WiBro PKMv2 EAP-AKA 기반 인증 과정에서의 Redirection Attack 에 대한 보안 취약성 및 개선 방안[1]

이현철, 엄성현, 조성재, 최형기
성균관대학교 정보통신공학부
e-mail : onepiece2hc@hotmail.com, {sheum, monocho, hkchoi}@ece.skku.ac.kr

Enhancement of WiBro PKMv2 EAP-AKA Authentication Security Against Rogue BS based Redirection Attacks

Hyun-Chul Lee, Sung-Hyun Eom, Sung-Jae Cho, Hyoung-Kee Choi
School of Information and Communication Engineering, SungKyunKwan University

요 약

WiBro는 무선랜과 3G 이동통신의 장점을 결합한 휴대 인터넷 기술로 최근 국내에서 상용화 되었다. WiBro의 장점인 이동성과 고속 무선 통신에 기인하여, 향후 지속적인 발전이 기대된다. 이러한 WiBro의 확산에 따라 개인 사용자에 대한 보안문제가 최근 크게 부각되고 있다. 현재 Wibro는 3G 이동통신 및 무선랜과 효율적인 연동을 위해 EAP-AKA 인증 기법을 사용하고 있다. 하지만 EAP-AKA는 단말이 기지국을 인증하지 못하는 치명적인 취약점이 있다. 따라서 공격자는 임의로 rogue BS를 설치할 수 있고, 정상 사용자의 데이터를 이종 네트워크로 보내는 Redirection Attack을 시도할 수 있다. Redirection Attack은 전송 속도 저하, Denial-of-Service (DoS) 을 초래하며, 데이터가 redirection 되는 이종 네트워크에 따라 암호화된 데이터가 노출될 수 있다. 본 논문에서는 EAP-AKA와 Redirection Attack에 대해 분석하고, 그 해결책을 제시한다. 논문은 1) 프로토콜을 일부 수정하여 공격을 막는 방법과 2) traffic 분석을 통한 공격 탐지 방식을 다루고 있으며, 이러한 두 가지 방법을 통해 Redirection Attack에 대한 취약점을 근본적으로 제거할 수 있다.

1. 서론

WiBro는 시간과 장소의 제한 없이, 이동 중에서도 고속의 데이터 전송을 제공하는 서비스이다. 전송용량의 광대역화, 고속의 이동성, 단말의 개인화라는 특징 외에도 언제 어디서나 무선 IP 기반의 각종 데이터, 커뮤니케이션, 멀티미디어 콘텐츠 등을 제공한다. 고속 이동 시에도 인터넷에 아무 문제없이 접속 할 수 없다는 점에서 무선랜과 차별성을 두며, 고속의 데이터 통신을 지원 하기 때문에 기존의 이동통신의 데이터 서비스와 차별화 되는 강점을 가진다. 즉, 무선랜과 이동통신이 제공하는 데이터 통신을 융합하고, 두 서비스의 장점을 극대화하는 형태의 무선 통신 서비스라고 할 수 있다. 이와 같은 이유로 WiBro는 국내 및 세계에서 차세대 이동통신 기술의 대표주자로 각광 받고 있다.

성공적인 WiBro 서비스 정착을 위한 필수 요소가 바로 보안이다. WiBro 시스템에서 보안 기능은 크게 트래픽 패킷 데이터에 대한 암호화 프로토콜과 기지국과 단말 사이에서 사용 되는 모든 키들을 안전하게 생성하고 공유하기 위해 정의하는Privacy Key Management (PKM) 프로토콜로 구성되어 있다. 암호화 프로토콜의 경우 새로운 알고리즘을 정의 하는 방식이 아닌 기존에 알려진 보안 알고리즘을 채택하여 적용 하는 개념이다. 따라서 WiBro는 인증 및 키 관리를 담당하는 PKM 프로토콜에 더욱 중점을 두고 있다.

본 논문은 2장에서 PKM 프로토콜의 인증 단계에 사용되는 EAP-AKA 인증 과정에 대해 분석한다. 3장은 PKM프로토콜에서 발생할 수 있는 문제점에 대해 다루고 있으며, 이에 대한 해결책을 4장에서 언급한다. 끝으로, 6장은 논문의 결론을 담고 있다.

2. WiBro PKMv2 인증 프로토콜

Wibro는 보안 기능을 제공하기 위해 Medium Access Control (MAC) 계층에 Privacy Sublayer를 정의하고 있다. Privacy Sublayer는 데이터에 대한 암호화 프로토콜 및 무선 구간의 키 설정을 위한 PKM프로토콜로 구성된다. PKM 프로토콜은 PKMv1과 PKMv2가 있으며, Wibro는 PKMv1에 상호 인증 및 EAP를 추가한 PKMv2를 적용하고 있다. PKMv2는 크게 인증 절차와 키 생성 및 관리 절차로 구성 된다.

Wibro는 RSA 기반 인증과 EAP 기반 인증을 지원한다. RSA기반 인증은 단말이 기지국으로PKMv2 RSA Request메시지를 보냄으로써 시작한다. 이 메시지를 수신한 기지국은 여기 포함된 단말의 인증서를 통하여 인증을 수행하게 된다. 합법적인 단말이라고 판별했을 경우 기지국은 Pre-PAK를 생성하고 단말에게 기지국의 인증서와 단말의 공개키로 암호화 된 Pre-PAK가 포함된 PKMv2 RSA Reply 메시지를 전송한다. 이 메시지를 수신한 단말은 포함된 기지국의 인증서를 검증하고 인증이 성공 했을 경우 기지국에게 PKMv2

[1] 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음

RSA Acknowledgement 메시지를 전송 하게 되며 이로써 RSA기반의 인증 절차가 완료된다.

EAP 기반 인증에서는 PKMv2 EAP-Start 메시지 및 PKMv2 EAP-Transfer 메시지가 사용된다. IEEE 802.16e에서는 다양한 EAP-기반 인증 방법을 지원하는데 현재 WiBro 시스템에서는 단말 인증뿐만 아니라 사용자 인증 기능도 제공하고 3G, WLAN등 타 망 과의 상호 로밍 연동을 위해 Universal Integrated Circuit Card (UICC) 기반의 EAP-AKA 프로토콜을 인증 방식으로 채택하고 있다 [1].

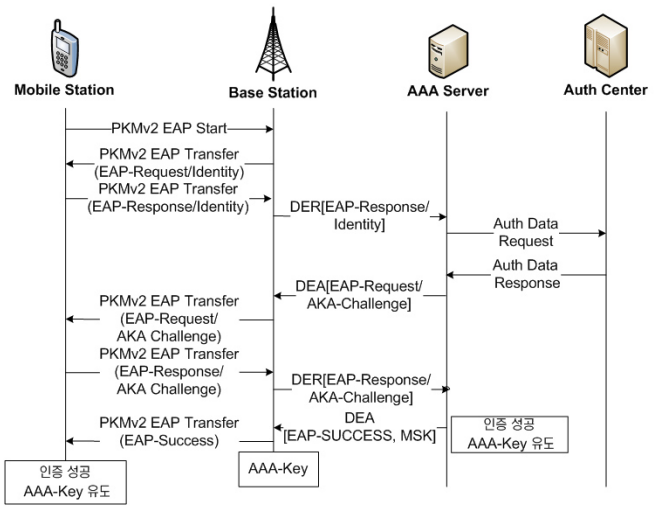

그림 1. WiBro PKMv2 EAP-AKA 인증

현재 WiBro에 적용되어 있는 EAP-AKA 인증 방식에 대한 자세한 설명은 그림 1과 같다. 우선, 단말은 인증을 요청 하기 위해 기지국에 EAP-Start 메시지를 전송한다. 기지국은 이 메시지를 받은 직후 EAP-Request/Identity 메시지를 단말에게 보내어, 단말의 Identity를 요구한다. 단말은 UICC에 저장된 자신의 Identity를 EAP-Response/Identity 메시지에 포함 시켜 전송한다. 이제 기지국은 EAP 관련 메시지를 수신한 경우 신뢰된 네트워크를 통하여 AAA 인증서버로 그대로 전송한다. AAA 서버에서는 사용자의 Identity를 식별한 후 사용자에 대해서 가용한 Authentication Vector (AV)가 있는지 확인한다. 사용 가능한 AV가 없을 경우 인증센터로부터 새로운 인증벡터를 요청하고 설정한다. 인증벡터를 수신한 AAA 서버는 AV의 인자 중 RAND와 AUTN을 EAP-Request/AKA-Challenge에 포함 시켜 기지국으로 전송하고 이를 수신한 기지국은 그대로 단말에 전송한다. 단말은 AKA 알고리즘을 수행하여 XMAC을 생성하고 AUTN에 포함된 MAC과 자신이 생성한 XMAC을 비교 검증하여 인증서버를 인증한다. MAC 검증이 성공하면 단말은 수신한 SQN값이 자신의 SQN값의 범위 안에 들면 동기화에 성공한다. 이 후 단말은 RES, CK, IK를 계산하고 RES를 EAP-Response/AKA-Challenge에 포함 시켜 인증서버로 전송한다. 인증 서버는 인증벡터의 XRES와 단말이 전송한 RES를 비교 검증하여 단말을 인증한다. 단말과 인증서버와의 상호 인증이 완료되면 인증서버는 EAP-Success 메시지 및 AAA key(Master Session Key, MSK)를 기지국에 전송하고 기지국은 EAP-Success 메시지를 단말에 전송한다. EAP-Success 메시지를 통해 단말과 기지국은 간접적으로 상호 인증에 성공하고 단말이 AKA 알고리즘을 통하여 AAA key를 도출해 내면서 단말과 기지국은 같은 인증키를 공유하게 된다. 이 후 단말과 기지국은 서로 공유한 pre-PAK 또는 MSK를 가지고AK를 생성 한다.

WiBro가 제공하는 PKMv2 EAP-AKA는 그림 1에에 설명한 내용과 같이 단말과 AAA 서버간의 EAP 인증 과정이다. 즉, 단말과 AAA 서버는 EAP-AKA를 통해 상호 인증 과정을 거친다. 하지만 기지국은 이 과정의 메시지들을 단순히 전달할 뿐, 실제 인증 과정에 참여하지 않는다. 따라서 EAP-AKA 과정이 종료한 후에도 단말과 기지국의 완전한 상호인증은 보장할 수 없다. 물론 기지국과 AAA 서버는 일반적으로 Diameter [2]와 같은 프로토콜로 보호되어 있다. 하지만, 단말과 기지국 사이의 무선 구간의 데이터는 키가 생성되기 전까지 보호할 수 없다.

3. EAP-AKA Redirection Attack

3.1 WiBro 취약성에 대한 가정

현재 WiBro에 대해 몇 가지 보안 위협이 존재하는데, 이러한 위협은 공격자가 다음과 같은 조건을 필요로 한다 [1].

1) 공격자는 단말의 MAC 주소를 알아내고 조작할 수 있다. 공격자는 WiBro 단말과 기지국 사이에서 송수신 하는 관리 메시지를 획득하여 MAC 주소를 알아낼 수 있다. MAC 주소의 변경 및 조작과 같은 경우, 현재 WiBro와 유사한 특성을 가진 무선랜에서 쉽게 가능하므로 WiBro 역시 유사한 방식으로 가능하다.
2) 공격자는 정상단말의 신호 또는 정상 기지국의 신호보다 강한 신호를 사용해야 한다. WiBro의 경우 무선랜과는 다르게 공격 메시지 전송 시점에 정상 기지국 또는 정상 단말의 신호가 동시에 전송되므로 보다 강한 신호를 보내야만 한다.
3) WiBro에 공격 메시지를 보내기 위해서는 정상 단말이 데이터를 송수신하는 같은 시간대에 메시지를 보내야 한다. WiBro는 기지국에 의해 할당된 송수신시간에만 메시지 송수신이 가능하다.

이러한 가정들은 높은 수준의 기술이 요구되는 사항이 아니며, 공격자는 무선랜의 상황과 마찬가지로 비교적 쉽게 위의 전제 조건들을 만족 시킬 수 있다.

3.2 Redirection Attack

EAP-AKA 인증 방식에서 기지국은 단순히 단말과 AAA 인증 서버 사이에 전송되는 EAP 메시지를 중계하는 역할만을 한다. 즉, 단말은 자신이 수신한 인증벡터가 자신이 인증을 요청한 기지국의 요청에 의해 전송된 것인지를 판단 할 수 없다. 이 점을 이용하여 공격자는 단말에 대해서는 기지국으로 위장하고, 기

지국에 대해서는 단말로 위장할 수 있다. 그림 2는 이 공격에 대한 자세한 설명을 다루고 있다.

그림 2의 (1)과 같이 공격자는 3GPP에서 사용되는 IMSI Catcher와 같은 장치를 사용해서 기지국으로 위장할 수 있다 [4]. 단말은 망에 접속하기 위해 기지국으로 (2)의 접속 요청 메시지를 전송한다. 공격자는 중간에서 (2) 메시지를 가로 챈 후, 기지국으로 위장하여 단말을 연결한다. 일단 단말이 위장 기지국으로 연결되면 다른 정상 기지국으로부터의 제어정보는 무시된다 [5]. 이 후 공격자는 (3)과 같이 위장 단말을 사용하여 정상 기지국에 연결을 요청한다. 이 과정이 성공하게 되면 공격자는 단말과 다른 네트워크의 기지국과의 연결을 성공 시킬 수 있으며, 중간에서 단말과 다른 기지국과의 메시지를 중개해 주는 역할을 할 수 있다. 결과적으로 공격자는 단말이 자신이 원하는 기지국이 아닌, 다른 기지국과 연결되어 인증과정을 거치고, 데이터를 주고 받게 된다. 이로 인해 전송속도의 저하, DoS 및 과금 문제 등의 문제가 발생 할 수 있다 [1]. 또한 공격자가 redirect 하는 네트워크가 공격자에 의해 사전 설정된 경우, 사용자의 비밀 데이터가 노출될 수 있다.

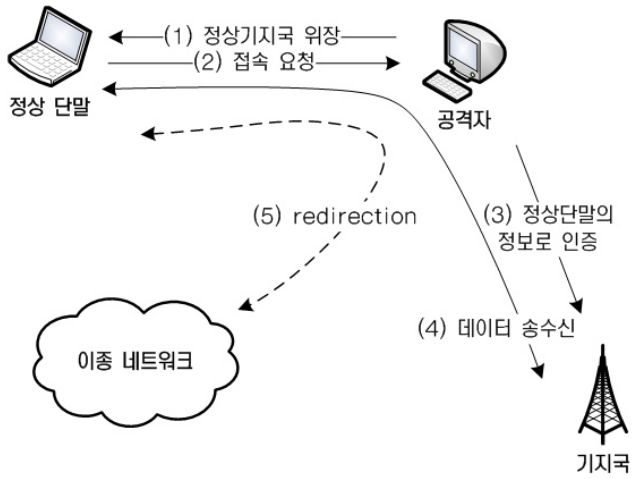

그림 2. Redirection Attack 공격 과정

Redirection Attack은 redirection 되는 네트워크에 따라 두 가지로 구별된다. 만약 공격자가 redirection 시키는 네트워크가 현재 네트워크와 동일한 보안 강도를 가지고 있거나, 공격자가 이종 네트워크를 설정할 수 없다면, Redirection attack은 단순히 전송 경로를 우회시키는 공격일 뿐이다. 물론, 이러한 공격도 전송속도 저하 등의 결과를 초래하지만, 공격자는 사용자의 비밀 통신을 엿들을 수 없고, 서비스는 정상적으로 진행 될 수 있다. 하지만, 만약 공격자가 redirection 시키는 네트워크의 보안 강도가 낮거나, 공격자가 통제할 수 있는 네트워크로 redirection 시키는 것이 가능할 경우 Redirection Attack은 치명적인 결과를 초래한다. 즉, 공격자의 네트워크 내에서 키가 노출될 수 있기 때문에, 비밀 통신을 위한 WiBro의 프로토콜이 의미를 잃게 된다.

4. Redirection Attack 에 대한 해결책

3장에서 언급한 바와 같이, WiBro에 적용된 EAP-AKA 인증 기법은 Redirection Attack에 대해 취약점을 가지고 있다. 이러한 취약점은 단말과 기지국간의 상호인증이 완벽하지 않기 때문이다. 단말은 EAP-AKA가 정상적으로 종료된 후에도, 인증서버에서 생성한 인증 벡터가 정상적인 기지국을 통한 것인지 확인할 수가 없다. 따라서, 공격자가 Redirection Attack을 하기 위해 다른 기지국에서 받은 인증벡터를 요청하고, 이를 단말에게 전송하여도 단말은 그 인증 벡터를 사용할 수 밖에 없다.

4.1. AAA 서버의 ID 를 이용한 방법

WiBro 에서 단말이 자신이 연결될 AAA 서버의 ID를 알 수 있다면 Redirection Attack 공격은 비교적 쉽게 제거될 수 있다. 이는 두 가지 방법으로 만족될 수 있다.

첫째, 모든 기지국이 자신이 연결된 AAA 서버의 ID를 broadcast 하도록 한다. 단말은 초기 접속 시, 다수의 기지국으로부터 AAA ID를 획득하게 되기 때문에, 만약 rogue BS가 다른 AAA ID를 broadcast 하면 이는 쉽게 발견될 수 있다.

둘째, rogue BS가 다른 기지국과 마찬가지로 정상적인 AAA ID를 broadcast 하는 경우, 초기 접속 시 발견될 수 없다. 이에 대한 해결책은 그림 3과 같다.

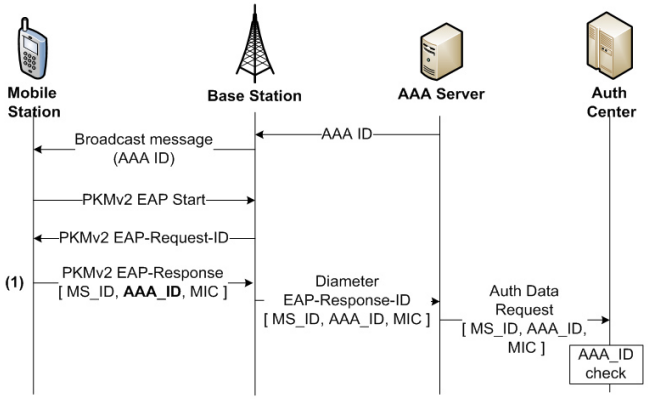

그림 3. Redirection Attack에 대한 해결

그림 3의 (1) 메시지와 같이, 단말의 ID를 전송 할 때 기지국이 broadcast 하는 AAA의 ID를 포함하여 전송한다. 메시지 (1)의 인자 전체는 단말이 인증서버와 사전에 공유한 키로 Message Integrity Code (MIC)를 생성하여 추가한다. 메시지 (1)의 내용은 기지국과 AAA 서버를 거쳐 최종 인증센터로 전달된다. 인증센터는 전달된 AAA 서버의 ID를 이용하여, 메시지가 정상적인 AAA 서버를 통해 전달되었는지 확인한다.

만약 공격자가 rogue BS를 통해 인증되지 않은 AAA 서버로 데이터를 전송한다면, 이 AAA 서버에서 인증센터로 전달되는 메시지들은 AAA서버의 ID와 실제 메시지를 전달하는 AAA 서버가 서로 다르게 된다. 따라서 인증 센터는 단순히 AAA의 ID 비교만으

로 Redirection Attack을 탐지할 수 있고, 공격자는 단말과 인증 센터간의 키로 생성된 MIC를 위조하거나 변조할 수 없다.

4.2. ACK-Pair 분석을 통한 방법

W. Wei 와 그의 팀은 무선랜에서 TCP ACK-Pair를 이용하여, rogue AP를 탐지하는 방법에 대해 연구하였다 [6]. ACK-Pair는 rogue AP 탐지뿐만 아니라, rogue BS 탐지에도 활용될 수 있다. 일반적으로 WiBro의 기지국과 AAA 서버는 일정한 영역 안에 포함될 수 있도록 전체적인 망이 구성된다. 따라서 단말과 AAA 서버 또는 기지국과 AAA 서버 간의 모든 통신은 일정한 범위 안에 ACK을 기대하게 된다. 따라서 AAA 서버가 탐지를 시작한 일정 기간 동안, ACK-Pair의 간격이 기준치를 초과하게 되면 Rogue BS의 Redirection Attack 공격을 의심할 수 있다.

ACK-Pair는 AAA 서버에서 탐지하게 되는데, AAA 서버는 해당 기지국과 기지국에 연결되는 단말의 거리를 쉽게 예측할 수 있다. 이는 AAA 서버와 기지국 설치가 동일한 사업자에 의해 지원된다는 가정이 필요하며, 이는 상당히 일반적인 가정이다. 결국 AAA 서버 입장에서 기지국과의 거리 및 기지국에서의 처리시간 등을 예측할 수 있는 상황에서 ACK-Pair 또한 근사적으로 예측 가능하다.

AAA서버에서 ACK-Pair의 기준을 설정하기 위해서는 정상적인 단말과 기지국을 통한 일정량의 데이터 수집이 선행 되어야 한다. 이를 W. Wei는 training set 으로 표현하고 있으며, 자세한 메커니즘은 [6]에서 구체적으로 언급하고 있다.

5. 결론

본 논문에서는 WiBro 의 보안 부계층에서 정의하는 PKMv2 EAP-AKA 프로토콜의 동작과정과 문제점을 다루었다. EAP-AKA 는 기존의 RSA 프로토콜보다 높은 보안 강도를 제공하지만 Rogue BS 를 사용하는 Redirection Attack 에는 취약 한 면이 있다. Redirection Attack 은 공격자가 Redirection 시키는 네트워크가 동일한 네트워크라면 전송 속도 저하 등의 미비한 문제로서만 작용하지만 상대적으로 보안강도가 낮은 이종 네트워크로의 연결이 성공 할 경우 큰 문제가 될 수 있다. Redirection Attack 은 EAP-AKA 에서 단말은 Request/AKA-Challenge 메시지에 포함된 인증벡터가 자신이 접속을 요청한 기지국의 요청에 의해 전송 된 것인지 여부를 확인 할 수 있는 방법이 없기 때문에 발생한다.

이런 문제점을 해결하기 위해 본 논문에서 두 가지 방법을 제안했다. 첫 번째는 단말이 자신이 접속하고자 하는 기지국과 연결된 AAA 서버의 ID 를 기지국이 Broadcast 는 방법이다. 이 방법은 단말과 AAA 서버가 전송하는 AAA 서버의 ID 를 비교함으로써 수행되므로 비교적 간단한 동작으로 Rogue BS 를 탐지할 수 있다는 장점을 가지고 있다. 두 번째로는 ACK-Pair 를 이용하는 방법이 있다. AAA 서버의 지속적인 모니터링으로 Rogue BS 를 검출 할 수 있는 방법으로, 기존 EAP-AKA 의 변경 없이 그대로 사용할 수 있는 장점이 있다. 향후 연구 과제로 우리가 제안한 프로토콜에 대해 보다 구체적인 모델의 정립과 분석이 필요하다.

참고문헌

[1] 임선희 외, “EAP-AKA 를 적용한 WiBro 무선 네트워크의 인증구조 연구”, KICS2005-11-457, March 2006

[2] P. Calhoun et al., “Diameter base protocol”, RFC 3588, September 2003

[3] 한국정보보호진흥원 발간 “WiBro 보안 기술 해설서”, September 2006

[4] M. Zhang and Y. Fang “Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol”, IEEE Transactions on wireless communications, March 2005

[5] 조석헌, 윤철식 “WiBro 시스템에서의 보안 기술”, 방송공학회지

[6] W. Wei et al., “Passive Online Rogue Access Point Detection Using Sequential Hypothesis Testing with Tcp Ack-Pairs”, IMC’07, October 2007