안전한 WiBro 서비스를 위한 새로운 인증 프로토콜

구중숙, 김진근*, 박종혁** 구중두***, 이기성***
*경찰청 사이버테러대응센터
**고려대학교 컴퓨터정보통신공학과
***호원대학교 컴퓨터게임학부
e-mail:ygslee@howon.ac.kr

A Novel Authentication Protocol for Secure WiBro Services

Jung-Sook Koo, Jin-Geun Kim*, Jong Hyeok Bak**,
Jung-Doo Koo***, Gi-Sung Lee***
*Center of Cyber Terror, National Police Agency
**Dept. of Computer and Information Communication Engineering, Korea University
***School of Computer Game, Howon University.

요 약

사용자가 안전한 WiBro 서비스를 받기 위해서 사용자 단말과 ACR(Access Control Router) 간에 인증이 선행되어야 한다. 그렇지 않을 경우, 많은 공격 위험으로부터 노출될 수 있다. 따라서 한국정보통신기술협회(TTA)에서는 휴대인터넷(와이브로™) 서비스를 위한 상호 인증 절차 표준을 제정하였다. 이 표준 프로토콜은 PISIM(Portable Internet Subscriber Identity Module)을 이용하여 PE(Portable Equipment)와 ACR 간에 상호 인증을 수행한다. 그러나 표준은 인증에 필요한 메시지의 수가 대체적으로 많은 편이며 PISIM의 분실과 에러가 발생했을 경우에는 사용자는 무선인터넷 서비스를 사용할 수 없게 된다. 따라서 본 논문에서는 ACR과 PSS 간에 키 동의 프로토콜을 수행하여 PSS를 인증한다. 이 때 PSS의 계산량을 지원하기 위한 PSD(Power Support Device)가 키 동의 프로토콜에 참여하게 된다. 이렇게 생성된 키는 ACR과 안전한 통신 세션을 맺고 있는 KAS(Key Authentication Server)에 PSS의 식별자와 키 정보를 암호화에서 저장한다. 끝으로 제안된 프로토콜의 안전성과 효율성을 분석한다.

1. 서론

WiBro 기술은 노트북, PDA, 휴대폰과 같은 이동 단말기 보급의 확산과 언제 어디서나 이동 중에도 다양한 단말기를 이용해서 높은 전송 속도로 무선인터넷 서비스를 필요로 하는 사용자들의 급증으로 인해 필요하게 되었으며 2007년 10월에 세계 최초로 3.5세대 IMT2000 국제 표준으로 채택되었다[1]. WiBro는 현재 상용화되는 이동성 지원 기술 중 가장 빠른 무선 전송속도를 제공하고 있으며 All-IP 기술을 채택함으로써 저렴한 비용을 기반으로 다양한 비즈니스 응용이 가능하다. WiBro 기술이 국제 표준으로 채택되기 이전에 한국정보통신기술협회에서는 2006년에 WiBro 기술과 관련해서 "WiBro 기술에서의 IPv6 기술(IPv6 over WiBro)[2]"와 휴대인터넷(와이브로 ™) 서비스를 위한 상호 인증 절차[3]"를 표준으로 채택했다. [3]의 핵심은 PE(Portable Equipment)에서 인증하는 것이 아니라 PISIM(Portable Internet Subscriber Identity Module)에서 AKA 절차를 수행하며, 사용자의 비밀 정보 및 키 값을 저장, 관

리한다. 단지 PE는 PISIM 탈/부착이 가능한 단말 또는 PISIM 기능을 hand-wired logic 형태로 제공하는 machine-to-machine 형태의 단말에 국한하고 있다. 이 표준 프로토콜의 문제점은 PISIM 카드의 분실이나 에러가 발생했을 경우에 ACR은 단말을 인증할 수 없기 때문에 사용자는 원활한 무선인터넷 서비스를 받을 수 없게 된다. 또한 인증 절차에 필요한 메시지의 수가 대체로 많은 편이다.

따라서 본 논문에서는 PSS의 계산량을 지원하기 위한 PSD(Portable Support Device)가 PSS와 ACR 간 키동의에 참여하게 된다. 인증키를 생성한 후에는 ACR과 안전한 통신 세션을 맺고 있는 KAS(Key Authentication Server)에 PSS 식별자와 키를 암호화해서 저장한다. PSS가 다른 네트워크로 이동하여 무선인터넷에 재접속을 해야 할 경우에는 인증키로 암호화한 재접속 요청 메시지를 새로운ACR은 수신한 후에 KAS로 그 메시지를 전송하면 KAS는 PSS를 인증한 후에 새로운 ACR에게 인증키를 전송한다. 인증키를 통해 새로운 ACR은 PSS로부터 수신한 메시지를 확인한 후에 접속을 허가한다. 이 논문의 구성은 다음과 같다. 2장에서는 본 연구를 위한 연구배경에 대해서 살펴보고, 3장에서는 제안하는 프로토콜에 대해 자세히 기술한다. 4장에서는 제안하는 프로토콜의 안전성과 효율성을 분석한다. 끝으로 5장에서는 결론과 향후 연구방향을 제시한다.

2. 프로토콜

본 절에서는 PSS와 ACR 간의 키 동의 프로토콜과 PSS가 외부 링크로 이동했을 경우 수행하는 프로토콜로 나뉜다. 제안하는 프로토콜에서 ACR과 KAS는 안전한 IPsec 터널을 통해 데이터를 주고받는다. PSD는 PSS에 대한 계산량을 지원하기 위한 장치로서 키 동의 프로토콜이 끝난 후에는 사용을 하지 않으며 USB와 같은 데이터 저장 공간으로 재사용할 수 있다. 또한 PSD가 분실되었을 경우에도 PSS가 추가 키 동의 프로토콜을 수행하지 않고 기존에 생성한 키를 가지고 외부 링크의 ACR과 접속을 위한 인증 절차를 수행할 수 있다. 본 프로토콜에서 RAS는 PSS로부터 전송된 메시지를 ACR에게 포워딩하는 AP(Access point) 역할만 수행한다.

2.1 표기법

표 1. 표기법

표기	의미
PSS	Portable Subscriber Station
RAS	Radio Access Station
ACR	Access Control Router
PSD	Power Support Device
KAS	Key Authentication Server
ID_X	X에 대한 식별자 or 주소
sig^X	X의 서명
g^X	X의 Diffie-Hellman 키동의에 필요한 파라미터
prf(k,m)	키 k와 메시지 m을 입력으로 하는 pseudo random function
h(m)	메시지 m을 입력으로 하는 MDC 해시 함수
$+k^X/-k^X$	X의 공개키/개인키
k^{DH}	Diffie Hellman 세션키
k^{AU}	PSS와 ACR 간의 인증키
$Cookie^I$	서비스 거부 공격과 경로변경 공격을 완화하기 위한 I번째 쿠키
n^I_X	노드 X의 I번재 nonce
NAI^I_X	노드 X의 I번째 network access identifier
L_X	노드 X의 Lifetime
m1||m2	메시지 m1과 메시지 m2의 비트 결합

2.2 프로토콜의 단계별 요약

키 동의 프로토콜은 그림 1과 같다. 먼저 PSS1은 무선인터넷 접속을 위해 RAS1을 거쳐 ACR1에게 다음과 같은 인증 요청 메시지를 전송한다.

① $PSS1 \rightarrow ACR1(REQ) : ID_{PSS1}, NAI^1_{PSS1}, g^x, N^1_{PSS1}, L_{PSS1}, Cookie^1_{PSS1}, Sig(-K_{PSS1}, h(ID_{PSS1} \| NAI^1_{PSS1} \| g^x \| N^1_{PSS1} \| L_{PSS1} \| Cookie^1_{PSS1}))$

PSS1은 네트워크 접속 식별자인 NAI[4]를 인증 요청 메시지에 추가하며 서명을 포함한 공개키 연산은 PSD에서 지원해준다. $Cookie^1_{PSS1}$[5]는 도스 공격과 경로 변경 공격을 완화하기 위해 추가

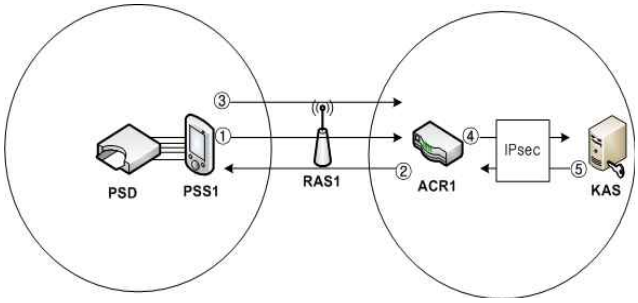

그림 1. PSS1과 ACR1 간 키동의 프로토콜

된 파라미터이며 서명은 Diffie-Hellman 키동의 프로토콜에서 발생할 수 있는 중간자 공격을 방지하기 위해 사용된다.

이 메시지를 수신한 ACR1은 네트워크 접속 식별자를 확인하고 PSS1의 공개키를 이용하여 서명을 확인한다. 그런후에 다음과 같은 응답 메시지를 전송한다.

② $ACR1 \rightarrow PSS1(REP) : ID_{ACR1}, g^y, N^1_{ACR1}, N^1_{PSS1}, L_{ACR1}, Cookie^2_{ACR1}, Sig(-K_{ACR1}, h(ID_{ACR1} \| g^y \| N^1_{PSS1} \| N^1_{ACR1} \| L_{ACR1} \| Cookie^2_{ACR1}))$

ACR1은 Diffie-Hellman 키 동의 파라미터 g^y 를 생성하여 응답 메시지에 추가하고 자신의 개인키로 서명하여 PSS1에게 전송한다. ACR1은 PSS1로부터 수신한 g^x와 자신이 생성한 g^y를 이용하여 Diffie-Hellman 키 $K^{DH}=g^{xy}$를 생성한다. PSS1 역시 PSD의 계산력을 이용하여 ACR1과 같이 $K^{DH}=g^{xy}$를 생성한다. 그런 후에 최종적으로 PSS1과 ACR1은 $K^{AU}=prf(K^{DH}, Cookie^1_{PSS1} \| Cookie^2_{PSS2})$를 생성한다. ACR1은 생성된 인증키를 KAS에게 PSS1 식별자와 함께 안전한 IPsec 터널을 통해 KAS에게 전송한다. 이때 PSS1은 생성된 인증키를 이용해서 무선 인터넷 접속을 시도하면 ACR1은 인증키로 PSS1을 인증하고 접속을 허용한다.

PSS1은 다른 네트워크로 이동하여 더 이상 ACR1의 서비스를 받지 못할 경우에는 PSS1은 접속 요청 메시지를 ACR2에게 전송하면 ACR2는 KAS에게 이 메시지를 넘겨주고 KAS는 이 메시지를 인증하여 ACR2에게 PSS1의 인증키를 전송한다. 이 키를 통해 ACR2는 PSS1을 인증하고 접속을 허가한다.

3. 성능분석

이번 절에서는 앞서 제안한 키 동의 프로토콜의 안전성과 효율성을 표준 프로토콜과 비교 분석할 것이다. 비교 분석은 표 2와 같다.

먼저 표준 프로토콜[3]과 제안하는 프로토콜의 안전성을 분석해보면 두 프로토콜 역시 DoS 공격, 경로 변경 공격 및 중간자 공격에는 안전하다는 것을 볼 수 있다. 특히, 제안하는 프로토콜에서는 쿠키를 이용해서 올바르지 않은 메시지일 경우에는 바로 수신

표 2. 프로토콜의 안전성과 효율성

				[3]	**제안하는 프로토콜**
DoS 공격				○	○
경로 변경 공격				○	○
중간자 공격				○	○
재생 공격				○	○
메시지 수				14	5
PSS	RSA	암호화		1*3028K	1*3028K
		DS(RSA-PSS)	서명	0	0
			검증	0	0
	MAC/prf			6*0.026K	1*0.026K
	합계			≈3028.156K	3028.026K
ACR	RSA	암호화		1*3028K	1*3028K
		DS(RSA-PSS)	서명	0	1*62000K
			검증	0	1*3019K
	MAC/prf			6*0.026K	1*0.026K
	합계			≈3028.156K	68047.026K

한 메시지를 드롭하기 때문에 경로 변경 공격이나 DoS 공격을 완화할 수 있다. 또한 Diffie-Hellman 키 동의 시 발생할 수 있는 중간자 공격은 서명을 통해 방지할 수 있다. 효율성 분석은 [6] 프로토콜을 이용한다. 제안하는 프로토콜의 경우 저전력 노드일 수 있는 PSS의 계산적 부담을 PSD에서 처리하기 때문에 실질적으로 PSS는 적은 계산량으로 키동의를 할 수 있다. ACR은 PSS보다 전력이나 계산량에 제한을 받지 않기 때문에 대체적으로 계산량이 많지만 별 무리가 없다. 또한 표준 프로토콜[3]보다 적은 양의 메시지와 간단한 방법으로 인증을 할 수 있다. 또한 PSS가 재접속을 요구할 경우에는 KAS로부터 인증만 받으면 되기 때문에 표준 프로토콜[3] 보다 더욱 간단한 방법으로 인증할 수 있다. 또한 저전력 노드인 PSS나 PE에서는 두 프로토콜 역시 계산적 부담이 적다.

4. 결 론

본 논문은 안전한 WiBro 서비스를 위한 새로운 인증 프로토콜에 대해서 제안했다. 제안하는 프로토콜 역시 표준 프로토콜[3]과 안전성 면에서는 큰 차이를 보이지 않았다. 그러나 효율성 분석에서는 적은 양의 메시지 사용과 재접속 시에 간단한 방법으로 인증이 가능하기 때문에 인증에 따른 트래픽을 줄일 수 있었다. 향후 연구 과제로는 IPv6 기반에서의 인증 프로토콜이 모바일 IPv6(MIPv6)에서 인증에 대한 처리를 좀더 간단하고 안전하게 처리할 수 있는 프로토콜에 대해 연구할 것이다.

참고문헌

[1] 이광희, “와이브로 기술의 국제표준채택에 따른 향후 전망”, Korea Telecommunications Operators Association, 제 49호, 2007.

[2] 김홍구, “와이브로에서의 IPv6 기술(IPv6 over WiBro)", 한국정보통신기술협회, 2006.

[3] 김홍구, “휴대인터넷(와이브로 TM) 서비스를 위한 상호 인증 절차”, 한국정보통신협회, 2006.

[4] A. Patel, K. Leng, H. Akhtar, M. Khalil, "Network Access Identifier Option for Mobile IPv6," IETF Internet Draft, July 2004.

[5] P. Kern, W. Simson, "Photuris: Extended Schemes and Attributes", RFC 2523, March 1999.

[6] Jung-Doo Koo and Dong-Chun Lee, "Extended Ticket-Based Binding Update (ETBU) Protocol for Mobile IPv6 (MIPv6) Networks, IEICE Transactions on Communications, vol.E90-B, no.4, pp.777-787, April 2007.