HIP 관련 IETF 연구 동향 분석

김건웅*, 송병권**, 이승훈***, 김원***
*목포해양대학교 해양전자・통신공학부
**서경대학교 정보통신공학과
***한국인터넷진흥원
e-mail:kgu@mmu.ac.kr

A Study on the Activities of IETF Working Group that Related to HIP

Geonung Kim*, Byung-Kwen Song**,
Seung-Hoon Lee***, Weon Kim***
*Division of Electronic & Comm. Engineering, Mokpo National Maritime University
**Dept of Information & Comm. Engineering, Seokyeong University
***National Internet Development Agency of Korea

요 약

현재 인터넷을 구성하고 있는 두가지 중요 이름공간(name space)인 IP(Internet Protocol) 주소와 DNS(Domain Name Service) 이름의 단점을 보완하기 위해 연구되고 있는 HIP(Host Identity Protocol)는 IP와 트랜스포트 계층 사이에 새로운 계층과 프로토콜을 제안함으로써 제한된 형태의 신뢰성을 제공하고 이동(mobility), 멀티홈(multihome), 동적 IP 주소변경 등을 지원하며 DoS(Denial of Service) 공격 등을 방어한다. 본 논문에서는 현재까지 IETF에서 진행된 HIP관련 연구 동향을 분석한다.

1. 서론

현재의 인터넷은 두개의 중요한 이름 공간을 가지고 있는데, 그것들은 IP(Internet Protocol) 주소와 DNS(Domain Name Service) 이름이다. 이들은 오늘날의 인터넷이 존재할 수 있도록 하는 여러가지 기능들을 제공하고 있다. 그러나 그것들은 두 개의 이름 공간만으로 모든 기능들을 담으려고 하는 과정에서 의미의 중복이 발생하고 과도한 기능 확장으로 이름 공간이 복잡해지는 문제점들이 발생했다.

호스트 정체성(HI: Host Identity) 이름공간은 이러한 IP와 DNS 이름 공간 사이를 채우기 위해 생겨난 것으로서, 호스트 식별자(HI: Host Identifier)들로 구성된다. 이때 하나의 HI는 암호화되어 있으며, 비대칭형 암호쌍 중 공개키로 볼 수 있다. 각 호스트는 적어도 하나의 HI를 가져야 하며, 일반적으로 하나 이상의 HI를 갖는다. 각 호스트 정체성은 하나의 호스트를 식별한다. 즉 두 호스트는 같은 HI를 가질 수 없다. 호스트 정체성과 그것에 대응하는 호스트 식별자는 공개적(DNS로 발표)일 수도 있고 미발표될 수도 있다.

이러한 호스트 식별자는 IKEv2와 같은, 많은 인증 시스템에서 이용될 수 있지만 HIP(Host Identity Protocol) 구조(architecture)에서는 HIP라고 부르는 새로운 프로토콜과 HIP 기본 교환(base exchange)라고 부르는 암호화된 교환을 제시한다. 새로운 프로토콜은 시스템들 간에 제한된 형태의 신뢰를 제공하며, 이동성, 멀티홈, 동적 IP 주소변경를 확장하며, 프로토콜 번역/변환을 지원하고 DOS(denail-of-service)와 같은 종류의 공격을 줄여준다[7].

본 논문에서는 IETF HIP WG에서 현재까지 진행한 연구 동향을 분석한다. 먼저 2장에서는 HIP가 연구되게 된 배경을 살펴보고 3장에서는 HIP 구조와

HIP 프로토콜 자체를 살펴본다. 다음 4장에서는 HIP를 DNS에 도입하기 위해 진행 중인 연구를 분석하고 5장에서 결론을 맺는다.

2. HIP 탄생 배경

인터넷은 3가지 중요 요소에 의해 만들어지는데, 그것들은 연산 플랫폼(종단), 패킷 전송(망간 연결) 하부구조, 그리고 서비스(응용)이다. 인터넷은 사람과 프로세스들에게 서비스를 제공하기 위해 존재한다. 이때 모든 요소들은 확장 가능한 형태로 상호 동작할 수 있도록 이름 지어질 필요가 있는데, 이들 요소들을 위한 두가지 중요 이름공간이 IP 주소와 도메인 이름이다. 전자우편, HTTP, SIP 주소들은 이러한 도메인 이름의 확장에 불과하다.

IP 주소는 호스트의 망 인터페이스 이름과 위치의 이름이 혼동(confounding)된 것으로 볼 수 있다. 여기서 혼동이라고 한 것은 인덱싱 과정의 이득을 위해 하나로 합쳐졌는데, 그 과정에서 정보의 손실이 일어난다는 것을 의미한다. 일반적으로 IP 번호는 망에 연결되어 있을 때만 망 인터페이스를 이름 짓는다. 원래 IP 주소는 장기간 의미를 가질 목적으로 만들어졌는데, 오늘날 거대한 양의 인터페이스들이 짧은 시간동안에만 이용되고 또한 유일하지 않은 IP 번호를 이용하기도 한다. 따라서 과거에 만들어진 IP 주소가 부적합한 경우가 생겨나고 있다.

또한 현재의 인터넷에서는 트랜스포트 계층과 IP 주소는 연관되어 있으며, 그 결과 둘 중 어느 하나도 다른 것에 분리되어 독립적으로 진화할 수 없는데, 이것 역시 인터넷의 진화에 걸림돌이 되고 있다.

도메인 이름은 어떤 연산 플랫폼이나 서비스들에게 계층적으로 명명된 이름을 제공한다. 각 계층은 한 단계 위 레벨에서 위임을 받는다. 따라서 도메인 이름에서는 익명성이 없다.

현재의 이름공간에는 3가지의 치명적인 결함이 있다. 그것들은 첫째, 동적인 재주소가 바로 관리될 수 없으며, 둘째, 일관되고 신뢰할 수 있는 형태로 익명성이 제공될 수 없고, 셋째, 시스템이나 데이터그램에 대한 인증이 제공되지 않는다는 점이다. 이러한 모든 결함들은 현재의 이름공간에서 연산 플랫폼이 제대로 명명되지 않는데서 비롯된다.

만약 연산 플랫폼에 대한 독립적인 이름공간이 제공된다면 이것들은 망 계층의 진화와 독립적으로, 많은 망 계층들을 거치면서 종단간 작업을 수행하는데 이용될 수 있다. 또한 이것은 이동성이나 리홈(rehoming), 번호재할당(renumbering)으로 인한 망 계층에서의 주소 재할당을 지원할 수 있다.

또한, 이러한 연산 플랫폼에 대한 이름공간이 공개키 기반 암호화에 기반을 두고 있다면 인증 서비스를 제공할 수도 있다. 만약 이러한 이름공간이 등록 절차 없이 지역적으로 생길 수 있다면 익명성을 제공할 수도 있다.

이러한 일련의 조건들을 고려하여 연산 플랫폼을 위한 이름공간과 이것이 가져야 할 특징을 [3]에서 정리하였다.

3. HIP

2장에서 언급한 특징들을 만족하는 새로운 이름공간을 호스트 정체성 이름공간이라고 한다. 이러한 이름공간을 이용한다는 것은 망 계층과 트랜스포트 계층 사이에 새로운 프로토콜 계층 - HIP를 필요로 한다. 또한 이들 이름은 인증 서비스를 제공하기 위하여 공개키 암호화에 기반을 두고 있다.

호스트 정체성 이름공간의 하나의 이름, 즉 하나의 호스트 식별자는 IP 스택을 가지고 있는 어떤 시스템을 명명할 수 있는, 통계적으로 전세계에 걸쳐 유일한 이름을 나타낸다. 이러한 정체성은 일반적으로 하나의 IP 스택에 연관되어 있고, 하나의 시스템은 여러 개의 정체성을 가질 수 있다. 이때 그들 중 일부는 '잘 알려진' 것들이고 일부는 미발표되거나 익명으로 된 것들이다.

또한 시스템은 스스로 자기 자신의 정체성을 주장할 수도 있고, 어떤 것들은 DNSSEC, PGP, X.509와 같이 정체성을 증명하기 위해 제 3의 인증자를 이용할 수 있다. HIP에서 호스트 식별자는 처음에 DNSSEC을 통해 인증받도록 되어 있고, 따라서 구현에서는 최소한 기본적으로 DNSSEC을 지원해야 한다. HIP의 저자들은 공개키 쌍의 공개키가 가장 좋은 HI로 판단하고 있다. HIP 프로토콜 문서에서 언급된 것과 같이 공개키 기반 HI는 HIP 패킷을 인증하고, man-in-the-middle 공격을 방어할 수 있다.

HIP의 denial-of-service 공격을 방어하기 위해 데이터그램의 인증이 필수적이므로 HIP의 Diffie-Hellman 교환은 인증되어야 한다. 따라서 실제로는 공개키 기반 HI와 인증된 HIP 메시지만이 지원된다.

호스트 정체성은 인터넷 프로토콜에 두가지 중요한 기능을 제공한다. 먼저 망과 트랜스포트 계층을 분리시킨다. 이러한 분리는 두 계층의 독립된 진화를 가능하게 한다. 또한 여러 망이 연결된 환경에서 종단간 서비스를 제공한다. 두 번째 기능은 호스트 인증 기능이다. HI가 하나의 공개키이므로 이 키는 IPSec과 같은 보안 프로토콜에서의 인증에서 이용될 수 있다.

실제로 인터넷 프로토콜에서는 호스트 식별자가 직접적으로 이용되지 않는다. 실제로는 대응하는 호스트 식별자가 다양한 DNS나 LDAP 디렉토리에 저장되어 있고, HIP 기본 교환에서만 전달된다. 다른 프로토콜에서는 HIT(Host Identity Tag)가 호스트의 정체성을 나타낸다. 호스트 정체성의 또 다른 표현인 LSI(Local Scope Identifier)도 프로토콜과 API들에서 이용될 수 있다.

HIT는 호스트 정체성을 128비트로 표현한 것이다. 일반적으로 이것은 호스트 식별자의 암호화 해쉬로 얻어지는데, 이러한 HIT의 사용은 고정된 길이로 인해 프로토콜 코딩이 용이하고, 작은 패킷 크기로 인해 전송 과정에서 이득을 볼 수 있다는 점과 암호화 알고리즘에 독립적으로, 일관된 형태로 식별이 가능할 수 있다.

LSI 역시 호스트 정체성의 다른 표현인데 32비트의 길이를 갖는다. 이것은 현재의 프로토콜과 API들에서 호스트 정체성을 이용하고자 할 때 유용하게 쓰일 수 있으며, 약점은 작은 크기로 인해 전세계적으로 이용할 수는 없고, 지역적으로만 이용이 가능하다는 점이다.

다음은 HIP 기본 교환을 보여준다. 초기자와 응답자 사이에는 4개의 메시지가 교환되고 그 과정을 거쳐 HIP 연관(Association)을 얻게 된다.

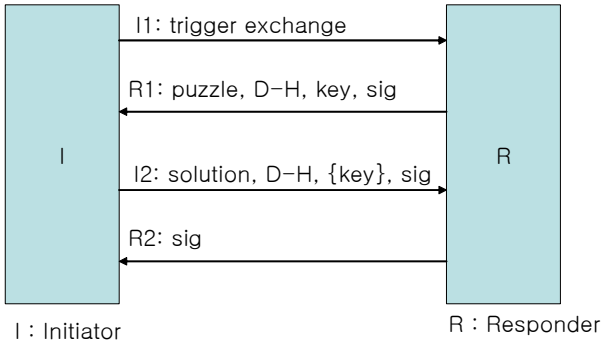

그림 1. HIP base exchange[2]

HIP에서는 이동성, 멀티홈, 동적 주소변경을 위해 랑데부 메커니즘을 제공하고 있는데, 이 경우 초기자는 응답자에게 직접 메시지를 보내는 것이 아니라 랑데부 서버에게 I1을 보내고 그것이 응답자에게 I1을 전달함으로써 HIP 연관을 얻게 된다.

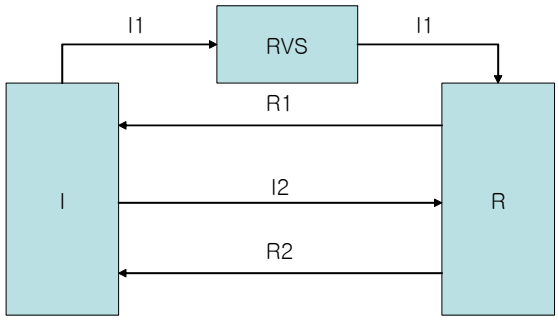

그림 2. RVS를 이용한 연관 설정 과정[2]

4. HIP와 DNS

.현재 인터넷 상에서 공식적으로 운영되고 있는 대표적인 등록 체계가 DNS인 관계로, 공개될 필요가 있는 호스트 식별자는 DNS에 저장하는 것이 가장 현실적인 대안으로 보여진다. 다음은 HIP의 연관 설정 과정에서 DNS가 참여하는 경우들을 보여주고 있다.

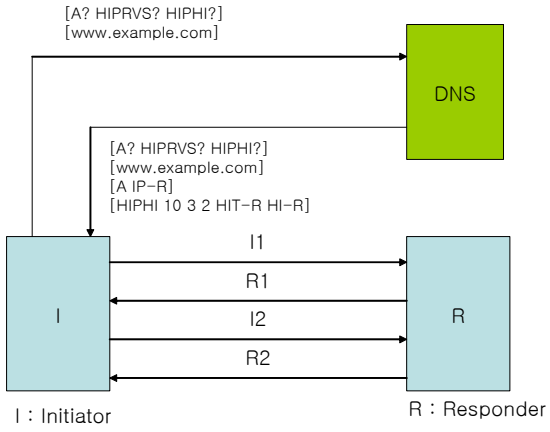

그림 3. 기본 교환에서 DNS의 참여[5]

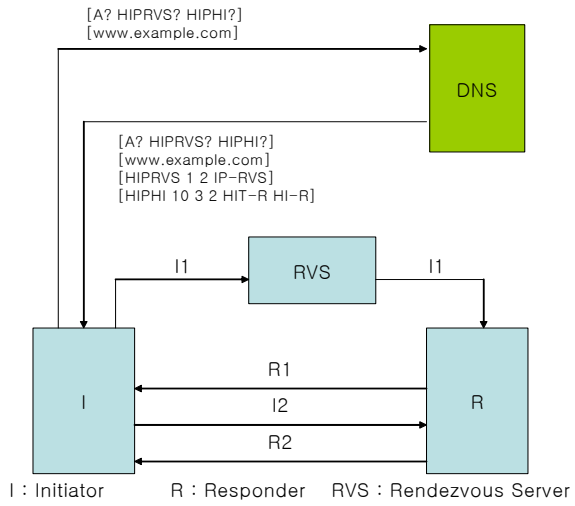

그림 4. 랑데부 서버가 있는 경우 DNS의 참여 [5]

DNS에서 저장할 공개된 호스트 식별자는 새로 정의하는 새로운 RR(Resource Record) 타입 HIPHI RR로 저장된다. 이러한 RR 타입은 IPSECKEY RR과 아주 유사하다.

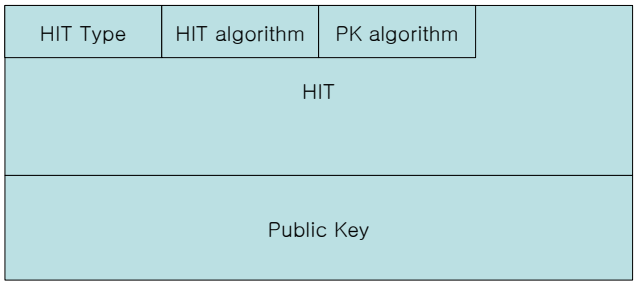

그림 5. HIPHI RR 형식[5]

5. 결론

HIP는 IP 주소가 가지고 있는 종단 식별자 기능과 위치 지시자 역할을 분리시키기 위한 시도로서 현재 IETF HIP WG에서 실험 문서를 작성 중이다. 현재 주로 작업 중인 것이 HIP 구조와 HIP 프로토콜 자체에 관한 문서 보완 작업이며, 그 외에도 랑데부 메커니즘과 DNS의 확장, HIP를 이용한 이동성, 멀티 홈 제공 시나리오 등이 연구 중이다.

HIP의 도입은 단순히 새로운 이름공간이 생긴다는 것뿐만 아니라 인터넷 전체 환경에도 큰 영향을 미칠 수 있다. 특히 현재의 IP 주소를 이용하는 코딩이 모두 HIP 연관을 이용하는 형태로 변화될 수도 있다.

호스트의 이름과 IP 주소를 분리하려는 HIP의 진행 방향을 주시할 필요가 있으며, 어느 정도의 의견이 모여지면 실제 도입을 추진하여 기술을 선점할 필요성도 엿보인다. 앞으로 이러한 HIP 관련 동향을 예의 주시하면서, BIND와 같은 공개 DNS 서비스 프로그램을 이용하여, 실험 환경을 구축하는 작업을 병행할 예정이다.

참고문헌

[1] http: //www.ietf.org/html.charters/hip-charter.html

[2] R. Moskowitz, P. Nikander, P. Jokela, T. Henderson, “Host Identity Protocol”, draft-ietf-hip-base-02.txt,February 21, 2005

[3] R. Moskowitz, P. Nikander, "Host Identity Protocol Architecture", draft-ietf-hip-arch-02, Jan. 11, 2004

[4] P. Nikander, J. Arkko, T. Henderson, "End-Host Mobility and Multi-Homing with the Host Identity Protocol", draft-ietf-hip-mm-01, Feb. 20, 2005

[5] P. Nikander, J. Laganier, "Host Identity Protocol (HIP) Domain Name System (DNS) Extensions", draft-ietf-hip-dns-01, Feb. 20, 2005

[6] J. Laganier, L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extension", draft-ietf-hip-rvs-01, Feb. 18, 2005

[7] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-14 (work in progress), June 2004.

[8] Eastlake, D. and C. Kaufman, "Domain Name System Security Extensions", RFC 2065, January 1997.

[9] Eastlake, D., "DSA KEYs and SIGs in the Domain Name System (DNS)", RFC 2536, March 1999.

[10] Eastlake, D., "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)", RFC 3110, May 2001.