情 報 保 護 學 會 誌
第22卷 第2號, 2012. 4

IPv6 보안기술 국제표준화 동향

송 중 석*, 이 행 곤**, 박 학 수***

요 약

현대 인터넷의 근간을 이루고 있는 IPv4의 주소공간(약 43억 개)이 고갈됨에 따라 128비트 주소길이를 제공하는 IPv6에 대한 관심이 지속적으로 증가하고 있다. IPv6는 IPv4에서는 고려하지 않은 인증 및 보안기능을 새롭게 추가하였으며, 그 외에도 호스트주소 자동설정, 점보그램을 이용한 패킷크기 확장, 효율적인 라우팅, 플로 레이블링, 이동성, QoS 등의 다양한 새로운 기능을 제공한다. 하지만, IPv6는 IPv4와는 다른 방식으로 동작하는 『새로운』 프로토콜이기 때문에, 예측 가능 또는 불가능한 다양한 보안상 위험요소가 존재한다고 할 수 있다. 따라서, IPv6를 실제 네트워크에 도입·구축하고 안전하게 운영하기 위해서는 보안상 해결해야할 많은 문제점들이 존재하며, 이를 위해 현재 IETF 및 NIST, ITU-T를 중심으로 IPv6 보안기술에 관한 국제표준을 진행하고 있다. 이에 본 논문에서는 각 표준화기관에서 진행하고 있는 IPv6 보안기술의 국제표준화에 관한 개요 및 특징에 대해서 살펴보고, IPv6 도입을 검토하고 있는 각급기관 및 네트워크 관리자들에게 IPv6 보안기술에 대한 방향성을 제시하고자 한다.

Ⅰ. 서 론

현재 인터넷의 대부분은 IPv4 (Internet Protocol version 4) 프로토콜을 기반으로 작동하고 있으며, 인터넷에 접속하는 단말의 개수가 늘어남에 따라 IPv4 주소공간 역시 빠른 속도로 고갈되고 있는 추세이다. 실제로, 약 43억 개의 IPv4 주소는 IANA (Internet Assigned Numbers Authority)에 의해 관리되고 있으나, 2012년 현재 IANA에 의한 추가적인 IPv4 주소의 할당은 없는 상태이다[1].

이러한 IPv4의 주소공간 부족문제를 해결하고, 폭발적으로 늘어나는 인터넷 사용에 대비하기 위하여, 32비트의 주소길이를 갖는 IPv4를 대신하여 128비트의 주소길이를 갖는 IPv6 (Internet Protocol version 6)가 1994년 IETF (Internet Engineering Task Force)에서 채택되었다[2]. 128비트 IPv6 주소공간은 지표면의 모든 공간에 10m^{2}당 1개씩의 IPv6/48 네트워크를 제공할 수 있을 만큼의 많은 개수를 갖는다. 이는 향후 도래할 유비쿼터스 시대에 대비하여 냉장고, TV, 전자레인지, AV 스피커, DVD 플레이어, 홈 보안장치, 전화기 등과 같은 대량의 통신 장치들이 상호 통신을 할 수 있도록 각 요소장비들이 주소를 할당 받을 수 있게 됨을 의미한다.

IPv6는 128비트 길이를 갖는 주소공간 이외에도 IPv4와 비교해서 다양한 장점을 갖는다. 특히, IPv4는 설계 당시에 보안요소를 전혀 고려하지 않았으나, IPv6는 인증 및 보안기능을 새롭게 추가하였으며, 호스트주소 자동설정, 점보그램을 이용한 패킷 크기확장, 효율적인 라우팅, 플로 레이블링, 이동성, QoS 등의 다양한 새로운 기능을 제공한다. 또한, 듀얼스택, 터널링 등과 같은 IPv4에서 IPv6로의 이행에 필요한 다양한 이행 메커니즘들을 제공한다.

상기와 같은 IPv6의 장점에도 불구하고, IPv6를 실제 네트워크에 도입·구축하고 안전하게 운영하기 위해서는 보안상 해결해야할 많은 문제점들이 존재한다. 왜냐하면, IPv6는 비록 보안기능들이 포함되어 있다 하더라도 IPv4와는 다른 방식으로 동작하는 『새로운』 프로토콜이기 때문에, 이는 예측 가능 또는 불가능한 다양한 보안상 위험요소가 존재함을 의미하기 때문이다.

이에 본 논문에서는 IPv6 보안기술에 대한 국제표준

* 한국과학기술정보연구원 첨단연구망센터(song@kisti.re.kr)
** 한국과학기술정보연구원 첨단연구망센터(hglee@kisti.re.kr)
*** 한국과학기술정보연구원 첨단연구망센터(hspark@kisti.re.kr)

화 동향에 대해서 IETF 및 NIST[3], ITU-T[4]의 세 가지 표준화기구의 활동을 중심으로 살펴보고, IPv6 도입을 검토하고 있는 각급 기관 및 네트워크 관리자들에게 IPv6 보안기술에 대한 방향성을 제시하고자 한다.

Ⅱ. IETF Security Area

IETF (Internet Engineering Task Force)는 인터넷 서비스의 품질을 보장하고 보다 향상된 인터넷 환경을 개발하기 위한 목적으로 1986년에 신설된 국제표준화 기구이다. IETF는 총 8개의 활동영역(Area)으로 구성되어 있으며, 그 중에서 보안영역(Security Area)은 인

〔표 1〕 IETF IPv6 보안기술관련 워킹그룹

워킹그룹명	목적
6man	IPv6 Maintenance
savi	Source Address Validation Improvements
dhc	Dynamic Host Configuration
v6ops	IPv6 Operations
opsec	Operational Security Capabilities for an IP Network
csi	CGA & Send maIntenance

〔표 2〕 IPv6 보안기술 관련 IETF RFC 리스트

RFC 번호	발행 연도	제 목	설 명
4864 [5]	2007	Local Network Protection for IPv6	네트워크 주소변환(NAT) 기술은 많은 장점들을 가지고 있지만, 그 중에서도 특히, 이용 가능한 주소공간을 "증식"할 수 있는 기능은 IPv6에서는 필요로 하지 않다. IPv6는 NAT를 사용하지 않는 것을 전제로 설계되었기 때문에, 이 문서는 IPv6를 사용하는 Local Network Protection(LNP)이 주소변환 기술 없이 어떻게 동일한 장점을 제공할 수 있는지에 대해서 기술하고 있다.
4942 [6]	2007	IPv6 Transition/Coexistence Security Considerations	IPv4 네트워크에서 IPv4와 IPv6가 공존하는 네트워크로의 이행은 많은 보안상 문제점들을 야기한다. 이 문서는 IPv6 프로토콜 자체에 의한 보안 이슈, 이행 메커니즘에 의한 보안 이슈, IPv6 구축에 따른 보안이슈에 대한 정보를 제공한다.
3964 [7]	2004	Security Considerations for 6to4	6to4는 IPv6 네트워크를 서로 연결하기 위해서 자동 Ipv6-over-IPv4 터널링을 사용한다. 6to4 아키텍처는 IPv4 노드로부터의 IPv4 protocol-41 트래픽을 받아들이고 디캡슐화 하는 6to4 라우터, 6to4 릴레이 라우터를 포함한다. 이는 서비스거부공격(DoS)과 같은 많은 보안상 문제점을 야기할 수 있다. 이 문서는 이러한 보안상 문제점들에 대해서 상세하게 기술하고 해당 문제점들을 해소하기 위한 방법을 제시한다.
4593 [8]	2006	Generic Threats to Routing Protocols	이 문서는 라우팅 프로토콜에 영향을 미치는 일반적인 보안위협 요소에 대한 설명 및 요약정보를 제공한다.
3971 [9]	2005	SEcure Neighbor Discovery (SEND)	IPv6 노드는 링크상의 다른 노드를 찾기 위해 이웃탐색 프로토콜(NDP)을 사용한다. 이 문서는 NDP를 위한 보안 메커니즘에 대해서 기술한다. 오리지널 NDP와는 달리 해당 메커니즘은 IPsec을 사용하지 않는다.
5969 [10]	2010	IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification	이 문서는 IPv4 네트워크 인프라를 통해 사용자에게 IPv6의 구축을 촉진시키기 위한 자동 터널링 메커니즘에 대해서 기술한다.
6092 [11]	2011	Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service	이 문서는 디바이스 제조사들을 위한 권고안들에 대해서 확인하고 인터넷으로의 접속이 가능한 가정 및 소규모 오피스 내부의 로컬 영역 IPv6 네트워크의 경계에서 『간단한 보안』 기능을 갖추기 위한 방법에 관해서 기술한다.
6105 [12]	2011	IPv6 Router Advertisement Guard	이 문서는 IPv6 RA 메시지를 안전하게 보호하기 위한 방법에 대해서 기술한다.
6106 [13]	2011	IPv6 Router Advertisement Options for DNS Configuration	이 문서는 IPv6 라우터가 IPv6 호스트에 대한 NDS 탐색 리스트 및 DNS recursive 서버 주소를 알리는데 필요한 IPv6 RA 옵션에 대해서 기술한다.
6169 [14]	2011	Security Concerns with IP Tunneling	이 문서는 IP 터널과 관련된 다수의 보안 위협요소에 대해서 기술한다.
6333 [15]	2011	Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion	이 문서는 서비스 공급자 네트워크 내에 IPv6를 구축하는 것에 대한 이점 및 듀얼스택 라이트 기술을 소개한다.
6434 [16]	2011	IPv6 Node Requirements	이 문서는 IPv6 노드들을 위한 요구사항에 대해서 정의한다.

터넷 환경에서의 보안과 관련된 이슈를 담당하고 있다. IETF 보안영역은 현재 총 15개의 실무반(Working group)으로 구성되어 있으며, IPv6 보안기술과 관련 된 표준을 진행하는 6개의 워킹그룹을 [표 1]에 나타낸다.

IETF는 현재까지 다수의 IPv6 보안기술 관련 표준안(RFC)을 개발하였으며, 주요 RFC 리스트는 [표 2]와 같다. [표 2]에서 나타낸 RFC들은 IPv6 이행 매커니즘(6rd, 6to4 등), 라우팅 프로토콜, 로컬 네트워크, 이웃 탐색 프로토콜, IP 터널링 등과 같이 IPv6 요소기술들에 대한 보안이슈를 주로 다루고 있다. 따라서, IPv6 도입을 검토하고 있는 각급기관은 IPv6 구축 시에 해당 RFC 표준안들을 참고·적용함으로써 IPv6 운용 시에 발생할지도 모르는 보안상 위험 요소들을 미연에 방지할 필요가 있다.

Ⅲ. NIST

미국의 국가표준기술원인 NIST(National Institute of Standards and Technology)는 2010년 12월에 『Guidelines for the Secure Deployment of IPv6』라는 IPv6의 도입 및 구축 시에 필요한 보안관련 이슈들을 다룬 표준안을 개발하여 공개하였다[17]. 해당 표준안은 IPv4에서 IPv6로의 이행에 필요한 보안이슈 보다는 IPv6 자체의 구축 및 운영 시에 필요한 보안요소에 초점을 맞추고 있다.

3.1 NIST IPv6 보안기술 표준안 개요

NIST의 『Guidelines for the Secure Deployment of IPv6』 표준안은 IPv6에 대한 소개를 시작으로 IPv6에 대한 전체적인 리뷰, IPv6 자체의 고급 기능 및 IPv6 보안관련 고급 기능에 대한 설명을 포함하고 있으며, 마지막으로 IPv6를 구축하고 운영할 시에 필요한 보안요소들에 대해서 기술적인 수준에서 매우 상세하게 기술하고 있다. NIST 표준안의 주요 목적은 다음과 같이 세 가지로 요약할 수 있다.

- IPv6의 주요 특징 및 이들 특징들이 어떠한 보안 위협 요소를 가지고 있는지에 대해 독자들에게 교육하는 것
- IPv6의 도입 및 구축 시에 사용되어질 수 있는 메커니즘에 대한 광범위한 요약정보를 제공하는 것
- IPv6 환경으로의 전환에 필요한 구축 전략을 제시하는 것

또한, NIST 표준안은 기관들이 IPv6를 구축할 시에 직면하게 되는 장애 요소들을 극복하기 위해서 따라야 할 다음과 같은 권고 사항을 제시하고 있다.

- 각 기관의 종사자들이 그들이 현재 가지고 있는 IPv4에 대한 지식과 비슷한 수준으로 IPv6에 대해서도 전문지식을 쌓을 것
- 필요이상으로 IPv6로의 이행 메커니즘을 구축하지 말것: 비즈니스 니즈를 지원하기 위해서 적절한 이행 메커니즘을 활용한 단계별 IPv6 구축계획을 세울 것
- 듀얼 IPv4/IPv6 공존을 이용하여 장기간에 걸친 이행 계획을 수립할 것

3.2 NIST IPv6 보안기술 표준안 주요내용

NIST IPv6 보안기술 표준안의 주요내용을 요약하면 [표 3]과 같다. 앞서 2장에서 기술한 IETF의 IPv6 표준 문서인 RFC가 IPv6의 각 요소기술들이 안고 있는 보안상 취약점을 어떻게 보완할 것인가에 대해서 초점을 맞추고 있다면, NIST의 IPv6 보안기술 표준안은 IPv6 도입을 검토하고 있는 각급기관이 안전한 IPv6 네트워크를 구축하기 위하여 IPv6의 각 요소기술을 실제로 어떻게 적용할 것인가에 대해서 중점적으로 기술하고 있다.

〔표 3〕 NIST IPv6 보안기술 표준안 주요내용

Section	설 명
2	IPv6에 대한 소개(IPv6의 역사, 특징 및 IPv4와의 비교)
3	IPv6 주소생성, 할당, 패킷 구성 및 ICMPv6에 대한 상세한 정보
4	IPv6의 주요 고급 기능들에 대한 소개 및 그들에 대한 보안적 위험요소(멀티호밍, 멀티캐스트, QoS, Mobile IPv6, 점보그램, 주소선택 등)
5	IPv6에 포함된 고급 보안 기능들에 대한 소개 (privacy 주소, IPsec, 안전한 자동 주소할당, 이웃 탐색 등)
6	IPv6를 안전하게 구축하기 위한 과정 및 위험요소, 다양한 이행 메커니즘 등에 대한 분석

Ⅳ. ITU-T SG17

ITU-T에서의 IPv6 보안기술에 관한 표준화는 Study Group 17 (Security)내 연구과제 2(Q.2)와 3(Q.3)에서 진행하고 있다[18]. 지난 2011년 4월 제네바 회의에서

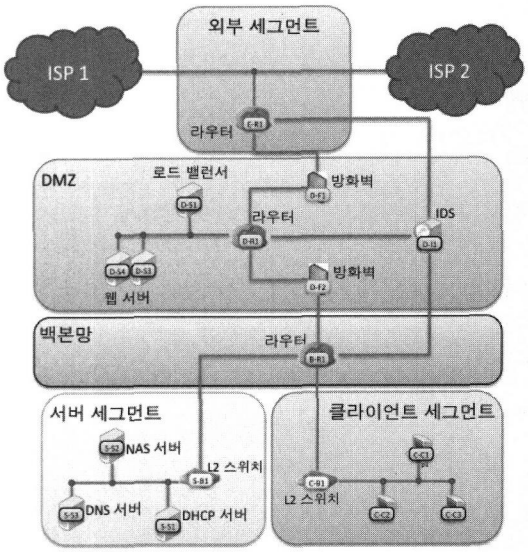
일본 총무성 산하 국책연구소인 일본정보통신연구원(NICT) 주도로 『Technical Security Guideline on Deploying IPv6』라는 IPv6 구축 시에 필요한 기술적인 보안 가이드라인이 연구과제 2에서 제안되었으며, 본회의에서 승인(X.ipv6-secguide)되었다. 또한, 연구과제 2에서 추진하는 표준안이 기술적인 수준에서의 보안가이드를 다루고 있는 반면에, 연구과제 3에서는 관리적인 측면에서의 보안가이드에 대한 표준화를 진행할 예정이다. 현재는 2011년 8월 제네바 회의에서 연구과제 2의 X.ipv6-secguide 초안이 발표되었으며, 2012년 3월 제네바 회의에서 NICT와 KDDI가 개정판을 제출하였다. 한편, 연구과제 3의 경우는 아직까지 표준화에 대한 구체적인 움직임은 없으며, X.ipv6-secguide에 대한 표준화가 진행된 후에 본격적으로 관리적 측면에서의 표준문서 작성이 이루어질 전망이다. ITU-T SG17의 연구과제 2에서 진행 중인 X.ipv6-secguide의 내용에 대해서 간략하게 소개를 하면 다음과 같다.

4.1 X.ipv6-secguide의 범위

X.ipv6-secguide는 IPv6에 있어서의 다양한 보안위협 요소에 대해서 기술하고 이들에 대한 실제적인 위험평가 결과를 제시하고 또한 IPv6를 안전하게 구축하기 위한 기술적인 솔루션을 제공한다. X.ipv6-secguide는 IPv6 네트워크상에 필수적으로 배치될 세 종류의 컴포넌트, 즉 네트워크 장치(라우터, 스위치 등), 서버/클라이언트 장치(단말, HDCP 서버 등), 보안 장비(IDS, FW 등)을 중심으로 기술한다. X.ipv6-secguide의 목적은 IPv6 도입을 계획하고 있는 기업의 네트워크 관리자에게 기술적인 보안 가이드라인을 제공하기 위함이다. 이를 통해, 기업의 IPv6 네트워크상에 존재하는 보안상 위험요소를 경감할 수 있게 될 것이다.

4.2 IPv6 네트워크 토폴로지

[그림 1]은 기업 네트워크에서 사용되어질 일반적인 IPv6 네트워크 토폴로지를 보여준다. 여기에는 IPv4 호스트는 물론, IPv6 호스트, 그리고 양쪽모두 사용가능한 호스트가 존재하게 된다. IPv4 네트워크와 같이 IPv6 네트워크 역시 크게 다섯 개의 세그먼트로 구성된다: 외부 세그먼트, DMZ, 백본망, 서버 세그먼트, 클라이언트 세그먼트. 외부 세그먼트는 ISP (Internet Service



〔그림 1〕 일반적인 IPv6 네트워크 토폴로지

Provider)와 기관의 경계 라우터 사이의 접점 역할을 하는 컴포넌트를 가리킨다. DMZ는 인터넷 사용자들에게 웹서버나 로드 밸런서와 같은 대외 서비스들을 제공하기 위한 영역을 말하며 일반적으로 IDS나 방화벽(Firewall)과 같은 보안장치가 여기에 배치된다. 백본망은 대용량·고속의 중앙구역으로 내·외부 세그먼트 사이를 연결하는데 이용된다. 서버 세그먼트에는 내부 사용자들을 위해 필수불가결한 DNS 서버, DHCP 서버 등의 다양한 종류의 서버들이 배치되며, 실제 사용자들의 단말이 클라이언트 세그먼트에 속하게 된다.

4.3 보안위협 및 대책의 예

4.3.1 라우터

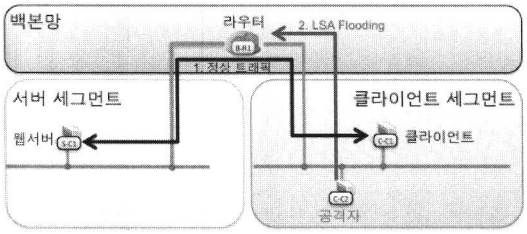
4.3.1.1 보안위협

OSPFv3은 RFC2740[19]에 기술되어져 있다. OSPFv3은 라우터간의 링크상태 정보를 공유하기 위하여 LSA를 사용한다. LSA에는 네트워크 LSA, 라우터 LSA 등 총 9 종류의 LSA 메시지가 있으며, LSA 헤더는 LSA 기능코드 및 플루딩 범위에 관한 정보를 포함한다. OSPFv3은 헤더의 "U"비트를 이용하여 알려지지 않은 LSA를 핸들링 할 수 있으며, 이 때 U비트는 1의 값을 갖는다. 또한, 라우터가 U비트의 값이 1인 LSA를 수신하게 되면 라우터는 해당 LSA를 모두 LSDB에 저장해

야만 한다. 따라서, 공격자가 대량의 알려지지 않은 LSA를 발행함으로써 특정 라우터의 LSDB를 공격할 수 있게 된다. 또한, OSPFv3은 "S1"과 "S2"비트를 이용하여 LSA의 플루딩 범위를 결정할 수 있기 때문에, 공격자는 이 두 비트를 악용함으로써 보다 용이하게 라우터에 대해서 DDoS공격을 감행할 수 있게 된다.

4.3.1.2 실제 위험도 평가

[그림 2]는 LSA 플루딩을 이용한 공격시나리오를 보여준다. 이 공격에서 웹서버(S-C1)와 클라이언트(C-C1)가 상호간에 통신을 하고 있는 상태에서 공격자(C-C2)는 대량의 LSA를 라우터(B-R1)로 끊임없이 전송하게 된다. 일본의 IPv6 기술검증협의회에서 실시한 위험도 평가실험에서 공격을 받은 라우터는 최대치를 초과한 LSA에 대해서는 저장을 할 수 없었으며, 또한 라우터의 동작이 매우 느려졌고 계속해서 정상적으로 동작하지 않음을 확인하였다.



〔그림 2〕 LSA 플루딩을 이용한 공격 시나리오

4.3.1.3 대책

이러한 LSA 플루딩을 이용한 공격에 대비하기 위해서는 라우터에서 OSPFv3을 이용할 시에 RFC4552[20]에 기반한 인증기능을 구현할 필요가 있다. 이를 통해 라우터는 비정상 노드로부터 전송된 LSA를 무시할 수 있으며, 해당 라우터가 관리할 수 있는 LSA의 최대치를 조정할 수 있게 된다.

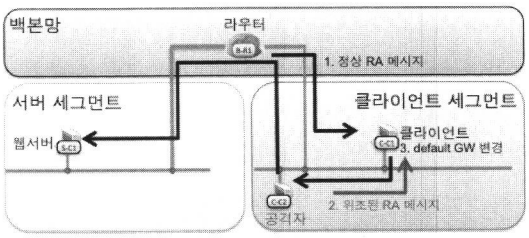
4.3.2 호스트

4.3.2.1 보안위협

IPv6 호스트는 자신들의 IP 주소를 ICMPv6 (Internet Control Message Protocol version 6)의 RA (Router Advertisement) 메시지를 이용하여 자동적으로 설정할 수 있다. 뿐만 아니라, IPv6 호스트는 RA 메시지에 포함된 정보를 이용하여 디폴트 게이트웨이도 선택할 수 있기 때문에, RA 메시지는 중간자공격에 악용될 가능성이 매우 높다. 다시 말해서, 만약 공격자가 디폴트 게이트웨이를 자기 자신으로 설정한 위조된 RA 메시지를 공격대상 호스트에 전송한다면, 공격대상 호스트의 모든 트래픽이 공격자의 단말로 전송되기 때문에 중간에서 공격대상 호스트의 트래픽을 가로챌 수 있게 된다.

4.3.2.2 실제 위험도 평가

[그림 3]은 위조된 RA 메시지를 이용한 공격 시나리오를 보여준다. 이 공격 시나리오에서 라우터(B-R1)는 웹서버(S-C1)와 통신하기를 원하는 클라이언트(C-C1)로 정상 RA 메시지를 보내고 있다고 가정한다. 이 때, 공격자 또한 디폴트 게이트웨이를 자기 자신으로 설정한 위조된 RA 메시지를 해당 클라이언트로 전송하게 된다. 일본 IPv6 기술검증협의회에서 실시한 위험도 평가의 결과, 공격자는 클라이언트와 웹서버 간의 모든 트래픽을 감청할 수 있다는 것을 증명하였다.



〔그림 3〕 위조된 RA 메시지를 이용한 중간자 공격

4.3.2.3 대책

이러한 위조된 RA 메시지에 의한 중간자 공격으로부터 피해를 최소화하기 위해서 각 호스트는 극히 짧은 생존기간을 갖는 모든 RA 메시지를 무시할 필요가 있다.

4.3.3 침입탐지시스템(IDS)

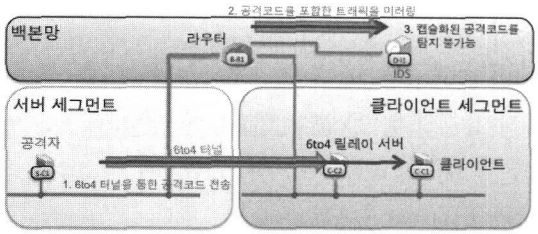
4.3.3.1 보안위협

6to4는 IPv4에서 IPv6로의 전환에 필요한 이행 메커니즘 중의 하나이다. 6to4 프레임워크에서 IPv6 호스트(또는 6to4 호스트)와 통신하기를 원하는 6to4 호스트는 외부로 나가는 IPv6 패킷에 대해서 캡슐화를 수행하고 반대로 내부로 들어오는 IPv6 패킷에 대해서는 디캡슐화를 수행하게 된다. 따라서, 6to4 호스트가 6to4 터

널을 통해서 IPv6 호스트를 공격하게 될 경우, 캡슐화된 IPv6 패킷에 대해서 디캡슐화 기능을 지원하지 않는 IDS는 해당 공격을 탐지할 수 없다는 문제점이 있다.

4.3.3.2 실제 위험도 평가

[그림 4]는 6to4 캡슐화를 이용한 공격 시나리오를 보여준다. 이 공격 시나리오에서 공격자(S-C1)는 공격코드를 6to4 터널을 통하여 클라이언트(C-C1)로 보내고 라우터(B-R1)는 해당 공격코드를 IDS(D-I1)으로 전송하게 된다. 일본 IPv6 기술검증협의회에서 실시간 위험도 평가실험의 결과, IDS는 캡슐화된 공격코드를 탐지할 수 없음을 확인하였다.



〔그림 4〕 6to4 캡슐화를 이용한 공격 시나리오

4.3.3.3 대책

IDS와 같은 보안장비들이 캡슐화된 IPv6 패킷에 대해서 디캡슐화 기능을 제공함으로써 6to4를 악용한 공격에 대비할 수 있을 것이다.

V. 결 론

현재 인터넷상에서 이용되고 있는 IPv4 주소가 빠른 속도로 고갈되고 있는 추세이며, 이러한 IPv4의 부족한 주소공간 문제를 해결하고, 인증 및 보안기능뿐만 아니라 호스트주소 자동설정, 점보그램을 이용한 패킷 크기 확장, 효율적인 라우팅, 플로 레이블링, 이동성, QoS 등의 다양한 새로운 기능을 제공하는 IPv6에 관심이 지속적으로 증가하고 있다.

향후 도래할 유비쿼터스 시대에 대비하기 위해서도 각급기관은 IPv6 네트워크를 도입·구축함으로써 현재의 IPv4 네트워크를 대체할 필요가 있다. 하지만, IPv6를 실제 네트워크에 도입·구축하고 안전하게 운영하기 위해서는 보안상 해결해야할 많은 문제점들이 존재하며, 이를 위해 IETF 및 NIST, ITU-T의 세 가지 표준화 기구에서는 IPv6 보안기술에 대한 국제표준화를 진행하고 있다. 본 논문에서는 상기 세 기구에서 진행하고 있는 표준안에 대해서 살펴보았으며, IPv6의 도입을 검토하고 있는 각급기관의 네트워크 관리자는 본 논문에서 제시한 정보를 기반으로 실제 IPv6 네트워크 구축 및 운영 시에 발생할 보안위협 요소를 사전에 제거할 필요가 있을 것이다. 특히, ITU-T SG17에서 진행 중인 표준안의 경우, IPv6 에서 고려해야할 보안요소를 기술적인 측면과 관리적인 측면에서 다루고 있으며, IPv6 네트워크상에 필수적으로 배치될 각 컴포넌트(네트워크 장치, 서버/클라이언트 장치, 보안장비)를 중심으로 기술하고 있기 때문에, IETF와 NIST의 표준안과 비교해서 실제 네트워크에의 적용이 매우 용이할 것으로 기대된다.

참고문헌

[1] http://www.icann.org/en/news/releases/release-03feb11-en.pdf.

[2] http://www.ietf.org/.

[3] http://www.nist.gov/.

[4] http://www.itu.int/ITU-T/.

[5] IETF RFC 4864, "Local Network Protection for IPv6", http://www.ietf.org/rfc/rfc4864.txt, 2007.

[6] IETF RFC 4942, "IPv6 Transition/Coexistence Security Considerations", http://www.ietf.org/rfc/rfc4942.txt, 2007.

[7] IETF RFC 3964, "Security Considerations for 6to4", http://www.ietf.org/rfc/rfc3964.txt, 2004.

[8] IETF RFC 4593, "Generic Threats to Routing Protocols", http://www.ietf.org/rfc/rfc4593.txt, 2006.

[9] IETF RFC 3971, "SEcure Neighbor Discovery (SEND)", http://www.ietf.org/rfc/rfc3971.txt, 2005.

[10] IETF RFC 5969, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification", http://www.ietf.org/rfc/rfc5969. txt, 2010.

[11] IETF RFC 6092, "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service", http://www.ietf.org/rfc/rfc6092.txt, 2011.

[12] IETF RFC 6105, "IPv6 Router Advertisement Guard", http://www.ietf.org/rfc/rfc6105.txt, 2011.

[13] IETF RFC 6106, "IPv6 Router Advertisement Options for DNS Configuration" http://www.ietf.org/rfc/rfc6106.txt, 2011.

[14] IETF RFC 6169, "Security Concerns with IP Tunneling", http://www.ietf.org/rfc/rfc6169.txt, 2011.

[15] IETF RFC 6333, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", http://www.ietf.org/rfc/rfc6333.txt, 2011.

[16] IETF RFC 6434, "IPv6 Node Requirements", http://www.ietf.org/rfc/rfc6434.txt, 2011.

[17] Sheila Frankel, Richard Graveman, John Pearce, Mark Rooks, "Guidelines for the Secure Deployment of IPv6", Recommendations of NIST, Special Publication 800-119, December 2010.

[18] http://www.itu.int/ITU-T/studygroups/com17/index.asp.

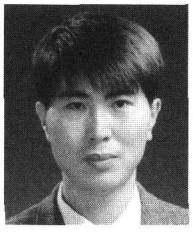
[19] IETF RFC 2740, "OSPF for IPv6", http://www.ietf.org/rfc/rfc2740.txt, 1999.

[20] IETF RFC 4552, "Authentication/Confidentiality for OSPFv3", http://www.ietf.org/rfc/rfc4552.txt, 2006.

〈著者紹介〉

송 중 석 (Jungsuk Song)
2003년 2월: 한국항공대학교 통신정보공학과 졸업
2005년 2월: 한국항공대학교 대학원 정보통신공학과 석사
2009년 3월: 교토대학교(일본) 정보학연구과 지능정보학전공 박사
2009년 4월~2010년 9월: 일본정보통신연구원 (NICT) 전공연구원
2010년 10월~2011년 9월: 일본정보통신연구원 (NICT) 선임연구원
2011년 10월~현재: 한국과학기술정보연구원 (KISTI) 선임연구원
<관심분야> 네트워크 보안, 데이터 마이닝, 기계학습, 보안관제, IPv6 보안

이 행 곤 (Haeng-Gon Lee)
1997년 2월: 호원대학교 컴퓨터공학과 졸업
2000년 2월: 전북대학교 대학원 전자계산학과 석사
2008년~현재: 전북대학교 대학원 정보보호공학과 박사과정
2000년~현재: 한국과학기술정보연구원(KISTI) 선임연구원
<관심분야> 네트워크 보안기술, 보안관제, 침해사고 조사 및 대응



박 학 수 (Hak-Su Park)
1989년 2월: 한남대학교 전자계산학과 졸업
1991년 2월: 한남대학교 대학원 컴퓨터공학과 석사
2003년 2월: 한남대학교 대학원 컴퓨터공학과 박사
1991년 3월~현재: 한국과학기술정보연구원(KISTI) 책임연구원
<관심분야> 보안관제, 침해사고대응, 네트워크 보안