IP Hijacking 유형 분석 및 방지 방안 연구

홍성철, 서신석, 홍원기
포항공과대학교 컴퓨터공학과
{pluto80, sesise, jwkhong}@postech.ac.kr

IP Hijacking Analysis and Prevention Method

Seong-Cheol Hong, Sin-Seok Seo, and James Won-Ki Hong
Dept. of Computer Science and Engineering, POSTECH

요 약

인터넷은 AS (Autonomous System) 간의 상호연결을 통해 사용자들에게 보편적 연결성을 제공하며, 이러한 AS 간의 상호연결에 사용되는 프로토콜인 BGP 는 많은 보안 취약점을 가지고 있다. 해당 취약점을 노리는 대표적인 공격인 IP hijacking 은 다른 네트워크에 속한 IP 주소 대역을 부정적인 공격 행위를 통해 훔치는 것을 뜻한다. BGP 경로 정보인 NLRI 와 AS_PATH 정보의 조작을 통해 이러한 IP hijacking 행위가 이루어지며, 이는 공격자의 고의적인 행위일 수도 있지만 관리자의 설정 실수에 의한 경우도 빈번히 발생한다. 이러한 BGP 보안 취약점을 해결하기 위해 S-BGP, So-BGP 등 프로토콜 기능의 확장에 의한 해결책과, PHAS, PG-BGP 등의 IP hijacking 탐지를 통한 해결책 등 많은 연구가 진행되어 왔다. 그러나 이런 방식들은 사용하기에 많은 비용이 소모되고 여러 문제점이 발생하기 때문에 실제로 적용되지 못하고 있다. 본 논문에서는 현재 사용되는 BGP 프로토콜을 그대로 유지하면서도 IP hijacking 행위를 탐지할 수 있는 방지 알고리즘을 제시한다. NLRI, AS_PATH 를 조작하는 두 가지 경우로 나누어 각각의 공격 유형에 대해 설명하고 이에 대한 방지 알고리즘을 제안하여 잘못된 라우팅 정보가 인터넷 상으로 전파되는 것을 막을 수 있도록 한다.

I. 서론

현재의 인터넷은 network of networks로도 정의되며, 수많은 AS (Autonomous System)들이 상호연결되어 사용자들에게 보편적 연결성(any-to-any connectivity)을 제공한다 [1]. 이러한 AS 간의 상호연결에 사용되는 라우팅 프로토콜은 EGP (Exterior Gateway Protocol)의 한 종류인 BGPv4[2]를 사용하고 있다. 그러나 BGP의 설계상 많은 보안 취약점을 가지고 있으며 IP hijacking에 의하여 특정 목적지에 대한 연결 불가 현상이 지속적으로 발생해왔다. 가장 잘 알려진 1997년도 사례로써 한 많은 수의 네트워크 prefix에 대한 짧은 경로를 자신의 상위 ISP로 announce 했던 AS7007의 사례가 있다 [3].

IP hijacking은 다른 네트워크에 속한 IP 주소 대역을 부정적인 공격 행위를 통해 훔치는 것을 뜻한다. IP hijacking은 BGP hijacking으로도 알려져 있는데, 이는 IP hijacking을 하기 위해서는 BGP를 통한 announce가 필요하기 때문이다. 인터넷은 수 만개의 AS로 이루어져 있으며, BGP의 기본 기능은 AS 간에 상호도달정보를 교환하여 각 BGP speaker가 AS 연결관계에 대하여 알 수 있도록 해준다. BGP 경로는 특정 prefix와 그 prefix로 가기 위해 거쳐야하는 AS path로 이루어지는데, 각각을 NLRI (Network Layer Reachability Information), AS_PATH 라 한다. IP hijacking은 어떤 AS가 특정 prefix에 대한 소유권을 가지고 있지 않으면서 마치 자기한테 할당된 prefix인 것처럼 announce하는 경우 발생한다. 이것은 공격자의 고의적인 행위일 수도 있지만, 관리자의 설정 실수에 의한 경우도 빈번히 발생한다. 문제는 이러한 잘못된 라우팅 정보가 BGP 설계 상의 취약점으로 인해 전체 인터넷으로 전파되어 나가는데 있다.

공격자들은 IP hijacking을 통하여 특정 IP 주소 대역을 확보하게 되면 자신의 존재를 쉽게 드러내지 않으면서 스팸이나 DoS 공격을 수행할 수 있다. 또한 의도적으로 훔친 주소 대역에 속한 호스트들에 대한 통신을 단절시킬 수가 있는데, 이 역시 DoS 공격의 한 종류에 속한다. 두 경우 모두 인터넷의 보안과 안정성에 커다란 장애 요소가 된다.

IP hijacking은 인터넷 라우팅 프로토콜인 BGP를 이용한 공격 행위이며, IETF의 RPSEC (Routing Protocol Security Requirements) 워킹 그룹에서는 일반적인 위협 요소에 대한 정보와 BGP 보안 요구사항에 대해 설명하였다 [4]. BGP 설계 상의 취약점을 극복하기 위해 PKI 기반 구조의 S-BGP[5]가 제안되었으나, 제안된 아키텍처를 적용하기에는 확장성의 문제가 존재한다. 유사한 연구로서 진행된 So-BGP[6]의 경우 S-BGP의 단점을 해결하면서 능동적인 비정상 행위 탐지 기능도 제공하고 있다. 그러나 앞의 두 가지 방법 모두 프로토콜에 대한 확장 기능을 추가하는 것으로써 이미 BGP가 널리 쓰이고 있는 상황에서 실제로 적용하기에는 어려움이 따른다.

프로토콜의 확장이 현실적으로 적용되기 어렵기 때문에 IP hijacking 행위를 탐지하여 대응하는 방법에 대한 연구도 진행되었다. PHAS[7]의 경우 전 세계의 BGP 메시지들을 분석하여 각 prefix의 origin AS에 대한 정보를 유지함으로써 IP hijacking 행위가 발생하였는지를 탐지해 낸다. 이는 전 세계의 BGP 메시지들을 수집해 주는 신뢰할 수 있는 기관이 있을 경우에만 가능하다. PG-BGP[8]는 업데이트 메시지에 대하여 지연을 두면서 해당 업데이트 메시지가 신뢰할 수 있는지를 분석하여 IP hijacking 행위를 미연에 방지한다. 그러나 PG-BGP는 아무런 문제가 없는 announce에 대해서도 신뢰성 여부를 판단하기 위해

본 연구는 2008 년도 지식경제부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음(IITA-2008-(C1090-0801-0045))

지연시키는 단점을 갖는다.

본 논문에서는 현재 사용되는 BGP 프로토콜을 그대로 유지하면서도 IP hijacking 행위를 방지할 수 있는 IP hijacking 방지 알고리즘을 제시한다. IP hijacking을 NLRI를 조작하는 경우와 AS_PATH를 조작하는 두 가지 유형으로 나누고, 각각에 대한 방지 알고리즘을 제안한다. 제안된 알고리즘은 IP hijacking 공격에 대한 사후 대처가 아니라, 실시간으로 잘못된 정보임을 인지하여 이 정보가 인터넷 상으로 전파되는 것을 막는다.

본 논문의 구성은 다음과 같다. 2 장에서는 BGP 의 취약점 및 이를 이용한 공격 유형에 대해 간략히 서술하고, 본 연구에서 해결하고자 하는 문제인 IP hijacking 에 대한 두 가지 유형에 대하여 설명한다. 3 장에서는 IP hijacking 방지 알고리즘을 각각의 hijacking 유형 별로 제시하고, 끝으로 4 장에서는 결론과 향후 연구에 대해서 기술한다.

II. IP Hijacking 의 유형 분석

IP hijacking 은 BGP 의 취약점을 이용한 공격 행위이며, 이를 이용한 다양한 공격 유형이 존재한다. 본 장에서는 BGP 를 이용한 공격 유형과 IP hijacking 의 유형에 대해 알아 본다.

2.1 BGP 의 취약점과 이를 이용한 공격 유형

BGP 는 다음과 같은 취약점으로 인해 다양한 보안 위협 요소를 가진다.

- Peer 사이의 통신에 사용되는 메시지에 대한 무결성, 상호 인증 등을 지원하는 내부 메커니즘을 지원하지 않는다.
- NLRI를 announce하는 AS의 소유권을 증명할 어떠한 방법도 정의되어 있지 않다.
- AS에 의해 전달되는 경로 정보가 확실하고 신뢰할 수 있는지 확인할 수 있는 방법이 없다.

이러한 BGP 취약점을 이용하여 공격자가 취할 수 있는 공격 유형은 다음과 같다.

- Blackholing: 거짓된 라우팅 정보를 전달함으로써 어떤 prefix에 대한 트래픽을 특정 라우터로 전달하게 하여 버리는 것을 목표로 한다.
- Redirection: 트래픽의 흐름을 다른 경로로 바꾸어 전달되게 만드는 것으로써, 트래픽이 공격자를 거쳐가게 함으로써 정보를 빼내거나 특정 링크에 부하를 주게끔 한다.
- Subversion: Redirection의 특수한 경우로, 트래픽이 공격자를 거쳐가게 될 때 트래픽의 내용을 변경하기 위한 목적으로 공격을 시도한다.
- Instablility: 동일한 네트워크에 대해 advertisement와 withdrawal을 반복함으로써 특정한 네트워크에 대한 접속을 막거나 다수의 BGP 트래픽을 생성하여 라우팅 테이블의 안정화를 지연시키는 행위이다.

2.2 IP hijacking의 유형

BGP의 근본적인 취약점으로 인해 IP hijacking이 손쉽게 가능하며, 잘못된 라우팅 정보에 대한 아무런 대응책도 없는 실정이다. 본 연구에서는 IP hijacking을 크게 두 가지로 나누어 접근하고자 한다. 그림 1, 2에서 해당 유형에 대해 간략히 묘사하였다.

- NLRI의 위조: 공격자가 피해자 AS의 IP prefix에 대한 소유자인 것처럼 announce하는 방법이다. 이 경우 해당 prefix의 목적지가 공격자 AS와 피해자 AS 모두에 해당되는 MOAS (Multiple Origin AS)가 발생하게 된다 [9].
- AS_PATH의 위조: 피해자 AS로 가기 위해서 공격자 AS를 거쳐 가는 경로가 있는 것처럼 알리는 방법이다. 이 경우에는 MOAS가 발생하지 않으며, 공격자 AS를 거쳐 피해자 AS로 가는 트래픽은 공격자가 손쉽게 도청, 수정, 삽입이 가능하다.

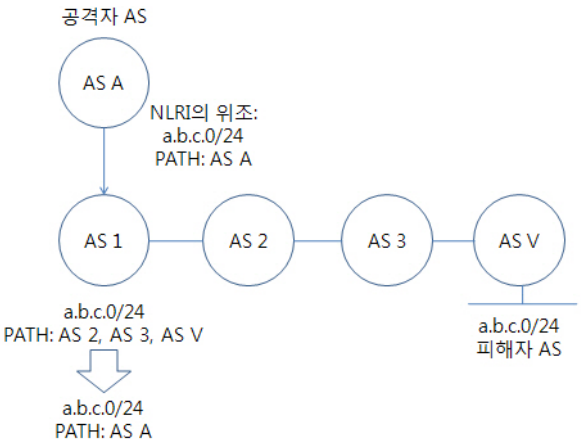

그림 1. NLRI 의 위조

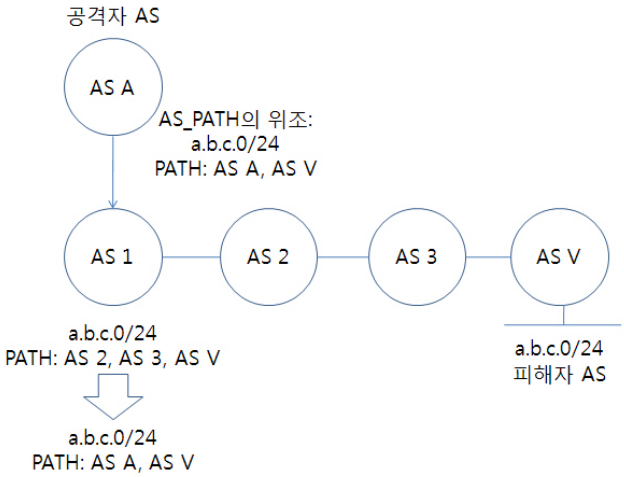

그림 2. AS_PATH 의 위조

그림 1 의 경우 공격자가 위조된 BGP 메시지를 announce 한 후에는, AS 1 이 a.b.c.0/24 IP 대역으로 트래픽을 보내기 위해서 AS 2 가 아닌 AS A 로 보내게 되는데, 라우팅 알고리즘은 기본적으로 AS PATH 가 짧은 경로가 우선 순위가 높기 때문이다. 그림 2 의 경우도 마찬가지인데, 차이점이 있다면 그림 1 의 경우에는 a.b.c.0/24 에 대해서 Origin AS 가 AS 1 과 AS V 둘 다 존재하게 되는 MOAS 가 생긴다는 것이다.

MOAS 가 IP hijacking 에 의해서만 생기는 것은 아니다 [10]. Multihomed-AS 가 static link 로 다른 AS 와 연결되거나 private AS 번호를 가지게 되는 경우 정당한 이유로 MOAS 가 생기게 된다. 따라서 IP hijacking 에 의한 경우와 정당한 이유에 의한 경우의 MOAS 를 구별해 내는 것이 필요하게 된다.

III. IP Hijacking 방지 알고리즘

BGP는 직접 연결된 BGP Peer 사이의 통신을 기본으로 한다. 본 연구에서 제시하는 IP hijacking 방지 알고리즘을 적용하기 위해서는 인접한 AS가 아닌 떨어져 있는 AS하고도 메시지를 주고 받을 수 있어야 하는데, 이는 notification 메시지를 수정함으로써 가능하다. AS끼리 주고 받아야 하는 메시지에 대해서는 IP hijacking의 유형 별로 방지 알고리즘을 설명하면서 언급하도록 한다.

IP hijacking 방지 알고리즘을 서술에 앞서 사전 가정은 다음과 같다..

- 각 BGP 라우터의 현재 라우팅 테이블은 공격에 의해 변경되지 않은 것으로 본다.
- 각 BGP speaker들은 서로 간에 IPSec을 통해 통신함으로써 BGP 통신에 대한 공격 시도에 대해서는 안전하다고 본다.
- 라우팅 테이블에는 특정 IP 대역에 대해서 여러 경로를 유지할 수 있다.

3.1 NLRI의 위조에 대한 방지 알고리즘

NLRI의 위조에 대한 공격을 방지하기 위한 알고리즘을 적용하기 위해서 몇 가지 가정을 하도록 한다.

- MOAS가 생긴 경우, 이것이 해당 IP prefix의 소유주에 의한 정당한 MOAS인지를 탐지하고 분석할 수 있다.
- 같은 prefix에 대해서 이전 경로가 새로운 경로보다 더 높은 우선 순위를 갖는다.
- 새로운 경로를 선택하기 위해서는 이전 경로에 대해서 withdrawn 메시지를 받아야만 한다. 즉, 이전 경로는 반드시 그 경로를 announce했던 소유주가 withdrawn 메시지를 통해 알려야 한다.

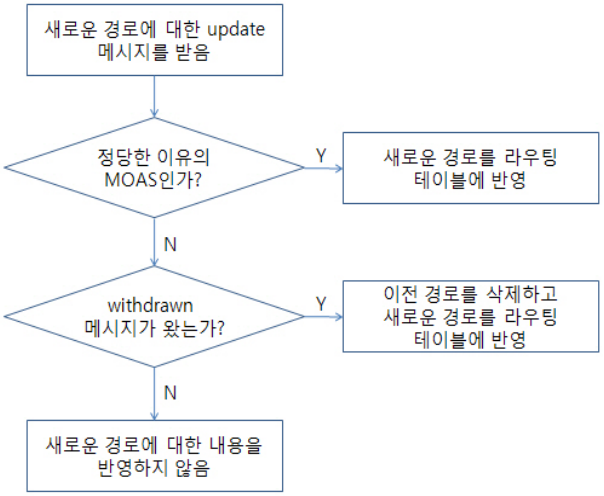

그림 3. NLRI의 위조에 대한 방지 알고리즘

그림 3은 NLRI의 위조에 대한 방지 알고리즘을 보여준다. 어떤 IP prefix에 대한 새로운 경로를 받게 되는 경우 발생한 MOAS에 대해서 정당한 이유에 의한 것인지부터 확인한다. 만약 정당한 이유에 의한 MOAS라면 이전 경로와 새로운 경로를 모두 라우팅 테이블에 유지하면서 경로 선택 알고리즘에 의해 우선 순위를 정한다. 정당한 이유에 의한 MOAS가 아닌 경우, 새로운 경로의 적용을 잠시 보류하면서 이전 경로에 대한 withdrawn 메시지를 기다린다.

withdrawn 메시지는 어떤 IP prefix에 대한 소유주가 현재 할당된 AS 번호를 더 이상 사용하지 않겠다고 직접적으로 알리는 정보를 담고 있다. 이 메시지를 받은 AS는 다시 주변 AS로 메시지를 전파하게 되고, 이전 경로와 새로운 경로를 모두 가지고 있는 AS가 withdrawn 메시지를 받게 되면 이전 경로를 라우팅 테이블에서 삭제하고 새로운 경로를 적용하게 된다. 만약 withdrawn 메시지가 오지 않는다면 새로운 경로는 IP hijacking에 의한 것으로 보고 라우팅 테이블에 반영하지 않는다.

3.2 AS_PATH의 위조에 대한 방지 알고리즘

BGP는 인접한 AS의 BGP peer 사이의 통신이기 때문에 AS_PATH 정보만으로 적절성 여부를 판단하는 것은 불가능하다. 따라서 AS_PATH의 적절성을 판단하기 위해서는 AS_PATH의 반대 방향, 즉 Origin AS 로부터 자신의 AS로의 경로를 통해 연결이 되어 있는지를 확인해야 한다. AS_PATH 방향으로 확인을 하지 않는 것은 중간에 공격자 AS가 포함되어 있는 경우 조작된 응답을 할 수가 있기 때문이다.

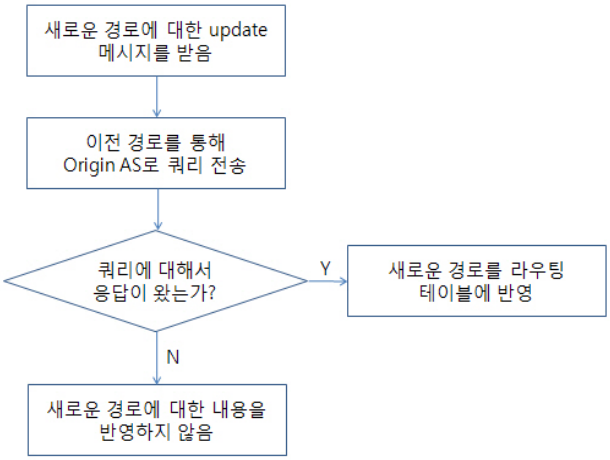

그림 4. AS_PATH의 위조에 대한 방지 알고리즘

그림 4는 AS_PATH의 위조에 대한 방지 알고리즘을 설명하고 있다. 새로운 경로 정보를 받았을 때, MOAS가 아니면서 여러 개의 경로가 존재하는 AS에 대해서 이 알고리즘을 적용하게 된다. 우선 새로운 경로에 대한 적절성 여부를 판단하기 위해 이전 경로를 통해 Origin AS로 쿼리 메시지를 보내는데, 이전 경로는 신뢰할 수 있는 경로이기 때문에 Origin AS까지 쿼리가 도달할 수 있다. 이 쿼리 메시지를 받은 Origin AS는 이전 경로가 아닌 새로운 경로를 통해서 응답 메시지를 보내게 된다. 만약 응답 메시지가 제대로 돌아온다면 새로운 경로는 적절한 것이므로 라우팅 테이블에 반영하게 되고, 응답 메시지가 돌아오지 않는다면 AS_PATH의 위조를 통한 IP hijacking으로 판단하고 라우팅 테이블에 반영하지 않는다.

이 알고리즘은 공격자가 존재하지 않는 경로를 announce 한 경우에는 탐지가 가능하나 실제로 존재하는 경로를 이용하여 redirection 공격을 하는 경우에는 IP hijacking으로 분류가 되지 않는 단점을 가진다. 이는 향후 연구를 통해 보완되어야 할 것이다.

IV. 결론

AS 간의 라우팅 정보를 주고 받는 프로토콜인 BGP는 설계 상의 취약점으로 인해 IP hijacking을 비롯한 많은 보안 위협에 노출되어 있다. IP hijacking 행위는 인터넷의 보안과 안정성에 큰 위협 요소가 될 수 있기에 이에 대한 대처 방안은 필수적이다. 본 연구에서는 BGP가 가지고 있는 취약점과 이를 이용하여 시도될 수 있는 공격에 대하여 알아보고, IP hijacking의 유형을 NLRI의 위조와 AS_PATH의 위조 두 가지 경우로 나누어 각각에 대한 방지 알고리즘을 제안하였다. 이를 위해서는 서로 인접하지 않은 BGP peer 사이의 주고 받아야 하는 정보가 필요한데, 이는 현재의 BGP 프로토콜을 확장하지 않고도 충분히 가능한 내용이다. 본 연구에서 제안하는 방법을 통해서 실시간으로 IP hijacking에 대한 탐지를 통해 잘못된 정보가 인터넷 상으로 전파되는 것을 미연에 방지할 수 있게 된다.

향후 연구로는 IP hijacking을 sub-prefix hijacking 까지 범위를 확장하여 보다 다양한 경우의 공격 방안에 대한 대응 방안을 만들고자 한다. 또한 MOAS의 적절한 경우와 부적절한 경우를 보다 정확히 분류해 낼 수 있는 방안을 연구하여 알고리즘의 정확도를 더 높일 예정이다. 그리고 제시한 알고리즘의 검증 방안에 대한 연구도 진행되어야 할 것이다.

참고문헌

[1] 김희수, “인터넷 상호접속 공정경쟁 이슈와 정책대안”, KISDI 이슈리포트, 03-10, 2003년 8월 11일.

[2] Y. Rekhter, T. Li, and S. Hares, “A Border Gateway Protocol 4 (BGP-4)”, RFC 4271, Jan. 2006.

[3] V. J. Bono, ”7007 Explanation and Apology”, http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html.

[4] A. Barbir, S. Murphy, and Y. Yang, “Generic Threats to Routing Protocols”, IETF Draft: draftietf-rpsec-routing-threats-07, April 2004.

[5] S. Kent, C. Lynn, and K. Seo, “Secure Border Gateway Protocol (Secure-BGP)”, IEEE Journal on Selected Areas in Communications (JSAC), Vol. 18, No. 4, Apr. 2000, pp. 582-592.

[6] P.C. van Oorschot, Tao Wan, and Evangelos Kranakis “On Interdomain Routing Security and Pretty Secure BGP (psBGP)”, ACM Transactions on Information and System Security (TISSEC), Vol. 10, No. 11, Article 11, 2007.

[7] M. Lad, D. Massey, D. Pei, Y. Wu, B. Zhang, and L. Zhang, “PHAS: A Prefix Hijack Alert System”, In Proc. of 15th USENIX Security Symposium, Vancouver, B.C., Canada, Jul. 31-Aug. 4, 2006.

[8] J. Karlin, J. Karlin, S. Forrest, and J. Rexford, “Pretty Good BGP: Improving BGP by Cautiously Adopting Routes”, In Proc. of the 2006 IEEE International Conference on Network Protocols (ICNP), Santa Barbara, CA, USA, Nov. 12-15, 2006, pp. 290-299.

[9] X. Zhao, D. Pei, L.Wang, D. Massey, A. Mankin, S.Wu, and L. Zhang, “An Analysis of BGP Multiple Origin AS (MOAS) Conflicts”, In Proc. of ACM SIGCOMM Internet Measurement Workshop, San Francisco, CA, USA, Nov. 2001.

[10] X. Hu and Z. M. Mao, “Accurate Real-time Identification of IP Prefix Hijacking”, In Proc. of IEEE Symposium on Security and Privacy, Oakland, CA, USA, May 20-23, 2007, pp. 3-17.