情報保護學會論文誌
第20卷 第2號, 2010. 4

와이브로의 초기인증에 적합한 명세기반의 침입탐지시스템

이 윤 호,† 이 수 진‡
국방대학교

Specification-based Intrusion Detection System for the Initial Authentication Phase of WiBro

Yunho Lee,† Soojin Lee‡
Korea National Defense University

요 약

IEEE 802.16e 표준을 기반으로 하는 와이브로(WiBro) 서비스는 순수 국내 기술로 개발된 초고속 무선 휴대인터넷 기술이다. 본 논문에서는 와이브로 초기인증 단계에서 생길 수 있는 보안취약점을 분석하고 그러한 보안위협을 대상으로 한 공격을 탐지할 수 있는 명세기반의 침입탐지시스템을 제안한다. 제안된 침입탐지시스템은 PKMv2 EAP-AKA 기반의 정상적인 초기 인증 동작방식을 명세화하여 상태전이머신으로 모델링한 후 명세에 기반한 침입탐지를 실시한다. 본 논문에서는 초기인증 과정에서 발생 가능한 다섯 가지의 공격들을 시나리오로 모델링하고, 시나리오 기반의 실험을 실시하여 제안된 침입탐지시스템의 탐지성능을 검증한다.

ABSTRACT

WiBro(Wireless Broadband), the service based on IEEE 802.16e(mobile WiMAX) standard, is a wireless broadband Internet technology being developed by the domestic telecommunication industry. In this paper, we analyze security vulnerabilities of WiBro focusing on initial authentication phase and propose a specification-based intrusion detection system that can detect those vulnerabilities. We first derive a specification from the normally operational process of the initial authentication based on PKMv2 EAP-AKA and formalize the derived specification as a state transition diagram. Proposed system executes the intrusion detection based on those specification and state transition diagram. In this paper, to verify the detection capability of proposed system, we construct a test bed network and execute scenario-based test.

Keywords: WiBro, Information security, Intrusion detection

I. 서 론

기술개발에서 표준에 이르기까지 모두 순수 국내기술로 개발된 와이브로(Wireless Broadband : WiBro)는 휴대 인터넷 단말기를 이용하여 정지 및 이동 중에도 언제 어디서나 고속으로 무선 인터넷 접속이 가능한 서비스이며, 4세대 이동통신의 핵심기술이 될 것으로 전망된다[1].

와이브로에서의 보안은 매체접근제어계층(Media Access Control : MAC) 내 3개 부계층(sub-layer) 중 보안 부계층(security sublayer)에서 담당한다. 보안 부계층은 인증 및 키 관리를 위한 프라이버시 키 관리(Privacy Key Management: PKM) 프로토콜과 패킷 데이터에 대한 암호화를 위

접수일(2009년 9월 14일), 수정일(2009년 12월 19일), 게재확정일(2010년 1월 22일)
† 주저자, yunholee@gmail.com
‡ 교신저자, cyberkma@gmail.com

한 프로토콜로 구성되어 있으며, PKM 메시지를 기반으로 하여 기지국/제어국 및 단말기 간의 인가 제어, PKI 인증, 키 관리, 확장형 인증프로토콜(Extensible Authentication Protocol:EAP) 캡슐화에 의한 기밀성 및 무결성 등을 제공한다. 그러나 와이브로 보안 부계층에 대한 분석 결과 초기 인증과정 시 보안취약점이 존재하며, 이러한 취약점을 이용하여 다양한 공격들이 수행 가능함을 발견하였다. 또한 발견된 문제점들은 이미 정의된 와이브로 규격상의 예방책 차원의 보안대책으로는 탐지나 제거가 불가능하며 보다 더 능동적인 차원에서의 보안대책인 침입탐지시스템의 적용이 필요한 상황이다.

침입탐지시스템은 탐지 방법에 따라 비정상행위탐지(anomaly detection), 오용탐지(misuse detection) 및 명세기반탐지(specification-based detection)로 구분할 수 있다. 비정상행위탐지는 일반적인 시스템 사용 패턴에서 벗어나는 비정상 행위들을 탐지한다. 오용탐지는 이미 알려진 공격 패턴을 이용하여 알려진 공격들에 대해 감시함으로써 탐지가 이루어진다. 명세기반의 탐지기법은 정상행위에서 벗어난 공격을 탐지한다는 점에서는 비정상행위탐지와 유사하다. 그러나 기계 학습 기법에 의존하지 않고, 적법한 시스템 행위들을 모델링하여 수동으로 개발한 명세를 기반으로 하며, 개발한 명세들에 보안 규칙을 적용시켜 그 규칙을 위험한 객체의 실제 동작과 비교해 탐지하는 특징이 있다. 이러한 명세기반의 탐지기법은 오용탐지의 단점인 알려지지 않은 침입에 대응할 수 있고, 비정상행위탐지의 단점인 오탐율을 낮출 수 있는 장점이 있다. [4]에서는 명세기반의 탐지기법을 적용하여 애드혹 네트워크에 대한 AODV 프로토콜의 정상적인 동작 과정을 유한상태머신(Finite State Machine: FSM)으로 모델링하고, 이를 이용하는 침입탐지기법을 제안하였다. [5]에서는 IEEE 802.11 무선 네트워크 프로토콜에 명세기반의 탐지기법을 적용하여 공격을 탐지할 수 있을 뿐만 아니라 정책순응을 모니터할 수 있는 침입탐지시스템을 제안하였는데, 이는 네트워크 프로토콜의 상태변화 모델과 사이트 보안 정책의 제약사항을 기반으로 한다. 이러한 연구 사례들과 국내 와이브로 환경의 특성 즉, 알려진 악성코드 데이터베이스가 부족하고, 다양한 단말기를 사용하고 있는 특징을 고려하면, 와이브로 환경에서는 명세기반의 탐지방법이 적합하다고 할 수 있다. 따라서 본 논문에서는 PKMv2의EAP-AKA(Authentication and Key Agreement)을 이용한 와이브로 초기 인증과정에 중점을 두고, 능동적으로 악의적인 공격행위를 탐지할 수 있는 명세기반의 침입탐지시스템을 제안한다. 이를 위해 우선 와이브로의 초기 인증 과정을 상태전이머신으로 모델링하고, 와이브로 표준을 분석하여 도출된 보안취약점들을 바탕으로 수행 가능한 공격행위 다섯 가지를 식별 및 정의하였다. 그리고 자원사용의 효율성을 보장하기 위해 모델링된 초기인증상태전이머신상에서 정상적인 상태전이와 제어 메시지 생성 등을 기반으로 간결한 탐지논리에 의해 악의적인 공격행위를 탐지해 낼 수 있는 명세기반의 침입탐지 모델을 제안하고, 프로토타입을 정의하여 구현하였다. 또한 제안된 침입탐지 모델의 탐지성능 검증을 위해 와이브로 기반의 실험환경을 구축하고, 식별된 다섯 가지의 공격행위를 모델링하여 시나리오 기반의 실험을 실시하였다.

본 논문의 구성은 다음과 같다. 2장에서는 와이브로의 기본 개념 및 와이브로에서 보안을 담당하는 보안 부계층에 대해 기술하고 3장에서는 초기 인증 시 생길 수 있는 보안위협에 대해 기술하고 그 위협을 탐지할 수 있는 명세를 명시한 초기 인증 상태 전이 머신과 W-IDS(WiBro Intrusion Detection System) 프로토타입을 정의한다. 4장에서는 W-IDS에 대해 공격 시나리오에 따라 실험을 실시하고 그 결과를 통해 W-IDS 적용 가능성을 증명한다. 마지막으로 5장에서는 향후 연구방향을 제시하고 결론을 맺는다.

II. 와이브로(Wireless Broadband : WiBro)

2.1 개요

와이브로는 무선랜(Wi-Fi)과 같이 무선환경에서 인터넷 서비스를 제공하고, 초고속 인터넷 서비스처럼 광대역 인터넷 접속이 가능하다는 의미에서 Wireless와 Broadband의 합성어로 만들어졌다. 전송속도, 이동성, 셀 반경 등의 측면에서 현재의 이동전화와 무선 LAN의 전달거리와 전송속도 면에서의 장단점을 보완할 수 있으며, 도심지 내에서 1Mbps이상의 무선 인터넷 서비스를 이동 중에도 끊김 없이 사용 할 수 있는 대표적인 차세대 이동통신 기술이다[2][3].

2.2 인증 및 키관리 기술

이번 절에서는 와이브로 보안계층의 핵심기능인 인증 및 키 관리기술을 살펴본다. 와이브로 인증 및 키

관리에 사용되는 PKM 프로토콜 및 동작방식을 우선 다루며, 초기 버전인 PKMv1보다는 개정된 PKMv2를 소개한다.

와이브로 보안 부계층은 인증, 키교환을 위해 PKM 프로토콜을 사용한다. PKM은 초기 접속, 인증, 등록, hand-off 등 60여개의 MAC 관리 메시지 중 보안 관련한 메시지 집합이다. PKM 프로토콜은 단말/기지국간 합법적인 단말/사용자를 인증하고, 인증된 단말/사용자에 대한 세션 키 및 데이터 암호화 키 관리 기능을 가지고 있다. PKM은 인증 및 키 관리를 위한 메시지만 정의하고 있으며, 실질적인 인증 및 키 관리 처리는 PKM 관리 메시지 Payload에 포함되어 있다.

PKMv2는 RSA 기반 인증방식과 EAP 기반 인증방식을 지원한다. RSA 기반 인증방식은 PKMv1과 같은 RSA 기반의 공개키와 단말의 MAC 주소를 결합한 X.509인증서를 사용하지만, 기지국도 단말에 인증서를 제공하는 양방향 인증방식을 사용하며, 인증 시 메시지 무결성 보장을 위해 전자서명이 포함되고, 재연공격을 방지하기 위한 난수 등이 추가되어 PKMv1에서 예상되었던 취약성을 개선하였다[2][3]. EAP 기반 인증방식은 IEEE 802.1x 포트 기반의 가입자 인증 데이터 전송을 위한 표준 프로토콜로, EAP-MD5, EAP-TLS, EAP-AKA 등 다양한 인증 프로토콜을 사용할 수 있으며, 사용자 인증 및 단말, 그리고 네트워크간 상호인증이 가능하다. 또한, 인증 서버를 통해 인증을 수행하기 때문에, 사용자가 증가해도 기지국에 오버헤드가 생기지 않는다는 장점이 있다.

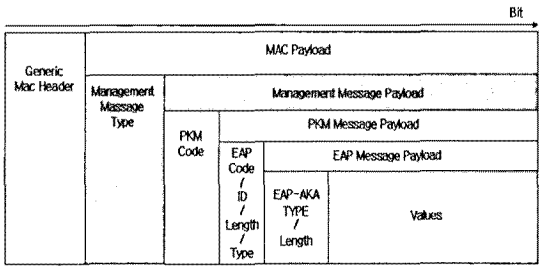
III. 명세기반의 침입탐지시스템

본 장에서는 와이브로의 초기 인증 시 보안 취약점에 대해 살펴보고 이러한 보안상 취약점을 보완하기 위하여 정상적인 초기 인증 과정의 명세를 모델링하고 이 명세를 위반하는 공격 형태를 정의한다. 그리고 악의적인 행위를 탐지할 수 있는 알고리즘을 제안하며, 이를 수행하기 위한 W-IDS를 설계한다.

3.1 와이브로 보안 위협

3.1.1 메시지 형식

PKMv2 EAP-AKA 메시지 형식은 그림 1과 같다. PKMv2 EAP-AKA 메시지는 Generic Mac Header로부터 Management Message Type, PKM Code까지가 와이브로에서 캡슐화된 부분이고 EAP, EAP-AKA 부분은 각각 [7],[8] 표준을 따른다. 보안관련 메시지 내용 요약은 표 1과 같다.



[그림 1] PKMv2 EAP-AKA 메시지 형식

3.1.2 위협분석

(1) 기본가정

와이브로의 근간이 되는 WiMAX의 보안취약점에 대해 연구 발표된 논문 [6]을 기반으로 향후 발생할 수 있는 보안위협을 보다 현실적으로 도출하기 위해 본 논문에서는 다음 3가지 조건을 전제 한다. 첫째, 공격자는 MAC주소를 탐지 또는 변경할 수 있다. 와이브로에서 모든 네트워크 장비는 48비트의 MAC 주

[표 1] 보안관련 메시지 내용

구 분	내 용
Manage_ment Message Type	Type 9: PKM-REQ, Type:10 PKM-RSP 이외 초기접속, 등록, handoff 등 60여개의 종류가 있음
PKM Code	0~255까지 있으며 Type6 : AuthReject ... , Type17 : PKMv2 EAP Start, Type18 : PKMv2 EAP Transfer ... Type29 : PKMv2 EAP Complete *Type17,18 : EAP-AKA 관련 메시지
EAP Code / ID /Length / Type	Type1 : Identity ... , Type4 : MD5-Challenge , Type5 : OneTimePassword... Type23 : AKA ... , Type255 : Experimentaluse *Type23 : AKA Method 사용 구분
EAP-AKA TYPE / Length	AKA-Challenge, AKA-Authentication-Reject... , AKA-Synchronization-Failure... , AT_RAND, AT_AUTN....

소를 펌웨어(firmware)에 내장하도록 되어있다. 이 값은 Ranging, 인증 절차 등에서 사용된다. 이러한 MAC 주소는 RNG-REQ(Ranging Request), RNG-RSP(Ranging Response)에 포함되기 때문에, 공격자는 인가된 단말의 MAC주소를 알아낼 수 있을 것으로 예상된다. 둘째, 공격자는 강한 시그널을 사용한다. 무선랜의 경우, 채널 사용이 가용할 때 단독으로 공격메시지가 전송되지만, 와이브로는 공격메시지 전송시점에 정상 기지국에서의 신호가 동시에 전송되므로, 정상기지국에서 전송되는 신호보다 강할 것이다. 셋째, 공격자는 정상 단말과 동일한 시점에 공격 메시지를 전송할 수 있다. 즉 와이브로는 기지국에 의해 할당된(bandwidth allocation) 송수신시간에만 트래픽을 송수신할 수 있으므로, 공격자는 각 단말에게 할당된 스케줄링, 통신방법을 알 수 있을 것이다.

(2) PKMv2 EAP-AKA 보안 위협

와이브로 표준에 의하면 PKMv2에서는 EAP-AKA의 보안위협 단점을 보완하고 일반적인 재연공격 및 메시지위변조를 막기 위해 PKM Code 부분에 HMAC/CMAC 및 키 일련번호로 캡슐화하여 보안을 한층 더 강화 했다. 하지만 와이브로 표준에 따르면 초기 인증 시(3-way handshake 과정 이전)에는 HMAC/CMAC 및 키 일련번호 값이 Null 값으로 전달되기 때문에 사실상 초기 인증 시 평문으로 데이터를 보내는 것과 같아 데이터 위변조 및 재연공격이 야기될 수 있다.

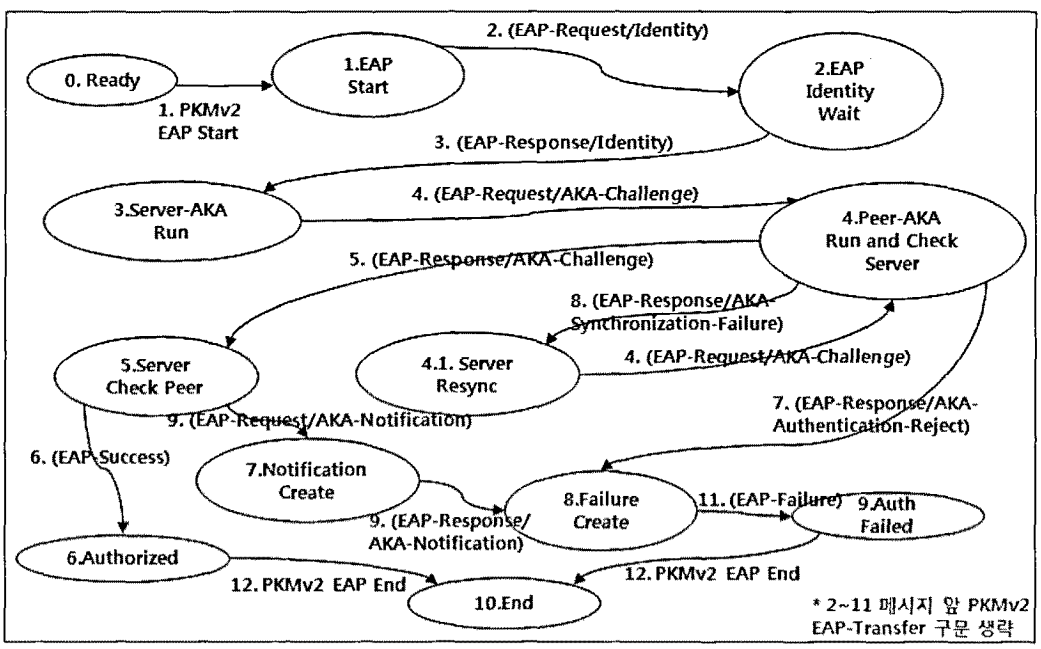
3.2 인증상태전이머신

위의 위협분석으로 와이브로의 초기 인증 시 보안이 취약하다는 것을 알 수 있다. 그러므로 이번 절에서는 정상적인 초기 인증과정의 명세를 모델링하여 그 명세를 위반하는 공격 형태를 정의한다.

3.2.1 정상 인증 상태 다이어그램

그림 2는 [7],[8]을 기준으로 PKMv2 EAP-AKA 인증과정 중 정상적인 행위 및 상태를 명세하여 정상 인증 상태 다이어그램을 제안한 것이다. 여기서 상태는 0~10까지로 나뉠 수 있으며 각 상태별 설명은 표 2와 같고 상태간의 간선 1~12는 상태간의 전송되는 메시지를 나타낸다.

PKMv2 EAP-AKA 초기 인증과정에서의 보안 취약점을 이용한 보안 위협 유형은 다음 다섯 가지 형태로 도출될 수 있다.



[그림 2] 정상 인증 상태 전이머신

(1) EAP-Failure 메시지에 의한 단말 DoS 공격

기지국으로 위장한 공격자가 단말에게 (EAP-Failure) 메시지를 전송하여 정상단말이 서비스를 받지 못하게 하는 공격이다. 이 공격은 초기 인증 시 키 일련번호 값과 HMAC Digest/CMAC Digest 값이 null 값으로 전송되고 EAP Payload 값이 평문으로 전송되기 때문에 Identity 값을 알아낼 수 있다면 가능하다.

〔표 2〕 정상 인증 상태 설명

상태명	설 명
0. Ready	인증상태 머신 초기 대기상태
1. EAP Start	단말이 EAP-Start 메시지를 받고 인증상태 머신 시작상태
2. EAP Identity Wait	단말이 (EAP-Request/Identity) 메시지를 받고 천이 후 단말의 Identity를 기다리는 상태
3. Server-AKA Run	서버가 (EAP-Response/Identity) 메시지를 받고 천이가 된 상태, 이때 서버에서는 RAND, AUTN 생성
4. Peer- AKA Run and Check Server	단말이 (EAP-Request/AKA- Challenge) 메시지 수신 후 천이가 된 상태, 이때 단말에서는 AUTN, MAC 검증 및 RES 생성
4.1 Server Resync	서버가 (EAP-Response/AKA- Synchronization-Failure) 메시지 수신 후 천이된 상태, 이때 서버는 다시 (EAP-Request/AKA-Challenge) 메시지를 단말에 전송
5. Server Check Peer	서버가 (EAP-Response/AKA- Challenge) 메시지 수신 후 천이가 된 상태, 이때 서버는 RES, MAC 검증
6. Authorized	단말이 (EAP- Success) 메시지 수신 후 천이가 되고 정상 인증 상태
7. Notification Create	단말이 (EAP-Request/ AKA-Notification) 메시지 수신 후 천이가 되고 서버 쪽에서 RES, MAC 검증이 안 된 상태
8. Failure Create	단말이 (EAP-Response/AKA- Authentication-Reject) 또는, (EAP-Response/AKA-Notification) 메시지 수신 후 천이가 되고 인증 실패 메시지를 전송하는 상태
9. Authentication Failed	단말이 (EAP-Failure) 메시지 수신 후 천이가 되고 인증에 실패한 상태
10. End	인증상태 머신 종료 상태

(2) EAP-Failure 메시지 유도 단말 DoS 공격

이 공격은 단말로 위장한 공격자가 기지국으로 하여금 PKMv2 EAP-Transfer(EAP-Failure) 메시지 전송을 유도하여 정상적인 단말이 서비스를 받지 못하게 하는 공격이다.

〔7〕,〔8〕에 의하면 PKMv2 EAP-Transfer (EAP-Failure) 메시지 전송을 유도하는 메시지들은 다음과 같다.

- PKMv2 EAP-Transfer(EAP-Response/AKA- Authentication-Reject)
- (EAP-Request/AKA- Notification)
- (EAP-Response/AKA- Notification)

이 메시지들 또한 초기 인증 시 키 일련번호 값과 HMAC Digest/CMAC Digest 값이 null 값으로 전송되고 EAP Payload 값이 평문으로 전송되기 때문에 Identity 값을 알아낼 수 있다면 가능하다.

(3) Resynchronization looping 서버 DoS 공격

이 공격은 단말로 위장한 공격자가 기지국으로 (EAP-Response/AKA-Synchronization- Failure) 메시지를 지속적으로 전송하여 기지국이 (EAP-Request/AKA-Challenge) 메시지를 반복적으로 전송하게 하는 공격이다. 이 때문에 정상단말 및 기지국은 서비스를 제공할 수 없게 된다.

(4) PKMv2 EAP-Start 메시지를 통한 단말 DoS 공격

이 공격은 정상단말의 CID와 Identity를 획득한 공격자가 정상단말로 위장하여 기지국으로 PKMv2 EAP Start 메시지를 지속적으로 전송하여 정상단말이 서비스를 받지 못하게 하는 것이다.

(5) RES-CMD 전송유도

RES-CMD 메시지는 Reset Command 명령어로 정상단말의 모든 통신을 중단시키고, 망접속을 초기화 시키는 명령어이다. 와이브로 표준에 의하면 RES-CMD 메시지는 '이 메시지는 단말이 기지국에게 응답하지 않을 때 또는 단말로부터 상향링크 전송 시 장애가 계속됨을 기지국이 감지할 때 이용될 수도 있다.'라고 기술되어 있다. 이에 정상적인 단말로 위장한 공격자가 기지국에 응답 메시지를 지속적으로 보낸다면 기지국은 RES-CMD 메시지를 정상단말에 전송하여 서비스를 받지 못하게 된다.

3.2.2 초기 인증 상태 전이머신

3.1.2절에서 PKMv2 EAP-AKA의 보안 위협을 유발할 수 있는 유형들을 찾아냈고 이를 정상 인증 상태 다이어그램에 포함하면 그림 3과 같은 초기 인증상태 전이머신을 도출할 수 있다. 초기 인증상태 전이머신에는 단말과 기지국/제어국간의 정상적인 인증 상태 전이도와 각 상태별로 전송 가능한 메시지 종류 및 정상 상태에서 같은 메시지를 받아도 정상 상태라고 감내할 수 있는 임계치 값이 정의 되어있다. 임계치 값은 재전송까지 허용하는 두 번으로 정의했다.

3.3 상태전이 위반 위협 탐지

초기 인증상태 전이머신은 PKMv2 EAP-AKA에서 생길 수 있는 위협을 탐지할 수 있다. 초기 인증상태 전이머신은 인증 받으려 하는 단말 및 기지국의 정상적인 인증 과정과 메시지 형식을 명세하고 있기 때문에 인증을 위해 전송되는 메시지의 진행과정을 추적하여 올바른 상태를 거치지 않고 전송되는 메시지나 지속적으로 같은 메시지를 전송하는 단말 및 기지국의 침입을 탐지할 수 있는 것이다.

다음은 초기 인증 상태 전이머신을 이용한 각 보안 위협으로부터 침입을 탐지하는 개략적인 방법이다.

(1) 위협탐지 공통사항

IDS에서는 각 인증과정 상태를 MAC Header의 CID(Connection Identifier)와 PKMv2 EAP-AKA의 Identity를 기준으로 인증과정 전이 상태를 유지한다.

(2) EAP-Failure 메시지에 의한 단말 DOS 공격탐지

그림3의 8번 상태가 아닌 상태에서 PKMv2 EAP-Transfer(EAP-Failure) 메시지를 전송 할 때 EAP-Failure 알람을 일으킨다.

(3) EAP-Failure 메시지 유도 단말 DOS 공격탐지

4번 상태가 아니면서 (EAP-Response/AKA-Authentication- Reject) 메시지를 전송 할 때, 5번 상태가 아닌 상태에서 (EAP- Request/AKA-Notification) 메시지를 전송 할 때, 7번 상태가 아닌 상태에서 PKMv2 EAP-Transfer(EAP- Response/AKA-Notification) 메시지를 전송할 때 EAP-Failure 유도 알람을 일으킨다.

(4) Resynchronization looping 서버 DOS 공격탐지

4번 상태에서 임계치 이상 (EAP-Response/AKA- Synchronization-Failure) 메시지를 전송할 때 Resynchronization looping 알람을 일으킨다.

(5) PKMv2 EAP-Start 메시지 이용 단말 DOS 공격탐지

CID를 기준으로 지속적으로 임계치 이상 PKMv2 EAP-Start 메시지를 전송할 때 EAP-Start 알람을 일으킨다.

(6) RES-CMD 전송유도 탐지

2번 상태에서 (EAP-Response/ Identity) 메시지가 임계치 이상 전송될 때, 4번 상태에서 (EAP-Response/AKA- Challenge)가 임계치 이상 전송될 때, 7번 상태에서 (EAP-Request/AKA-Notification) 메시지가 임계치 이상 전송될 때 RES-CMD 알람을 일으킨다.

3.4 W-IDS 설계

3.4.1 운영개념

W-IDS는 초기 인증 시 발생하는 모든 와이브로 패킷을 스니핑(Sniffing)하여 모니터링하며 'MaintainSessionState', 'IEASM(Init EAP Auth State Machine) Constraints' 정보를 가지고 있다. 'MaintainSessionState'는 와이브로 패킷을 전송할 때 모니터링 대상인 초기 인증 시 발생하는 패킷만을 필터링하고 초기 인증 상태 머신에 정의되어 있는 각 상태별로 구분하여 유지하는 역할을 하며, 'IEASM Constraints'는 각 세션별 상태가 정상인지 비정상인지를 확인하여 위협탐지를 한다.

3.4.2 설계

W-IDS는 세션의 상태를 유지하는 부분과 침입을 탐지하는 부분으로 나눠서 구현된다. 그림 4는 세션의 상태를 유지하는 의사코드의 일부이다.

W-IDS에서 스니핑한 패킷은 패킷내 source,

address, destination address, CID, Identity로 구분되고 세션의 각 상태별로 전송될 수 있는 메시지를 정의하여 올바른 상태에서 메시지가 전송된다면 그 다음 상태로 전이되게끔 설계하였다. 그림 5는 침입을 탐지하는 의사코드의 일부이다.

침입을 탐지하는 방법은 크게 두 가지이다. 첫 번째는 세션의 현재 상태(current.state),그리고 스니핑된 패킷내 메시지 타입을 전송할 수 있는 상태(packet.state)가 초기 인증 상태 머신에 정의되어 있는 상태(initAuth.state)와 다르면서 세션의 현재 상태에서 전송될 수 있는 메시지 타입 (pkt.message_type)과 스니핑된 패킷내 메시지 타입(packet.message)과 같을 때 이는 정상적인 상태에서 전송된 메시지가 아니라 판단하여 탐지한다. 두 번째는 세션의 현재 상태(current.state),그리고 스니핑된 패킷내 메시지 타입을 전송할 수 있는 상태(packet.state)가 초기 인증 상태 머신에 정의되어 있는 상태(initAuth.state)와 같지만 동일 메시지가 임계치 값을 넘었을 때 탐지한다.

```
public void notified_by_message(packet t)
{
 switch(state) {//각 상태별 전송가능 메시지 정의
  case STATE_INIT:
   if(TransitionState(t, client_address,
      server_address, CID, Identity,
      packet.EAP_START, STATE_EAP_START))
      threshold++
  case STATE_EAP_START:
   if(TransitionState(t, server_address,
      client_address, CID,Identity,
      packet.EAP_REQUEST_IDENTITY,
      STATE_EAP_IDENTITY_WAIT))
      threshold++
  case ...
}
boolean TransitionState(packet t,
  String server_addr, String dest_addr,
  String CID, String Identity, int msg_type,
  int transition_state)
{
   if(t.source_address.equals(server_addr)
     && t.dest_address.equals(dest_addr)
     && t.CID.equals(CID)
     && t.Identity.equals(Identity)
     && t.message_type==msg_type)
     {state=transition_state}
}
```

〔그림 4〕 세션의 상태를 유지하는 의사 코드

```
if(initAuth.state!= current.state &&
initAuth.state!= packet.state &&
 pkt.message_type==packet.message)
 DetectAttack("Alarm_Type");
if(initAuth.state == current.state ==
packet.state &&
 threshold>=MAX_THRESHOLD)
 DetectAttack("Alarm_Type");
```

〔그림 5〕 침입을 탐지하는 의사 코드

IV. W-IDS 구현 및 동작 시뮬레이션

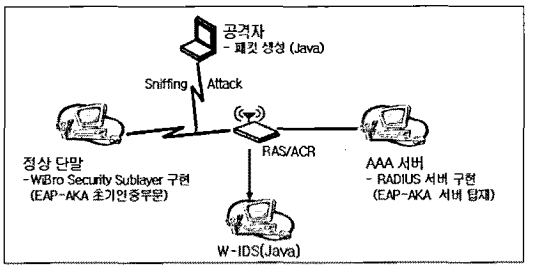
와이브로 초기 인증 시 보안 취약점을 이용한 침입의 효과적인 탐지에 대한 검증을 위해 상용화된 KT의 와이브로 환경에서 실질적인 실험을 하여야 되나 현실적으로 불가능하여 본 논문에서는 와이브로의 실제 환경을 고려한 RAS/ACR, 정상단말, AAA(Authentication Authorization and Accounting) 서버 및 기능에 대해서 구현 및 시뮬레이션 하였다.

4.1 구현모델

실험환경은 그림 6과 같고 구성 요소는 정상단말, RSA/ACR, 공격자, W-IDS, AAA 서버이다. 모든 구성 요소는 Java 언어로 구현하였으며 이중 정상단말은 와이브로 표준, RFC4187(EAP-AKA)을 참조하여 EAP-AKA 초기인증부분 및 와이브로 보안부계층을 구현하였다. RAS/ACR은 802.1X를 지원하는 AP(Access Point)를 이용하여 RAS 역할인 무선 패킷 수신 및 ACR 역할인 EAP 메시지를 AAA 서버로 전송하도록 하였다. AAA 서버는 EAP-AKA 서버를 탑재한 RADIUS 서버로 구현하였다. 또한, 공격자는 무선 통신에서의 패킷을 스니핑하고 초기인증과정에서 평문으로 전송되는 CID와 Identity를 위/변조하여 공격하도록 구현하였다. W-IDS는 세션 상태 전이결과를 유지하며, 본 논문에서 분석한 다섯 가지 위협에 대해 정상상태에서 전송될 수 있는 메시지와 스니핑된 패킷내 메시지를 비교하고, 지속적인 메시지 전송은 상태별 임계치 값과 비교하여 침입탐지를 할 수 있도록 구현하였다.

4.2 공격 시나리오

본 절에서는 3장에서 분석한 초기 인증 시 생길 수 있는 위협을 탐지할 수 있는지를 검증해 본다. 검증을 위해 사용된 공격 시나리오는 다음과 같다.



[그림 6] 실험환경

• 시나리오 #1

인증과정 중 정상 기지국으로 위장한 공격자가 단말에게 (EAP-Failure)를 전송하여 정상적인 상태에서 전송되지 않은 EAP-Failure를 W-IDS가 탐지하는지를 확인한다.

• 시나리오 #2

인증과정 중 정상단말로 위장한 공격자가 (EAP-Response/AKA-Authentication-Reject) 메시지를 기지국으로 보낸 후 AKA-Authentication- Reject를 W-IDS가 탐지하는지를 확인한다.

• 시나리오 #3

정상단말로 위장한 공격자가 기지국으로 (EAP-Response /AKA-Synchronization- Failure)를 3번이상 전송했을 때 W-IDS가 위협을 탐지하는지 확인한다.

• 시나리오 #4

공격자가 정상적인 인증 과정을 마친 단말의 Identity와 CID를 획득하여 정상단말 보다 먼저 기지국으로 3번이상 EAP-Start 메시지를 전송하고 정상단말 또한 EAP-Start 메시지를 기지국으로 보냈을 때 W-IDS가 위협을 탐지하는지 확인한다.

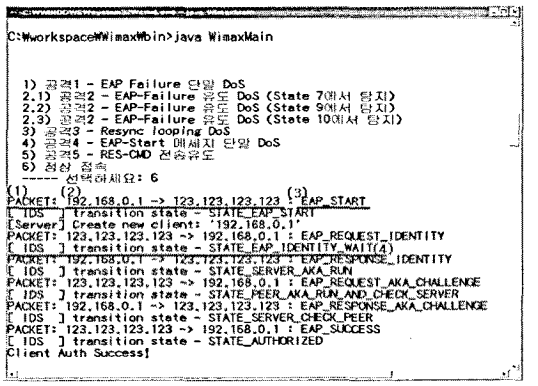
• 시나리오 #5

인증과정 중 공격자가 3번 이상 (EAP- Response/Identity) 메시지를 기지국으로 전송했을 때 W-IDS가 RES-CMD 유도 경보를 내는지 확인한다.

4.3 탐지 결과

본 논문은 W-IDS의 논리적 구현 모델을 기반으로 가상의 공격 시나리오에 따라 다섯 가지 유형의 공격을 수행하고, 이를 탐지하는 과정을 4.1절에서 설명한 실험 환경에서 시뮬레이션 했다.

시뮬레이션은 정상 접속과정과 다섯 가지 공격 형



[그림 7] 정상 접속 과정

태를 실험하였으나 지면 관계상 두 가지 공격 시나리오에 따른 탐지 결과만을 기술한다.

• 정상 접속 과정

먼저 그림 7은 정상 접속 과정을 W-IDS에서 모니터링 한 결과이다. (1)은 패킷을 전송했다는 것을 의미하며, (2)는 Source_address와 Destination_address, (3)은 패킷내 메시지 타입, (4)는 W-IDS에서 유지하는 세션상태를 의미한다.

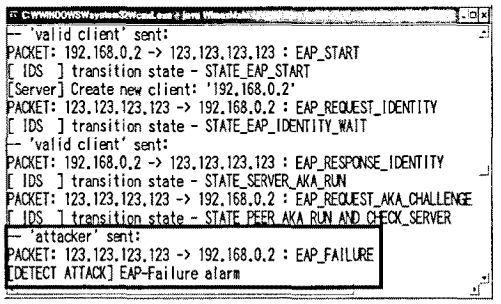
• 시나리오 #1 탐지 결과

그림8과 같이 탐지 결과를 살펴보면 정상적인 단말이 정상적인 인증과정을 거치고 있는 중 기지국을 가장한 공격자가 단말에게 EAP-Failure메시지를 전송하여 단말이 서비스를 받지 못하게 하고 있으며 W-IDS는 이 공격을 탐지하였다는 것을 보여준다.

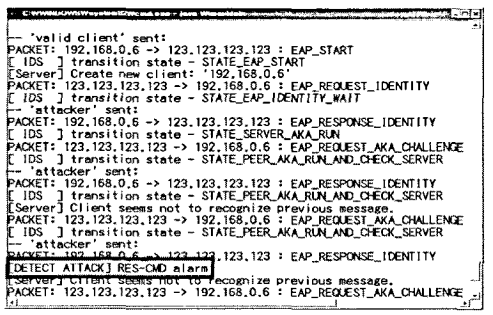
• 시나리오 #5 탐지 결과

그림9와 같이 탐지 결과를 살펴보면 세션상태가 State-eap-identity-wait 상태일 때 공격자가 EAP-response-identity 메시지를 3번 전송하는 것을 나타내고 있으며 이것은 RES-CMD 메시지를 전송하도록 유도하는 것으로 볼 수 있다. 이에 W-IDS에서는 RES-CMD 경보를 내며 탐지하는 것을 볼 수 있다. 동일한 방법으로 시나리오 #2, #3, #4에 대해서도 실험을 하였으며 실험 결과 제안한 침입탐지시스템에서 탐지가 가능하다는 것을 알 수 있었다.

시뮬레이션 결과 와이브로와 관련된 침입탐지시스템이 현재까지 연구된 결과가 없어 비교분석은 할 수 없었지만 와이브로에서 EAP-AKA를 사용할 시 초기 인증 과정에서의 개별 명세를 개발하여 이를 기반으로 탐지할 수 있는 침입탐지시스템의 적용 가능성을 증명했다는 점에서 의미가 있다고 할 수 있다.



〔그림 8〕 시나리오 #1 탐지 결과



〔그림 9〕 시나리오 #5 탐지 결과

V. 결 론

본 논문에서는 와이브로의 초기 인증 과정 시 평문으로 인증관련 메시지가 전송되는 것에 착안하여 PKMv2 EAP-AKA의 초기 인증 과정에서의 보안취약점을 식별하고 정상적인 초기 인증 과정에 대한 상태전이머신을 도출하였다. 그리고 도출된 상태전이머신을 이용하여 정상적인 상태전이를 어기고 초기 인증 과정에서 발생 가능한 악의적인 공격 행위들을 효율적으로 탐지해 낼 수 있도록 명세기반의 침입탐지시스템인 W-IDS를 제안하였다. W-IDS는 Network 기반 IDS로 운영되도록 정의하고 플랫폼 독립적으로 운영될 수 있도록 Java 언어를 이용해 구현하였으며, 제한적인 와이브로 환경에서 시나리오 기반의 탐지 실험을 통해 와이브로 적용 가능성을 증명하였다.

본 논문은 와이브로의 초기 인증 단계에 중점을 두고 있지만, 와이브로 환경에 명세기반 침입탐지시스템을 최초로 적용한 연구이다. 또한 제안한 W-IDS는 비정상행위탐지 및 오용탐지방식을 적용하기가 제한적인 와이브로 환경에서 오탐율을 줄이면서 향후 발생 가능한 알려지지 않은 공격에 대해서도 효율적인 침입탐지가 가능하다.

향후 연구방향으로는 본 논문에서 제시한 초기 인증 과정 시 생기는 다섯 가지 보안취약점 이외의 공격 가능한 공격유형을 지속 연구하고 모델링하여 침입탐지할 수 있는 알고리즘을 계속 발전시켜 나가야 할 것이다. 그리고 초기 인증 과정이외도 생길 수 있는 보안취약점을 도출하여 악의적인 행위를 탐지할 수 있도록 W-IDS 기능을 향상시켜 나가야 할 것이다.

참 고 문 헌

〔1〕 박윤옥, 최정필, 김준우, 방승재, 안지환, "4세대 이동통신 핵심기술 WiBro Evolution 시스템 개발," 전자통신동향분석, 24(3), pp. 44-53, 2009년 6월.

〔2〕 배성수, 최동훈, 최규태, 와이브로 기술과 시스템, 세화, 2006년 8월.

〔3〕 이재일, 원유재, 지승구, 이태진, "와이브로 보안기술 해설서," 한국정보보호진흥원, 2006년 8월.

〔4〕 C.Y. Tseng, P. Balasubra-manyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, "A Specification-Based Intrusion Detection System For AODV," 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03), pp. 125-134, Oct. 2003.

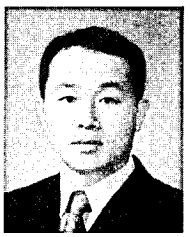
〔5〕 R. Gill, J. Smith, and A. Clark, "Specification-Based Intrusion Detection in WLANs," Proceedings of the 22nd Annual Computer Security Application Conference, pp. 141-152, Dec. 2006.

〔6〕 M. Barbeau, "WiMax/802.16 Threat Analysis," Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, pp. 8-15, Oct. 2005.

〔7〕 B. Aboba, B. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol(EAP)," RFC 3748, June 2004.

〔8〕 J. Arkko and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement(EAP-AKA)," RFC 4187, Jan. 2006.

〈著者紹介〉



이 윤 호 (Yunho Lee) 학생회원
1999년 2월: 육군사관학교 전자공학과 졸업
2005년 2월: 서울대학교 컴퓨터공학과 석사
2009년 1월~현재: 국방대학교 전산정보학과 박사과정
〈관심분야〉 침입탐지 시스템, 네트워크 보안

이 수 진 (Soojin Lee) 정회원
1992년 2월: 육군사관학교 전산학과 졸업
1996년 2월: 연세대학교 컴퓨터과학과 석사
2006년 2월: 한국과학기술원 전산학과 박사
2006년 3월~현재: 국방대학교 전산정보학과 교수
〈관심분야〉 침입탐지 시스템, 모바일 웹 보안, 네트워크 보안