BGP 보안 위협 요소와 대처방안

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

A Survey of BGP Security Threats and Countermeasures

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

요 약

인터넷은 AS (Autonomous System)라 불리는 무수히 많은 독립적인 네트워크들이 서로 연결되어 구성된다. 이 AS 들 간에 라우팅 정보를 교환하는 프로토콜은 현재 BGPv4 가 사실상의 표준으로 사용되고 있다. 그러나 BGP 는 여러 가지 보안 위협 요소를 안고 있으며, 아직까지는 그에 대한 명확한 해결책이 제시되어 있지는 않다. BGP 의 보안 위협 요소로는 무결성 위반, 메시지 재전송, 메시지 삽입, 메시지 삭제, 메시지 변형, man-in-the-middle 공격, 서비스 거부, 네트워크 운영자의 설정 실수 등 매우 다양하다. 이런 여러 위협 요소에 대해 BGP MD5 인증, Secure BGP (S-BGP), Secure Origin BPG (So-BGP), Pretty Good BGP (PG-BGP), A Prefix Hijack Alert System (PHAS) 등 많은 해결 방안이 제시되고 있다. 그러나 이런 방식들을 적용하려면 많은 비용이 들고, 제반 문제점들이 발생하기 때문에 널리 사용되지 않고 있다. 본 논문에서는 여러 위협 요소들을 정리하고, 이런 위협 요소들에 대한 해결 방안 및 그 해결 방안들이 가지고 있는 또 다른 문제점들에 대해 정리·분석한다.

I. 서론

인터넷은 무수히 많은 수의 네트워크가 서로 연결되어 구성된다. 이 각각의 네트워크들은 AS (Autonomous System) 라고 불리며, ASN (Autonomous System Number) 으로 상호 구분될 수 있다. 이와 같은 AS 들간의 관계를 그림 1에 나타내었다. 또한 인터넷은 계층적 구조를 이루고 있다. 각 인터넷 이용자가 다른 이용자들과 통신할 수 있는 것은 ISP 들이 수직적 계층구조를 이루고 있기 때문이다[1].

라우팅 프로토콜은 크게 AS 내부에서 사용되는 IGP (Interior Gateway Protocol)과 EGP (Exterior Gateway Protocol)로 구분될 수 있다. AS는 말 그대로 하나의 독립적인 네트워크이기 때문에 AS 내부의 라우팅 프로토콜은 AS 외부에 영향을 미치지 않는다. 하지만 AS들 간의 트래픽 교환을 위해서는 AS들 끼리 공통적인 프로코톨을 이용하여 라우팅 정보를 교환하여야 한다.

AS들 간에 라우팅 정보를 교환하는 프로토콜은 현재 BGPv4[2]가 사용되고 있으며, 사실상 (de facto) 표준이다. 하지만 BGP 프로토콜을 설계할 당시에는 오늘날과 같이 AS들 간의 관계가 복잡하지 않았고, 여러가지 보안과 관련한 문제를 고려하지 않았기 때문에 특정 공격에 매우 취약할 수 있다.

최근에 발생한 가장 대표적인 BGP 보안 위협 사례로는 유투브의 사례를 들 수 있다[3]. 파키스탄 텔레콤은 정치·종교적 이유로 파키스탄 국민들이 유투브 사이트에 접속하는 것을 막고자 했으며, 2008년 2월 24일 18시 47분 경에 유투브의 IP 주소를 자신들의 AS에 속해있는 것처럼 BGP 업데이트 메시지를 announce 했다. 파키스탄 텔레콤의 상위 ISP인 PCCW Global은 이 announcement를 전 세계로 전파했으며, 그 결과 파키스탄뿐만 아니라 전 세계의 다른 국가에서도 유투브 사이트에 접속할 수 없는 사태가 발생했다.

이와 같이 BGP는 ISP 상호 간에 인증을 하는 것과 같은 보안 메커니즘이 부족하기 때문에, 해커가 하나 또는 그 이상의 BGP 스피커 라우터에 대한 제어를 갖게 되는 경우 매우 쉽게 해킹을 할 수 있는 문제점을 안고 있다. 그렇기 때문에 이제까지 BGP를 보완·개선하고자 하는 많은 연구가 진행되어 왔지만 이 방식들을 적용하려면 많은 비용이 들고, 제반 문제점들이 발생하기 때문에 아직까지 널리 이용되고 있지는 않다.

본 연구에서는 이제까지 알려진 BGP 보안 위협 요소를 알아보고, 그에 대한 대처 방안과 그 대처 방안들이 가지고 있는 또 다른 문제점들에 대해 조사해 정리하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 BGP가 가지고 있는 보안 위협 요소에 대해 알아보고,3장에서는 이러한 위협 요소를 원천적으로 방지하기 위해 반드시 만족되어야 하는 BGP 보안 목표에 대해 논의 한다. 4장에서는 BGP의 여러 위협 요소를 극복할 수 있는 여러 대처 방안에 대해 정리한다. 끝으로 5장에서는 결론과 향후 연구에 대해서 기술한다.

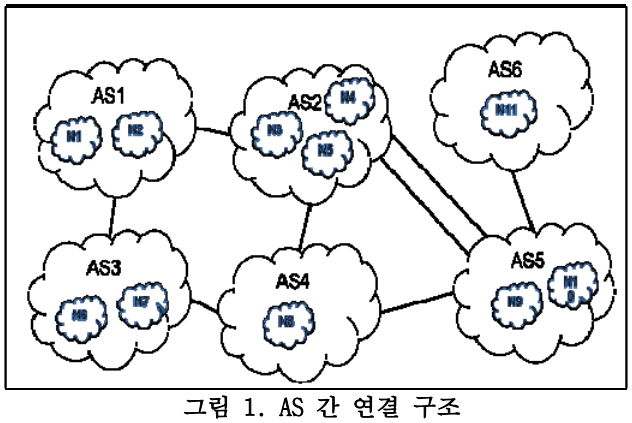

그림 1. AS 간 연결 구조

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

II. BGP 보안 위협 요소

BGP는 다음과 같은 세가지 원론적인 취약점 때문에 다양한 보안 위협 요소를 가질 수 밖에 없다[4].

- BGP는 peer 사이의 BGP 통신에 사용되는 메시지에 대해 무결성, freshness, peer 간의 상호 인증 등을 지원하는 충분히 강력한 내부 메커니즘을 가지고 있지 않다. 무결성은 전달되는 메시지가 변경되지 않았다는 것을 보장하는 것이며, freshness는 수신측이 재전송된 메시지가 아니라 실제로 새로운 메시지를 받는 것을 보장하는 것이다. peer 간의 상호 인증은 메시지를 송신한 AS가 해커가 아닌 정당한 AS임을 보장한다.

- BGP에는 NLRI (Network Layer Reachability Inforamtion)을 announce하는 AS의 권한을 증명할 어떠한 메커니즘도 정의되어 있지 않다. 이것은 path subversion 이라 불리는 공격 방법과 관련이 있는 항목이다. 즉 AS가 자신의 네트워크에 속하지 않은 IP 주소 대역을 announce 해도 BGP 프로토콜 상에서는 아무런 문제가 되지 않는다. 만약 특정 AS가 다른 AS의 IP 대역에 대해서 좀 더 자세한 prefix로 announce하게 되면, 다른 AS로 가야할 트래픽을 중간에서 가로챌 수 있게 된다. 이러한 공격 방법은 ip hijacking, prefix hijacking, bpg hijacking 등으로 불리기도 한다.

- BGP에는 AS에 의해 announce 되는 경로의 속성이 확실하고 신뢰할 수 있는지 확인할 수 있는 어떠한 메커니즘도 정의되어 있지 않다. 중간에 있는 AS가 라우팅 Path를 변경해도 그 사실을 알아낼 수 있는 방법이 없기 때문에 여러 가지 공격이 가능할 수 있다.

위와 같은 세 가지 BGP의 원론적인 취약성 때문에 매우 다양한 BGP에 대한 공격이 가능하다. BGP의 보안 위협 요소로는 무결성 위반, 메시지 재전송, 메시지 삽입, 메시지 삭제, 메시지 변형, man-in-the-middle 공격, 서비스 거부, 네트워크 운영자의 설정 실수 등 매우 다양하다[4].

- 무결성 위반: BGP를 통해 전달되는 라우팅 데이터는 평문으로 전달되며, 라우팅 데이터를 중간에 가로채서 그 내용을 알아낼 수 있다.
- 메시지 재전송: BGP는 메시지 재전송을 방지하는 방법을 제공하지 않는다.
- 메시지 삽입: BGP는 새로운 메시지 삽입 공격을 막을 수 있는 방안을 제공하지 않는다. 그러나 BGP는 TCP를 이용하기 때문에 이미 연결이 이루어진 BGP 세션에 새로운 메시지를 삽입하기 위해서는 정확한 sequence 번호를 알아야 한다.
- 메시지 삭제: BGP는 메시지를 삭제하는 공격을 막을 수 있는 방안을 제공하지 않는다.
- 메시지 변경: BGP는 중간에 메시지를 변경하는 공격을 막을 수 있는 방안을 제공하지 않는다.
- Man-in-the-middle 공격: BGP는 man-in-the-middle 공격을 방지할 수 있는 방안을 제공하지 않는다. BGP는 peer에 대한 인증을 하지 않기 때문에, 이러한 유형의 공격은 매우 쉬울 수 있다.
- 서비스 거부: 좀 더 자세한 대량의 경로를 전달함으로써 BGP 트래픽과 라우터의 테이블 크기가 극단적으로 증가할 수 있다. 그렇게되면 라우터의 처리속도가 현저히 감소하고 원활한 서비스 제공이 어렵게 된다.
- 네트워크 운영자의 설정 실수: 사소한 설정 실수가 전체 인터넷 트래픽의 흐름에 심각한 영향을 줄 수 있다.

만약 해커가 하나 또는 그 이상의 BGP 라우터에 접근할 수 있고, 그 라우터를 원하는대로 조정할 수 있게된다면 다음과 같은 공격도 가능하다[5].

- Blackholing: Prefix가 대부분의 인터넷 망에서 접근할 수 없을 때 발생한다. 거짓된 라우팅 정보를 전달함으로써 발생하며, 이것은 특정 라우터로 트래픽을 유도한 후 해당 트래픽을 버리는 것을 목표로 한다.
- Redirection: 특정 네트워크로 전달되어야 하는 트래픽의 흐름을 다른 경로로 전달되게 만드는 것이다. 이것의 한 목적은 기밀의 정보를 얻는 것이고, 또 다른 목적은 특정 링크에 과부하를 주어 혼잡하게 만드는 것이다.
- Subversion: Redirection의 특수한 경우로 트래픽을 특정한 링크를 지나도록 하여, 트래픽의 내용을 엿보거나 변경하기 위해 이러한 공격을 시도한다. 이 공격에서는 트래픽을 다시 원래의 목적지로 전달하기 때문에 발견하는 것이 매우 힘들다.
- Instability: 동일한 네트워크에 대해 연속적으로 advertisement와 withdrawal을 반복할 때 발생한다. 이 공격의 목적은 특정한 네트워크에 대한 접속을 막는 것이다. 또한 다수의 BGP 트래픽을 생성해서 컨버전스 딜레이를 길게 만들기 위해 이 공격을 시도하기도 한다.

III. BGP 보안 목표

앞서 살펴본 바와 같이 BGP는 심각한 보안 취약점을 가지고 있다. 이런 보안 취약점을 해결하기 위해서는 다음과 같은 요구사항이 만족되어야 한다[6].

- AS 번호 인증: AS 번호 s_i를 사용하는 주체가 실제로 AS 번호 할당 기관으로부터 AS 번호 s_i를 할당받은 AS인지 확인할 수 있어야 한다.
- BGP 스피커 인증: AS 번호 s_i를 announce하는 BGP 스피커는 AS 번호 할당 기관으로부터 AS 번호 s_i를 할당받은 AS에의해 인증된 라우터인지 확인할 수 있어야 한다.
- 데이터 무결성: BGP 메시지가 불법적으로 변경되지 않았는지 확인할 수 있어야 한다.
- Prefix Origination 확인: 특정 Prefix를 announce하는 AS가 해당 Prefix를 실제로 소유하고 있는 AS인지 확인할 수 있어야 한다.
- AS 경로 확인: BGP 경로 (f, p_k)의 AS_PATH(p_k = [$s_1, s_2, \cdots, s_k$]가 실제로 s_1으로부터 시작되었으며, $s_2, \cdots, s_k$ 의 순서대로 전달되어 왔는지 확인 할 수 있어야 한다.

IV. 대처방안

BGP 프로토콜이 많은 보안 취약성을 가지고 있는 만큼 그에 대한 많은 해결책이 제시되고 있다. 본 장에서는

방 법		네트워크 기반	종단 호스트 기반
탐 지		MOAS[8], geo[9], PHAS[10], finger-printing[11], hop-count[12], routing information objects[13]	ACR[14]
Reactive		Manual response to install filters, ACR[14], MIRO[16]	Overlay routing, *e.g.*, RON[15]
Proactive	암호화 기반	S-BGP [17], So-BGP [18], SPV [19], listen-whisper[20], route purging promotion	-
	비암호화 기반	PG-BGP[21], intentional deaggregation, bogon filter, Hi-BGP[22], customer route filtering	-

표 1. 대처방안

현재까지 제시된 많은 해결책들 중에서 주요한 몇가지에 대해 알아보고, 또한 각각의 방안들이 가지고 있는 문제점에 대해서도 알아본다.

표 1은 현재까지 제시된 대처방안들을 정리한 것이다[7]. 수 많은 대처방안 중에서 MD5 인증, Secure BGP (S-BGP), Secure Origin BGP (So-BGP), PHAS 방식의 대처방안에 대해서 알아본다.

4.1 BGP MD5 인증

이 방식은 IETF RFC 2385에 제안된 것으로 BGP 세션의 확실성을 보호하기 위해 고안되었다[23]. 모든 TCP 패킷은 MD5 알고리즘을 이용해 생성된 16 바이트의 MD5 다이제스트를 포함해야 한다. 이렇게 함으로써 RST 패킷에 오염된 TCP 세그먼트가 들어오는 것을 방지할 수 있다. 그러나 이 방식은 각 TCP 세그먼트에 대해 MD5 다이제스트를 계산하고 검증하기 위해 CPU 자원을 사용하게 된다. 몇몇의 BGP 취약성에 대해서 MD5 인증방식은 적절한 대처방안이 될 수 있다.

4.2 Secure BGP (S-BGP)

S-BGP는 IP 주소 블록, AS 번호, AS id, BGP 라우터 id를 인증하기 위해 PKI와 IPSec과 같은 여러 메카니즘을 사용하는 방식이다[17]. 이 PKI는 엄격한 계층 구조를 이루고 있다. 또한 PKI 기반구조는 기존의 AS 번호와 IP 주소공간 할당 기관들과 공존하며, 기존의 시스템에 영향을 미치지 않는다. BGP 라우팅 정보는 디지털 서명으로 암호화되어 전달되며 디지털 서명을 전달하기위해 BGP 업데이트 메시지에는 새로운 속성이 추가된다. BGP 메시지의 수신측에서는 이 디지털 서명을 이용하여 주소 Prefix와 경로 정보를 검증할 수 있다. 또한 데이터의 무결성을 보장하고 BGP 라우터들이 상호간에 인증을 하기위한 BGP 제어 트래픽을 교환하는데 IPSec을 사용한다. 이러한 방식들을 사용함으로써 Prefix Origin의 검증과 AS_PATH의 무결성을 확실히 보장할 수 있다.

S-BGP는 기존의 AS번호와 IP 주소 대역 할당 메커니즘에 영향을 미치지 않으면서 BGP 보안 문제를 해결했지만, 실제로 구현하여 사용하기 위해서는 여러가지 문제점이 따른다. 우선 제안된 PKI 자체도 매우 복잡하며, 규모가 큰 시스템에 적용하기에는 Scalable 하지 못하다. 또한 AS_PATH를 검증하는데에는 많은 계산이 필요하며, 경로의 유출 정책을 위반하는 것은 발견하지 못한다.

4.3 Secure Origin BGP (So-BGP)

So-BGP는 전달되는 prefix를 검증하는 것을 목표로 한다[18]. BGP SECURITY라는 새로운 BGP 메시지가 보안과 관련한 정보를 전달하는데 사용된다. AS의 공개키를 인증하기위해 web-of-trust 모델을 이용하며 IP Prefix의 소유주를 검증하기 위해 계층적인 구조를 이루고 있다. 각각의 AS는 공개키 인증서를 가지며, AS 번호는 이 공개키와 함께 암호화된다.

So-BGP를 실제로 적용하는데 있어서도 여러가지 문제점이 따른다. IP Prefix는 AS에 대해서 할당되는 것이 아니라, 회사나 학교와 같은 조직에 할당되기 때문에 So-BGP를 적용하는 것이 실제적으로 가능한지 명확하지 않다. 또한 IP 주소의 할당 대역은 수시로 바뀔 수 있는데, 이것을 엄격한 계층 구조안에서 추적하는 것은 매우 어려운 일이다.

4.4 Pretty Good BGP (PG-BGP)

PG-BGP는 의심가는 경로의 전파와 사용에 자동적으로 지연을 두는 시스템이다[21]. 이렇게 지연을 두면 네트워크 관리자와 자동화된 시스템이 의심가는 경로에 대해 조사하여 문제가 없는 announcement인지 판단할 수 있는 시간을 얻을 수 있다. 또한 어떤 경우에는 의심가는 경로가 일정 시간이 흐른 후 스스로 사라질 수도 있다. 최근의 BGP Update 메시지 정보에 기록되어 있는 신뢰할 수 있는 라우팅 테이블을 참조하여 의심가는 경로를 알아낼 수 있다. 일정 기간 동안에는 의심가는 경로에 가장 낮은 우선순위를 두면, 대체 경로가 있는 경우에는 의심가는 경로를 사용하는 대신 다른 경로를 이용하여 트래픽을 전달하게 된다. 일정 기간 후 의심가는 경로가 문제가 없는 경로라고 판단된다면, 이 경로를 일반적인 우선 순위로 바꾸어 정상적으로 동작하게 한다.

PG-BGP의 가장 큰 문제점은 아무런 문제가 없는 경로의 announceemnt도 지연을 시킨다는 것이다.

4.5 A Prefix Hijack Alert System (PHAS)

PHAS의 목표는 특정 preifx의 origin이 바뀌면 알리는 것이다[10]. 첫 번째 단계로 Route Views[24]의 BGP 테이블을 실시간에 가깝게 모니터링하고 각각의 prefix에 도달하기 위한 origin들의 데이터 베이스를 유지한다. 새로운 origin이 발생하면 그것을 알려서 데이터 베이스에 저장한다. 만약 정해진 시간 동안 특정 origin이 사용되지 않으면 그 origin은 데이터 베이스에서 제거된다. 이런식으로 데이터베이스를 유지하고 Route Views의 BGP 테이블을 모니터링하다가 문제가 발생하면 이메일과 같은 방식을 이용하여 네트워크 관리자에게 알린다.

V. 결론

BGP 프로토콜은 AS 간의 라우팅 정보를 교환하는데 있어서 필수적인 프로토콜이고 사실상의 표준으로 현재 널리 사용되고 있지만, 여러가지 취약점을 가지고 있다. 그렇기 때문에 유투브의 사례처럼 심각한 문제가 발생할 가능성이 매우 크다. 본 연구에서는 BGP가 가지고 있는 여러가지 취약점에 대해 알아본 후 그 취약점을 극복하기 위해 제시된 여러가지 방안들을 비교 분석했다. 그렇지만 이제까지 제시된 대처방안들을 실제 BGP 프로토콜에 적용하기 위해서는 많은 제약사항과 문제점이 따르기 때문에, 현재까지는 널리 쓰이고 있지 않다.

앞으로는 이러한 연구 조사에 기반하여 실제 BGP 프로토콜에 적용하여 구현하기 용이한 대처방안을 연구할 예정이다.

참 고 문 헌

[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] RIPE, "YouTube Hijacking: A RIPE NCC RIS case study", http://www.ripe.net/news/study-youtube-hijacking.html/.

[4] S. Murphy, "BGP Security Vulnerabilities Analysis", RFC 4272, Jan. 2006.

[5] O. Nordstrom and C. Dovrolis, "Beware of BGP Attacks", ACM SIGCOMM Computer Communications Review, Vol. 34, No. 2, April 2004, pp.1-8.

[6] Evangelos Kranakis, P.C. van Oorschot, and Tao Wan, "Security Issues in the Border Gateway Protocol (BGP)", Technical Report 05-07, Carleton University, Ottawa, Canada, Mar. 19, 2005.

[7] Z. Zhang, Y. Zhang, Y. C. Hu, and Z. M. Mao, "Practical Defenses Against BGP Prefix Hijacking", In Proc. of ACM CoNEXT, New York, NY, USA, Dec. 10-13, 2007.

[8] 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. 1-2, 2001, pp. 31-35.

[9] C. Kruegel, D. Mutz, W. Robertson, and F. Valeur, "Topology-Based Detection of Anomalous BGP Messages", In Proc. of the 6th Symposium on Recent Advances in Intrusion Detection (RAID), Pittsburgh, PA, USA, Sep. 8-10, 2003, pp. 17-35.

[10] 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.

[11] 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.

[12] C. Zheng, L. Ji, D. Pei, J. Wang, and P. Francis, "A Light-Weight Distributed Scheme for Detecting IP Prefix Hijacks in Real-Time", ACM SIGCOMM Computer Communication Review, Vol. 37, No. 4, Oct. 2007, pp. 277-288.

[13] J. Qiu, L. G. S. Ranjan, and A. Nucci, "Detecting Bogus BGP Route Information: Going Beyond Prefix Hijacking", In Proc. of SecureComm, Nice, France, Sep. 17-20, 2007, pp. 381-390.

[14] D. Wendlandt, I. Avramopoulos, D. Andersen, and J. Rexford, "Don't Secure Routing Protocols, Secure Data Delivery", In Proc. of ACM HotNets, Irvine, CA, USA, Nov. 29-30, 2006, pp. 7-12.

[15] D. G. Andersen, H. Balakrishnan, M. F. Kaashoek, and R. Morris, "Resilient overlay networks", ACM SIGOPS Operating Systems Review, Dec. 2001, pp. 131-145.

[16] W. Xu and J. Rexford, "MIRO: multi-path interdomain routing", ACM SIGCOMM Computer Communication Review, Vol. 36, No. 4, Oct. 2006, pp. 171-182.

[17] 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, April 2000, pp. 582-592.

[18] James Ng, "Extensions to BGP to Support Secure Origin BGP (soBGP)", Internet Draft, draft-ng-sobgp-bgp-extensions-01, June 2003.

[19] Y.-C. Hu, A. Perrig, and M. Sirbu, "SPV: A Secure Path Vector Scheme for Securing BGP", ACM SIGCOMM Computer Communication Review, Vol. 34, No. 4, Oct. 2004, pp. 179-192.

[20] L. Subramanian, V. Roth, I. Stoica, S. Shenker, and R. H. Katz, "Listen and Whisper: Security Mechanisms for BGP", In Proc. of the 1st conference on Symposium on Networked Systems Design and Implementation (NSDI), San Francisco, CA, USA, Mar. 29-31, 2004, pp. 127-140.

[21] 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.

[22] J. Qiu and L. Gao, "Hi-BGP: A Lightweight Hijack-proof Inter-domain Routing Protocol", Technical report, Univ. of Massachusetts, Amherst, MA, USA, 2006.

[23] A. Heffernan, "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385, Aug. 1998.

[24] Route Views, "University of Oregon Route Views Project", http://www.routeview.org/.