IPFIX 표준을 이용한 IPv6 이상트래픽 모니터링[1)]

김종기, 신성호, 최순병, 이영석, 김기영*
충남대학교 전기정보통신공학부 컴퓨터전공
*전자통신연구원

IPFIX-based IPv6 Anomaly Traffic Monitoring

J. Kim, S. Shin, S. Choi, Y. Lee, and K. Kim*
Dept. of Computer Science and Engineering, Chungnam National University
*Electronics and Telecommunications Research Institute

요 약

IPv6 프로토콜은 현재 인터넷 프로토콜로 사용되고 있는 IPv4 프로토콜이 가지고 있는 주소 부족 문제, 미흡한 QoS의 제공, 다양한 보안 문제 등을 해결하도록 설계된 차세대 인터넷 표준이다. IPv4에서 IPv6로의 전환이 이루어지고 있는 과정이지만, 아직까지 IPv6가 많이 사용되고 있지는 않고 있어 IPv6 트래픽 모니터링 도구 및 침입대응 장비도 많이 나와 있지 않다. 그러나, IPv6 네트워크가 점진적으로 등장하고 전환이 됨에 따라 IPv6에서 발생할 수 있는 각종 인터넷 침해사고에 대한 대비가 필요하다. 이미 IPv6 프로토콜의 허점을 이용한 서비스 거부공격, 디폴트 라우터 위장공격 등 IPv4에서 발생했던 이상트래픽, IPv6 확장헤더를 이용한 이상트래픽 및 IPv6-over-IPv4 터널링 등의 이상트래픽 발생이 보고되고 있다. 이에 본 논문은 IPv6 프로토콜에서 발생할 수 있는 이상트래픽에 대해 살펴보고, 이러한 이상트래픽의 탐지를 위해 IETF 표준인 IPFIX 템플릿을 이상 트래픽 탐지가 가능하게 제안한다. 제안된 IPFIX 플로우 메시지를 이용하여 간단하게 IPv6 이상 트래픽을 분류하는 방법도 제시하였다.

1. 서 론

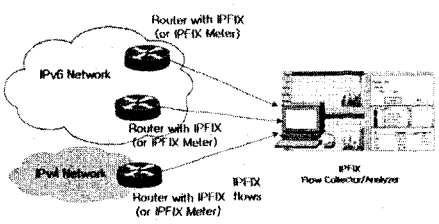
IPv6 프로토콜은 현재 사용되고 있는 IPv4 프로토콜의 주소부족, 미흡한 QoS 등의 단점을 보완하기 위해 설계된 차세대 인터넷 프로토콜이다. IPv6 프로토콜은 IPv4의 주소부족 문제뿐만 아니라, IPSec을 기본 탑재시키면서 IPv4에서 발생했던 여러 보안 문제점을 해결하도록 설계됐다. IPSec은 IPv4와 달리 IPv6에서 반드시 구현되어야하는 표준이기 때문에 IP계층에서의 보안성은 향상되었다. 하지만, IPv4에서 나타났던 수많은 공격 트래픽과 해킹은 IPSec이외의 다른 응용 프로토콜이나 운영체제의 취약점을 이용하고 있기 때문에 IPv6에서도 위해 트래픽이 비슷할 것을 예측되고 있다. 한편, IPv4에서 가능했던 IPv4 주소 공간을 임의로 스캔하여 웜이나 바이러스를 감염시키는 행위는 주소 공간이 넓은 IPv6에서는 매우 어렵다고 예상된다. 하지만, 순수 IPv6 프로토콜 자체의 기능을 이용한 공격 행위도 가능할 것으로 예상되고 이를 응용한 실제 사례들도 보고되고 있다 [1].

IPv6 프로토콜에서는 IPv4와 다른 많은 기능들이 탑재되어 있는데, 이를 이용한 공격이 발생할 수 있다고 알려져있다. 예를 들면, IPv6 프로토콜은 주소 자동설정을 지원하고 있다. 그러나, IPv6 주소 자동설정 기능을 악용하게 되면, 새로운 호스트가 신규 주소를 자동설정하지 못하도록 방해하는 서비스 거부공격이 발생할 수 있다 [2]. 따라서, IETF에서는 SEND(SEcure Neighbor Discovery) [3]를 표준으로 채택하여, 이러한 문제를 해결하고 있다. 하지만, 현재 구현된 많은 IPv6 프로토콜 스택이 IPSec이나 SEND와 같은 기능을 구현하지 않고 있기 때문에 IPv6 이상 트래픽이 발생할 수 있다. 한편, IPv4/IPv6의 전환 과정에서 전환 기술인 터널링이나 듀얼스택을 이용하면, IPv6 패킷을 IPv4 패킷에 캡슐화하여 보낼 수 있다. 방화벽, IDS 또는 IPS 등이 이러한 IPv6-over-IPv4 프로토콜을 인식하지 못하게 되면, 기존의 네트워크 보안 장치들이 제기능을 수행하지 못하게 된다. 또한 IPv6 프로토콜의 확장헤더를 이용하는 공격트래픽도 발생할 수 있다고 알려져 있다.

따라서, 다양한 형태의 IPv6 위해 트래픽이 가능할 것으로 예상되지만, 본 논문에서는 현재까지 알려진 다음과 같은 대표적인 IPv6에서의 이상 트래픽을 우선적으로 고려하였다.

- IPv6 중복주소탐지(DAD)를 남용한 공격 [2]
- IPv6 프로토콜의 확장 헤더를 이용한 은닉(Covert) 채널 [4,5,6]
- IPv4 네트워크에서의 IPv6 터널링을 이용한 위해 트래픽 [7]

현재 IPv6 네트워크에서의 트래픽 모니터링에 관한 연구는 초기단계에 있다. 즉, 네트워크 관리를 위해 많이 사용되는 SNMP, RMON, Cisco NetFlow [8] 등은 부분적으로 IPv6 트래픽의 모니터링 기능을 제공하고 있으며, 이를 이용한 몇몇 IPv6 트래픽 분석 도구들이 최근에 등장하기 시작했다. 또한, 방화벽/IDS/IPS 등의 네트워크 보안제품들 역시 아직까지는 IPv6를 완벽히 제공하고 있지 않다. SNMP와 같이 단순히 패킷 또는 바이트 카운터를 이용하여 트래픽 모니터링 하는 것은 일반적인 트래픽 통계정보를 생성해준다. 하지만, Cisco NetFlow와 같이 플로우별 트래픽 분석 기능은 이상 트래픽 탐지에 효과적이라고 알려져 있다. 특히, IETF IPFIX(IP Flow Information eXport) [9] WG에서는 Cisco NetFlow v9을 기반으로 유연한 구조의 트래픽 모니터링 표준인 IPFIX를 제정하고 있다. IPFIX 표준은 다양한 필드들을 이용하여 유연하게 플로우 정보를 정의할 수 있는 "템플릿" 구조를 사용하기 때문에 IPv6 트래픽을 분석할 수 있다. [그림 1]에서와 같이 IPFIX 기능은 라우터 또는 패킷들을 수집할 수 있는 IPFIX 미터[10]에서 IPFIX 플로우를 생성하여 수집 및 분석 서버[11]에 전송한다.



[그림 1] IPFIX를 이용한 트래픽 모니터링

1) 본 연구는 정보통신부 및 정보통신연구진흥원의 대학IT연구센터 지원사업(IITA-2005-(C1090-0502-0020))과 전자통신연구원의 지원으로 수행되었음.

현재까지 제시된 IPFIX 표준에서는 기본적인 IPv6 트래픽 분석에 대한 가능성만 설명되어 있다. 따라서, 다양한 IPv6 이상 트래픽 분석을 위해서는 새로운 IPFIX 템플릿과 이를 활용한 측정 방법이 필요하다. 따라서, 본 논문에서는 IPv6 네트워크에서 발생할 수 있는 대표적인 이상트래픽에 대해서 기술하고, 이를 탐지하기 위해 새로운 IPFIX 템플릿을 제안하고, IPFIX 기반의 이상 트래픽 모니터링 방법을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 IPv6 라우터/스위치에서 트래픽 모니터링 기능의 표준으로 제공될 IPFIX의 표준을 소개하고, 3장에서는 IPv6 이상트래픽과 이를 탐지하기 위한 IPFIX를 확장하여 정의한 템플릿에 대해 설명하고, 4장에서는 IPFIX 플로우를 이용한 IPv6 이상 트래픽 탐지 방법을 제시하고, 마지막으로 5장에서는 결론 및 향후 과제를 다룬다.

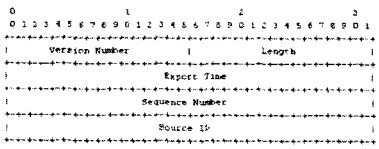
2. IPFIX 표준을 이용한 IPv6 트래픽 모니터링

IETF에서 제정되고 있는 IPFIX는 일정시간동안 네트워크의 관찰지점을 통과하는 IP패킷들을 공통 속성(src addr, src port, dst addr, dst port, protocol)으로 분류한 플로우를 전달하기 위한 프로토콜이다.

2.1 IPFIX 구조

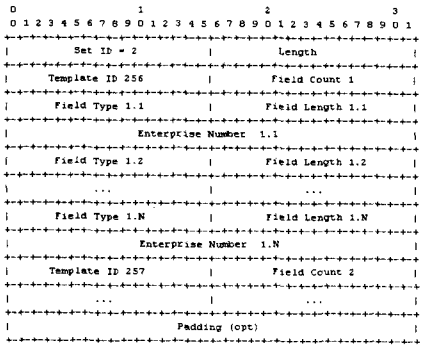
IETF IPFIX 워킹그룹에서는 Cisco NetFlow v9을 바탕으로 표준화 작업을 진행 중이다. 하나의 IPFIX 플로우 메시지는 IPFIX 헤더[그림 2], IPFIX 템플릿 세트[그림 3], IPFIX 데이터 세트[그림 4]의 3가지 포맷으로 구성되어있다.

- IPFIX 헤더



[그림 2] IPFIX 헤더 구조

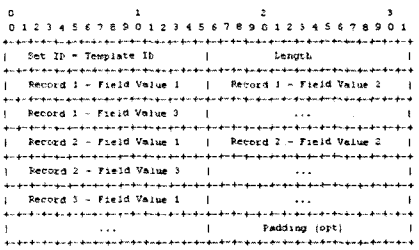
- IPFIX Template Set: IPFIX의 큰 장점 중 하나는 플로우 정보를 전달할 때 가변적으로 필요한 정보만으로 데이터 레코드를 구성하여 보낼 수 있도록 설정하는 것이다. Template Set은 가변적으로 데이터 레코드를 구성하기 위해 플로우 정보를 전달하기 전에 플로우 정보가 어떻게 구성되어있는지 알려주는 정보이다. 주요 필드들은 다음과 같다.



[그림 3] IPFIX Template Set 구조

1. Template ID [식별번호]: Data Set에 해당되는 Template 식별값.
2. Field Count [flow 순번]: NetFlow 데이터 패킷으로 전송할 Field type의 개수.
3. Field Type [flow 순번].[field 순번]: Flow 특성. (e.g. bytes, packets, protocol, addr...)
4. Field Length [flow 순번].[field 순번]: Field Type에 해당하는 값의 저장 공간 크기

- IPFIX Data Set: 플로우 정보를 실제로 전달할 때 [그림 6]과 같은 포맷을 이용한다.



[그림 4] IPFIX Data Set

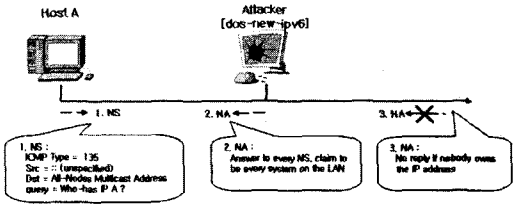
1. Record [flow 순번]
2. Field Value [flow 순번]: 측정 값이 저장됨.

3. IPv6 이상 트래픽 탐지를 위한 IPFIX 템플릿

3.1 IPv6 이상트래픽

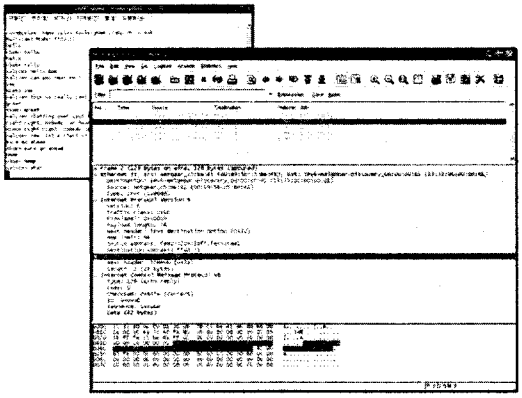
본 논문에서 다음과 같은 IPv6 이상 트래픽을 우선적으로 고려하였다.

- **IPv6 중복주소탐지(DAD)를 남용한 공격**: IPv6에서 상태 없는 자동주소할당 방법은 라우터에서 전송되는 RA(router advertisement) 메시지로부터 서브넷의 프레픽스 및 길이 디폴트 라우터 주소 등의 정보를 받고, 자신의 주소가 서브넷에서 사용되고 있지 않음을 확인하기 위해 메시지를 보낸다. 이 메시지에 대한 응답이 없는 것이 정상적인 것이지만, 공격자가 자동주소설정을 방해하기 위해서 응답을 하게 되면, 새로운 호스트에게 주소할당이 되지 않게 된다. 이 문제는 SEND와 같은 표준을 이용하여 해결할 수 있지만, IPSec와 SEND가 구현되지 않고 사용되는 경우도 있기 때문에 우선적인 이상 트래픽으로 분류한다. [2]에서는 [그림 5]와 같이 IPv6 중복주소탐지를 남용한 dos-new-ipv6 라는 공격도구를 발표하였다.



[그림 5] IPv6 중복주소탐지를 남용한 공격

- **IPv6 프로토콜의 확장 헤더를 이용한 은닉(covert) 채널**: 은닉채널은 정규채널 또는 대역폭을 보안 정책에 위배되는 방법으로 활용하여 정보를 숨겨서 전송하는 것이다. 기존의 IPv4 또는 TCP 프로토콜 헤더에서 사용되고 있지 않는 필드들을 이용한 은닉 채널에 관한 기법이 많이 제시되었는데, 최근에는 IPv6 프로토콜에서도 가능한 방법이 알려졌다. 대표적으로, IPv6 확장헤더 중 목적지 옵션은 현재 이동 IPv6에서 바인딩 확인 메시지에 활용되는데, 이를 활용하여 데이터전송을 하는데 사용되었다. [5]에서는 [그림 6]과 같이 IPv6 목적지 옵션을 이용하여 채팅을 할 수 있는 방법을 발표하였다.



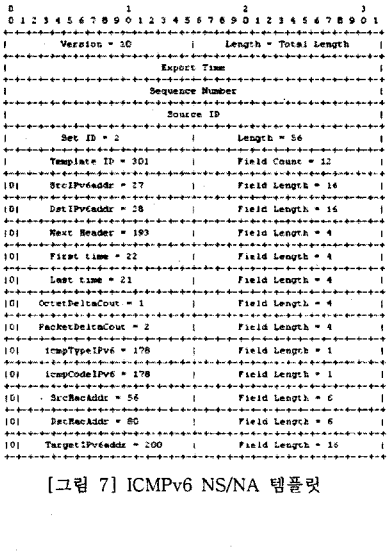
[그림 6] IPv6 목적지 옵션을 변형한 은닉 채널

● **IPv4 네트워크에서의 IPv6 터널링을 이용한 위해 트래픽**: IPv4에서 IPv6로 전환되기 위한 대표적인 방법으로 IPv6-over-IPv4 터널링 기법이 사용될 것으로 전망된다. 특히, 정적으로 설정되는 터널링과 달리 사용자에 의해 동적으로 설정되는 표준들인 6to4, Teredo 등이 사용되게 되면 IPv4 방화벽에서 IPv6 프로토콜 메시지를 구분할 수 있어야 위해 트래픽을 차단할 수 있다. 본 논문에서는 IPv4헤더의 프로토콜 필드 중 41번을 사용하는 IPv6-over-IPv4 터널링 트래픽만을 고려한다.

3.2 제안하는 새로운 IPFIX 템플릿

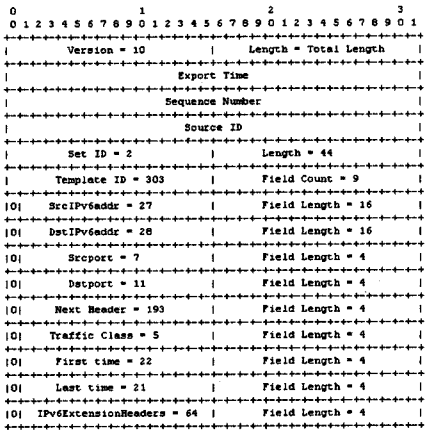
본 논문에서 IPv6 이상트래픽의 탐지를 위해서는 IPv6 라우터에서 적절한 IPFIX 플로우 생성을 하여 IPFIX 플로우 수집 및 분석기에 전송하여야 한다.

● **ICMPv6 NS/NA 템플릿**: IPv6 DAD를 이용한 자동주소할당 방해와 같은 공격을 탐지하기 위해서는 IPv6 기본 헤더 정보 뿐만 아니라 확장헤더의 내용도 모니터링할 수 있어야한다. ICMPv6 NS(neighbor solicitation)/NA(neighbor advertisement) 메시지를 이용하여 IPv6 프로토콜의 주소자동설정 기능을 방해하는 dos-new-ipv6 서비스 거부공격을 탐지할 수 있다. [그림 7]에서 IPv6 확장헤더에 포함되는 ICMPv6 타입 및 필드 값을 포함시켜 NS/NA 메시지를 식별할 수 있도록 하였고, DAD 연산을 수행하는지 확인하기 위하여 TargetIPv6addr 를 포함시켰다.



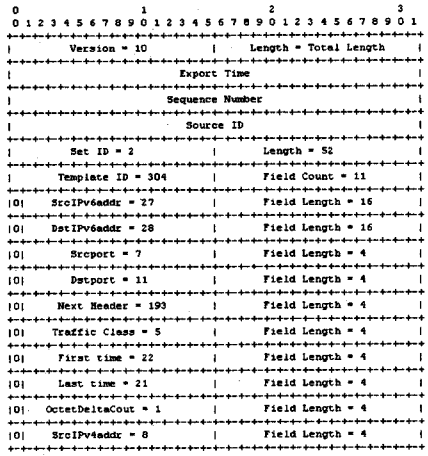
[그림 7] ICMPv6 NS/NA 템플릿

● **IPv6 확장헤더 플래그 템플릿**: IPv6 확장헤더들은 동시에 여러 가지들이 사용될 수 있다. 하지만, 일반적으로 동시에 사용되는 헤더들이 아닌 것들은 우선적으로 이상 트래픽으로 의심될 수 있다. 대표적으로 IPv6 목적지 옵션헤더는 현재 이동 IPv6에서 사용되고 있기 때문에 목적지 옵션헤더와 이동 헤더 또는 ESP/AH와 같은 IPSec 헤더들이 같이 사용된다. [5]에 알려진 목적지 옵션과 ICMPv6 를 동시에 사용한 은닉채널은 비정상적인 확장헤더들의 조합이기 때문에 확장헤더들의 조합을 모니터링하게 되면 간단하게 IPv6 이상 트래픽을 판단할 수 있는 기초 정보를 줄 수 있다. [그림 8]에서와 같이 특정 플로우에 대하여 IPv6 확장헤더들의 플래그를 사용하여 비정상적인 IPv6 확장헤더들의 조합을 이용하는 트래픽을 탐지하도록 하였다.



[그림 8] IPv6 확장헤더 플래그 템플릿

● **IPv6-over-IPv4 터널링 트래픽 템플릿**: IPv6 트래픽이 IPv4 프로토콜에 캡슐화될 때 프로토콜 41이 사용되고 있기 때문에 이 프로토콜 번호가 사용되는 트래픽에 대해서 IPv4 뿐만이 아니라 IPv6 트래픽에 관한 정보를 [그림 7]에서와 같이 포함하게 하여 IPv6 터널에서 어떤 트래픽이 사용되는지 분석가능하게 하였다.

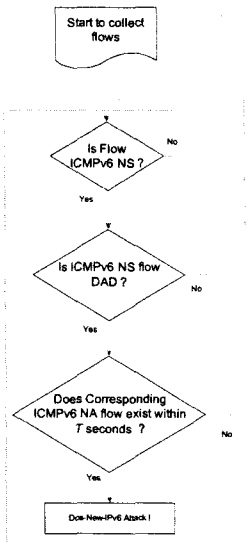


[그림 9] IPv6-over-IPv4 터널링 템플릿

4. IPFIX 메시지를 이용한 IPv6 이상 트래픽 탐지 방법

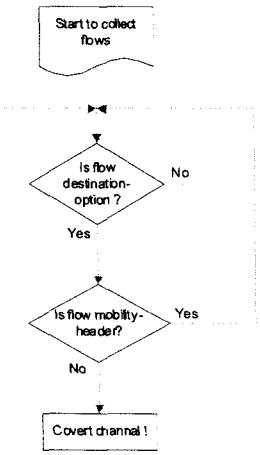
3장에서 제시된 IPFIX 템플릿을 이용하여 다음과 같은 간단한 방법을 이용하면 IPv6 이상 트래픽을 탐지할 수 있다.

[그림 9]에서는 dos-new-ipv6 와 같은 IPv6 DAD를 이용한 공격 트래픽을 탐지할 수 있는 방법이다. 즉, 일반적인 ICMPv6 NS 메시지가 아니라 DAD를 수행하는 NS 플로우가 관찰되었을 경우에 일정 시간 이내에 NA 메시지 응답이 있게 되면 자동주소 할당을 방해하게 되므로 NS 플로우에 해당되는 NA 플로우가 존재하는지를 검사하여 dos-new-ipv6 공격을 탐지하게 된다.



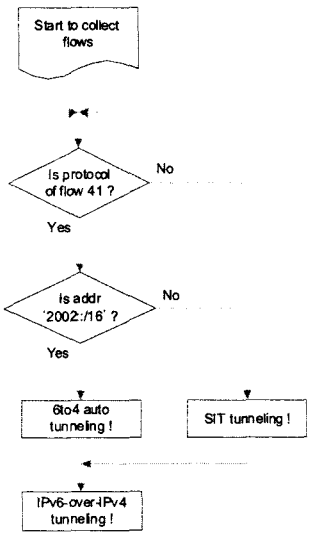
[그림 9] dos-new-ipv6 이상 트래픽 탐지 순서도

[그림 10]에서는 IPv6 목적지 옵션 확장헤더의 현재 활용되는 예인 이동 IPv6를 제외한 다른 옵션들은 이상트래픽 후보로 간주하는 플로우 분석 순서도이다.



[그림 10] IPv6 목적지 옵션을 이용한 은닉채널 탐지 순서도

[그림 11]에서는 IPv6-over-IPv4 터널링 트래픽을 탐지하는 순서도이다. 기본적으로 41번 프로토콜에 대하여 동적인 IPv6 터널이 사용되는 IPv6 주소인 2002::/16 프래픽스를 구분하여 탐지한다.



[그림 11] IPv6-over-IPv4 터널링 템플릿

5. 결론

본 논문에서는 IPv6 이상 트래픽을 모니터링하기 위하여 차세대 라우터에서의 트래픽 측정 표준인 IPFIX 에 기반한 새로운 템플릿을 제안하였다. 제안한 IPFIX 템플릿을 이용하면, IPv6 자동주소할당을 방해하는 공격 트래픽, IPv6 확장헤더를 이용하는 은닉채널 및 IPv6-over-IPv4 터널링과 같은 트래픽을 탐지할 수 있다는 것을 보였다. 하지만, 본 논문에서 고려된 IPv6 이상 트래픽은 이제까지 알려진 것들을 우선적으로 고려하였기 때문에 다양한 이상 트래픽을 모니터링하기 위해서는 추후 다양한 IPFIX 템플릿과 이를 이용한 이상 트래픽 분류 방법이 필요하다. 본 논문에서는 기본적인 IPv6 이상 트래픽 탐지 방법만을 제안하였기 때문에 제안한 방법을 트래픽 분석 시스템에 구현하여 실제 네트워크에 적용하는 것이 추후 필요하다.

6. 참고문헌

[1] S. Convery and D. Miller, "IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation," Cisco White Paper, March 2004.
[2] The Hackers' Choice Attack Tool, http://thc.segfault.net/
[3] J. Arkko, J. Kempf, B. Zill, and P. Nikander, "SEcure Neighbor Discovery (SEND)," IETF RFC3971, March 2005.
[4] N. B. Lucena, G. Lewandowski and S. J. Chapin, "Covert channels in IPv6," Workshop on Privacy Enhancing Technologies, 2005
[5] T. Graf, "Messaging over IPv6 Destination Options." The Swiss Unix User Group, Switzerland, http://gray-world.net/papers/messip6.txt , 2003.
[6] D. Llamas, C. Allison, and A. Miller, "Covert channels in Internet Protocols: A Survey", Workshop on Privacy Enhancing Technologies, 2005
[7] http://seclists.org/lists/honeypots/2002/Oct-Dec/0105.html
[8] Cisco NetFlow, http://www.cisco.com/warp/public/cc/pd/iosw/ioft/netflct/tech/napps_ipfix-charter.html
[9] J. Quittek, T. Zseby, B. Claise, and S. Zander, "Requirements for IP Flow Information Export (IPFIX)," IETF RFC3917, Oct. 2004.
[10] nProbe, http://www.ntop.org/
[11] WinIPFIX, http://networks.cnu.ac.kr/~winipfix/