인터넷에서의 보안관리를 위한 네트워크 맵핑 프레임워크

최대식[0] 강형우 남건우
ETRI 부설 국가보안기술연구소
{dschoi[0], kanghw, daemon99}@etri.re.kr

The Internet Mapping Framework for Security Management

Dae-Sik Choi[0] Hyoung-Woo Knag Geon-Woo Nam
National Security Research institute In ETRI

요 약

인터넷의 발달과 이로 인한 보안의 중요성이 점점 강조되고 있다. 이에 IDIP나 CITRA[3]같은 여러 가지 보안 도구와 시스템의 통합을 통한 전역적인 보안 관리 체계가 대두되고 있는 실정이다. 그러나 이들 대부분이 자신들의 관리영역에 한정하여 이미 결정된 맵을 사용함으로 실제 인터넷에 적용하기에는 많은 어려움이 있다. 인터넷을 통한 전역적이고 실질적인 보안 관리를 하기 위해서는 알려지지 않은(unknown) 망인 인터넷에 대한 정확한 맵핑이 이루어져야 하며, 이를 이용하여 공격자의 공격 경로와 지리학적 위치 판단, DoS 대응을 위한 망의 고립 또는 차단 등의 응용에 이용될 수 있다. 이에 본 논문에서는 맵핑을 위한 여러 가지 휴리스틱한 기법을 소개하고 이를 이용하여 인터넷 맵핑을 위한 프레임워크를 제안한다. 제안된 프레임워크는 기존 방법들의 여러 가지 장점을 취합하여 보다 세밀하고 정확한 맵핑에 효과적이다.

1. 서 론

인터넷의 발전에도 불구하고 서로 다른 관리 도메인과 인터넷이 가지는 불확실성 때문에 인터넷 망의 관리 및 기타 목적을 위한 맵핑 작업에 많은 어려움이 있었다. 그러나 최근 들어와서 네트워크 트래픽 분석 및 인터넷을 기반으로 한 인프라의 연구 차원에서 caida[1]를 위시한 여러 연구 기관에서 인터넷의 맵핑에 대한 연구가 진행되고 있다. 보안 관점에서 보았을 때 이러한 인터넷 맵핑 기술의 습득 및 응용이 많이 요구된다. 기존의 DNS 나 NMS등이 관리 망에 대한 응용이 되고 있듯이, 인터넷 자체에 대한 관리 및 상황 파악 등이 점점 증대되고 있다. 본 연구는 보다 정확한 맵핑 기술을 적용하기 위한 휴리스틱한 방법과 이를 이용한 프레임워크를 제시하고 이의 활용과 발전방향을 논하는 걸 목적으로 한다. 2장에서는 인터넷 맵핑을 위한 관련연구에 대하여 설명하고 3장에서는 적용될 휴리스틱한 방법을 기술한다. 4장에서는 이러한 방법을 이용하여 보다 효율적인 맵핑 프레임워크를 제안하고 5장에서는 제안된 프레임의 활용과 한계에 대하여 언급하고 6장에서 결론을 맺는다.

2. 관련연구

최근 들어와서 네트워크 트래픽 분석 및 인터넷을 기반으로 한 인프라의 연구 차원에서 여러 연구 기관에서 인터넷의 맵핑에 대한 연구가 진행되고 있으며[1][2], 보안 분야에서도 보안 관제 및 시뮬레이션, 망의 생존성 등의 연구에 대한 기본 기술로 인식되며 흥미를 갖는 분야가 되었다[3]. 인터넷 맵핑에 대한 연구방향은 크게 두 가지로 볼 수 있다. 첫 번째는 BGP[4]의 테이블을 사용하여 인터넷의 구조를 파악하는 방법과 근원지에서 목적지까지 패킷을 보냄으로서 IP 주소를 탐색하는 방법을 들 수 있다.

기존의 많은 연구들이 각 라우터의 BGP 테이블을 이용하여 인터넷의 구조[5]를 유추하였다. 이러한 BGP의 사용은 AS간의 경로를 탐색함으로 실제적으로 트래픽이 목적지까지 가기 위해 지나간 실지 경로를 반영하지 못한다. 근원지에서 목적지까지 패킷을 보냄으로서 IP 주소를 탐색하는 방법은 대부분 traceroute의 방법을 이용한다. 그러나 다수의 인터페이스를 가지는 라우터 문제, 백업라인이나 라우팅 정책을 통한 문제 등으로 정확한 인터넷 맵핑을 하기에는 많은 제약조건을 가진다. 이에 본 논문에서는 휴리스틱한 방법을 통하여 보다 정확한 인터넷 맵핑을 할 수 있는 프레임워크를 제시한다.

3. 맵핑 휴리스틱

가. Informed address Probing[2]

라우터간의 adjacency를 추론하기 위해 Hop-limited probe를 할 경우 외부 DB를 이용한 타겟 선정을 배제하기 위하여, 전체 IP 주소 필드에서 타겟을 랜덤 하게 선택하는 Informed random Hop-limited probes를 사용한다. 아래의 2가지 방법을 이용하여 계속해서 전체 IP 주소 필드로 확대해 나가는 방식을 사용한다

- 임의의 IP 주소 A 에서 Hop-limited probes에 대한 응답이 오는 경우 보안관제를 위한 인터넷 맵핑 프레임워크는 A의 prefix P 가 주소지정이 가능한 노드를 포함한다고 가정한다.
- P가 주조지정이 가능한 prefix라면 보안관제를 위한 인터넷 맵핑 프레임워크는 이웃에 있는(neighboring) P'도 주소 지정이 가능하다. (예 : 128.8/16과 128.10/16은 128.9/16의 이웃에 있는 prefix이다.)

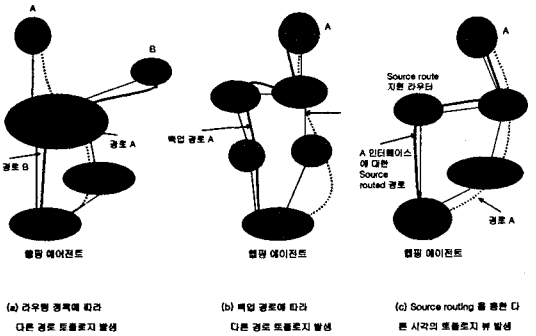
나. Path Probing

인터넷 맵을 탐색하기 위해서 인터넷 맵핑 프레임워크는 Pre-CIDR[6] address allocation 정책을 기반으로 반복하여 Prefix를 선택하고 해당 Prefix내에서 선정된

주소 A까지 경로를 탐색한다. 일반적으로 대부분의 ISP들이 traceroute를 막아 놓았다고 생각하지만, ISP들은 자신들의 인프라의 디버깅과 기타 여러 목적으로 열어 놓아 실제적으로 사용이 가능하다[2].

다. Path Probe 이용시 발생되는 문제의 보완

Path probing을 통한 맵의 탐색은 아래 <그림 1>과 같은 문제를 야기한다.



<그림 1> Path Probing 작업시 발생되는 문제

1) Source-Routed Path Probing

인터넷 맵핑 프레임워크는 IP 옵션중 source-routed 기능을 이용하여 이러한 문제를 해결하려고 하였다. 사실 대부분의 사람들이 알고 있듯이 보안이나 기타 여러 가지 이유 때문에 대부분의 라우터들은 IP 옵션의 여러 기능을 사용하지 못하게 막아놓고 있다. 그러나 이를 간과하는 일부 ISP나 전체 인프라의 상태를 점검하기 위해 이러한 기능이 꼭 필요한 백본 provider의 경우 IP 옵션을 지원하고 있다. 실험에 의하면 전체 인터넷 라우터의 8%가 이들을 사용하고 있으며, 전체 라우터에서 5%정도의 라우터가 source-routed 기능을 지원을 하는 경우, 90%가 넘는 링크를 찾을 수 있다[2].

2) Alias resolving

일반적으로 하나의 라우터에는 2개 이상의 인터페이스가 존재하므로 path probing작업은 같은 라우터의 다른 인터페이스를 여러 가지 라우터로 잘못 인지하여 표시하는 문제를 발생시킨다. 이러한 문제를 해결하기 위해 2가지 방법을 사용하였다. 하나는 IP 구현[7]에 제안된 (요구되지는 않은) 특성을 적용하였다. 제안된 방법은 많이 사용되는 라우터 회사의 제품에서 검증되었다[2][8].

- Alias probe 를 인터페이스 X에게 보낸다.
- 결과로 오는 ICMP 메시지에 소스 어드레스가 Y라면 X와 Y는 같은 라우터의 인터페이스이다.

두 번째 방법은 troubleshooting에 의한 방법이다. 양방향에서 Path probing을 하게 되면 Path probe의 경로가 역방향으로 똑같이 일치하지 않지만 Path Probing이 시작된 양 종단부터 몇 홉까지(비대칭 경로로 전환되기까지)는 C클래스의 개념으로 유추하거나 /20 서브넷 마스크 등을 고려하면 서로 다른 인터페이스를 찾을 수 있다.

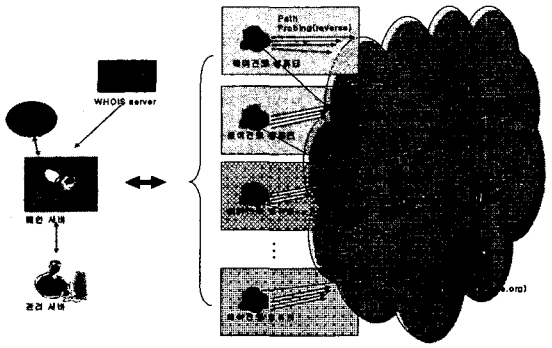
라. 지리학적 위치 맵핑

인터넷 맵핑 프레임워크는 NetGeo[8]에서 제공되는 기능과 위치정보 시스템을 조합해 지리학적 위치 매핑을 한다. IP 주소와 도메인 네임 그리고 AS 넘버를 지리학적 위치에 맵핑시키는 Perl 스크립트의 집합과 DB를 이용하여 지정학적 위치를 정해 주어 맵의 보다 정확한 위치를 제공해주는 역할을 한다.

4. 인터넷 맵핑 프레임워크

가. 보안관계를 위한 인터넷 맵핑 프레임워크

크게 인터넷 프레임워크는 각각의 path probing과 정련 과정을 수행하는 에이전트 컴퓨터와 이들을 취합하여 whois서버와의 정보교환 및 자체 DB와 연관시켜 지리학적 위치를 결정하는 메인 서버 그리고 이를 관리 모니터링 하는 관리 서버로 나뉘어진다. 아래 <그림 2>는 인터넷 맵핑 프레임워크의 전체 구조도이다.



<그림 2> 인터넷 맵핑 프레임워크 전체 구조도

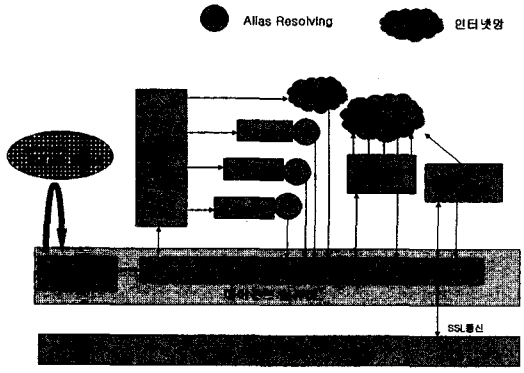
나. 에이전트 컴퓨터 프레임워크

에이전트 컴퓨터는 주로 Path Probing과, 각각의 휴리스틱 방법을 이용한 맵의 정련 과정 등을 수행하는 에이전트이다. <그림 2>에서 보듯 임이의 지역에 설치되어 Path probing을 수행한다. 여기서 임이의 지역이란 AS와 같은 일종의 관리 도메인이나 인터넷의 허브(Hub) 역할을 하는 지역을 의미한다. 에이전트 컴퓨터를 다수 이용해서 탐색을 하는 이유는 아래와 같다.

- 전체 인터넷 도메인의 주소영역을 최대한 수용
- 트리 구조 형식의 맵의 지양
- 역방향 경로 및 중복 경로를 통한 맵의 정밀도 향상

아래 <그림 3>는 인터넷 맵핑 프레임워크를 위한 에이전트 컴퓨터의 프레임워크다. 동작 구조를 살펴보면 크게 에이전트 맵의 생성 단계와 정련 단계로 나눌수 있다. 에이전트 맵의 생성단계는 informed address probing작업으로 수행되며 정련 단계는 생성된 맵을 source-routed Path probing과 Looking glass 등을 사

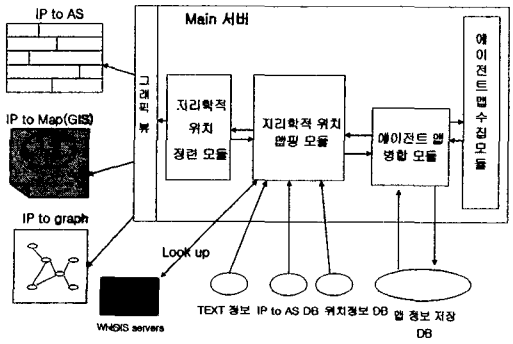
용하여 정련 한다.



<그림 3> 에이전트 컴퓨터 프레임워크

다. 메인 서버 프레임워크

메인 서버는 에이전트의 맵을 취합하여 이들을 ISP단위로 정련 하거나 지리학적 위치로 변환하는 역할을 하며 지리학적 위치를 결정하기 위하여 RTT time과 Whois 서버, GIS 그리고 각종 DB를 이용한다. <그림 4>는 메인 서버 프레임워크이다.



<그림 4> 메인 서버 프레임워크

메인 서버 프레임워크의 동작을 살펴보면 에이전트의 정보를 취합하고, 맵이 취합되면 에이전트 취합된 맵을 맵 정보저장 DB를 참조하여 노드간의 연결과 맵의 인터페이스, RTT등의 정보를 이용 병합 및 정련 한다. 전체 맵이 정련 되면 지리학적 위치 맵핑 모듈은 IP 주소를 가진 해당 노드를 위도, 경도를 가진 지리학적 위치로 정련 시킨다. 지리학적 맵핑 단계가 끝나면 지리학적 위치 정렬 모듈은 해당 경로에 속한 노드에 할당된 주소가 적당한 건지 검사해 주는 일을 한다. 지리학적 위치 정렬 모듈의 검사는 RTT의 차이를 이용하여 검증한다.

5. 활용 및 한계

다수 에이전트의 설치는 인터넷의 효율이나 트래픽등을 연구하기 위해 전 세계적으로 설치된 서버를 이용하거나 각 지역 ISP들의 양해를 구해야 한다. 다분히 제도적/관리적 문제이므로 더 이상 고려하지 않는다. Path Probing을 위하여 논문에서 제시한 프레임워크는 주로 ICMP나 UDP를 이용한 traceroute를 이용하였다. 대부분의 사람들이 이들이 막혀있어 활용도를 의심하지만 백본망간의 자기진단의 이유나 실지 실험[2]에 의해 많은 수의 노드에 사용이 가능한 것을 알 수 있다. 더불어 본 논문의 프레임워크에서는 UDP와 ICMP등을 조합하여 실패율을 줄였다.

제안된 프레임워크는 alias resolving, source-routed, troubleshooting등의 휴리스틱한 방법으로 다수의 인터페이스 또는 백업링크나 인터넷의 로드 발란싱된 경로를 찾아 보다 근사한 맵을 찾으려고 노력하였으나 그래프 이론적 분석을 통한 정확한 알고리즘 및 적용의 필요성이 있으며 인터넷 전체에 대한 샘플링 방법에 대한 연구도 필요하다. 그럼에도 불구하고 제안된 프레임워크는 변화하는 인터넷망에 대한 계속된 자료의 축적과 변경을 통하여 보안관제를 하려는 관제 시스템에서 보다 정확한 상황 파악을 할 수 있도록 응용될 수 있다.

6. 결론

인터넷의 사용이 계속 가속화되고 모든 서비스들이 인터넷을 중심으로 통합되면서 인터넷에 대한 관리와 모니터링의 이슈가 점차 늘어나고 있다. 보안 관점에서도 보안관제 및 기타 여러 응용의 관점에서 보았을 때 인터넷 맵핑은 중요한 기반기술이 되어질 것이다. 본 논문에서는 여러 가지 휴리스틱 방법과 다수의 에이전트 컴퓨터를 이용하여 인터넷 매핑 프레임워크를 제안하였다. 제안된 프레임워크는 기존의 노력에 여러 가지 휴리스틱 방법의 적용과 개선된 구조를 통하여 보다 근사한 맵핑을 할 수 있다. 향후 연구로는 ISP의 도움을 받아 맵핑의 유효한 부분에 대한 정확도를 검사하고 보다 정확한 휴리스틱 방법 및 알고리즘을 고안할 것이다. 또한 실지 보안 관제 시스템과 연동하여 볼 것이다.

참고문헌

[1] http://www.caida.org
[2] www.isi.edu/scan/mercator/maps/html "Heuristics for Internet Map Discovery"
[3] www.darpa.mil
[4] Y .Rekhter and T. Li. BGP-4 Request for comments 1771, Internet Directory services, March, 1995
[5] Hal Burch and Bill Cheswick. Mapping the internet. IEEE Computer, 32(4):97-98, April 199
[6] V. Fuller, T. Li,j. Yu, and K. Varadhan. Classless Inter-Domain Routing: An address Assignment and Aggregation strategy. RFC1519
[7] R. Barden. RFC 112, internic Directory Services, October 1989
[8] Bradley Huffaker, Daniel Plummer, David Moore, and K clffy, " Topology discovery by active probing" IEEE Sym. 2001.