AS 별 특징 수집을 통한 IP Hijacking 탐지 방법

홍성철 [O,1], 주홍택 [2], 홍원기 [3]

[1] 포항공과대학교 컴퓨터공학과, [3] 정보전자융합공학부

[2] 계명대학교 컴퓨터공학과

[1]pluto80@postech.ac.kr, [2]juht@kmu.ac.kr, [3]jwkhong@postech.ac.kr

요 약

본 연구에서는 네트워크 도달성 검사에 기초하고 있는 간단하면서도 유효한 IP hijacking 탐지 방법을 제안한다. 만약 IP hijacking 이 발생하면 목적으로 하는 네트워크에 도달하지 못하고 hijacking 을 시도한 공격자 네트워크에 도달하는데, 목적으로 하는 네트워크에 도달했는지 여부는 그 네트워크의 특징을 확인함으로써 가능하다. 본 논문에서는 IP hijacking 의 도달성을 검증하기 위한 네트워크의 특징 수집 방법과 수집된 특징을 활용하여 IP hijacking 을 검출하는 방법을 제시한다. 이와 같이 네트워크 도달성을 기반으로 한 IP hijacking 검출 방법은 액티브 프로빙(active probing)을 이용하므로 간단하고, 수집된 특징들은 각 네트워크의 현재 상태를 반영하므로 매우 유용한 방법이다.

1. 서 론

BGP 는 IP 네트워크 혹은 prefix 의 내용을 관리하는 도메인 간의 사실상 표준 라우팅 프로토콜이며, 인터넷을 구성하는 수많은 AS (Autonomous System) 간의 네트워크 도달성을 지정한다. 그런데 BGP 는 근원지 정보나 경로 정보에 신뢰성을 검사하는 것 같은 다른 라우터로부터의 잘못된 라우팅 정보를 막을 수 있는 보안을 구현하지 않고 있다. 따라서 인터넷 라우팅 구조는 보안 공격에 취약한 면을 가진다.

IP hijacking 은 BGP 라우터가 악의적인 혹은 잘못된 설정에 의하여 그 라우터가 소유하고 있지 않은 IP prefix 를 알림(announcement)으로써 발생하는 BGP 보안 공격이다. 이러한 잘못된 알림은 인터넷을 통하여 도달성 문제나 통신 장애 등을 초래한다.

잘못된 라우팅 정보로 인한 영향을 완화하기 위해, S-BGP(Secure BGP)[1]나 soBGP(Secure Origin BGP)[2] 같은 BGP 프로토콜 향상 방안이 제안되었다. 이러한 방법들은 사용되는 디지털 서명 기법이 복잡하고 많은 계산이 필요하기에 실제 네트워크에 적용하기 어려운 문제를 가지고 있다.

기존의 다른 많은 연구들은 IP hijacking 을 탐지할 수 있는 방법을 제안하였다[3, 4, 5, 6, 7, 8, 10, 11, 12]. 이 방법들은 패시브 모니터링이나 액티브 프로빙(active probing) 사용하기에 현재의 인터넷에 적용 가능하지만, 사용하는 정보나 탐지 주체, 탐지 가능한 공격 종류 면에서 한계를 가지고 있다. 사용되는 라우팅 정보가 실시간으로 제공되지 않거나 많은 프로빙 데이터를 필요하기도 하다. 또한 다양한 방식의 IP hijacking 을 모두 탐지하지 못하거나 각 공격 종류별로 다른 탐지 방법을 제안하고 있어 복잡하고 실용적이지 않다.

본 연구에서는 현실적으로 유효하고 간단한 IP hijacking 검출 방법으로 네트워크 도달성에 근거한 새로운 방법을 제시한다. 네트워크 도달성(Network Reachability)이란 어떤 네트워크에 도달할 수 있는가에 대한 판단이다. 즉, 단순히 어떤 IP 대역을 갖는 네트워크에 도달하였나가 아니라 그 IP 대역을 실제로 소유하고 있어야 하는 네트워크에 도달하였나에 관한 판단이다. 라우팅 경로가 변경되어도 이러한 네트워크 도달성은 유지되어야 하는 특성이 있다. 따라서 제안하는 IP hijacking 검출 방법은 라우팅 경로 갱신(route update)이 요청되면 변경된 경로로 기존의 네트워크에 도달할 수 있는지를 검사하여 IP hijacking 발생 여부를 알아내는 것이다.

본 논문의 구성은 다음과 같다. 2 장에서는 IP hijacking 에 대한 설명과 관련 연구들을 소개한다. 3 장에서는 네트워크 도달성과 IP hijacking 및 탐지 방법과의 관계를 서술한다. 4 장에서는 호스트 fingerprinting 과 네트워크 fingerprinting 방법을 소개하고 이를 이용하여 IP hijacking 을 탐지하는 방법을 제시한다. 마지막으로 5 장에서 결론과 향후 연구에 대하여 기술한다.

2. 관련 연구

IP hijacking 은 BGP 의 보안 취약점을 이용한 공격이며, 다른 네트워크에 속한 IP 주소 대역을 부정적인 공격 행위를 통해 훔치는 것을 뜻한다. IP hijacking 은 BGP hijacking 으로도 알려져 있는데, 이는 IP hijacking 을 하기 위해서는 BGP 를 통한 라우팅 갱신 알림이 필요하기 때문이다. IP hijacking 은

본 연구는 한국연구재단을 통해 교육과학기술부의 세계수준의 연구중심대학육성사업(WCU)(R31-2010-000-1010 0-0), 지식경제부 및 정보통신산업진흥원의 대학 IT 연구센터 지원사업(NIPA-2011-C1090-1131-0009)과 2010 년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(2010-0028239)

어떤 AS 가 특정 prefix 에 대한 소유권을 가지고 있지 않으면서 마치 자기한테 할당된 prefix 인 것처럼 announce 하는 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.

BGP 보안과 관련한 초기 연구에서는 라우팅 정보의 무결성을 제공하는 암호화에 초점을 두었다. BGP 보안 아키텍처인 S-BGP [1]와 soBGP [2]는 여러 보안 메커니즘을 설계하였지만, 현재 인터넷 인프라에 적용하는 것은 쉽지가 않다. 라우팅 레지스트리(routing registry)[13]는 prefix 소유자, AS 수준의 연결 및 라우팅 정책에 대한 정확한 정보를 가지고 보안에 민감한 AS 들이 잘못된 경로를 탐지하고 삭제할 수 있게 해준다. 그러나 이러한 레지스트리를 사용하기 위해서는 레지스트리 자체가 보안에 철저하고 가진 정보가 완전하면서 정확하다는 것이 보장되어야만 한다. BGP 라우터들은 흔히 자신들의 경로 정책에 기반하여 들어오거나 나가는 경로를 필터링한다. 그러나 많은 AS 들이 정확하게 필터링을 수행하지 않기도 하며, 멀리 떨어진 AS 로부터의 잘못된 경로 정보를 판별하는 것은 대단히 어렵기에 경로 필터링에도 한계가 있다.

앞서 언급했듯이 암호화 기법과 라우팅 레지스트리 및 경로 필터링만으로는 모든 IP hijacking 공격에 대응하는데 문제점 및 한계를 가지고 있다. 그렇기 때문에 많은 기존 연구들이 IP hijacking 행위를 탐지하는 방법들을 제안해 왔다. IP hijacking 탐지 방법은 사용되는 데이터, 탐지 주체, 공격 유형 측면에서의 각자 특징을 가지고 있다. IP hijacking 을 탐지하기 위해 사용되는 데이터에는 제어 평면(control plane)과 데이터 평면(data plane) 정보가 있다. 제어 평면은 라우팅 테이블이나 라우팅 프로토콜에 의해 수집될 수 있는 정보를 뜻하고, 데이터 평면 정보를 사용하는 방법들은 실시간 액티브 프로빙에 의존하며, 비정상적인 경우가 발생하였는지를 알아내기 위해 프로빙 결과를 분석한다. 탐지 주체는 오직 자신의 네트워크만을 모니터링 하는 피해자 중심(victim-centric), 중앙집중식 데이터베이스나 여러 모니터링 위치를 사용하는 인프라 기반(infrastructure-based), 자신의 네트워크를 통과하는 라우팅 메시지를 분석하여 인터넷 상에 발생한 비정상 행위를 탐지하는 제 3 자 방식(third-party)으로 나눌 수 있다. 마지막으로 IP hijacking 공격 유형에는 prefix hijacking 과 AS 경로 위조(AS path falsification)가 있다. 본 연구에서는 일반적인 prefix hijacking 과 sub-prefix hijacking 을 따로 취급하지 않으며, AS 경로 위조는 라우팅 갱신 메시지의 경로 속성을 위조함으로써 IP hijacking 을 시도하는 것을 의미한다.

표 1 은 다양한 IP hijacking 탐지 연구에 대하여 사용되는 데이터, 탐지 주체, 공격 유형 측면에서의 비교를 보여준다. 많은 연구들이 IP hijacking 탐지에 대해서 서로 다른 특징들을 활용하고 있다.

기존 연구들은 비정상적 행위를 탐지하기 위해 제어 평면 혹은 데이터 평면 정보를 사용하였다. 제어 평면 정보를 사용하는 기법은 라우팅 테이블을 분석하고 BGP 라우팅 메시지를 패시브 모니터링 한다. 이러한 라우팅 정보는 근원지 AS 변화나 잘못된 AS 링크 같은 비정상적 증상을 내포할 수 있다. 데이터 프로빙은 모니터링 순간에 목표로 하는 IP prefix 까지의 도달성을 확인하는 방법을 제공한다. 이 때는 호스트 특성을 수집하거나 IP prefix 까지의 홉 수를 측정할 수 있는 등 적절한 모니터링 지점을 선정하는 것이 중요하다.

IP hijacking 탐지 방법은 탐지 주체에 따라 피해자 중심, 인프라 기반, 제 3 자 방식으로 분류될 수 있다. 피해자 중심 탐지 시스템은 자신의 IP prefix 혹은 협력 네트워크의 잠재적인 hijacking 을 모니터링 하며, prefix 소유자가 IP hijacking 발생 여부를 내부적으로 판단한다. 인프라 기반 접근 방법에는 두 종류가 있다. 하나는 전체적인 라우팅 시스템에 관한 정보를 인터넷 상의 서로 다른 몇몇 백본이나 특정 지점에서 실시간으로 수집하는 중앙집중식 데이터베이스를 사용하는 것이다. 다른 하나는 다양한 액티브 프로빙 결과를 얻기 위해 모니터링 지점을 인터넷 상에 고르게 지정하고 IP hijacking 을 탐지하기 위해 과거의 데이터 혹은 모니터링 지점 간에 수집된 정보끼리 비교하는 것이다. 제 3 자 방식의 탐지 시스템은 자신의 네트워크를 통과하는 라우팅 메시지를 분석하고 탐지 알고리즘을 적용하여 의심스러운 상황이 인터넷 상에 방생했는지를 알아내는 방식이다.

표 1. 비정상 탐지 시스템 간의 비교

관련 연구	사용되는 데이터		탐지 주체			공격 유형	
	제어 평면	데이터 평면	피해자 중심	인프라 기반	제 3 자 방식	Prefix Hijacking	AS 경로 위조
Topology [3]	O			O		O	O
PHAS [4]	O			O		O	
Distance [7]		O		O		O	
Fingerprint [10]	O	O		O	O	O	O
pgBGP [11]	O				O	O	
iSPY [8]		O	O			O	
Strobelight [12]		O	O			O	
Reachability (Proposed)	O	O			O	O	O

IP hijacking 의 공격 유형은 prefix hijacking 과 AS 경로 위조로 나눌 수 있다. prefix hijacking 은 공격자가 BGP 메시지의 NLRI 필드를 조작함으로써 hijacking 을 유발하는 것을 말한다. 일반적인 IP hijacking 과 sub-prefix hijacking 은 공격에 영향 받는 오염(polluted)된 또는 비오염(unpolluted)된 AS 관점에서 보면 분명히 서로 다른 영향을 끼치지만, 본 연구에서는 이 두 가지를 구분하지 않는다. AS 경로 위조 공격은 공격자가 IP hijacking 을 유발하기 위해 BGP 메시지의 경로 속성을 조작할 때 발생한다.

본 연구에서 제안하는 방법은 제어 평면과 데이터 평면 정보를 모두 사용하고, 모든 종류의 IP hijacking 을 다루며 제 3 자 방식에 초점을 두고 있다. 제어 평면과 데이터 평면 정보를 모두 사용하는 것은 탐지 정확성을 높이는 효과를 가져온다. 또한 제 3 자 방식에 기반하기 때문에 상호 협력 인프라를 구축하지 않고도 IP hijacking 을 탐지할 수 있다. 그러므로 본 연구에서 제안하는 방법은 인터넷 상에 쉽게 적용이 가능하며 모든 종류의 IP hijacking 공격을 보다 정확하게 탐지할 수 있다.

3. 네트워크 도달성 모니터링

인터넷은 BGP 를 이용하여 라우팅 정보를 교환하는 AS 들로 이루어진 거대한 분산 시스템이다. 라우팅의 기본 목적은 직접 연결되지 않은 호스트들 사이에 통신이 가능하도록 연결 경로를 설정하는 것이다. 그러나 네트워크는 라우팅 경로의 변화, 토폴로지의 변화 및 장비 설정 변경 등 수시로 영향을 받는다. 여기서 네트워크 도달성이란 라우팅에 의하여 설정된 경로로 실제 데이터를 전달할 수 있는가에 대한 판단 결과이다. BGP 라우팅은 분산 라우팅 방법으로 일부의 오류나 고장에 의하여 도달성이 보장되지 않을 수도 있다. 따라서 라우팅 정보만으로는 목적지까지의 도달성을 확신할 수 없기 때문에 실제 검증을 통하여 확인할 필요성이 있다.

IP hijacking 은 이러한 네트워크 도달성에 영향을 주는 공격이다. IP hijacking 이 발생하면 실제 데이터가 의도한 목적지 네트워크가 아닌 공격자 네트워크로 보내진다. 즉, 목적지 네트워크까지의 도달성이 보장되지 않는 상황이 발생하게 된다. 만약 목적지 네트워크에 대한 사전 정보를 바탕으로 액티브 프로빙을 수행하여 응답을 분석하게 되면 네트워크 도달성이 보장되는지 여부를 확인할 수가 있다.

네트워크 도달성 모니터링을 수행하는데 있어 특정 네트워크에 대한 특징을 어떻게 수집할지 정하는 것은 매우 어려운 문제이다. 일반적으로 네트워크 도달성 검증은 액티브 모니터링에 의존하는데, 패시브 모니터링으로 수집되는 정보에는 한계가 있으며 실시간 검사가 어렵기 때문이다. 액티브 모니터링 방법 중에서 기존의 도달성 검증은 ICMP 를 이용한 직접적인 방법을 사용했으며, ping 과 tracroute 같은 도구들이 존재한다. 이 방법들은 인터넷 보안 강화로 인하여 방화벽을 통과하기 힘들거나 혹은 응답 패킷을 보내지 않도록 설정되어 있는 경우 사용하기 힘들다.

본 연구에서는 네트워크의 특징 수집을 2 가지 방법을 통해 수행한다. 하나는 네트워크 내의 대표적인 서버들, 예를 들어 웹 서버나 DNS 서버 같은 호스트를 선정하여 호스트 fingerprinting 을 수행하는 것이다. 이러한 대표 서버들로의 접근은 방화벽을 손쉽게 통과할 수 있으며 동작 중인 서비스들은 받은 패킷에 대해 적절하게 응답해야만 하기 때문에 손쉽게 정보를 수집할 수 있다. 다른 하나는 네트워크의 방화벽 정책을 기반으로 하여 네트워크 내부의 특징을 수집하는 네트워크 fingerprinting 이다. 목표 네트워크로의 액티브 프로빙을 수행하여 방화벽 정책을 추론해 내고, 이를 바탕으로 네트워크의 특징을 효율적으로 수집할 수 있는 방안을 구상하여 네트워크 fingerprint 를 수집한다.

4. AS 별 특징 수집을 통한 IP Hijacking 탐지 방법

이 장에서는 각 네트워크의 특징을 내포하고 있는 호스트 fingerprint 와 네트워크 fingerprint 를 이용하여 IP hijacking 을 탐지하는 방법을 제안한다. 제안하는 방법은 라우팅 정보 갱신 요청을 받는 라우터가 직접 IP hijacking 을 검출하기 때문에 인프라에 의존적이지 않고, 도달성 확인이라는 단정적인 방법을 이용하기에 정확한 탐지가 가능하다.

4.1 호스트 fingerprinting

네트워크를 특징 지을 수 있는 것 중 하나는 해당 네트워크가 운영 중인 대표적인 서버들이다. 대부분의 기관들은 자신들의 네트워크를 대표하는 웹 페이지를 운영하거나 IP 주소를 매칭시켜 주기 위한 DNS 서버를 운영한다. 여기서 DNS 서버는 임의의 특정 IP 를 이름으로 구성된 주소와 일치시켜 주는 역할을 하는데, 현재 인터넷 구성에서 필수적인 요소이다. 따라서 서로 다른 DNS 서버 간의 fingerprint 를 정확히 구분해 낼 수 있다면 이를 이용하여 IP hijacking 을 탐지할 수 있다. IP hijacking 이 발생하면 특정 네트워크로의 도달성에 문제가 생긴 것인데, 해당 네트워크 내의 DNS 서버 fingerprint 에 변화가 생겼다면 이는 기존의 DNS 서버가 아닌 다른 호스트에 도달했다는 의미이기 때문이다.

본 논문에서는 각 AS 마다 DNS 서버를 찾아내기 위하여 다음과 같은 과정을 거친다. 먼저 각 AS 별로 IP Prefix 를 얻기 위해서 라우팅 테이블 데이터를 활용한다. 라우팅 테이블에는 특정 IP prefix 로 패킷을 전달하기 위한 AS 경로 정보가 포함되어 있어서, 최종 목적지 AS 가 소유한 IP prefix 를 알 수 있다. AS 가 소유한 IP prefix 를 알아보고, 각 AS 내에서 동작하고 있는 DNS 서버를 찾기 위해 AS 가 소유하고 있는 IP prefix 를 /24 prefix 로 나눈다. 여기

서 IP prefix 를 /24 로 나누는 이유는 CIDR (Classless Inter-Domain Routing)을 지원하지 않는 DNS 역방향 질의(reverse lookup)를 사용하기 때문이다.

다음으로 각 AS 내에서 동작하고 있는 DNS 서버를 찾기 위해 가공한 IP prefix 에 DNS 역방향 질의를 수행한다. DNS 역방향 질의 수행 통해 해당 IP Prefix 에 대한 DNS 서버의 도메인 이름을 알 수 있다. 마지막으로 DNS 서버의 도메인 이름으로 DNS 질의를 수행하면 DNS 서버의 IP 주소를 얻을 수 있으며, 추가적으로 해당 DNS 서버와 함께 운영되는 보조 DNS 서버들 정보까지 파악할 수 있다.

찾아진 DNS 서버의 호스트 fingerprint 중 하나로 구동 중인 DNS 서버가 어떤 프로그램을 사용하는지가 있다. 'fpdns'라는 도구는 DNS 서버의 구현 방식을 추론할 수 있는데, 'nmap' 등을 통한 OS fingerprinting 와 달리 몇 개의 DNS 질의만을 사용하기에 매우 빠른 시간 내에 결과를 얻어낼 수 있는 장점이 있다.

4.2 네트워크 fingerprinting

네트워크 fingerprint 는 해당 네트워크를 식별할 수 있는 고유한 특징을 말한다. 네트워크 fingerprint 를 생성하기 위해서는 액티브 모니터링을 통해 해당 네트워크의 특징을 수집하고 분석하는 과정이 필요하다. 예를 들어 해당 네트워크에 분포한 호스트들의 가용성(availability)을 탐지하고 이를 수치화함으로써 네트워크 fingerprint 로 활용할 수 있다. 하지만 실제 네트워크 환경에서는 보안 상의 이유로 방화벽에서 차단될 수가 있기 때문에 네트워크의 상태를 정확하게 파악하는 것은 어려움이 있다.

이러한 문제를 해결하기 위해 방화벽 정책을 추론하여 이를 기반으로 한 네트워크 fingerprinting 기법을 제안하고자 한다. 해당 네트워크의 방화벽에서 통과하는 패킷의 IP 대역, 프로토콜 종류 및 포트 번호를 추론하여 방화벽 정책을 생성하고, 생성된 방화벽 정책에 맞추어 해당 네트워크의 정보를 수집한다. 방화벽 정책에 기반을 두기 때문에 프로빙 패킷이 손쉽게 방화벽을 통과할 수 있으므로 응답이 오지 않음으로써 발생하는 시간 초과 상황을 줄일 수 있어서 효율적이다. 또한 네트워크에서 차단되지 않는 패킷을 사용하기 때문에 호스트들의 가용성으로 만들어진 네트워크 fingerprint 의 정확도가 높아진다.

방화벽 정책을 추론하기 위해 FireCracker [14]의 방법을 이용한다. FireCracker 는 아무런 사전 지식 없이 방화벽 정책을 발견하는데 사용할 수 있는 프레임워크를 제안하였다. 이 프레임워크는 공격자가 네트워크에 맞는 패킷으로 방화벽을 탐지하여 정책이 어떻게 생겼는지를 형성하고, 이를 통해 방화벽의 정책을 재구성할 수 있는 방법들을 보여준다. 본 연구에서는 네트워크 fingerprint 를 생성하기 위한 최소한의 방화벽 정책을 알아내는데 초점을 둔다.

제안하는 방법에서 사용하는 네트워크 fingerprint 는 해당 네트워크 호스트들의 가용성이다. 추론해낸 방화벽 정책에 기반하여 허용되는 패킷 위주로 프로빙 전략을 구상하고 응답 결과를 수집하여 호스트 IP 들의 가용성 시퀀스를 만들어 얻어진 벡터 값을 [0, 1]로 정규화하여 하나의 네트워크 fingerprint 로 나타낼 수 있다.

4.3 IP hijacking 탐지 알고리즘

본 연구에서는 수집된 호스트 fingerprint 와 네트워크 fingerprint 를 이용한 네트워크 도달성 모니터링을 통해 IP hijacking 을 탐지한다. 탐지 알고리즘을 적용하기 이전에 미리 수집해야 하는 데이터들이 있다. 우선적으로 MOAS (Multiple Origin AS)[9] 발생 여부나 AS 경로 정보에 문제가 있는지를 파악하기 위해 탐지 시스템과 연동된 라우터의 라우팅 테이블 정보가 필요하다. 그리고 앞서 언급했듯이 호스트 fingerprinting 에 사용하게 될 DNS 서버 정보들과 각 서버들의 특징 정보 및 네트워크 fingerprinting 에 활용될 정보들을 사전에 모아둔다. 여기서 사용되는 호스트 fingerprint 와 네트워크 fingerprint 는 각 AS 별로 수집되어야 하며 이를 이용해 의심스러운 BGP 갱신 메시지가 왔을 경우 제안하는 알고리즘을 적용하면 IP hijacking 을 탐지할 수 있다.

그림 1 은 제안하는 IP hijacking 탐지 과정을 보여준다. 의심스러운 BGP 갱신 메시지에는 두 가지가 있는데, 하나는 MOAS (subMOAS 를 포함하는)가 발생한 경우이고, 다른 하나는 AS 경로 상에 기존의 라우팅 테이블에서 보지 못한 AS 간 연결이 확인된 경우이다.

MOAS 가 발생하면 목적지 AS 와 NLRI 필드를 확인하여 사전에 수집해 둔 호스트 fingerprint 를 활용할 수 있는지 확인한다. NLRI 에 속하는 DNS 서버가 존재한다면 이를 이용하여 호스트 fingerprint

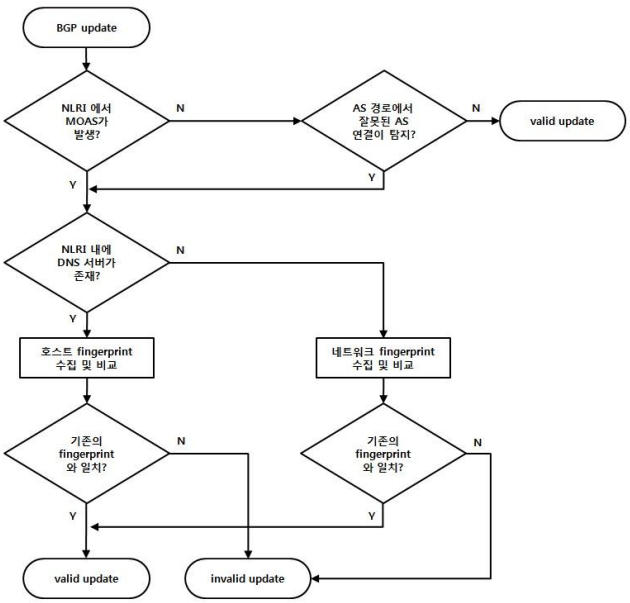

그림 1. IP hijacking 탐지 알고리즘

를 비교하고, 모순되는 점이 있는지를 확인하면 목적지 네트워크에 제대로 도달 가능한지 혹은 IP hijacking 에 의한 것인지 탐지할 수 있다. 만약 DNS 서버를 활용할 수 없는 IP 대역이라면 네트워크 fingerprinting 을 적용한다. 해당 AS 에 대한 방화벽 정책은 이미 알고 있기 때문에 이를 바탕으로 네트워크 가용성 정보를 수집하고 기존의 네트워크 fingerprint 와 비교하여 탐지를 수행한다.

AS 경로 상에 의심스러운 내용이 포함되어 있다고 판단되는 경우, 즉 현재의 라우팅 테이블에서 전혀 확인할 수 없는 AS 간 연결이 보인다면 그 AS 간 연결의 적절성 여부를 검토한다. 여기에는 두 AS 간의 지리적 거리 및 해당 AS 까지 프로빙을 수행했을 때 걸리는 시간 등이 포함된다. 적절성이 의심된다고 판단되면 해당 BGP 갱신 메시지는 MOAS 가 발생한 경우와 마찬가지의 알고리즘을 적용하여 IP hijacking 여부를 확인한다.

사실 BGP 라우터로 들어오는 대부분의 갱신 메시지는 위 두 가지 경우에 포함되지 않으며[10], 극히 일부의 메시지에만 알고리즘을 적용하면 되기에 제안하는 알고리즘은 충분히 효율적이며 다른 인프라의 도움이 필요가 없으므로 손쉽게 현재 인터넷에 적용 가능한 방법이다.

5. 결론 및 향후 연구

본 연구에서는 BGP 라우팅 보안에 관련된 기존의 연구들을 살펴보고, 특히 IP hijacking 탐지 기법을 중심적으로 다루었다. 제안하는 방법은 네트워크 도달성 모니터링에 기반하여 추가적인 인프라 없이 IP hijacking 을 탐지할 수 있다. 각 AS 에 대한 특징을 가지는 호스트 fingerprint 와 네트워크 fingerprint 를 사전에 수집하는 방법을 기술하였고, 이를 이용해 네트워크 도달성 검증을 통한 IP hijacking 탐지 방법은 현재 인터넷에 충분히 적용할 수 있으며 정확하고 효율적인 특징을 가진다.

향후 연구로는 DNS 서버의 호스트 fingerprint 로 사용 가능한 데이터를 더 확보하여 호스트 간의 구별 가능한 특성들을 더 제안하고자 한다. 또한 네트워크 fingerprinting 을 수행할 때 방화벽 정책 추론 및 네트워크 특징 수집에 있어서 시간적 측면의 성능 향상 방법을 연구하는 것이 필요하다. 이를 기반으로 하여 제안하는 IP hijacking 탐지 방법을 실제 인터넷 상에서 검증하고 성능 분석을 할 계획이다.

참고 문헌

[1] C. Lynn, J. Mikkelson, and K. Seo, “Secure BGP (S-BGP),” IETF Draft: draft-clynn-s-bgp-protocol-01.txt, June 2003.

[2] Brian Weis, “Secure Origin BGP (soBGP) Certificates,” IETF Draft: draft-weis-sobgp-certificates-02.txt., July, 2004.

[3] C. Kruegel, D. Mutz, W. Robertson, and F. Valeur, “Topology-based Detection of Anomalous BGP Messages,” In Proceedings of the 6th Symposium on Recent Advances in Intrusion Detection (RAID), LNCS 2820, Pittsburgh, PA, USA, September 2003, pp. 17-35.

[4] M. Lad, D. Massey and D. Pei, “PHAS: A Prefix Hijacking Alert System,” In Proceedings of the 15th USENIX Security Symposium, Vancouver, B.C., Canada, August 2006, pp. 153-166.

[5] M. Tahara, N. Tateishi, T. Oimatsu, S. Majima, “A Method to Detect Prefix Hijacking by Using Ping Tests,” In Proceedings of the 11th Asia-Pacific Symposium on Network Operations and Management (APNOMS 2008), LNCS 5297, Beijing, China, October 2008, pp. 390-398.

[6] Z. M. Mao, J. Rexford, J. Wang, and R. H. Katz, “Towards an Accurate AS-level Traceroute Tool,” In Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, Karlsruhe, Germany, August 2003, pp. 365-378.

[7] 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, Vol37, Issue4, October 2007.

[8] Z. Zhang, Y. Zhang, Y. C. Hu, Z. M. Mao, and R. Bush, “iSPY: Detecting IP Prefix Hijacking on My Own,” In Proceedings of the ACM SIGCOMM 2008 conference on Data Communication, Seattle, USA, 2008, pp. 327-338.

[9] X. Zhao, D. Pei, L. Wang, D. Massey, A. Mankin, S. F. Wu, and L. Zhang, “An Analysis of BGP Multiple Origin AS (MOAS) Conflicts,” In Proceedings of the 1st ACM SIGCOMM workshop on Internet Measurement, San Francisco, USA, November 2001, pp. 31-35.

[10] X. Hu and Z. M. Mao, “Accurate Real-time Identification of IP Prefix Hijacking,” In Proceedings of the IEEE Security and Privacy, Oakland, California, USA, May 2007, pp. 3-17.

[11] J. Karlin, S. Forrest and J. Rexford, “Pretty Good BGP: Improving BGP by Cautiously Adopting Routes,” In Proceedings of the 14th IEEE International Conference on Network Protocols, Santa Barbara, California, USA, November 2006, pp. 290-299.

[12] J. W. Mickens, J. R. Douceur, W. J. Bolosky and B. D. Noble, “StrobeLight: Lightweight Availability Mapping and Anomaly Detection,” In Proceedings of the 2009 conference on USENIX Annual technical conference, CA, USA, 2009.

[13] T. Bates, E. Gerich, L. Joncheray, J. M. Jouanigot, D. Karrenberg, M. Terpstra and J. Yu, “Representation of IP Routing Policies in a Routing Registry,” RFC 1786, Mar. 1995.

[14] T. Samak, A. El-Atawy, and E. Al-Shaer, “FireCracker: A Framework for Inferring Firewall Policy using Smart Probing,” Icnp, pp.294-303, 2007 IEEE International Conference on Network Protocols, 2007.