# 무선 LAN 보안시스템 보호 프로파일 개발

김춘수*, 최희봉*, 최명길*, 장병화*
*국가보안기술연구소
e-mail:hbchoi@etri.re.kr

# Development of Wireless LAN Security System Protection Profile

Choon-Soo Kim*, Hee-Bong Choi*, Mung-Gil Choi*, Bung-Hya Chang*
*NSRI

요 약

무선 LAN 보안시스템 보호 프로파일은 취약한 무선 LAN 통신구간에 대한 보안대책을 체계적으로 수립하여 보안기능 및 보안평가기준을 작성한 문서이다. 이 무선 LAN 보안시스템 보호 프로파일은 개발자, 사용자, 평가자 등이 편리하게 사용할 수 있다. 본 논문에서는 CC기반의 무선 LAN 보안시스템 보호 프로파일을 통하여 이동 환경용 무선 LAN에 대한 보안대책을 체계적으로 수립할 수 있음을 보이고 이러한 보안대책으로 설계된 무선 LAN 보안시스템을 객관적으로 평가할 있음을 보인다. 본 논문에서 설계한 무선 LAN 보안시스템 보호 프로파일은 EAL 2를 만족시키는 수준이다. 본 연구 결과로 개발된 보호 프로파일은 무선 LAN 보안시스템을 개발하는 개발자, CC에 기반하여 무선 LAN 보안시스템을 평가하는 평가자, 무선 LAN 보안시스템을 사용자 요구사항에 적합하게 사용하는 사용자 등에 유용한 문서로 사용될 수 있다.

## 1. 서론

무선 LAN은 무선 LAN 클라이언트와 무선 LAN AP(Access Point)사이의 무선통신 및 무선 LAN 클라이언트끼리의 무선통신을 지원하여 일반 사무실에서 네트워크 배선 없이 통신할 수 있고 노트북의 이동성을 극대화할 수 있는 편리성을 갖추고 있다. 그러나 무선 LAN의 통신구간은 무선으로써 개방되어 있어 보안에 취약할 뿐 아니라 무선 LAN 클라이언트의 악의적 접속을 가능하게 한다. 이러한 무선 LAN에 대한 보안대책은 무선 LAN 보안시스템을 사용하여 세울 수 있다.

무선 LAN 보안시스템을 설계할 때 필요한 보안기능은 무선 LAN 보안시스템 보호 프로파일이라는 문서로부터 도출될 수 있다. 또한 무선 LAN 보안시스템 보호 프로파일은 이러한 보안기능을 구현한 무선 LAN 보안시스템을 객관적으로 평가할 수 있는 보안평가 기준을 포함하고 있다. 그러므로 이 보호 프로파일은 개발자, 평가자, 사용자에게 매우 중요한 문서이다.

현재 사용하고 있는 정보 보호 시스템 평가기준은 미국의 TCSEC(Trusted Computer System Evaluation Criteria), 유럽의 ITSEC(Information Technology Criteria), 한국의 K평가체계 등이 있다. 최근 미국, 유럽, 캐나다 등은 CC(Common Criteria)라는 모든 제품에 공통적으로 적용할 목적으로 개발된 국제 공통 평가기준을 표준으로 제정하여 사용하고 있다[1].

본 논문에서는 국제 공통 평가기준인 CC에 기반한 무선 LAN 보안시스템 보호 프로파일 내용을 요약하여 설명한다. 그리고 CC기반의 무선 LAN 보안시스템 보호 프로파일을 통하여 이동 환경용 무선 LAN에 대한 보안대책을 체계적으로 수립할 수 있음을 보이고 이러한 보안대책으로 설계된 무선 LAN 보안시스템을 객관적으로 평가할 있음을 보인다. 본 논문에서 설계한 무선 LAN 보안시스템 보호 프로파일은 보증등급 EAL(Evaluation Assurance Level) 2를 만족시키는 수준이다. 본 연구 결과로 개발된 보호 프로파일은 무선 LAN 보안시스템을 개발하는 개발자, CC에 기반하여 무선 LAN 보안시스템을 평가하는 평가자, 무선 LAN 보안시스템을 사용자 요구사항에 적합하게 사용하는 사용자 등에 유용한 문서로 사용될 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 본 연구에서 개발된 무선 LAN 보호 프로파일을 요약하여 설명한다. 3장에서는 무선 LAN 보호 프로파일 개발에 대한 분석결과를 설명한다. 마지막으로 4장에서 결론을 맺는다.

## 2. 무선 LAN 보안시스템 보호 프로파일

보호 프로파일에 대한 구성 및 구체적인 설명은 CC Part1 Annex B에 기술되어 있다. 다음에서 무선 LAN 보안시스템 보호 프로파일의 구성과 내용을 요약하여 설명한다.

### 2.1 개요

본 연구의 프로파일은 민간에 적용될 무선 LAN 환경에서 사용되도록 개발되었다. 이 프로파일은 정책, 가정, 위협, 보안목적, 보안기능 요구사항, 보안보증 요구사항에 대하여 설명한다.

#### 2.1.1 식별

본 프로파일은 일반 상용 무선 LAN 보안시스템 보호 프로파일이라 명칭한다. 이 절에서는 작성자, 버전번호, 보증등급 수준을 설명한다.

#### 2.1.2 보호프로파일 개요

본 프로파일은 무선 LAN과 AP에 필요한 보안사항을 규정한다[2]. 무선 LAN은 단독 네트워크가 될 수 있고 유선 네트워크의 무선접속이 될 수 있다. 본 프로파일은 민간 암호 알고리즘을 이용하여 무선 LAN을 통한 통신의 프라이버시와 무결성을 보장할 수 있도록 개발된다. 또한 AP에 대한 보안관리가 필요하다. 본 프로파일에 규정된 보안요구사항은 보증등급 EAL 2를 규정하고 있다. 그 외에 본 프로파일을 구성을 설명한다.

#### 2.1.3 참고문서

본 프로파일에 언급하는 모든 문서를 기술한다.

### 2.2 TOE 설명

본 연구의 프로파일에서 정의하는 TOE(Target of Evaluation)은 AP(Access Point)와 이동 환경용 클라이언트를 포함하는 모델로서 정의할 수 있다. 이동 환경용 클라언트는 유선 네트워크에 로밍할 수 있고 AP를 사용하여 유선 네트워크에 접속할 수 있다. 각 AP는 LAN의 지역 세그먼트를 제공한다. 다음 그림은 무선 클라이언트를 로밍할 수 있는 AP를 갖춘 무선 LAN을 보인다.

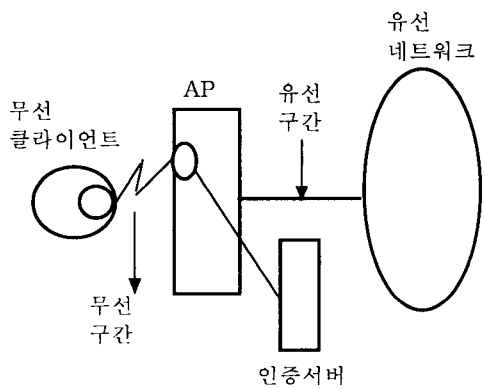


그림 1 무선 LAN 보안시스템 구조도

그림 1에서 음영영역이 본 연구의 프로파일의 TOE 영역이다.

### 2.3 TOE 보안환경

본 절에서는 보호되어야 할 자산과 가정사항, 위협, 조직의 보안정책을 설명한다.

#### 2.3.1 자산

본 보호 프로파일에서 보호되어야 할 자산은 사용자의 정보, 보안시스템을 운영할 때 필요한 보안성 데이터, 설계도, 실제 구현물 등이다.

#### 2.3.1 가정사항

본 절에서는 운영시스템에 대한 가정사항(가정사항 1 : TOE가 안전하게 운영될 때, TOE 연동환경에는 어떠한 취약성도 없다고 가정한다), 보안관리자에 대한 가정사항, 사용자에 대한 가정사항, 사용자 데이터 저장에 대한 가정사항 등 9개 항목을 설명한다.

#### 2.3.2 위협

본 절에서는 무선 LAN에 대한 위협을 다음과 같은 5개 항목으로 설명한다.

위협 1 : 인가되지 않은 사용자는 TOE로부터 전송되는 신호를 탐색 및 검출하여 사용자의 데이터를 얻을 수 있다.

위협 2 : TOE에서 생성되지 않은 신호가 TOE 전송을 방해하거나 중단시킬 수 있다.

위협 3: 인가되지 않은 사용자는 인증절차를 공격하여 TOE의 일정 영역에 접근할 수 있다.

위협 4 : 공격자는 합법적인 사용자로 위장하거나 위조된 메시지를 전송하여 무선 LAN에 접속할 수 있다.

위협 5 : 공격자는 무선 통신구간의 정보를 탈취하여 수정할 수 있다.

#### 2.3.3 조직의 보안정책

본 절에서는 사용자의 책임에 대한 정책(정책 1 : 인가된 사용자는 보안 관련 행위에 대하여 책임을 져야 한다.), 사용자 요구사항에 대한 정책(정책 2 : TOE의 구현 및 사용은 사용자의 요구사항을 만족하여야 한다.) 등 6개 항목을 설명한다.

### 2.4 보안목적

#### 2.4.1 TOE 보안목적

본 절에서는 TOE 보안목적 10개 항목 즉 접근통제, 식별, 감사, 암호, 데이터 보호, 보안속성 주입, 환경, 문서보안, 구현 및 사용 보증을 설명한다. 즉 예를

돌면 보안목적 1은 위협 3에 대한 보안대책으로서 TOE에 접근통제를 적용하여야 한다는 것이다.

#### 2.4.2 환경에 대한 보안목적

본 절에서는 환경에 대한 보안목적 11개 항목 즉 관리자, 운영 시스템, 교육, 설치, 물리적 보안, 사용책임, 공개키 기반 구조, 사용자 요구사항 일치, 사용기록 감사를 설명한다. 예를 들면 환경 보안목적 1은 인가된 관리자는 모든 관리자 준수지침을 따라야 한다는 것이다.

### 2.5 IT 보안 요구사항

본 절에서는 TOE가 만족해야 하는 보안기능 및 보안보증 요구사항을 설명한다. 보안기능 요구사항은 CC의 Part 2의 보안기능 컴포넌트들 중에서 선택하였고 보안보증 요구사항은 CC의 Part 3의 EAL 2에 해당하는 보안보증 컴포넌트들 중에서 선택하였다.

#### 2.5.1 보안기능 요구사항

본 절에서는 보안기능 요구사항 29개 항목 즉 감사 데이터 생성, 고유번호 지정, 암호키 생성, 암호키 파괴, 암호연산, 정보흐름통제, 보안속성, 내부 전송 보호, 무결성 검사, 인증 실패 관리, 사용자 속성 정의, 작동이전의 사용자 인증, 보호된 인증귀환, 작동이전의 사용자 식별, 사용자에 관한 정보 숨김, 보안기능 동작 관리, 보안속성 관리, 일반속성 초기화, 보안기능 데이터 관리, 복구, 보안역할 등이 있다.

#### 2.5.2 TOE 보안보증요구사항

본 절에서는 평가기준인 TOE 보안보증 요구사항을 설명한다. 보안보증 요구사항은 CC의 Part 3의 EAL 2에 해당하는 보안보증 컴포넌트들로 구성된다. 보안보증 요구사항은 5개의 클래스, 클래스 아래에 보증 패밀리, 또 패밀리 아래에 보증 컴포넌트로 구성된다. 본 보호 프로파일을 보안보증 등급 2를 만족해야 할 보증요구사항은 CC의 Part 3에 언급된 바와 같이 아래와 같다.

| 보증클래스 | 보증 컴포넌트 |
|---|---|
| 형상관리 | ACM_CAP.2 |
| 배포/운영 | ADO.DEL.1, ADO.IGS.1 |
| 개발 | ADV_FSP.1, ADV_HLD.1, ADV_RCR.1 |
| 설명서 | AGD_ADM.1, AGD_USR.1 |
| 시험 | ATE_COV.1, ATE_FUN.1, ATE_IND.2 |
| 취약성평가 | AVA_SOF.1, AVA_VLA.1 |

### 2.6 근거사항

#### 2.6.1 보안목적의 근거사항

본 절에서는 가정사항, 위협, 조직의 보안정책으로부터 보안목적이 유도된 합당한 근거를 설명한다.

#### 2.6.2 보안요구사항의 근거사항

본 절에서는 보안요구사항들이 보안목적을 만족하는 합당한 근거를 설명한다.

## 3. 무선 LAN 보안시스템 보호 프로파일 분석

개발된 무선 LAN 보안시스템 보호 프로파일은 기본적으로 사용자 요구사항을 만족해야 함을 요구하고 있다. 식별할 수 있는 가정사항, 위협, 조직의 보안정책은 보안기능에 대한 최신 공격기술 동향, TOE, TOE 운용환경을 정확히 분석함으로써 얻을 수 있으므로 본 보호 프로파일을 통하여 이러한 분석작업을 수행하였음을 알 수 있다. 또한 가정사항, 위협, 조직의 보안정책으로부터 보안대책을 체계적으로 수립하였다. .
평가방법 및 평가절차가 객관적이라고 가정한다면 본 연구결과, 국제 공통 평가기준의 보안보증요구사항에 의거 EAL 2 수준의 평가기준으로 무선 LAN 보안시스템에 대한 객관적인 평가를 실시할 수 있다 [1][3].
보안환경에서 보안 요구사항까지의 유도가 명백한 근거를 가진다는 것을 2.6절에서 알 수 있다.

## 4. 결론

본 논문에서는 상용 환경에서 사용될 수 있는 EAL 2 수준의 무선 LAN 보안시스템 보호 프로파일을 개발한 것을 요약 설명하였고 이를 분석하였다.
본 논문에서는 CC기반의 무선 LAN 보안시스템 보호 프로파일을 개발함으로써 이동 환경용 무선 LAN에 대한 보안대책을 체계적으로 수립할 수 있음을 보였다. 그리고 이러한 보안대책으로 설계된 무선 LAN 보안시스템은 객관적으로 평가될 수 있음을 보였다. 본 논문에서 설계한 무선 LAN 보안시스템 보호 프로파일은 EAL 2를 만족시키는 수준이다. 본 연구 결과로 개발된 보호 프로파일은 무선 LAN 보안시스템을 개발하는 개발자, CC에 기반하여 무선 LAN 보안시스템을 평가하는 평가자, 무선 LAN 보안시스템을 적합하게 사용하는 사용자 등에 유용한 문서로 사용될 수 있다.

## 참고문헌

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, CCIMB-99-021, 032, 033, August 1999.
[2] Peer-to-Peer WLAN Protection Profile for Sen sitive But Unclassified Environments, Version 0.1, March 2001.
[3] Common Mehtodology for Information Techno logy Security Evaluation, Version 1.0, CEM-99/045, August 1999.