른 체인보다 더 긴 체인을 생성한다.
2) 공격자 노드는 최소 난이도로 긴 체인을 생성한다.
3) 희생자 노드는 공격자 노드 각 블록의 난이도를 확인한다.
4) 희생자 노드는 난이도를 확인할수록 최소 난이도 파라미터가 점차 증가하며 결국 최근 블록체인의 난이도보다 높아져 다른 정상 블록체인과 동기화가 불가능해진다.

2.4 Monopolize Connection Eclipse Attack

이 공격[3]은 희생자 노드가 다른 노드에게 outgoing 연결을 하기 이전에 공격자 노드로 빠르게 TCP 연결을 생성하는 공격이다. 공격 방법은 아래와 같다.

1) 공격자는 maxpeers보다 더 많은 수의 노드를 미리 생성한다.
2) 미리 생성한 공격자 노드에서 희생자 노드 리부팅 시 TCP 연결 메시지를 전송해 테이블을 빠르게 채운다.

위의 방법은 Geth 1.8 이전에 적용이 가능했고 1.8 이후에는 outbound와 inbound로 연결 가능한 Peer 수를 각각 1/3×maxpeers, 2/3×maxpeers로 제한하여 들어오는 TCP 연결로만 테이블이 다 채워지지 않도록 적용됐다.

2.5 Table Poisoning Eclipse Attack

이더리움은 노드 탐색 프로토콜을 통해 생성된 Table을 참조하여 연결을 설정한다. Table Poisoning은 테이블을 악의적인 노드로 채워 넣어 연결을 독점화 시키는 공격이다. 이 방법은 outbound와 inbound 연결 제한을 우회할 수 있다. 대표적인 공격 방식은 두 가지가 있다.

첫 번째는 inbound 연결을 생성하는 UDP listener이 outbound 연결을 보장하는 테이블 seeding 과정 보다 더 먼저 실행되는 점을 이용한 공격[3]이다. 이는 하나의 IP로도 공격이 가능하고 방법은 아래와 같다.

1) 공격자는 미리 많은 수의 노드를 생성한다.
2) 희생자 노드에게 ping을 전송해서 db에 공격 노드를 삽입한다.
3) 희생자 노드 리부팅 시, ping을 다량 전송하여 테이블을 공격자 노드로 포화시켜 db에 있는 노드들이 테이블로 들어오지 못하게 한다.

이러한 공격 방식은 Geth 1.8 이후부터는 테이블에 IP subnet을 적용하여 테이블이 하나의 IP로 다 채워지지 않도록 수정됐다.

하지만 여전히 IP subnet을 우회할 수 있는 이클립스 공격[4]이 가능하다. 공격 방법은 아래와 같다.

1) 공격자 노드는 미리 많은 수의 노드를 생성한다.

2) 희생자 노드에게 지속적인 TCP 연결을 신청한다.
3) 희생자 노드에게서 FIND_NODE 패킷이 왔을 때, 미리 생성해둔 노드ID들 중 타깃과 가장 가까운 노드를 답장한다.

Inbound 연결은 특정 노드 탐색 프로토콜 버전에서 여전히 지속적인 TCP 연결로 장악이 가능하다.

Outbound 연결의 절반은 ReadRandomNodes 과정으로 선택하고 나머지 절반은 lookup buffer 과정으로 선택하며 악의적인 노드로 연결이 가능하다.

ReadRandomNodes는 테이블 내에서 무작위 노드를 선택하는데 노드 탐색 프로토콜의 버전에 따라 다른 랜덤 한 방식을 선택한다. 버전 4에서는 테이블 내 존재하는 모든 노드를 랜덤하게 선택하여 연결을 설정하며 테이블을 독점화하는 데에 다량의 IP가 필요하다. 하지만 버전 5에서는 테이블 내 노드가 아닌 버킷 선택만 랜덤하게 하고 이후 버킷의 헤더 노드만 추출하여 피어를 연결한다. 따라서 버전 5에서는 IP subnet 개념이 적용되었더라도 실제 Peer로 연결되는 각 버킷의 헤더만 채우면 되어 적은 수의 IP로도 outbound 연결의 절반을 장악할 수 있다. Ping을 지속적으로 보내면 노드가 버킷의 헤더로 이동함으로 버킷 내 공격 노드가 들어가 있다면 헤더로 올리는 방법은 간단하다.

Lookup-buffer은 희생자 노드가 FIND_NODE 패킷을 보낼 때, 미리 생성해둔 노드 ID 중 타깃과 가장 가까운 노드들을 전송하면 공격 노드로 채울 수 있다. 따라서 outbound 연결 중 나머지 절반을 공격 노드로 마저 채울 수 있다. 이와 같은 공격이 가능하게 하는 근본적 이더리움 네트워크 취약점 점 중 하나는 노드 ID가 비용 없이 다량 생성이 가능하다는 점이다. 즉, 이더리움 네트워크 참여가 비용이 거의 발생하지 않아 공격 노드를 다량 생성할 수 있어 이클립스 공격에 취약하다.

또한 이더리움은 노드 ID와 테이블이 공개되어 있고 노드 ID 간 거리를 구하는 방식이 모두 같다는 점이 취약할 수 있다. 공개된 노드 ID와 공격 노드 ID의 거리를 구한 뒤 희생자 노드의 테이블 내 원하는 버킷에 공격 노드를 삽입할 수 있기 때문이다.

III. 결론

다양한 블록체인 플랫폼 기술이 발전하고 이를 활용하는 서비스가 증가함에 따라 DAO와 같은 보안 위협 또한 증가하고 있다. 하지만 대부분 최상위 계층에서의 보안연구가 이루어지고 있고 네트워크 계층에서의 보안은 미비하다. 본 논문에서 대표적인 네트워크 공격인 이클립스 공격의 개념을 살펴보고 다양한 공격 방식에 대해 분석하였다. 이를 통해 이더리움 네트워크의 취약한 부분을 이해하며 위협요소들을 보완한다면 더욱 안전한 서비스를 구축할 수 있을 것이다.

Acknowledgement

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원(2019-0-01343,융합보안핵심인재양성사업) 및 4단계 BK21, 동남권4차산업혁명리더양성사업단에 의하여 지원되었음.

[참고문헌]

[1] Go Ethereum, Retrieved Feb., 3, 2021, from https://github.com/ethereum/ethas

[2] K. Wüst and A. Gervais, "Ethereum eclipse attacks," ETH Zurich, Tech. Rep., 2016.

[3] Y. Marcus, E. Heilman, and S. Goldberg, "Low-resource eclipse attacks on Ethereum's peer-to-peer network," IACR, vol. 246, 2018

[4] Sebastian Henningsen, Daniel Teunis, Martin Florian, and BjörnScheuermann. Eclipsing ethereum peers with false friends.In 2019 IEEE European Symposium on Security and PrivacyWorkshops (EuroS&PW), pages 300 - 309. IEEE, 2019.