무선랜 인증시스템 보호프로파일 개발

한광택○ 최희봉 정지훈
국가보안기술연구소
kthan@etri.re.kr, hbchoi@etri.re.kr, jihoon@etri.re.kr

Development of Protection Profile for Wireless LAN Authentication System

Kwangtaek Han○ Heebong Choi Jihoon Jeong
National Security Research Institute

1. 서 론

현재 대부분의 국가·공공기관에서는 정보보호를 위해 다양한 정보보호제품을 설치 및 운영함으로서 통신 인프라 상에서의 안전한 정보교류와 일상작업을 전개하고 있으며, 이러한 정보보호제품에 대한 신뢰성을 보증하기 위해 국제공통평가기준(Common Criteria)을 사용하여 보안기능을 평가하고 있다. 국제공통평가기준 기반 하의 보호프로파일은 제품에 대한 TOE를 설정하고 TOE의 보안문제에 대응하기 위한 보안요구사항을 기술한 문서로서, 시스템 개발자와 시스템 조달자 사이의 통신수단으로 사용된다.

보호프로파일 개발은 관련 정보보호 제품의 보안성 평가·인증 업무를 지원함으로서 관련 제품군의 시장에 영향을 준다. 이에 각 국가마다 보호프로파일을 지속적으로 개발하고 있으며 우리나라에도 현재 14종의 보호프로파일이 개발되어 있고 금년 4종의 보호프로파일 개발을 진행 중에 있다. 국내의 보호프로파일 개발은 보호프로파일 개발체계에 따라 보호프로파일 개발 자문위원회에서 시장 동향 및 산업체 개발 동향을 바탕으로 선정하여 보호프로파일을 개발하고 있다.

무선랜 인증시스템은 보호프로파일 개발체계에 의거하여 2005년 말에 보호프로파일 개발 자문위원회에서 선정한 4개의 정보보호 제품군 중 하나인 무선랜 보안 제품군에 속한 정보보호 제품으로서, 무선랜 클라이언트[1]와 무선랜 접근시스템[2]과 달리 보호프로파일이 개발되어 있지 않은 제품이다. 물론 무선랜 인증시스템의 보안요구사항을 일부 포함하는 보호프로파일[3]이 CC포털사이트에 등재되어 있기는 하나 무선랜 보안 표준 프로토콜에서 요구하는 보안기능은 배제되어 있어 부적절하다.

이에 무선랜 인증시스템에 대한 보안환경을 분석하여 보안목적을 도출하고 다시 도출된 보안목적으로부터 IT보안요구사항을 도출하였으며, 이들 사이의 이론적 근거를 제시한 보호프로파일을 개발하였다.

본 논문에서는 이렇게 개발되어 IT보안인증사무국 홈페이지에 등록된 무선랜 인증시스템 보호프로파일에 대해 분석해 본다.

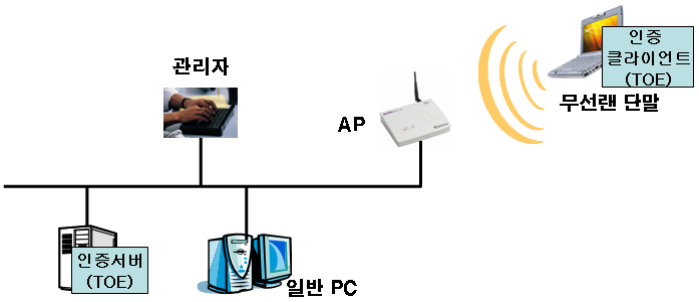
2. 본 론

본 보호프로파일의 TOE인 무선랜 인증시스템은 특정 무선랜에 접근하려는 일반사용자를 상호인증하고, 신뢰된 IT 환경인 AP에게 접근통제 정책을 전송하며, 인가된 일반 사용자의 안전한 무선통신을 지원하기 위한 마스터키를 생성 및 분배하는 시스템으로 [그림 1]과 같이 무선랜 인증서버와 무선랜 인증클라이언트로 구성된다.

본 보호프로파일에서는 TOE가 보호하고자 하는 자산 및 TOE의 동작지원에 필요한 자산의 가치와 위협의 수준을 고려하여 TOE 보안기능요구사항과 TOE 보증요구사항을 도출하였다.

TOE 보안기능 요구사항으로는 무선랜 단말과 AP 사이에 전송되는 사용자 데이터의 안전한 통신을 지원하는데 사용되는 마스터키를 생성·분배·파기하기 위한 FCS 클래스가 요구되며, 무선랜 인증서버

와 무선랜 인증클라이언트를 사용하는 일반사용자가 상호 인증하고 무선랜 서버가 원격의 AP와 관리자를 식별 및 인증하기 위한 FIA 클래스가 요구된다. 또한, 비인가된 사용자에 의한 무선랜 접근통제를 위해 무선랜 인증서버에서 신뢰된 IT 환경인 AP로의 접근통제 정책을 전달하는 TOE 보안기능요구사항인 FMT_SMF.1(관리기능 명세) 컴포넌트와 실질적인 접근통제를 수행하는 IT 환경 보안기능 요구사항인 FDP_ACC.2(완전한 접근통제) 컴포넌트가 요구된다.



[그림 1] TOE 운영환경

본 보호프로파일에서 TOE가 보호하는 자산은 TOE 자체를 포함하여 조직의 무선 네트워크 전송 데이터 및 네트워크에 연결된 컴퓨터의 저장 데이터로서, 자산의 가치는 비교적 높은 수준의 중간이고 위협 수준은 위협원이 획득할 수 있는 접근 정도, 위험 허용치, 가용자원, 전문지식, 동기 등을 고려하여 낮게 평가되었다. 이에 보증등급은 IATF 견고성 등급 결정 지침에 따라 EAL4가 적절한 평가보증등급으로 판단하여 선택하였으며[4], 보안기능 강도는 공통평가방법론의 권고에 의거 공격성공가능성, 자산의 가치 등을 고려하여 확률 및 순열 메커니즘에 대한 기능강도를 중간으로 선택하였다. 또한, 선택된 보증등급을 바탕으로 무선랜 인증시스템 보호프로파일에 대한 TOE 보증요구사항을 도출하였다.

3. 결 론

본 논문은 보호프로파일 개발체계에 의거하여 보호프로파일 개발 자문위원회에서 선정한 무선랜 보안에 속한 정보보호 제품인 무선랜 인증시스템에 대한 보호프로파일 개발 내용을 분석하였다. 이를 통해 무선랜 인증시스템 보호프로파일의 주 사용자인 시스템 개발자와 시스템 조달자가 해당 보호프로파일의 이해를 넓힘으로서 무선랜 인증 제품군에 대한 CC 평가가 활성화 될 것으로 판단된다.

무선랜 인증시스템 보호프로파일을 이용하는 사용자의 주 관심사인 보증등급은 IATF 견고성 등급 결정 지침에 따라 결정되었으며 선택된 보증등급을 기준으로 보증요구사항도 도출되었다.

이러한 IATF 견고성 등급 결정 지침은 정확한 자산 가치와 위협 수준에 대한 판단을 요구하며 이는 위험분석을 통해 이루어질 수 있다. 그러나 정확하고 일관되지 않은 위험분석 결과는 개발되는 보호프로파일 사이에 일관성을 깰 수 있으며, 사용자에게 보호프로파일에 대한 신뢰도를 잃을 수 있다. 이에 관련 연구로서 보호프로파일 보증등급 산정기준 방안에 대한 연구를 통해 이러한 문제점이 해결되어야 할 것으로 사료된다.

4. 참고문헌

[1] "U.S. Government Wireless Local Area Network (WLAN) Client Protection Profile for Basic Robustness Environments", 2003.10

[2] "U.S. Government Wireless Local Area Network (WLAN) Access System Protection Profile for Basic Robustness Environments", 2004.04

[3] "U.S. Government Protection Profile Authentication Server for Basic Robustness Environments", 2005.06

[4] "Information Assurance Technical Framework, National Security Agency Information Assurance Solutions Technical Directors", 2002.09