CC V3.1 기반의 무선침입방지시스템(WIPS) 보안기능 요구사항에 관한 연구

이현정O
한국시스템보증
hjlee@kosyas.com

A Study of WIPS(Wireless Intrusion Prevention System)'s Security Functional Requirements based on Common Criteria Version 3.1

Hyun-Jung LeeO
Korea System Assurance Co., Ltd.

요 약

무선은 편리함만큼 위험성도 높다. 누구나 편리하게 접속할 수 있는 것은 장점이지만, 이 누군가가 악의적 목적의 공격자라면 장점이 아닌 단점으로 순식간에 변화할 수 있는 것이다. 이에 무선 네트워크를 보호할 수 있는 방안 마련은 무선랜 활성화의 선행과제로 꼽힌다. 무선랜 보안의 한 축으로 무선침입탐지시스템(WIDS) 혹은 무선침입방지시스템(WIPS)이라고 불리는 보안시스템 구축에 대한 요구가 증가하고 있는 추세이다. 이에 본 논문에서는 무선침입방지시스템에 대한 보안기능 요구사항을 개발한다. 개발된 보안기능 요구사항은 WIPS 제품 개발자, 제품 도입자 및 WIPS 제품 평가자가 시스템 평가 및 도입 시 참고자료로 충분히 활용될 수 있다.

1. 서 론

무선랜은 통신선로 없이도 쉽게 접근할 수 있다는 편리성이 최대 강점이다. 하지만 편리함이 높다는 것은 그만큼 위험성이 높음을 의미한다. 통신선로 없이도 쉽게 접근 가능한 무선의 장점은 악의적 목적을 지닌 공격자 또한 네트워크에 쉽게 접근할 수 있다는 말과 동일하다. 이러한 위험은 무선랜 네트워크 초기부터 지적된 부분이다. 보안을 중시하는 공공기관이나 일부 기업에서는 무선랜 이용을 아예 금지시켰을 정도다. 보안성에 대한 우려는 무선랜 네트워크는 물론 무선랜 보안 시장을 위축시킨 요소로 작용했다.

무선랜 보안은 최근 전사회적인 보안 강화의 흐름에 따라 새롭게 조명 받고 있다. 유선에 버금가는 속도를 제공하는 802.11n의 등장으로 무선랜은 점차 보편화가 예상되고 있다. 이에 기존 보안성을 이유로 무선을 배제했던 기업과 공공기관에서도 무선랜을 피할 수 없는 과제로 인식하고 있다는 것이 무선랜 보안이 부각되는 첫 번째 요인이다.

또 기존 별다른 보안 의식 없이 무선랜을 구축, 이용하던 고객군에서도 전사회적인 보안 의식 강화로 인해 무선랜 구축의 필요성을 강하게 느끼고 있다는 점이다. 무선랜 기술은 취약성을 가지고 있기 때문에 무선랜 보안을 통한 지속적인 보완이 필요하다. 또 무선랜은 그 특성상 기존 보안시스템의 우회 침입이 가능할 뿐 아니라 침입로그가 남지 않으며, 무선이 도달하는 어느 위치에서건 공격이 가능해 공격자의 물리적 위치 역시 찾기 어려워 무선랜 보안솔루션을 이용한 보안이 필수적이라고 할 수 있다.

무선랜 보안은 크게 두 가지로 나눌 수 있다. 하나는 무선랜 인증과 관련된 부문이며, 다른 하나는 무선침입탐지시스템(WIDS) 혹은 무선침입방지시스템(WIPS)이라고 불리는 보안시스템을 구축하는 것이다.

WIDS/WIPS는 기존 유선 방화벽과 VPN 보안 시스템에서 제공되던 보안 기능을 무선랜으로 확장한 것으로 불법 AP 사용으로 인한 해커 침입 및 기업 내부정보의 유출을 방지할 수 있다. 또 보안 취약점을 야기하는 기업 내외부의 부적절한 AP와 클라이언트의 연결을 차단, 보안사고를 예방하게 된다.

본 논문의 2장에서는 무선침입을 방지할 수 있는 WIPS제품에 대한 소개 및 CC 소개, 3장에서는 무선랜 보안위협, 4장에서는 CC기반 무선랜 보안위협을 대응하기 위한 WIPS제품의 보안기능요구사항을 분석하고 5장에서는 WIPS 보안기능 요구사항 설명 및 세부 보안기능 요구사항, 6장에서는 결론을 맺는다.

2. 관련 연구

2.1 CC(ISO/IEC 15408) 소개

국제공통평가기준(CC: Common Criteria)은 국가마다 다른 정보보호시스템 평가기준을 연계시키고 평가결과를 상호인증하기 위해 제정된 평가기준으로, IT 제품의 보안기능성과 평가 과정에서 그 제품에 적용되는 보증수단에

대한 공통의 요구사항들을 제시함으로써, 독립적으로 수행한 보안성 평가 결과들 간에 상호비교를 가능하게 한다. 공통평가기준은 소비자, 개발자, 평가자에 의해 활용되며, 소비자, 개발자는 자신이 원하는 제품의 보안기능을 공통평가기준에 의거하여 나열하고 서술 할 수 있다.

CC는 크게 세부분으로 구성되어 있다. 제1부 소개 및 일반 모델, 제2부와 제3부는 정보보호시스템에 요구되는 보안기능요구사항과 보안보증요구사항으로 이루어져 있다. 보안기능요구사항에는 보안활동을 정의하고, 보증요구사항은 정보보호시스템이 보안수준에 맞게 정확하게 구현되어있는지에 대한 신뢰를 입증할 수 있는 기록을 제공한다. CC의 핵심은 제2부와 제3부로 정보보호시스템이 제공해야 하는 기능 및 보증요구사항을 기술하고 있으며, 개발자는 기술된 요구사항을 참조하여 정보보호시스템을 개발하거나 소비자는 자신에게 맞는 요구사항을 요청할 수 있다.[2]

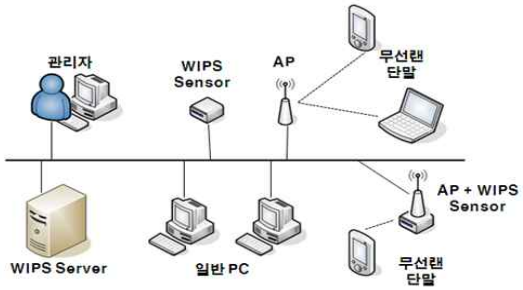
본 논문에서는 공통평가기준 3.1을 바탕으로 WIPS 시스템에 필요한 보안기능요구사항을 도출함으로써, WIPS 시스템을 운영하는데 필요한 기본적인 기능요구사항을 살펴보고자 한다.

2.1 WIPS 시스템 개요

WIPS는 특정 조직에서 운영되는 무선랜을 지속적으로 모니터링하여 인가되지 않은 무선장비들의 접근을 자동으로 탐지 및 방지함으로써, 무선랜의 안정성을 높이고 통합 관리를 할 수 있도록 지원하는 시스템으로 하드웨어, 펌웨어 또는 소프트웨어 형태 등으로 구현된 다양한 형태의 시스템을 포함한다.[3][4][5][6][7][8]
WIPS는 노출돼 있는 무선 네트워크에서 이용되는 무선 AP의 범위 내 불법AP나 사용자 단말기를 이용한 침입 시도, 애드혹(Ad-Hoc)연결, AP의 MAC변조 공격 등을 탐지 및 차단하는 기능을 제공한다.

2.2. WIPS 운영환경

WIPS는 무선랜에 대한 보안정책을 수립하는 WIPS 서버와 무선랜을 통해 전송되는 무선 데이터를 수집하는 센서로 구성된다.



(그림 1) TOE 운영환경

또한 WIPS는 크게 중앙집중형태와 분산 형태의 두 가지 형태 시스템으로 구성할 수 있다. 중앙 집중형 WIPS는 WIPS 센서로부터 수집된 무선 데이터를 모두 서버로 전송하여 중앙집중 처리하는 형태를 의미하며, 분산형 WIPS는 WIPS 서버의 보안정책을 WIPS 센서에 적용되어 센서를 통해 수집된 무선랜 데이터에 센서가 직접 보안정책에 따라 무선 트래픽에 대한 필터링 및 공격 탐지/차단 기능을 수행하는 구조이다.

WIPS 서버와 센서는 각각 독립된 하드웨어 상에 존재하거나 동일 하드웨어 상에서 구동될 수 있다. 특히 센서는 AP와 독립적으로 존재하거나 AP와 결합된 형태로 구성될 수 있다.

WIPS 서버는 물리적으로 안전한 환경에 위치하며, 반드시 관리자만이 접근할 수 있어야 한다.
관리자는 지역 또는 원격으로 WIPS 서버에 접근하여 보안관리 및 감사기록 관리 등을 수행할 수 있다.
관리자와 WIPS 서버 사이, WIPS 서버와 WIPS 센서 사이에 전송되는 데이터를 보호하기 위해 안전한 경로/채널 설정의 보안기능이 제공되어야 하며, 송수신되는 데이터는 사용자 데이터 혹은 TSF(TOE Security Functionality) 데이터가 될 수 있다. 또한 TOE에서 실시간으로 발생하는 감사데이터의 시간 유효성을 확보하기 위해 시간 동기화 기능이 제공되어야 한다.

3. 무선랜 보안 위협분석[1]

WIPS의 보안기능요구사항을 도출하기 위해 현재 무선랜 환경에 대한 위협에 대한 분석이 요구되며, 다음은 현재 무선랜 환경에 존재하는 무선위협요인다.

3.1 Rouge AP(사내 불법 AP 설치)

[문제점]
- 보안관리자의 허가를 받지 않고 사내(기관) 유선망에 비인가 무선AP를 연결하여 사용
- 악의적인 사용자에 의한 비인간 AP 불법 설치

[위협요소]
- 비인가 AP를 통해 기업(기관)의 유선 방화벽이나 다른 보안 솔류션을 우회하여 유선 네트워크로 침투 가능

3.2 Mis-Configuration AP(사내 정책위반 AP)

[문제점]
- 관리자의 실수로 인한 보안정책 미적용 AP 사용
- 악의적인 사용자가 인가된 AP의 보안정책 변경

[위협요소]
- 악의적인 사용자가 보안정책에 위반된 AP를 통해 내부 네트워크 침투 가능

3.3 도청(패킷 모니터링)

[문제점]
- AP에 무선 구간 데이터의 암호화 정책 부재

[위협요소]
- 악의적인 사용자가 통신내용을 감청

3.4 서비스 거부 공격

[문제점]
- 악의적인 공격자의 인증요청시 자원을 할당하는 구조적인 원인에 의해 DoS 공격에 취약

[위협요소]
- 악의적인 공격자에 의한 무차별적인 인증요청으로 무선랜 서비스 무력화 가능

3.5 비인가 접근(사내 AP불법 접속)

[문제점]
- 외부의 악의적인 비인가 사용자가 정상적이 사내 인가 AP에 접속

[위협요소]
- 비밀번호 또는 인증서 없이 AP에 연결하는 개방시스템 인증 방식의 경우 인증절차 없이 사내 네트워크에 침투 가능
- 무선랜 보안을 위해 적용되는 다양한 인증방식을 (WEP, pre-shared key WPA 등) 해킹하여 접속 가능

3.6 Mis-Association(외부 AP/서비스 접속)

[문제점]
- 내부 네트워크를 사용하는 인가된 사용자가 인근 지역의 외부 AP에 접속 가능

[위협요소]
- 인가된 사용자가 외부의 AP에 접속하여 내부의 기밀 자료 유출 가능

3.7 Ad-Hoc Connection(무선네트워크 공유)

[문제점]
- 무선랜 카드에서 제공하는 기능인 AD-Hoc통신을 이용하여 무선 AP를 거치지 않고 무선 사용자끼리 네트워크 구성

[위협요소]
- 인가된 악의적인 사용자가 내부 데이터를 노트북에 저장한 후 Ad-Hoc통신을 이용해 외부에 자료유출
- 해커가 사용 가능한 무료 무선랜으로 위장하여 사용자 유인 후 사용자가 접속을 시돌 할 경우 해커와 네트워크 연결이 되어 내부 자료 유출

3.8 Honeypot AP/Evil Twin(사내 AP서비스 ID도용)

[문제점]
- SSID는 무선 네트워크의 ID이며 의도적 또는 비의도적으로 동일한 SSID로 구성이 가능

[위협요소]
- 사내 사용자는 Honypot AP와 같은 공격 발생 시 정상적인 인가 AP로 판단 접속하게 되고 접속된 인가 사용자의 내부 자료 유출

3.9 MAC Spoofing(사용자 MAC 하드웨어 주소 도용)

[문제점]
- 무선랜 AP로부터 주기적으로 전송되는 Beacon 정보에 의한 AP MAC정보 전송

[위협요소]
- 소프트웨어 기반의 해킹 툴을 사용하여 AP에 전송하는 Beacon정보 해킹
- MAC 주소를 도용하여 중복된 AP를 구성하여 인가된 사용자의 접속을 유도 후 내부 자료 탈취

4. CC를 통한 WIPS 보안기능 요구사항 도출

4.1 TOE 및 TOE 보안문제정의

TOE(Target of Evaluation)는 평가 대상으로 가능한 설명서가 함께 제공되는 소프트웨어, 펌웨어 및/또는 하드웨어의 집합으로 정의된다. 본 논문에서 TOE는 무선랜 취약점 공격에 대응하는 WIPS시스템이다. 보안문제정의는 TOE 및 운영환경에 의해 대응되어야 하는 위협, 수행되어야 하는 조직의 보안정책, 지원되어야 하는 가정사항을 서술한다. 위협은 TOE 및 TOE의 운영환경에 위험을 초래할 수 있는 모든 요소를 의미한다. 조직의 보안정책은 운영환경 내의 실제 또는 가정상의 조직에 의해 현재 및/또는 향후 부과되는 보안규칙 절차 지침을 의미한다. 가정사항은 보안기능성을 제공하기 위해 요구되는 운영환경에 대한 요구사항을 의미한다. [표 1]는 본 논문이 수용하는 TOE의 운영환경에 적용되는 가정사항, 위협, 조직의 보안정책을 나타낸다.

위협	
T.기록실패	위협원은 TOE의 보안관련 사건이 기록되지 않도록 감시기록 저장용량을 소진시킬 수 있다.
T.위장	위협원은 인가된 사용자로 가장하여 TOE에 접근할 수 있다.
T.연속인증시도	위협원은 연속적으로 인증을 시도하여 인가된 사용자 권한을 획득할 수 있다.
T.저장데이터훼손	위협원은 TOE에 저장된 TSF 데이터를 인가되지 않은 방식으로 노출, 변경 또는 삭제할 수 있다.
T.전송데이터훼손	위협원은 TOE 구성요소 사이에 전송되는 사용자 데이터 또는 TSF데이터 및 TOE 관리자와 TOE 사이에 전송되는 TSF데이터를 인가되지 않은 방식으로 노출, 변경할 수 있다.
T.불법네트워크접속	위협원은 사내 AP불법접속, 사내정책위반 AP, 무선단말기 MAC주소도용, WEP Cracking, Hoyneypot AP접속 등의 공격을 통해 보호대상 무선 네트워크에 불법으로 접근함으로써 내부 자산에 손상을 입힐 수 있다.
T.내부정보유출	인가된 사용자는 비인가 외부 AP접속 또는 인가되지 않은 클라이언트 접속(Ad-Hoc접속)등을 통해 사용자데이터에 손상을 입힐 수 있다.
T.보안정책우회	위협원은 보호 대상 네트워크에 비인가 AP(Rouge AP) 설치를 통해 방화벽이나 타 보안 솔루션을 우회하여 유선 네트워크로 접근할 수 있다.
T.서비스거부공격	위협원은 TOE 운영환경에 있는 무선네트워크의 자원을 비정상적으로 조과 사용하여 정상적인 사용자들의 사용을 방해할 수 있다.
조직의 보안정책	
P.감사	보안과 관련된 모든 행동에 대한 책임을 추적하기 위해 보안관련 사건은 기록 및 유지되어야 하며, 기록된 데이터는 검토되어야 한다.
P.안전한관리	TOE는 인가된 관리자가 안전한 방식으로 TOE를 관리할 수 있도록 관리 수단을 제공해야 한다.
가정사항	
A.물리적보안	TOE는 인가된 관리자만이 접근 가능한

	물리적으로 안전한 환경에 위치한다.
A.신뢰된관리자	TOE의 인가된 관리자는 악의가 없으며, TOE 관리 기능에 대하여 적절히 교육받았고, 관리자 지침에 따라 정확하게 의무를 수행한다.
A.운영체제보강	불필요한 운영체제상의 서비스나 수단 등을 모두 제거하는 작업과 운영체제상의 취약점에 대한 보강작업을 수행하여 운영체제에 대한 신뢰성과 안정성을 보장한다.

[표 1] 보안환경

4.2 보안목적

보안목적은 보안문제정의에서 서술된 문제에 대한 해결책을 서술하는 것이며, TOE 보안목적과 운영환경에 대한 보안목적으로 나뉜다. TOE 보안목적은 보안문제정의에서 서술된 문제의 특정 부분을 해결하기 위한 보안 기능성을 제공하며, 이는 TOE가 달성해야 하난 목적의 집합니다. 운영환경에 대한 보안목적은 TOE가 보안기능성을 정확히 제공할 수 있도록 지원하는 기술적·절차적 수단을 말하며, 운영환경이 달성해야 하는 목적을 서술한다. 본 논문은 다음 장에서 TOE 보안목적에 대한 보안기능요구사항을 도출하며, 환경에 대한 보안목적은 다루지 않는다. 다음 [표 2]은 [표 1]를 바탕으로 도출된 보안목적이다.

TOE 보안목적	
O.감사	TOE는 보안과 관련된 행동에 대한 책임을 추적하기 위해 보안관련 사건을 정확하게 기록하고 안전하게 유지해야 하며, 기록된 감사 데이터를 적절하게 검토할 수 있는 수단을 제공해야 한다. 또한 감사 데이터가 포화 상태에 도달했을 때 대응기능을 제공해야 한다.
O.관리	TOE는 TOE의 인가된 관리자가 TOE를 효율적으로 관리할 수 있는 관리 수단을 안전한 방법으로 제공해야 한다.
O.저장데이터보호	TOE는 TOE에 저장된 TSF 데이터를 인가되지 않은 노출, 변경, 삭제로부터 보호해야 한다.
O.식별및인증	TOE는 사용자를 유일하게 식별 및 인증해야 하며, 실패한 인증시도가 연속적으로 발생할 경우 이를 탐지 및 대응해야 한다. 또한, WIPS 서버는 WIPS 센서간의 상호인증을 수행해야 한다.
O.네트워크접근통제	TOE는 사내AP불법접속, 사내정책위반AP, MAC주소도용, WEP Cracking, Honeypot AP접속 등의 공격을 통해 보호대상 네트워크에 불법으로 접근을 통제하여야 한다.
O.내부정보유출방지	TOE는 인가된 사용자가 비인가 외부 AP접속 또는 인가되지 않은 클라이언트 접속(Ad-Hoc접속)등을 통해 사용자 데이터가 유출되는 것을 탐지하고 대응해야 한다.
O.보안정책우회방지	TOE는 보호 대상 네트워크에 비인가 AP(Rouge AP) 설치를 통해 방화벽이나 다른 보안 솔루션의 정책을 우회하여 유선 네트워크에 접근을 통제하여야 한다.
O.서비스거부공격차단	TOE는 보호하는 컴퓨터의 무선 네트워크 서비스가 정상적인 사용자들이 사용할 수 있도록 하기 위하여, 공격자들이 비정상적으로 무선네트워크 자원을 초과 사용할 경우 이를 차단해야 한다.
O.전송데이터보호	TOE는 TOE 구성요소 사이에 전송되는 사용자 데이터 또는 TSF데이터 및 TOE 관리자와 TOE 사이에 전송되는 TSF 데이터를 인가되지 않은 노출, 변경으로부터 보호해야 한다.
환경에 대한 보안목적	
OE.물리적보안	TOE는 인가된 관리자만이 접근 가능한 물리적으로 안전한 환경에 위치해야 한다.
OE.신뢰된관리자	TOE의 인가된 관리자는 악의가 없으며, TOE 관리 기능에 대하여 적절히 교육받았고, 관리자 지침에 따라 정확하게 의무를 수행해야 한다.
OE.운영체제보강	불필요한 운영체제상의 서비스나 수단 등을 모두 제거하는 작업과 운영체제상의 취약점에 대한 보강작업을 수행하여 운영체제에 대한 신뢰성과 안정성을 보장해야 한다.
OE.타임스탬프	TOE는 TOE 운영환경에서 제공하는 신뢰할 수 있는 타임스탬프를 사용해서 보안관련 사건을 정확하게 기록해야 한다.

[표 2] 보안목적

4.3 IT보안요구사항

보안요구사항은 보안목적을 만족시키기 위한 TOE의 요구사항이다. TOE는 모든 보안목적에 충족되도록 도출되어야 하며, [표 3]은 [표 2]을 바탕으로 도출한 WIPS 시스템이 갖추어야할 필 수 보안기능 요구사항이다.

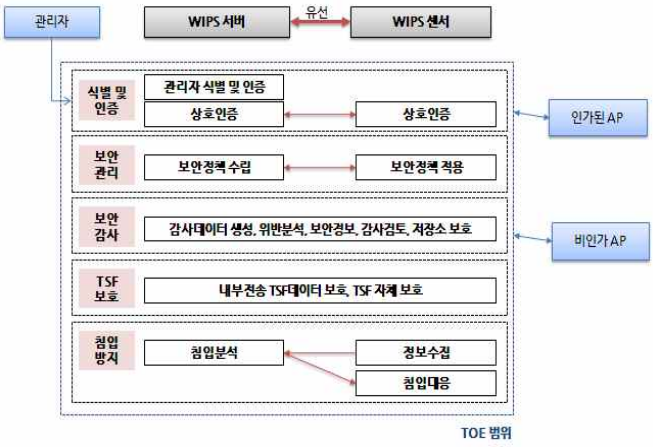
보안기능 클래스	보안기능 컴포넌트	
보안감사	FAU_ARP.1	보안감사
	FAU_GEN.1	감사 데이터생성
	FAU_SAA.1	잠재적인 위반 분석
	FAU_SAR.1	감사 검토
	FAU_SAR.3	선택가능한 감사 검토
	FAU_STG.1	감사 증적 저장소 보호
	FAU_STG.3	감사 데이터 손실 예측시 대응행동
	FAU_STG.4	감사 데이터의 손실 방지
사용자 데이터 보호	FDP_IFC.1	부분적인 정보흐름통제
	FDP_IFF.1	단일 계층 보안속성
식별 및 인증	FIA_AFL.1	인증 실패 처리
	FIA_ATD.1	사용자 속성 정의
	FIA_SOS.1	비밀정보의 검증
	FIA_UAU.1	인증
	FIA_UAU.7	인증 피드백 보호
	FIA_UID.1	식별
보안관리	FMT_MOF.1	보안기능 관리
	FMT_MTD.1	TSF 데이터 관리
	FMT_SMF.1	관리기능 명세
	FMT_SMR.1	보안 역할
침입방지	FIP_COL.1 (확장)	침입방지대상사건 정보 수집
	FIP_ANL.1 (확장)	침입분석
	FIP_RCT.1 (확장)	침입대응
TSF 보호	FPT_ITT.1	내부전송 TSF 데이터의 기본적인 보호

보안기능 클래스	보안기능 컴포넌트	
	FPT_TST.1	TSF 자체 시험
TOE 접근	FTA_SSL.3	TSF에 의한 세션 종료

[표 3] 보안기능요구사항

5. WIPS 보안기능 요구사항 설명

WIPS의 주요 보안기능 (그림 2)와 같다.



(그림 2) TOE 범위

1) 식별 및 인증(FIA)

TOE는 무선침입방지시스템에 접근하는 관리자에 대해 사용을 허가 이전에 관리자에 대한 식별 및 인증 수행을 통해 정당한 사용자 인지를 확인하며, 관리자 인증 실패 시 대응행동을 제공하도록 보장한다. 또한, WIPS 서버와 WIPS 센서 상호 간의 식별 및 인증 기능을 제공한다.

2) 보안관리(FMT)

TOE는 보안기능, 보안속성, TSF 데이터, 보안역할 등과 관련된 사항을 관리한다. 전체적인 TOE의 보안관리는 관리자에 의해 수행된다.

3) 무선침입방지(FDP, FIP)

TOE는 무선랜을 통해 송수신 되는 데이터를 중재하기 위해 관련 보안 정책이 수행됨을 보장한다. 즉, TOE는 무선랜을 통해 유입되는 데이터를 사전에 탐지한 후 차단하여 무선랜 위협으로부터 내부망의 정보자산 및 자원을 안전하게 보호한다. 무선랜에서 발생하는 위협은 비인가 AP, 사용자 단말기를 이용한 침입시도, Ad-Hoc 연결, AP의 MAC 변조 공격등을 포함한다.

4) 보안감사(FAU)

TOE는 보안과 관련된 행동에 대한 책임을 추적하기 위해 보안 관련 사건들의 감사 레코드를 생성, 기록, 검토한다. 또한 감사된 사건에 대한 잠재적 보안 위반을 탐지하고 대응행동을 수행한다.

5) TSF보호 및 접근(FPT)

TOE는 장애 시 안전한 상태를 유지하고, TSF 데이터 및 실행코드의 무결성을 검증하기 위한 자체시험을 수행한다. 또한, WIPS 서버와 WIPS 센서간에 전송되는 TSF 데이터는 기본적인 보호방안 및 사용자 비활동 기간 이후에 대한 세션관리 기능을 제공한다.

5.1 WIPS 세부 보안기능요구사항 도출

CC를 통해 도출된 보안기능요구사항을 구체적인 기능으로 도출하면 다음과 같으며, 이는 WIPS 제품에 필수적으로 구현되어야 현존하는 보안 무선랜 보안위협에 대응할 수 있다.

5.1.1 무선침입 탐지 및 대응기능

1) 비인가 클라이언트 탐지 및 대응기능
- 복수의 인가된 사내 AP에 불법 접근하는 비인가 Client 탐지 및 차단
- 인가된 사내 AP에 불법 접근하는 비인가 Client의 위치 추적
- 재시작 되는 인가된 사내 AP탐지

2) 비인가 AP 탐지 및 대응기능
- 사내 네트워크에 연결된 비인가 AP탐지 및 차단
- 비인가 AP의 보안 구성분석(Open, WEP, WPA, WPA2 등)
- 복수의 비인가 AP로 접근하는 복수의 인가 Client 탐지 및 차단
- 비인가 AP의 위치 추적 및 정확성
- 비인가 AP에 접근하는 인가 client의 위치 추적

3) 외부 AP 탐지 및 대응기능
- 외부 AP 접속을 시도하는 인가 Client 탐지 및 차단
- 외부 AP에 접속하는 인가 Client의 위치 추적

4) 정책 위반 AP 탐지 및 대응기능
- 보안 정책을 위반한 인가 AP 탐지 및 차단
- 정책위반 AP로 접근하는 인가 Client 탐지 및 차단
- 정책 위반 AP의 위치 추적

5) 기타 탐지 및 대응기능
- 인가 Client의 Adhoc 통신 탐지 및 차단
- Blutooth, HSDPA, WiBro등 다양한 무선 연결에 대한 통제 기능 지원

5.1.2 해킹 방어 기능

1) DoS 공격 방어 기능
- 인가 Client에게 DoS 공격 탐지 및 방어 기능 (Deauth, Disassoc, 기타)
- 인가 AP에 대한 DoS 공격 탐지 및 방어
- DoS 공격 탐지/방어 상태에서 새로운 DoS 공격에 대한 탐지 방어 수행

2) WEP Cracking
- 인가 AP대상 WEP Craking 공격 탐지 및 방어

3) MAC Spoofing
- 인가 client 대상 MAC Spoofing 공격 시 탐지 및 방어

4) Fake AP
- 인가 AP의 BSSID와 동일한 불법 AP 탐지
- 인가 AP의 SSID와 동일한 불법 AP 탐지
- Fake AP에 접근하는 인가 Client 탐지 및 차단

5) 다중공격
- 공격이 동시 다발적으로 발생할 경우 탐지 및 방어
- 공격 발생 시 복수의 공격자의 위치 추적

6) 기타
- Active Probing 시 다양한 Probing Tool에 대한 탐지 및 차단
- 공격자의 서비스 지역 이동 시 탐지 및 차단

5.1.3 식별 및 인증

1) 관리자 식별 및 인증
- 정당한 사용자만이 WIPS서버에 접속할 수 있도록 사용자의 정당성을 증명할 수 있는 기능

2) 에이전트/서버 상호인증
- 정당한 에이전트만 네트워크에 접속할 수 있음을 증명할 수 있는 기능
- 정당한 서버만이 에이전트에 정책을 송신할 수 있음을 증명할 수 있는 기능

5.1.4 보안감사

1) 보안감사 생성기능
- 위협 탐지 및 대응에 대한 보안감사 생성기능
- 해킹 탐지 및 대응에 대한 보안감사 생성기능
- 식별 및 인증에 대한 보안감사 생성기능

2) 보안 경고기능
- 센서에러 등 센서 장애 시 이상 유무 탐지 및 위치 정보 제공 기능
- 장애 및 침해사고 발생 시 경고. 통지 기능 제공
- 장애 및 침해사고 수준에 따른 경고 기능 제공

5.1.5 WIPS 보안 관리 기능

1) 정책관리
- 환경설정, 보안정책, 탐지 패턴 등에 대한 설정
- 정책 백업기능
- 자원관리 기능 및 보안정책 일괄 적용, 중앙집중 관리
- 센서 수량, 탐지 현황, 위치 등 정보의 실시간 파악

2) 로그관리 기능
- 센서에서 탐지되는 모든 이벤트에 대한 로그 저장 및 분석
- 다양한 로그분석 기능(센서별/시간별/장소별 현황 분석)

3) 패치 및 업그레이드
- 탐지 패턴 및 보안 정책 추가 시 업그레이드 기능
- 패턴 추가 시 패턴에 대한 정보 제공

5.1.6 TSF보호 및 접근

1) 접근관리 기능
- 관리 콘솔 접근 시 인증 및 세션 암호화 기능 수행 (SSL, SSH 등)

2) 보안기능 보호
- 주요 프로세스에 대한 감시를 통한 제품의 안정성 보장
- 주요 파일에 대한 무결성 검증을 통한 제품의 안정성 도모

5. 결론

WIDS/WIPS는 무선 네트워크에 대한 24시간 모니터링을 통해 무선랜상의 위협을 탐지함으로써 보안사고를 예방하게 된다. 주변에 불법적으로 설치돼 있거나 침입을 시도하는 공격자의 위치까지도 실시간으로 탐지해 사전에 위험요소를 제거할 수 있는 보안조치를 수행할 수 있기 때문이다.

본 논문은 공통평가기준을 기반하여 무선침입방지시스템의 보안성에 대한 객관적인 평가를 위해 CC(ISO/IEC 15408)을 기반으로 필수 보안기능 요구사항을 도출하였다.

무선랜 확산에 따라 무선랜 보안의 상당부분을 해소할 수 있는 WIPS 도입이 기대되고 있으나, 올바른 제품에 대한 선택만이 무선랜 보안의 이러한 기대를 충족시킬 것이다. 이에 본 논문은 WIPS 도입하는 기관 및 WIPS를 개발하는 개발자, WIPS의 제품의 품질을 평가하는 평가기관에 참고자료로 활용됨으로써 무선랜 보안에 이바지 할 것으로 기대된다.

6. 참고문헌

[1] 한국인터넷진흥원, “무선랜 보안 안내서”, 2010.1

[2] 정보보호시스템 공통평가기준(행정안전부고시 제2009-52호)

[3] http://www.airmagnet.com

[4] http://www.airdefense.com

[5] http://www.cisco.com

[6] http://www.aruba.com

[7] http://www.3com.com

[8] http://www.kwise.co.kr