通信情報保護學會誌
第 11 券 第 2 號, 2001. 4

IPSec 제품의 적합성 및 상호운용성 시험

이 광 수*, 신 은 경**, 이 홍 섭**

요 약

IPSec 제품은 호스트에 구현될 수도 있고, VPN 장비의 형태일 수도 있으며, 방화벽이나 라우터에 구현되어 있을 수도 있다. 또한, IPSec은 동일한 조직의 네트워크에서뿐만 아니라 독립된 조직의 네트워크들 사이에서도 사용될 수 있어야 하며, 따라서 여러 제품들끼리의 상호운용성이 그 사용에 있어서의 기본 요건이다. IPSec 제품의 상호운용성을 위해 IPSec 제품이 표준을 준수하고 있는지에 대한 적합성 시험과 IPSec 제품들 사이에 상호 운용 여부를 시험하는 상호운용성 시험이 필요하며, 본 논문에서는 IPSec 제품에 대한 적합성 시험과 상호운용성 시험 기술과 방법을 미국과 일본의 사례를 중심으로 조사한다.

Ⅰ. 서 론

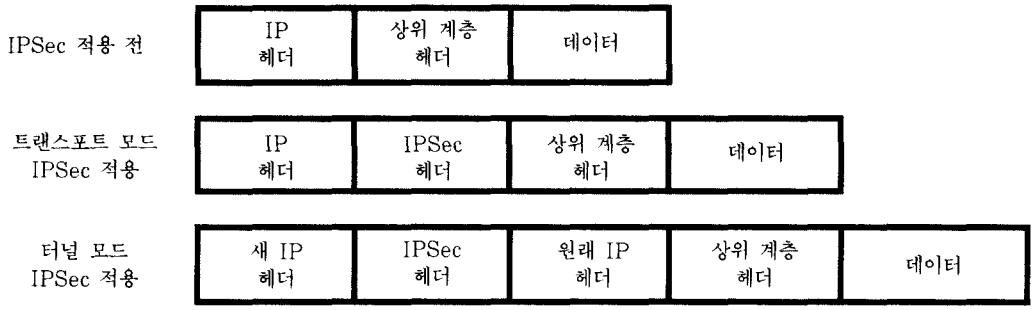
인터넷을 위한 네트워크 계층의 기본 프로토콜은 IP(Internet Protocol)이며, 이는 인터넷을 위한 모든 데이터를 전달하는 역할을 맡고 있는데, 현재의 IP 설계에는 보안 기능이 포함되어 있지 않다. IP에 보안 기능을 추가하기 위한 프로토콜이 IPSec(IP Security)이며, 제공되는 보안 기능에는 데이터 기밀성, 데이터 근원 인증, 데이터 무결성, 재전송 공격 방지, 제한적인 트래픽 플로우 기밀성, 접근 제어 등이 포함된다. IPSec은 네트워크 계층에서 구현되므로 인터넷의 응용 계층 또는 전송 계층 프로토콜과 독립적으로 작용하며, 모든 인터넷 서비스에 대해 이상의 보안 기능들이 편리하게 제공될 수 있다.

IPSec은 현재의 IP (버전 4) 상에서는 선택 사항으로 되어 있으며, 필요에 따라 구현되어 사용될 수 있다. 차세대 IP 프로토콜인 IPv6에서는 IPSec은 필수 구현 사항으로 되어 있다. IPSec은 호스트에서 구현될 수도 있고, 라우터나 방화벽 등의 네트워크 보안 게이트웨이에 구현될 수도 있다. 따라서, IPSec은 두 호스트 사이의 패킷 보호에 적용될 수도 있으며, 두 개의 보안 게이트웨이 사이에 적용될 수도 있고, 또한 호스트와 보안 게이트웨이 사이에 적용될 수도 있다.

IPSec은 보안 서비스를 제공하기 위해 암호 알고리즘들을 사용하며, 이들 암호 알고리즘은 키 공유 메커니즘을 필요로 한다. IPSec은 수동식 키 관리를 필수 구현 사항으로 정해두고 있으며, 이를 이용하여 IPSec 구현들 사이의 최소한의 상호운용성을 보장한다. 그러나, 수동식 키 관리 메커니즘은 대규모 네트워크에 적합하지 않을 뿐 아니라 재전송 공격 방지 등의 일부 보안 서비스를 제공하지 못하는 등의 단점이 있다. 따라서, 동적으로 통신 상대방을 인증하고, 보안 서비스를 협상하며, 공유 키를 생성하기 위한 자동적인 메커니즘이 필요하다. 현재, IETF의 IPSec 작업반[1]에서 정의한 자동식 키 관리 메커니즘에는 IKE(Internet Key Exchange)가 있으며, IPSec은 다른 메커니즘의 사용 가능성을 배제하지 않는다. 실제로, 최근 형성된 IETF의 KINK(Kerberized Internet Negotiation of Keys) 작업반[2]에서는 커버로스 기반의 키 공유 메커니즘을 개발하고 있다.

IPSec은 본질적으로 통신 프로토콜이며, 따라서 IPSec 제품들 사이의 상호운용성은 IPSec의 채택을 위한 기본 요건이다. IPSec 제품의 상호운용성을 위해 IPSec 제품이 표준을 준수하고 있는지에 대한 적합성 시험과 IPSec 제품들 사이에 상호 운

* 숙명여대 정보과학부 교수 (rhee@sookmyung.ac.kr)
** 한국정보보호센터



〔그림 1〕 IPSec 운용 모드와 패킷 구조

용 여부를 시험하는 상호운용성 시험이 미국과 일본을 중심으로 수행되어 오고 있다. 본 논문에서는 IPSec 제품에 대한 적합성 시험과 상호운용성 시험 기술과 방법을 미국과 일본의 사례를 중심으로 조사한다.

본 논문의 남은 부분은 다음과 같이 구성된다. 2절에서는 IPSec 프로토콜을 간략히 소개한다. 3절에서는 IPSec 제품에 대한 시험 사례들을 조사한다. 4절에서는 결론을 제시한다. IPSec이 적용될 때, IPv4와 IPv6에서 패킷 구조는 달라지지만, 본고에서는 이들의 미세한 차이는 다루지 않으며, 남은 부분의 설명에서는 IPv4를 기준으로 한다.

II. IPSec 개요

IPSec이 IP 데이터그램 또는 상위 프로토콜 데이터를 보호하기 위해 사용하는 프로토콜에는 인증 헤더(AH: Authentication Header)와 캡슐화 보안 페이로드(ESP: Encapsulating Security Payload) 두 가지가 있다. AH는 데이터 근원 인증, 데이터 무결성, 재전송 공격 방지 등의 보안 서비스를 제공한다. ESP는 AH가 제공하는 서비스들과 데이터 기밀성, 제한적인 트래픽 플로우 기밀성을 추가로 제공한다. AH와 ESP가 공통적으로 제공하는 서비스들의 경우 두 프로토콜에 조금의 차이가 있다.

1. IPSec 구조

IPSec의 구조 문서인 RFC2401[3]은 IPSec이 제공하는 보안 서비스와 IPSec의 작동 방법 및 작동 위치, 패킷의 구성과 처리 방법, 보안 정책과의 연동 등을 기술한다. IPSec 프로토콜은 전체 IP 패킷을 보호하기 위해 사용될 수도 있고, 상위 프로토콜 데이터만을 보호하기 위해 사용될 수도 있다. 이 중 상위 프로토콜 데이터만을 보호하는 IPSec 운용 모드를 트랜스포트 모드라고 하며, 전체 IP 패킷을 보호하는 운용 모드를 터널 모드라고 한다. 그림 1은 IPSec이 적용되지 않은 IP 패킷, 트랜스포트 모드의 IPSec이 적용된 IP 패킷, 터널 모드의 IPSec이 적용된 IP 패킷을 보여 주고 있다. 트랜스포트 모드에서는 IPSec 헤더가 원래의 IP 헤더와 상위 프로토콜 헤더 사이에 들어간다. 터널 모드의 경우 원래의 IP 헤더도 IPSec에서 데이터처럼 취급되며, IPSec 처리 결과 별도의 새로운 IP 헤더가 만들어진다. 트랜스포트 모드는 IPSec의 양 종단점이 호스트일 경우에만 사용될 수 있으며, 터널 모드는 양 종단점이 호스트이건 보안 게이트웨이이건 무관하게 사용될 수 있다.

IPSec 패킷의 작성과 복원을 위해 그 패킷에 적용되는 보안 서비스와 암호키를 해당 트래픽에 연계시키는 방법이 필요하며, IPSec에서는 이러한 정보를 보안 연계(SA: Security Association)라는 개념으로 표현한다. SA는 일방성이다. 즉, 두 시스템 A와 B가 IPSec 통신을 하고 있다면, A에서 B의 방향으로 적용되는 SA와 B에서 A의 방향으로 적용되는 SA가 별도로 존재한다. 그리고, 하나의 SA는 AH와 ESP 프로토콜 중 하나만 지정할 수 있다. 따라서, 경우에 따라서는 두 종단점 사이에 두 개 이상의 SA가 필요할 수도 있으며, 이 경우 함께 사용될 여러 개의 SA들을 묶어 일컫는 표현으로 SA 번들이라는 용어를 사용한다.

SA가 수동식으로 설정되면 다시 변경될 때까지 유효 기간 없이 계속 사용될 수도 있다. 자동식 SA 관리 메커니즘에 의해 설정될 때는 유효 기간이 정해지며, 유효 기간이 만료되면 자동적으로 다시 설

정되며, 이는 재전송 공격 방지 서비스에 있어 중요하다.

IPSec 구현 시스템은 통신 보안 정책을 표현하고 있는 데이터베이스를 유지하는데, 이를 SPD (Security Policy Database)라고 부르며, 통신 상대 호스트 또는 네트워크에 따라 적용되어야 할 보안 서비스들을 규정하고 있으며, 보안 서비스의 구체적 내용은 적용될 SA들을 사용하여 표현한다. 현재 유효한 SA들은 별도의 SA 데이터베이스에 저장되어 있는데, 이를 SAD라고 부른다. SPD의 각 항은 SAD의 SA들을 가리키는 포인터를 갖는데, 이 포인터는 SPI(Security Parameter Inde)라고 불린다.

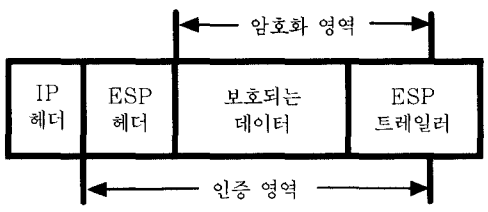
2. ESP - 캡슐화 보안 페이로드

ESP는 RFC 2406[4]에 정의되어 있으며, 인증과 기밀성 모두를 제공할 수 있다. ESP의 보안 서비스 제공을 위해 IP 헤더와 상위 프로토콜 헤더 사이에 ESP 헤더를 그림 2에서와 같이 끼워 넣으며, IP 패킷 끝에 ESP 트레일러를 덧붙인다.

ESP의 암호화 영역은 상위 프로토콜 전체와 ESP 트레일러의 일부이며, 인증 영역은 ESP 헤더까지도 포함한다. 인증 데이터는 ESP 트레일러 부분 중 인증 영역에 포함되지 않는 부분에 들어가게 된다.

ESP는 인증과 기밀성 제공을 위해 각기 적당한 암호 알고리즘을 선택하는데, 이 때 NULL 알고리즘[5]을 선택함으로써 해당 서비스를 포기할 수 있다. 그러나, 두 가지 서비스 모두를 포기하는 것은 허용되지 않는다.

ESP에서 암호화를 위해 사용되는 알고리즘은 모두 CBC(Cipher Block Chaining) 모드를 사용하며, DES, 3DES, CAST-128, Blowfish, IDEA, RC5 등의 사용이 규정되어 있으나, 다른 알고리즘의 사용이 배제되지는 않는다[6,7,8].



〔그림 2〕 ESP로 보호되는 IPSec 패킷

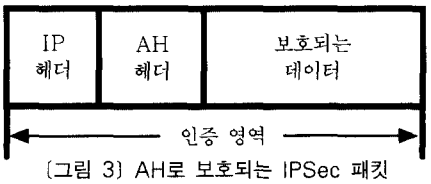
ESP의 인증 알고리즘은 암호키를 사용하는 MD5[9], HMAC-MD5[10], 그리고 해쉬 출력 결과를 96비트만 남기고 절삭하여 사용하는 HMAC-MD5-96[11], HMAC-SHA-1-96[12], HMAC-RIPEMD-160-96[13] 등이 규정되어 있다.

3. AH - 인증 헤더

인증 헤더에 관한 사항은 RFC 2402[14]에 규정되어 있다. 인증 헤더는 기밀성을 제공하지 않는 대신에 그림 3과 같이 인증 영역이 ESP의 인증 영역에 포함되어 있지 않던 IP 헤더가 포함되어, 출발지와 목적지 IP 주소 등의 정보도 보호될 수 있다. 이 때, IP 헤더의 모든 필드가 보호 대상은 아니며, 전송 중에 변경되지 않는 부분만이 보호 대상이다. 또한, 지역 정책에 의해 암호화 기능을 갖춘 ESP의 사용이 규제되는 상황에서 AH가 사용될 수도 있을 것이다. 인증 헤더에서 사용되는 암호 알고리즘은 ESP에서의 인증 알고리즘과 같다.

4. IKE - 인터넷 키 교환 프로토콜

IPSec은 외부로 보낼 패킷을 위한 보안 서비스를 SPD에서 찾으며, 해당 SPD 항은 SA 번들을 가리키도록 되어 있다. 이 때, SA 번들을 가리키는 필드가 비어 있으면, 통신 상대방과의 SA 협상이 필요하며, 이 때 IKE 프로토콜이 사용된다. IKE 프로토콜은 두 단계로 이루어져 있다. 첫 번째 단계는 IKE의 협상 내용을 보호하기 위한 보안 패러미터의 교환을 위한 단계이며, 충분한 보호를 제공하며 효율성이 다소 떨어지는 메인 모드와 신원 보호를 제공하지는 못하지만 메시지 교환 회수를 줄이는 공격적 모드가 사용된다. 두 번째 단계가 실제로 IPSec에서 사용될 보안 서비스, 암호 알고리즘, 키 등의 정보를 협상하고 교환하는 단계이며, 퀵 모드라고 불리는데, 이 통신 내용은 첫 번째 단계에서 협상된 보호 메커니즘에 의한 보호를 받는다. IKE



〔그림 3〕 AH로 보호되는 IPSec 패킷

는 RFC 2409[15]에 규정되어 있으며, IKE 교환의 프레임워크는 RFC 2408[16] ISAKMP(Internet Security Association and Key Management Protocol)를 사용한다.

Ⅲ. IPSec 제품 시험 방법

IPSec 제품에 대한 인증이나 상호운용성 시험을 수행하고 있는 곳은 ICSA 시험소와 NIST 두 곳이며, IPSec 기반의 VPN 제품에 대한 표준적합성 및 상호운용성에 대한 시험은 VPNC에 의해 수행되고 있다. 일본의 TAHI 프로젝트는 IPSec 적합성과 상호운용성 시험을 위한 시험 스위트와 시험 도구 등을 개발하고 있다. IETF에서는 IPSec과 IKE를 연동하는 상호운용성 시험을 위한 표준 절차를 개발하고 있다.

1. ICSA의 IPSec 제품 인증 프로그램[17]

ICSA IPSec 제품 인증 프로그램은 IPSec 제품에 대한 상호운용성 시험과 그 제품이 기밀성, 데이터 무결성, 인증 등의 보안 서비스를 적절히 제공한다는 것을 평가 인증하는 것을 목적으로 하고 있다.

IPSec 제품은 우선 ICSA 암호 제품 인증을 받아야 한다. 그리고, 보안 정보 관리 및 암호키 설정을 위한 IKE를 적절히 지원하는지를 검사하는데 메인 모드와 퀵 모드 모두 시험된다. CA와의 연동 작용이나 기타 IPSec 프로토콜의 기본 사항들을 지원하는지가 검사되며, 다음으로 기존 인증된 IPSec 제품들과의 상호운용성 시험을 거치게 된다. 평가 기준은 버전 1.0, 버전 1.0A을 거쳐 현재 CA 처리 기능 시험이 추가된 버전 1.1에 이르고 있다. 그리고, 강도가 높은 암호 알고리즘 채택을 평가하는 SCr(Strong Crypto) 기준, 압축 선택 사항 구현 여부에 대한 평가인 EFn (Enhanced Functionality) 기준, 인증서 처리 기능이 강화되어 있는지를 평가하는 ECA (Enhanced Certificate Authority) 기준 등이 있다.

1.1 IPSec 제품 인증 기준

기본 평가 기준인 버전 1.0A에서는 다음의 내용을 검증한다.

- ○ 보안 연계 관리 및 암호키 설정을 위한 IKE를 적절히 지원해야 한다.
- ○ IPSec 프로토콜의 기본 사항들을 지원하며, ICSA에 의해 인증된 다른 제품들과 상호운용되어야 한다.
- ○ 알고리즘, 구현, 블랙 박스 시험 등에서 ICSA 암호 제품 인증 요건을 만족해야 한다.

버전 1.0A 인증 기준을 만족하는 제품은 강도 높은 암호 알고리즘 채택을 평가하는 SCr 기준, 압축 선택 사항 구현 여부에 대한 평가인 EFn 기준 등에 대한 시험을 추가로 받을 수 있다. SCr 기준에 추가되는 시험 항목은 IKE 메인 모드에서의 DH 그룹 2 키 교환과 3DES-CBC 데이터 암호화, IKE 퀵 모드에서의 변환/속성에서 3DES/ MD5/SHA1의 지원, ESP에서의 3DES-CBC에 대한 필수적인 지원과 IDEA, CAST-128, RC5-128 등에 대한 선택적 지원 등이다.

버전 1.0A 인증 기준을 만족하는 제품은 또 인증기관과의 기본적인 연동에 대한 지원을 시험하는 버전 1.1에 대한 시험을 추가로 받을 수 있으며, 버전 1.1 인증 기준을 만족하는 제품은 강화된 인증기관과의 연동 요구 사항에 대한 지원을 시험하는 ECA 기준에 대한 시험을 추가로 받을 수 있다. ECA 기준에 추가되는 시험 항목은 인증서 검증, 인증서 경로 처리 (계층 구조나 교차 인증 포함), CRL 요청에서 LDAP 버전 2 지원 등이다.

1.2 IPSec 제품 시험 가이드

IPSec 제품 시험 가이드는 인증 시험에 앞서 제품 개발업체가 작성하여 ICSA에 제품과 함께 제출하는 문서이며, 그 내용은 다음과 같다.

- ○ 회사 연락처
- ○ 제품 마케팅 및 특성에 관한 자료
- ○ 암호 구현 관련 자료
- ○ IPSec 기능 지원에 관한 자료
  - ■ IKE
  - ■ IP ESP
  - ■ 게이트웨이 사이의 터널 모드와 게이트웨이와 호스트 사이의 터널 모드
  - ■ 호스트와 호스트 사이의 전송 모드

■ 버전 1.1의 경우 다음과 같은 CA와의 연동
- CA 루트 인증서
- RSA 서명
- RFC 2314의 PKCS #10 인증서 요청
- RFC 2315의 PKCS #7 인증서 수령
- RFC 2510의 인증서 관리 프로토콜
- RFC 2511의 인증서 요청 메시지 양식
- 인증서 저장소
- CRL 요청, 수령, 저장

1.3 IPSec 제품 시험 절차와 결과

IPSec 제품 시험 절차는 두 단계로 구성된다.

첫 번째 단계는 친숙화 단계이며, 다음의 작업이 수행된다. 이 단계에서는 제품 개발업체의 참여를 요청할 수 있다.

○ ICSA 시험 요원들이 제품 개발업체, 제품, 관련 기술과 제품의 구성 요소들을 파악한다.
○ 개발업체에서 작성하여 제출한 제품 시험 가이드의 내용을 검토한다.
○ 제품의 운용성, 시험 장비와의 인터페이스, 설치 유의 사항 등을 점검한다.
○ 제품에 대한 적응 훈련의 절차와 지침을 마련한다.
○ 디버깅 절차를 마련한다.
○ 여러 가지 제품의 설치 구성을 점검하고 잘못된 부분을 교정한다.

두 번째 단계는 인증 시험 단계이며, 시험 기준의 만족 여부를 시험한다. 이 단계에서는 제품 개발업체는 직접 참여하지는 않으나 시험 도중에 발생하는 기술적 문제 등에 대한 문의나 장비의 추가 요청 등에 응할 수 있어야 한다. 다음의 시험 절차는 인증 기준 1.1에 대한 것이며, IKE 1단계, IKE 2단계, CA 연동 시험 등을 시험한다.

IKE 1단계

○ 인증을 위한 RSA 서명 모드
■ 루트 인증서
■ 교환된 인증서 검증
■ CRL 요청, 수령, 저장
■ 디지털 서명을 위한 keyUsage 비트 값 점검
○ 인증서 유효일자 시험
○ ISAKMP SA 유효일자가 협상 당사자들의 인증서 유효일자를 초과하지 않아야 한다.
○ 인증서 용도 검증
■ 인증서는 사전에 로드될 수 있다.
■ 인증서 사용자명과 사용자 대체명 확장 필드
- IPv4 주소
- DNS
- RFC 822의 전자우편 주소에 쓰이는 도메인 이름

IKE 2단계

○ ISAKMP SA 유효일자가 협상 당사자들의 인증서 유효일자를 초과하지 않아야 한다.

인증기관과의 연동 시험

○ 최소한 한 개의 루트 인증서를 안전하게 로드할 수 있어야 한다.
○ PKCS #7/#10 패킷을 이용하는 경우와 업체의 고유한 인증서 전송 방식을 이용하는 경우들에 대하여 인증서 등록 절차를 제대로 수행되어야 한다.
○ 다음과 같은 방법들을 사용하여 CRL 처리를 지원해야 한다.
■ RFC 2585의 HTTP/FTP 기반의 CRL 배포
■ LDAPv2
■ 네트워크 관리 스테이션에 의한 제어

시험에 사용되는 시나리오는 3가지이며, 각 시나리오에 대하여 ESP 터널 모드와 X.509 인증서를 사용하는 RSA 서명 방식의 IKE가 시험된다.

○ 시나리오 1
■ 게이트웨이 사이의 전송
■ ID: IPv4 주소, FQDN (RFC 822 이름은 선택 사항)
■ 프록시 ID: IPv4 주소 또는 서브넷 (EFn 검사 때는 range도 사용)

○ 시나리오 2
■ 게이트웨이와 호스트 사이의 전송

- ID: IPv4 주소, FQDN, RFC 822 이름 (게이트웨이의 경우 RFC 822 이름은 선택사항)
- 프록시 ID: IPv4 주소 또는 서브넷 (EFn 검사 때는 range도 사용, 주소는 호스트에만 사용)

○ 시나리오 3
- 호스트 사이의 전송
- ID: IPv4 주소, FQDN, RFC 822 이름
- 프록시 ID: IPv4 주소

시험에 합격된 제품에 한해 그 결과가 웹사이트를 통해 공개되는데, 결과 보고에는 시험 플랫폼, 설정 환경, 시험 중에 발생한 사항들에 대한 메모, 암호 제품 인증 결과, 다른 인증 IPSec 제품들과의 제품별 상호운용성 결과 등이 포함되어 있다. 다른 제품과의 상호운용성 결과에는 시험시 발생된 문제 사항들에 대한 메모가 포함된다.

2. NIST의 IPSec WIT[18]

NIST의 IPSec WIT는 IPSec 제품이 NIST의 IPSec 참조 구현 Cerberus와 IKE 참조 구현 PlutoPlus과 상호운용되는지의 시험을 웹을 통해 할 수 있게 만든 시험기이다. 시험을 위해 필요한 보안 연계값은 수작업으로 설정될 수도 있고 IKE 흥정에 의해 설정될 수도 있다. 시험의 결과는 웹 브라우저로 즉시 확인하거나 전자 우편으로 보내진다. 시험 시스템은 시험 엔진과 지원 프로그램, 시험 스위트 등으로 구성되어 있다.

2.1 Cerberus

NIST Cerberus는 리눅스 플랫폼용으로 개발된 IPSec 참조 구현으로 다음의 문서들에 기반한 ESP와 AH를 구현하고 있으며, AES 알고리즘들도 지원하고 있다: RFC 1828, 1829, 2085, 2104, 2401-2406, 2411, 2451, AES 관련 IPSec 인터넷 드래프트.

Cerberus는 호스트와 호스트, 호스트와 라우터, 라우터와 라우터 사이의 IPSec 서비스를 제공하고 있다. 그 소프트웨어 구조는 4개의 요소로 구성되어 있는데, 보안 연계 데이터베이스(SAD) 관리 루틴, IPSec 프로토콜 엔진, 암호 변환 및 알고리즘 모듈, IP 인터페이스 등이며, 다음 페이지의 그림에서처럼 다른 네트워크 모듈들과 연동하고 있다.

SAD 관리 루틴은 SAD에 대하여 SA 항목의 추가, 삭제, 검색 등의 요구를 처리한다. 또한 SAD 관리 루틴은 시스템 정책에 대한 관리 기능도 보유하고 있다.

IPSec 프로토콜 엔진은 입력 처리 모듈과 출력 처리 모듈의 두 부분으로 구성되며, IP가 데이터를 전송해 내보내기 전에 출력 처리 모듈을 거치게 되어 있으며, 또 외부로부터 수신된 데이터는 먼저 입력 처리 모듈을 거치게 되어 있다.

변환 모듈은 암호 알고리즘들과 밀접한 연관을 맺고 있으며, IPSec에 의해 보호되는 패킷 캡슐화 및 캡슐 제거에 필요한 기능들을 제공하고 있다.

SADB에 대한 추가 작업이나 삭제 복원 작업, 출력 패킷에 IPSec 프로토콜 데이터를 만들어 넣는 일, 수신된 패킷에서 IPSec 프로토콜 데이터를 제거하는 작업 등을 수행한다.

지원되고 있는 암호 알고리즘은 blowfish-CBC, DES-CBC, RC5-CBC, IDEA-CBC, MD5, SHA-1과 AES 알고리즘 (MARS, RC6, Rijndael, Serpent, Twofish) 등이다.

2.2 PlutoPlus

PlutoPlus는 IKE에 대한 참조 구현이며, 다음의 문서들에 기반하고 있다: RFC 2401, 2407-2409, 2411, 2412.

PlutoPlus는 다음과 같은 용도를 위하여 만들어졌다.

① 사용자들이 IPSec을 실험할 수 있게 한다.
② IPSec의 배치를 용이하게 하며 사용을 촉진시킨다.
③ IPSec 상호운용성 시험을 가능하게 한다.

PlutoPlus는 완성품으로 사용될 수 있는 성능을 보유하고 있지 않으며, 특히 대규모의 안정성을 요하는 네트워크에서의 사용은 적합하지 않다. 그러나, 소규모의 실험적인 네트워크에서는 사용할 만하다. PlutoPlus는 컴파일 옵션의 변경으로 여러 가지 실행모드를 선택할 수 있는데, 진단 기능이나 선택 기능의 채택, 그 외 다른 특별한 실행 모드 등이 있다.

3. VPNC IPSec 적합성 시험

1999년 구성된 VPNC는 현재 31개의 VPN 개발업체가 참여하고 있다[19]. 컨소시엄의 주요 목표는 VPN 제품, 기술, 관련 표준에 대한 일반의 이해를 고양시키는 것과 함께 VPN 제품들의 상호운용성을 증진하자는 것이었다. 특히, 상호운용성 시험 결과를 나타내는 차트를 만들자는 것이 초기의 의도였으나, 몇 가지 기술적인 어려움에 봉착하여 지금은 표준적합성 시험 정도로 후퇴한 입장을 취하고 있다.

VPNC에서는 표준적합성과 상호운용성을 다음과 같이 구분하고 있다. 표준적합성 시험에서는 지정된 한 두 개의 참조 구현과 상호운용되는지를 시험한다. 반면에, 상호운용성 시험에서는 다른 상용 제품들과의 상호운용을 시험하며, 궁극적으로는 시험 대상에 포함된 모든 제품들과의 시험을 거치게 된다.

VPN 제품들 사이의 상호운용성 확보의 어려움은 다음의 사례들에 의해 드러난다.

- 제품 A가 착신 게이트웨이이고 제품 B가 송신 게이트웨이일 때는 두 제품이 문제없이 상호연동하다가, 역할이 반대로 바뀔 경우 더 이상 상호연동하지 않는 경우가 있다.
- 제품 C와 제품 D가 상호운용되었다가, 제품 E와의 상호운용을 위해 제품 C를 변경한 후 제품 C와 제품 D 사이의 상호운용성을 잃게 되는 경우가 있다.
- 제품 F와 제품 G는 디폴트 설정 상태에서 상호운용되는 것으로 검증되었다. 그러나, 제품 H와의 상호운용을 위해 제품 F의 설정을 일부 변경했을 때, 제품 F와 제품 G가 더 이상 상호연동되지 않는 경우가 있다. 상황에 따라서는, 제품 F, G, H들이 설정에 따라 서로 두 개씩은 상호연동되지만 세 개의 제품을 동시에 사용할 있는 설정 상태를 찾을 수 없는 경우도 있다.

이상의 사례들은 VPN 제품에 있어 표준적합성이 상호운용성을 보장하지 않음을 의미하며, 상호운용성 증진을 위해 참여 업체들이 협력하는 자세로 자사 제품들을 고쳐 나가는 것이 필요한데, 위의 사례에서 보듯이 어느 제품을 어떻게 고쳐야 최대한의 상호운용성을 얻게 될지 등에 대한 결정은 어렵고도 미묘한 문제이며, 이의 해결이 단기간 내에 이루어질 수 없음을 인식한 VPNC는 우선 가능한 표준적합성 시험을 수행하고, 상호운용성을 뒤로 미룬 것이다. 또한, 상호운용성 시험은 많은 제품들 사이에서 수행되어야 하는데, 두 제품 사이의 시험도 여러 가지 설정 상태에서 수행되어야 하므로 전체적으로 많은 시간이 소요된다.

VPNC의 표준적합성 시험은 IPSec ESP 터널링에 대한 기본 시험과 추가적인 IPSec 기능들에 대한 시험들로 나누어져 있으며, 현재는 기본 시험과 Rekeying 시험만 수행되고 있다. 기본 시험에서는 현재 OpenBSD[20]와 KAME[21] 두 개의 참조 구현으로 구성된 각각의 게이트웨이 뒤의 서버에 도달할 수 있는지를 시험하며, 현재 9개의 VPN 제품이 기본 시험에서 합격하였다. Rekeying 시험은 자동 Rekeying 기능과 PFS (Perfect Forward Secrecy) 기능을 시험하며, 시험 방법은 기본 시험과 유사하다. 현재 Rekeying 시험에 합격된 제품은 한 개이다.

4. 일본의 TAHI 프로젝트[22]

TAHI 프로젝트는 차세대 인터넷 IPv6의 개발과 검증 기술제공을 목적으로 하는 연합 프로젝트로서 동경대학교, YDC주식회사, 요코가와전기주식회사 등이 참가하고 있으며, KAME 프로젝트의 IPv6 참조구현을 테스트 플랫폼으로 활용하고 있다. TAHI 프로젝트는 IPSec과 관련된 시험 기술로 IPSec 적합성과 상호운용성 시험을 위한 시험 스위트와 관련 도구 등을 제공하고 있으나, IKE에 관한 부분은 전혀 다루고 있지 않다.

4.1 IPSec 적합성 시험

적합성 시험 대상 IPSec 표준은 다음 9개의 RFC들에 명세되어 있다: RFC 2401-2406, 2410, 2451, 2857.

IPSec은 다음과 같은 요소들의 다양한 조합에 의해 많은 시험 케이스가 발생한다.

- 구현 장비
  - 호스트
    - 터널 모드
    - 트랜스포트 모드

- 라우터
- 적용 서비스:
  - AH
  - ESP: 인증 기능 유/무
- 처리 위치: 인바운드와 아웃바운드
- 암호 알고리즘의 종류
  - AH: HMAC-MD5, HMAC-SHA-1, HMAC-RIPEMD-160
  - ESP: NULL, DES-CBC, 3DES-CBC
- 기타
  - SA 번들의 사용
  - 단편화 헤더 포함 여부
  - AH에서의 IP 헤더 변경 탐지 여부 조사
  - AH와 ESP의 조합
  - 패딩에 관한 시험

적합성 시험 스위트에서는 각각의 시험 케이스에 대해 정확한 상황과 시험을 위한 구체적인 시험 데이터, 시험 장비와 시험 대상 장비의 배치 등을 규정하여야 하며, 자동적으로 시험이 이루어질 수 있도록 시험도구가 마련되어 있어야 한다. TAHI 프로젝트에서는 시험에 사용될 패킷을 생성하기 위한 C 코드가 제공되며, 패킷을 발생시켜 시험 대상 장비에 전달하고 그 결과를 수신하여 점검하기 위한 perl 코드로 작성된 패킷 발생기가 제공된다. 또한, 이들 시험 케이스들을 차례대로 자동 처리하고 그 결과를 보고할 수 있는 종합적인 시험 평가 도구가 사용된다. 또한, 패킷 생성 데이터의 계산을 위해서는 IPSec 참조 구현이 사용된다.

4.2 상호운용성 시험 시나리오

상호운용성 시험에서는 라우터와 호스트, 그리고 보안 서비스의 조합 등에 의해 다음과 같은 기본적인 시험 케이스들이 발생하며 이들 각각에 대한 시험을 차례로 수행해야 한다. ([AH]는 AH 헤더, [ESP]는 ESP 헤더, [IPn]은 n 번째 IP 헤더를 나타낸다.)

- 라우터 (보안 게이트웨이)
  - 터널 모드 AH
    [IP2][AH][IP1]
  - 터널 모드 ESP
    [IP2][ESP][IP1]
  - 두 개의 보안 게이트웨이에 의한 이중 터널
    [IP3][AH][IP2][AH][IP1]
    [IP3][AH][IP2][ESP][IP1]
    [IP3][ESP][IP2][AH][IP1]
    [IP3][ESP][IP2][ESP][IP1]
  - 트랜스포트 모드 AH + 터널 모드 ESP
    [IP2][AH][ESP][IP1]

- 호스트
  - 트랜스포트 모드 AH
    [IP][AH]
  - 트랜스포트 모드 ESP
    [IP][ESP]
  - 트랜스포트 모드 AH + ESP
    [IP][AH][ESP]
  - 터널 모드 AH
    [IP2][AH][IP1]
  - 터널 모드 ESP
    [IP2][ESP][IP1]
  - 다른 호스트와의 트랜스포트 모드 AH + 터널 모드 ESP
    [IP2][AH][ESP][IP1]
  - 다른 호스트와의 터널 모드 (AH 또는 ESP) + 트랜스포트 모드(AH 또는 ESP)
    [IP2][AH][IP1][AH]
    [IP2][AH][IP1][ESP]
    [IP2][ESP][IP1][AH]
    [IP2][ESP][IP1][ESP]

5. IETF IPSec/IKE 상호운용성 시험 절차[23]

IPSec 게이트웨이, 클라이언트, 종단 시스템 등의 운용은 간단하지 않으며, 시스템 설정과 관련된 여러 가지 문제들이 있으며, 일반 네트워크 노드 진단 기술로는 접근하지 어려운 측면이 있다. 또한, IPSec 게이트웨이들이 제공하는 다양한 설정 옵션과 일관된 진단의 결여로 인해 이들의 운용은 더욱 어려워진다. 연결 실패의 경우 그 원인이 네트워크 기본 연결에 있는지, IPSec에 있는지, 또는 IKE가 문제인지 등의 구분도 일반 네트워크 관리자로서는 판단하기 어렵다.

서로 다른 네트워크 제품들 사이의 상호운용성 시험은 기본적으로 복잡한 작업이며, IPSec의 경우는 특히 보안 기능과 상호 연동되어야 할 IKE와 IPSec

두 개의 프로토콜이 있음으로 인해 더욱 복잡해지며, 이들을 고려한 시험 방법이 필요하다.

이 절에서는 두 게이트웨이 사이의 상호운용성 시험을 위한 절차를 제시하며, 클라이언트 사이의 상호운용성 시험은 설정 항목의 수가 게이트웨이의 경우보다 적기 때문에 조금 더 단순해진다. 게이트웨이 사이의 시험 환경은 그림 4와 같이 주어지며, 그림에서 Ix, Ox는 각각 게이트웨이에서의 내부 인터페이스와 외부 인터페이스를 나타낸다.

시험은 모두 11개의 단계를 거치며, 이들 일부에서 행해지는 ping 시험은 6개 크기의 ICMP 메시지를 순서대로 포함하는데, 그 크기는 각각 64 바이트, 256 바이트, 512 바이트, DF=1(단편화 금지)인 1480 바이트, 2048 바이트, 다시 64 바이트이다. 이 결과로 단편화된 ICMP와 단편화되지 않은 ICMP 테스트를 모두 포함한다. 암호화 알고리즘으로는 3DES-CBC가 사용되며, 해쉬 알고리즘으로는 SHA-1이 사용된다.

ⓐ **시험을 위한 시스템 준비**

앞의 그림 4와 같이 네트워크를 구성하고 통신 요청자(initiator)가 될 게이트웨이 G1을 정한다.

ⓑ **ICMP ping 시험**

G1에서 G2쪽으로 ICMP ping 메시지들을 보낸 후 G2쪽에서 ping 메시지 도달 여부를 검사한다. 또, G1에서 응답 메시지를 검사하며, 이 과정에서의 실패는 기본 네트워크 연결의 실패로 진단한다.

특정 크기의 메시지 전달의 실패는 다른 터널이나 침입차단시스템, NAT 장비, 또는 다른 IPSec 장비의 존재 등으로 진단될 수 있다.

ⓒ **수동식 키 시험**

수동식 키를 위한 SPD를 설정하고, 진단이 쉬운 AH를 먼저 사용하여 점검하며, ESP 점검은 그 다음에 수행한다. 게이트웨이 G1의 SPI는 0x00001111, G2의 SPI는 0x00002222로 하며, G1의 키는 0x0000ffff0000ffff, G2의 키는 0x1111ffff1111ffff로 둔다.

운용 모드는 터널 모드이다. 출발지 주소는 I1이 되며, 목적지 주소는 I2이다. ESP의 경우 G2쪽에서는 패킷이 암호화되어 있는지 점검하며, G1쪽에서는 복호화되어 있는지를 점검한다.

이 단계의 완료 후에는 G1과 G2에서 수동식 키 항들을 제거한다.

ⓓ **IKE전 통지**

IKE를 사용하지 않은 상태에서 G1에서 G2쪽으로 ISAKMP 통지 페이로드를 보내본다. G2쪽에서 이 패킷이 수신되는지, 또 그 페이로드가 UDP 포트 500에 도달하는지를 점검한다.

ⓔ IKE 단계 1에서의 사전 공유된 비밀 키 사용 시험

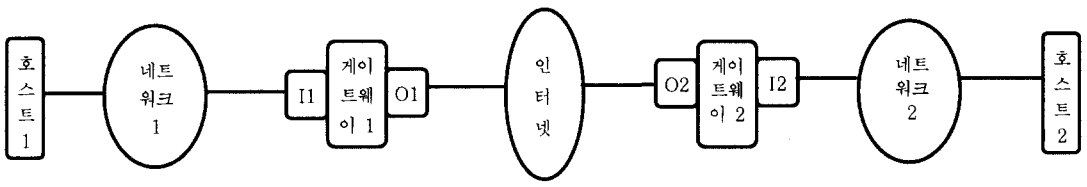
G1과 G2 사이에 사전 공유된 비밀키로 IKE 설정을 하고, AH와 ESP를 시험하며, Diffie-Hellman Group 2를 사용해 본다.

2 단계의 협상을 1 단계 ISAKMP 메시지 보호 기능을 이용해 수행 해 본다. G2에서 페이로드가 제대로 도달하는지, 암호화가 된 상태인지, 메시지 유형은 맞게 되어 있는지 등을 점검한다.

ⓕ IKE 단계 2에서의 사전 공유된 비밀 키 사용 시험

앞의 단계와 동일한 설정을 이용하여 2 단계 메시지 교환을 실행해 본다. SA는 출발지는 I1과 호스트 H1을 포함하는 네트워크 주소를 사용하며 원격지 주소는 I2와 H2를 포함하도록 한다.

ping 시험을 통해 IKE 2 단계의 결과를 사용하



〔그림 4〕 게이트웨이간의 시험 환경

는 보호 기능의 작동 여부를 시험하며, 이 단계의 완료 후에는 사전 공유된 비밀키 항들은 지운다.

⑧ 공개키 인증

G2의 자체 서명된 인증서를 G1의 저장소에 두고, G1의 자체 서명된 인증서를 G2의 저장소에 둔다. G1과 G2 사이의 IKE는 서명 인증 상태로 둔다.

ping 시험을 수행하며, 이 단계의 완료 후에는 여기서 사용된 자체 서명된 인증서들은 각 저장소에서 지운다.

⑩ 잘 알려진 공개키 시험

잘 알려진 공개키들을 G1과 G2의 저장소에 두고, 대응되는 개인키들을 이용해 적절한 인증서들을 생성한다. 단계 ⑧와 같이 진행하며, 단계 완료 후 사용된 키와 인증서들은 지운다.

⑪ 인증서

G1과 G2로 하여금 동일한 루트 인증기관을 신뢰하도록 하고, 각자 루트 인증서의 다이제스트를 계산한 후 그 값이 동일함을 확인한다. 단계 ⑧와 같이 진행하며, 단계 완료 후 사용된 인증서들은 지운다.

각자 상대방의 인증서를 검증하며, 인증서의 유효기간이나 키 용도 등도 점검한다. CRL의 요청, 수령, 저장 등의 기능을 시험한다.

⑫ 호스트 사이의 트래픽 보호 시험

출발지와 도착지를 I1, I2 대신 호스트들로 두며 시험을 수행한다.

⑬ 역할 전환

G1과 G2 사이의 역할을 전환하여 지금까지의 시험을 반복해본다.

이상의 단계들에서 3DES-CBC 이외의 다른 암호화 알고리즘이나 SHA-1 이외의 다른 해쉬 알고리즘, ISAKMP의 다양한 페이로드, SA 종단점의 다양한 식별 방법, Diffie-Hellman 군 유형들, 여러 종류의 서명 방법, 여러 범위의 키 길이 등에 대한 시험을 첨가하여 보다 정밀한 시험을 수행할 수도 있다.

Ⅳ. 결 론

이상으로 IPSec 제품에 대한 적합성 및 상호운용성 시험에 관한 현황을 조사하였다. IPSec에 대한 IETF에서의 표준화는 완료 단계에 이르러 있으며, VPN 장비나 혹은 방화벽, 라우터, 독립된 시스템 등에서 IPSec의 사용이 빠른 속도로 확산될 것이 기대되는데, IPSec 제품의 보급을 위해서는 상호운용성을 보장하기 위한 시험 기술의 확보가 절실하다.

IPSec 제품에 대한 적합성 및 상호운용성 시험에서 먼저 고려되어야 할 사항은 시험에 포함될 IPSec 요소를 정하는 것이며, 그 결과로 시험 스위트가 만들어진다. 그리고, IPSec 제품의 적합성 시험에서는 일반적으로 참조 구현이 사용되므로, 시험에 적합한 참조 구현의 확보가 필요하다. 또한, 시험 케이스들에 따른 시험 시나리오와 시험 환경의 적절한 설정 방법을 마련해야 하며, 시험 데이터를 생성하고, 응답 패킷을 수집 분석하는 도구와 시험 과정을 자동화하여 시험 작업을 효율적으로 진행할 수 있는 통합 시험 도구가 개발되어야 한다.

참 고 문 헌

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

[2] http://www.ietf.org/html.charters/kink-charter.html

[3] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, 1998. 11

[4] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406, 1998. 11

[5] R. Glenn and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec," RFC 2410, 1998. 11

[6] P. Karn et al., "The ESP DES-CBC Transform," RFC 1829, 1995. 8

[7] C. Madson and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With

Explicit IV," RFC 2405, 1998. 11
[8] R. Pereira and R. Adams, "The ESP CBC-Mode Cipher Algorithms," RFC 2451, 1998. 11
[9] P. Metzger and W. Simpson, "IP Authentication using Keyed MD5," RFC 1828, 1995. 8
[10] H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," RFC 2104, 1997. 2
[11] C. Madson and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH," RFC 2403, 1998. 11
[12] C. Madson and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH," RFC 2404, 1998. 11
[13] A. Keromytis and N. Provos, "The Use of HMAC-RIPEMD-160-96 within ESP and AH," RFC 2857, 2000. 6
[14] S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402, 1998. 11
[15] D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)," RFC 2409, 1998. 11
[16] D. Maughan et al., "Internet Security Association and Key Management Protocol (ISAKMP)," RFC 2408, 1998. 11
[17] TruSecure IPSec Community, http://www.icsa.net/html/communities/ipsec/
[18] IP Security Web Based Interoperability Tester, http://ipsec-wit.antd.nist.gov/
[19] Virtual Private Network Consortium, http://www.vpnc.org/
[20] OpenBSD, http://www.openbsd.org/
[21] KAME Project, http://www.kame.net/
[22] TAHI Project, http://www.tahi.org/
[23] Steps for IPSec Interoperability Testing, http://www.ietf.org/internet-drafts/draft-hoffman-ipsec-testing-01.txt

〈著者紹介〉

이 광 수 (Gwangsoo Rhee)
1981년 2월 : 서울대학교 계산통계학과 졸업
1986년 12월 : 워싱톤대학교 컴퓨터과학과 석사
1990년 5월 : 워싱톤대학교 컴퓨터과학과 박사
1990년 9월~현재: 숙명여자대학교 정보과학부 교수
관심분야 : 네트워크 보안, 알고리즘, 암호학

신 은 경 (Eunkyung Shin)
2000년 2월 : 숙명여자대학교 전산학과 졸업(학사)
2000년 3월~현재: 한국정보보호센터 기술표준팀 연구원
관심분야 : 컴퓨터·네트워크 보안, 정보보호 관리

이 홍 섭 (Hong Sub Lee)
본호의 "국내 정보보호제품의 표준적합성 시험과 인증체계" 저자 소개 참조