[5A-34]

공개된 인터넷 키 교환 프로토콜 구현에 대한 규격 시험

임재덕, 김정녀
한국전자통신연구원(ETRI)
{jdscol92, jnkim}@etri.re.kr

Conformance Test for Open Internet Key Exchange Protocol Implementation

JaeDeok Lim, JeongNyeo Kim
Electronics and Telecommunications Research Institute(ETRI)

요 약

인터넷을 통한 원격 업무 및 전자 상거래의 급증으로 사용자 정보 누출 및 변조를 예방하기 위해 사용자의 트래픽에 대한 기밀성 및 무결성을 제공하기 위한 IPsec 기반의 VPN 이 널리 보급되어 사용되고 있다. IPsec 터널을 형성하기 위해서는 터널 엔드 포인트 간의 보안 정책 및 사용할 키에 대한 협상이 필요하며 이는 키교환 프로토콜을 이용하여 가능하다. 키교환 프로토콜의 구현은 각 제품마다 호환성을 유지하기 위해 표준으로 제정된 규격에 따라 구현되어야 하며, 현재 몇 몇 공개된 구현들이 있다. 본 논문에서는 Linux 환경에서 동작하는 IPsec 기반의 VPN 프로그램인 FreeS/WAN 에 포함된 키협상 프로토콜의 구현에 대해 규격 시험 과정과 분석 결과를 정리한다.

I. 서론

인터넷 키교환 프로토콜(Internet Key Exchange, 이하 IKE)은 ISAKMP 에 사용되거나 IETF IPsec DOI 에서의 AH, ESP 와 같은 기타 보안 연계들을 위해 사용하기 위한 인증된 키 재료를 획득하기 위해 사용되는 Oakley 와 SKEME 의 일부와 ISAKMP 를 결합한 혼합형 프로토콜이다[1]. ISAKMP 프로토콜은 인증과 키 교환을 위한 프레임워크를 제공하고, 여러가지 상이한 키 교환들을 지원하기 위해 키 교환과는 독립적으로 설계되었다[2]. Oakley 는 '모드'로 불리는 일련의 키 교환을 설명하고 키들을 위한 완전 전방 기밀성(Perfect Forward Secrecy, PFS), 신원 보호 및 인증 등과 같은 서비스들을 설명한다[3]. SKEME 는 익명성, 부인 가능성, 신속한 키 갱신 등을 제공하는 다기능 키 교환 기법을 설명하고 있다[4]. IKE 는 Oakley 와 SKEME 의 전체 기능이 아닌 일부일 뿐이지만, 어떤 방법으로도 Oakley 와 SKEME 에 종속되지 않는다.

IPsec 기반의 VPN 제품 및 프로그램들은 각기 다른 제품 및 프로그램들간의 상호 호환을 위해 위에서 설명된 표준 규격들을 따라야 한다. 그렇지 않은 경우 IPsec 기반의 VPN 을 도입하려는 사용자는 모두 한 종류의 제품 혹은 프로그램 만을 선택해야 하며 상대방도 같은 제품 혹은 프로그램일 경우에만 서로 호환이 된다. 이는 매우 비효율적이라 할 수 있다. 따라서, 독립적인 처리가 가능한 세부적인 논리는 각 제품 및 프로그램에 따라 다르게 설계될 지라도 표준에 정의된 구조 및 처리는 표준 규격에 맞게 설계되어야 한다.

FreeS/WAN 은 IPsec 기반의 VPN 을 구현한 몇 몇 공개 프로그램들 중의 하나로 Linux 환경에서 동작하는 프로그램이다[5]. FreeS/WAN 은 사용자 트래픽에 대해 기밀성 및 무결성을 제공하기 위해 커널 모듈 형태로 구현된 klips 라는 IPsec 엔진과 보안 정책 및 키 등을 협상하는 IKE 프로토콜 프로그램인 pluto 라는 사용자 데몬으로 구성되어 있다. FreeS/WAN 은 현재 급속히 늘어가는 Linux 환경에서 동작하고 소스가 공개되어 있어 IPsec 기반의 VPN 을 구현하려는 많은 사용자 및 업체에 참조 모델이 되고 있다.

본 논문은 FreeS/WAN 의 IKE 프로토콜의 구현인 pluto 데몬에 대해 규격 시험 툴을 이용하여 규격 시험 과정과 분석 결과를 정리한다.

II. 시험 환경

본 논문에서 사용할 규격 시험 툴은 Automated Network Validation Library(이하 ANVL)로 IXIA 사에서 상용으로 제공되고, 표준화된 RFC 문서를 기반으로 프로토콜 수준의 네트워크 제품의 유효성을 검사할 수 있다[6]. ANVL 은 DUT(Device Under Test)에 연결된 시스템에서 동작하는 프로그램으로, 시험 중에 네트워크 상의 하나 혹은 그 이상의 노드 역할을 한다. ANVL 은 DUT 로 시험 패킷을 보내거나, DUT 로부터 응답 패킷을 받아 분석하고 평가하며 그에 상응하는 대응을 한다. 또한 DUT 에서 기대되는 것처럼 동작을 하는지에 대해 그 정보를 기록한다.

시험하고자 하는 네트워크 환경은 그림 1 과 같다. 터널은 DUT 의 eth0 와 기존 라우터의 인터페이스 간에 생성되고, 보호되는 클라이언트는 local client 와 기존 라우터의 터널 엔드인 remote client 이다. 점선으로 표시된 부분이 ANVL 에서 애뮬레이트 해 주는 부분이다.