# 국가기관용 VPN의 보호프로파일 보안환경 작성방법에관한 연구

이 동 춘* · 김 점 구** · 김 귀 남***

## 요 약

가상사설망(Virtual Private Network, VPN)은 전용선과 같은 보안성을 유지하고, 비용을 획기적으로 절감할 수 있는 기술로서 수요가 갈수록 증가하고 있다. 지난해 말 국가기관용 VPN 보호프로파일이 개발되어 사용되고 있으나, 몇 가지 문제를 포함하고 있는 것으로 보인다.

본 논문에서는 현재 사용중인 국가기관용 VPN 보호프로파일(Protection Profile, PP)이 가지고 있는 문제점들을 살펴보고 이에 대한 개선 방향을 모색하여 보고자 한다.

# A Study on Specification Scheme of PP Security Environment for Government's VPN

Dong Chun Lee* · Jeom Goo Kim** · Kuinam J. Kim***

## ABSTRACT

Virtual Private Network (VPN) is the technology that can reduce the cost revolutionary and maintain the security like an private line, and the demand is increased more and more. Two kinds of current VPN Protection Profiles(PP) for the national organ are used on development, but it is considered by being several problems.

In this paper we consider the VPN's PP problems that has been used currently, and describe to an improvement direction.

* 호원대학교 컴퓨터학부
** 남서울대학교 컴퓨터학과
*** 경기대학교 정보보호기술공학과

# 1. 서 론

IT 보안성 평가를 위한 공통평가기준(CC 2.1)이 1999년 12월 국제표준(ISO/IEC 15408)으로 제정되었고, 국내의 경우 2002년 8월 정보화촉진기본법 제15조 제1항의 규정에 의거 정보보호시스템 공통평가기준을 CC를 기반으로 마련하여 침입차단 시스템, 침입탐지 시스템, 그리고 가상사설망 제품을 평가 적용하고 있다[1].

정보보호시스템을 사용하고자 하는 보안환경 및 보안목적을 정의하고, 이에 적합한 보안요구사항을 CC에서 선택하여 단일제품별 평가기준으로 작성한 것이 보호프로파일(Protected Profile, PP)이다. PP의 작성목적은 정보보호시스템의 구현기술을 서술하고자 하는 것이 아니라, 보안환경에 의해서 정의한 보안목적을 만족하도록 보안대책을 체계적으로 세우고 이에 합당한 보안요구사항을 도출하여 정보보호시스템 평가를 위한 논리적 기초를 마련하고자 하는 것이다.

PP 및 보안목표명세서 작성가이드 표준은 기본적으로 PP 및 보안목표명세서 개발자를 고려하여 작성하였지만, PP 및 보안목표명세서 평가자에게도 유용한 정보를 제공할 수 있다. 또한 일반 사용자들에게는 보호프로파일 및 보안목표명세서 개발자의 의도 및 개발원리에 대한 이해를 도모시킬 수 있다[5].

이에 발맞추어 발표된 국내 국가기관용 게이트웨이형 VPN PP V1.01은 향후 민간기관용 VPN PP 개발에 많은 도움이 될 것이다[1]. 본 논문에서는 국가기관용 VPN의 보안환경 서술 부분을 고찰함으로써 PP의 보안환경 서술 방법을 익히고 향후에 개발될 민간기관용 PP의 보안환경 서술에 도움을 주고자 한다.

# 2. 국가기관용 VPN PP V1.01

## 2.1 개요 및 정의

2002년 12월 9일 국가기관용 VPN PP로 승인된 CC기반 VPN PP V1.01은 네트워크 경계점인 게이트웨이 위치에서 동작하는 게이트웨이형 VPN 제품에 대한 최소한의 보안요구사항을 서술하고 있다. 평가 대상인 TOE(Target of Evaluation)는 상대 TOE가 소속된 다른 네트워크와 통신할 경우, 송수신 정보를 안전하게 주고받을 수 있는 암호통신 기능을 제공할 수 있어야 하며, 보안이 제공되지 않는 일반 네트워크를 통해 상대 TOE와 비암호통신도 수행할 수 있어야 한다. TOE는 VPN 게이트웨이 내부에 저장된 데이터들의 안전성을 보장하지 않고, 네트워크를 통해 데이터들을 송수신할 경우에만 안전성을 제공할 수 있으면 된다[2].

TOE간에 암호통신 기능을 이용한 비밀통신이 수행될 때 두 TOE는 같은 보안정책 하에서 동작될 수 있어야 하며, 인가된 관리자의 인증 및 발생 가능성이 있는 보안 관련 사건들에 대한 감사를 적용할 수 있어야 한다. 보호프로파일은 다음과 같은 사항을 정의하고 있다.

- TOE가 사용되는 보안 관점의 환경에 대한 가정 사항
- TOE와 TOE 운영환경에 대한 위협 사항
- TOE와 TOE의 환경에 대한 보안목적
- 보안목적과 합치되는 보안기능요구사항 및 보증요구사항
- 각 요구사항과 보안목적이 어떻게 합치되는지를 뒷받침하는 이론적 근거

## 2.2 보호프로파일의 구성

총 6개의 절로 구성되어 있으며, 제1절은 보호프로파일의 소개 내용으로 문서의 관리, 보호프로파일을 식별하는 필요한 개관적은 정보 등을 서술하고 있고, 제2절은 TOE설명으로 TOE를 정의하고 일반적인 보안요구사항을 참고하여 TOE의 상황 수립 등을 서술한다. 제3절은 TOE 보안환경(TSE : TOE Security Environment)에 관한 내용으로 TOE가 사용될 운영환경에 대하여 서술하고, 제4절은 보안목적으로 TOE의 운영환

경과 TOE가 반드시 충족해야 하는 보안목적을 정의한다. 제5절은 IT 보안요구사항에 관한내용으로 TOE가 반드시 충족해야 하는 정보보호 시스템 공통평가기준 2부와 3부로부터 발췌된 보안기능 요구사항 및 보증 요구사항을 정의하고, 끝으로 제6절은 본 보호프로파일에 언급된 내용들에 대한 이론적 근거에 관한 내용으로 위협과 정책을 만족시키는 보안목적을 논증하는 이론적 근거를 서술한다.

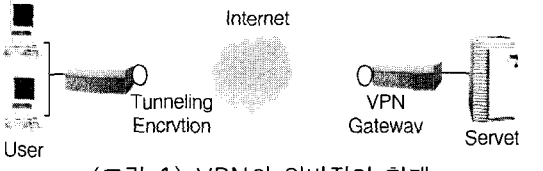
## 3. TOE의 보안정책과 보안환경

### 3.1 보안정책

보호프로파일에서 언급하는 TOE는 VPN에서 반드시 제공해야할 기본적인 보안기능과 게이트웨이 장비가 가져야하는 TOE 가용성 유지, TOE 자원활용 및 TOE 접근에 대한 제어 등과 같은 부가적인 보안기능에 대한 요구사항도 반드시 만족할 수 있어야 한다. (그림 1)은 VPN의 개념적인 그림으로 본 보호프로파일에서 TOE로 언급하고 있는 VPN 게이트웨이의 네트워크상의 설치 위치를 보여준다. 서브넷의 VPN 게이트트웨이는 다른 서브넷에 위치한 시스템과 보안채널을 통한 암호화 및 인증이 적용된 통신이 가능함과 동시에 또 다른 서브넷에 위치한 시스템과는 보안채널을 사용하지 않고 일반채널을 통한 비암호 및 비인증 통신이 가능해야 한다. 즉, VPN의 보안채널을 통한 안전한 연결과 VPN을 사용하지 않는 일반 연결이 동시에 가능해야 한다. 안전한 보안채널의 사용 여부는 TOE에 설정된 보안정책 및 보안연계에 의해 결정된다.

TOE에 적용되는 보안정책은 다음과 같다[2].

- 상대 TOE와 보안통신을 수행해야 하는 경우, 송신패킷은 로컬 TOE에 의해 두 통신 주체 사이에 보안채널을 설정하거나 현재 설정된 채널을 이용하여 전송되어야한다.
- 상대 TOE와 보안통신을 수행하지 않아야 하는 경우, 송신 패킷은 로컬 TOE에 의해 보안채널을 설정하지 않으며 어떤 보안 메커니즘도 적용하지 않는다.
- 상대 TOE와 보안통신을 수행해야 하는 경우, 수신 패킷은 로컬 TOE에 의해 두 통신 주체 사이에 보안채널을 설정하거나 현재 설정된 채널을 이용하여 받을 수 있어야 한다.
- 상대 TOE와 보안통신을 수행하지 않아야 하는 경우, 수신 패킷은 로컬 TOE에 의해 보안채널을 설정하지 않으며 어떤 보안 메커니즘도 적용하지 않는다.




(그림 1) VPN의 일반적인 형태

### 3.2 보안환경

국가용 VPN PP 보안환경은 관리자의 숙련도, 물리적 보안환경, 보안정책, 서브넷 내부방어, 암호 알고리즘, 운영체제보강, 일반데이터, 일반 프로그램, TOE 위치 등 총 9개 항목에 대한 TOE 환경 상에 존재한다고 가정하는 가정사항과 감사대상사건, 감사데이터유실, 결함코드, 고장, 신원 위장, 스푸핑공격, 암호공격, 암호키노출, 잠재적공격, 재전송공격, TOE의 형상 데이터를 독해/변경/파기를 시도하는 형상데이터공격, 인가된 관리자의 인증정보추측을 위해서 반복적으로 시도하는 BF공격 등 총 12개 항목의 TOE 자체에 대한 위협, 부실한관리, 형상 등 총 2개의 TOE 운영환경에 대한 위협이 있다.

그리고 제정된 PP에 순응하는 TOE에 대해서만 적용하는 감사정보검사, 관리, 무결성, 비밀성, 암호, 우회, 책이, 키교환관리 등 총 9개 항목으로 조직의 보안 정책 평가를 정의하고 있

으며, 천재지변이나 TOE 우회 공격, 고도의 위협 행위자에 대해서는 고려하지 않는다.

## 4. 국가기관용 VPN PP의 보안환경 분석

### 4.1 가정사항

국가기관용 가상사설망 보호프로파일 V1.01(이후에는 게이트웨이 PP라 칭함)은 9개의 가정사항을 포함하고 있으며, 국가기관용 가상사설망 보호프로파일 V1.0(이후에는 VPN PP라 칭함)은 6개의 가정사항을 포함하고 있다. 대부분의 가정사항들은 납득할 만한 수준에서 기술되고 있으나, 몇 가지 문제점을 포함하고 있는 것으로 생각된다.

#### 4.1.1 용어 통일의 문제

VPN PP의 가정사항 A.통신상대에는 '호환가능한 보안정책'이라는 항목이 존재하는데, '호환가능한' 수준에 대한 명확한 언급이 생략되어 있다. 이에 반하여 게이트웨이 PP의 가정사항 A.보안정책에는 '호환가능한' 수준에 대한 설명이 부가되어 있다. 이들 두 PP는 모두 국가기관용으로 작성된 것이므로, 이들 용어에 대한 통일이 필요할 것이다.

또한 VPN PP의 가정사항 A.신뢰된관리자와 게이트웨이 PP의 가정사항 A.관리자, VPN PP의 가정사항 A.운영체제와 게이트웨이 PP의 A.운영체제보강은 동일한 내용의 가정사항을 언급하고 있는 것으로 보이는데, 이에 관하여서는 서로 문구가 다르게 명시되어 있다. 국가기관에서 사용할 PP에서 동일한 내용에 대하여 서로 다른 용어와 설명을 사용하고 있는 것은 자칫 혼란을 야기할 우려가 있으므로 이를 통일하여야 할 것으로 생각된다.

#### 4.1.2 기술 깊이의 문제

앞서 언급한 것처럼 용어들이 제각기 사용되고 있는 것과 함께, 기술의 깊이에 대하여서도 차이가 있다. VPN PP는 간단한 언급 수준에 머물러 있는 반면, 게이트웨이 PP는 세부적인 언급까지 포함하고 있는 것이다. 예를 들어, VPN PP의 가정사항 A.운영체제와 게이트웨이 PP의 A.운영체제보강은 다음과 같이 구성되어 있다.

- A.운영체제 : TOE의 하부 운영체제는 안전하고 신뢰할 수 있다.
- A.운영체제보강 : TOE에 의해 필요하지 않은 운영체제상의 모든 서비스나 수단 등은 모두 제거하는 작업을 통해 운영체제상의 취약점에 대한 보강작업이 수행되어야 하며, 운영체제에 대한 신뢰성과 안정성을 보장하여야 한다.

이들 두 가정사항은 유사한 내용을 언급하면서도 기술상의 깊이에서 차이가 나는 대표적인 예가 될 수 있을 것이다. 이 부분에 대하여서는, 보호프로파일의 가정사항 부분에서 지나치게 세부적인 내용까지 언급할 필요는 없을 것으로 생각된다. 어차피 상용 운영체제를 사용하는 경우가 많을 것이고, 이러한 경우에는 가정사항의 조건을 맞추기 어려운 경우도 발생할 수 있을 것이므로, 단순히 '안전하고 신뢰할' 수 있음을 언급하는 수준에서 기술하는 것이 바람직한 것으로 생각된다.

#### 4.1.3 기술 범위의 문제

앞서 언급하였던 것처럼, 두 종류의 보호프로파일은 가정사항의 수가 다르다. 따라서 기술범위의 문제가 발생하게 된다. 이 중에서 가장 우려되는 부분은 게이트웨이 PP의 A.일반프로그램 및 A.일반데이터 등으로 생각된다.

- A.일반프로그램 : TOE에는 컴파일러, 에디터, 응용 프로그램 등과 같은 일반적인 범용 프로그램을 가지지 말아야 한다.
- A.일반데이터 : TOE에는 TOE가 사용하는

데이터만을 수용하고 있어야 하며, 일반적인 데이터는 수용하지 말아야 한다.

보안상의 이유로 일반적인 데이터 및 범용 프로그램을 가지고 있지 않도록 한다는 것은 충분히 납득할 만한 내용으로 받아들여지지만, 예를 들어 기술한 내용은 불필요한 것으로 생각된다. 또한, 앞서 정의한 VPN PP의 A.운영체제의 내용으로 보아 '하부 운영체제가 안전하고 신뢰할 수' 있으려면 당연히 A.일반프로그램과 A.일반데이터의 내용을 포함하여야 할 것으로 생각된다. 그러므로 중복되는 내용을 기술하고 있는 듯한 느낌을 주게 되는 것이다.

### 4.2 위 협

위협 부분의 기술에 있어서도 앞서 언급하였던 것과 유사한 내용들이 대부분 그대로 적용된다. 간단히 예를 들자면, 게이트웨이 PP에는 T.스푸핑 공격이라는 항목이 있다.

- T.스푸핑 공격 : 위협 행위자가 인가된 관리자 또는 외부 IT 실체인 것처럼 가장하기 위하여 데이터의 발신지 주소를 변경하여 TOE의 보안정책을 뚫을 수 있다.

이 항목은 많은 문제점을 내포하고 있는 것으로 생각되는데, 우선 다른 항목들과 비교할 때 지나치게 기술 깊이가 깊은 편이며, 상당히 세부적이고 기술(technical)적인 내용까지 포함하고 있는 것으로 생각된다. 보호프로파일의 위협 기술 수준이라면 이와 같은 수준까지 진행하지 않는 것이 바람직한 것으로 생각된다. 또한 '보안정책을 뚫을 수 있다'는 표현은 T.잠재적 공격의 '보안정책을 우회하고자 하는 시도를 행할 수 있다'라는 표현을 사용하는 것이 올바른 것으로 보인다.

또한 VPN PP의 TE.관리자의 경우에는, 이미 가정사항 A.신뢰된관리자 항목을 사용하였으므로 추가하지 않아도 될 것으로 보인다. 가정사항을 만족하는 경우라면 이와 같은 위협은 발생하지 않을 것이기 때문이다. 물론 강조를 위하여 반복하여 사용하였다고도 볼 수 있겠지만, 동일한 내용을 문구만 변경하여서 가정사항과 위협에 모두 기술하는 것은 바람직하지 않은 것으로 생각된다.

## 5. 결론 및 향후 연구 방향

앞서 살펴본 바와 같이 현재 공개되어 있는 가상 사설망 관련 보호프로파일들은 몇 가지 문제점들을 내포하고 있는 것으로 생각되며, 이러한 내용들은 향후의 추가적인 연구를 통하여 개선하여 나가야 할 것이다.

본 논문에서는 보안 환경 부분 중에서 정책과 관련된 내용을 언급하지 않았는데, 이것은 국가기관의 정책을 반영한 것으로 생각되기 때문이다. 만일 민간기관용 가상 사설망 보호프로파일을 작성하는 경우라면 이들 문제들을 파악하여 개선할 수 있는 방안을 모색하여 보아야 할 것이고, 각 민간기관들이 가지고 있는 보안정책들을 살펴보아야 할 것이다.

또한 이들 두 개의 가상 사설망 관련 보호프로파일들은 무선 환경에 대한 고려를 생략하고 있는 것으로 생각되는데, 현재의 기술 발달 수준으로 보아 향후에는 무선 가상 사설망 전용 제품들이 출시되는 것도 가능하다고 할 경우에 대한 사전 연구가 진행될 필요가 있을 것으로 생각된다.

## 참 고 문 헌

[1] 정보보호시스템 공통평가기준, 정보통신부 한국정보보호진흥원, 2002. 8.

[2] 국가정보원 홈페이지, 보호프로파일 등재현황, http://www.nis.go.kr/kr/security/index_product.html.

[3] ZUM Strarten hier kicken, "IP VPN Solution for Service Provider", Cisco Systems,

1999. 5.

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

[5] 권현조, 보호프로파일 및 보안목표명세서 작성가이드 표준(안), http://www.kisa.or.kr/K_trend/KisaNews/199911/4_4guideline.htm.

**이 동 춘**

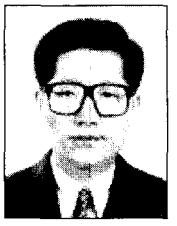
연세 대학교 컴퓨터과학과 공학박사

1989~현재 호원대학교 컴퓨터학부 정교수

JPDC, JHSN, ETT, Performance Eval., and JOIN(SCI급) 국제 논문지 심사위원

KISA 개인정보보호 중장기대책 위원회 운영위원, KISA 정보보호자격시험(SIS) 운영 위원회 운영위원, 정통부산하 프로그램 심의조정 위원회 감정평가위원

관심분야 : 컴퓨터 네트워크, 이동통신(소프트웨어분야), 네트워크 보안, 무선통신 보안



**김 점 구**

1990년 광운대학교 전자계산학과 이학사

1994년 광운대학교 대학원 전자계산학과 이학석사

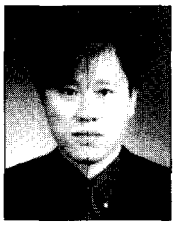
2000년 한남대학교 대학원 컴퓨터공학과 공학박사

1990년~1994년 (주) 제성프로젝트 연구원

1995년~1998년 (주) 시사 컴퓨토피아 인터넷사업부장

1999년~현재 남서울대학교 컴퓨터학과 조교수

관심분야 : 정보보호, 컴퓨터네트워크, 무선통신



**김 귀 남**

미국 캔자스대학 수학과(응용수학사)

미국 콜로라도주립대학 통계학과(통계학석사)

미국 콜로라도주립대학 기계·산업공학과(기계·산업공학박사)

현재 경기대학교 정보보호기술공학과 주임교수