상호인증을 강화한 3G 모바일 인증방법에 대한 연구

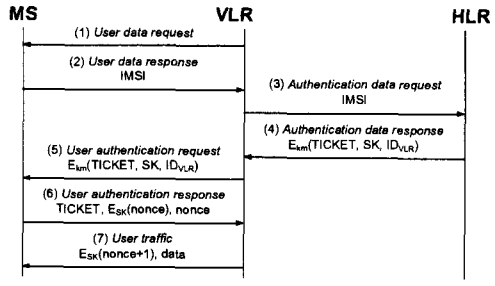
한찬규° 최형기
성균관대학교 정보통신공학부
{hedwig,hkchoi}@ece.skku.ac.kr

Mobile Authentication Method in 3G networks for Strengthening the Mutual Authentication

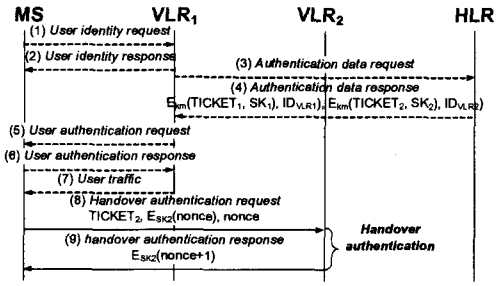
Chan-Kyu Han° Hyoung-Kee Choi
School of Information and Communication Engineering, Sungkyunkwan University

최근 들어 사용자의 이동성을 보장하며 음성 및 데이터 서비스를 지원하는 이동통신 서비스가 대두되고 있다. 반면 이동통신 서비스는 편리한 기능의 제공 외에 가입자 정보, 통신 정보 등을 대상으로 하기 때문에 보안이 중요한 요소이다. Third Generation Partnership Project(3GPP)에서는 모바일 환경에서 보다 강화된 보안을 제공하기 위해 3GPP Authentication and Key Agreement(AKA) 표준을 발표하였다[1]. 3GPP AKA는 홈네트워크의 인증서버(Home Location Register:HLR)와 단말 간에 공유된 비밀값을 이용하여, 단말과 단말이 이동한 방문네트워크의 서버(Visited Location Register:VLR)간에 상호인증 및 세션키 생성을 정의한다. 그러나 3GPP AKA는 적어도 다음의 세 가지 공격에 취약하다. 첫째, 공격자는 False base station[2]을 이용하여 단말의 인증요청을 보안강도가 낮거나 과금이 비싼 VLR로 redirect할 수 있다. 둘째, 공격자는 공격자에게 노출된 VLR에서 생성된 세션키를 사용하여 사용자의 통신정보를 도청할 수 있다. 마지막으로 사용자의 핸드오버 시 VLR 간에 교환되는 인증정보를 가로채어 사용자의 통신정보를 도청하는 공격이 가능하다. 위 3가지 문제점과 같이 3GPP AKA에서 발견된 보안 문제점은 사용자와 VLR 간의 상호인증이 취약하다는 문제점에서 기인한다. 3GPP AKA에서는 상호인증을 제공하기 위한 다양한 연구가 진행되어 왔으나[2][3] 완전한 상호 인증 메커니즘을 제공하지 못하고 있다.

본 논문에서는 보다 완전한 상호인증을 보장하고, 자원소모를 감소시키기 위해 Kerberos[4]를 활용하여 단말과 VLR 간의 상호인증을 도모하고자 한다.



(그림 1) Kerberos-AKA의 메시지 흐름



(그림 2) Hadover를 고려한 Kerberos-AKA

(그림 1)은 본 논문에서 제안하는 Kerberos-AKA의 메시지 흐름을 나타낸다. 단말이 VLR을 인증하는 방식은 다음과 같다. 단말은 메시지 (6)에서 *nonce*을 생성하고, VLR은 메시지 (7)에서 *nonce+1*을 *SK*로 암호화하여 전달한다. 단말은 *SK*로 암호화되어 있는 *nonce+1*을 복호화하여, VLR이 *SK*를 소유한 인증요소인지 확인할 수 있다. VLR이 단말을 인증하는 방식은 다음과 같다. VLR은 메시지 (6)에서 *TICKET*을 복호화하여 *SK*를 알 수 있다. 메시지 (6)에 포함된 *nonce*값과 $E_{sk}(nonce)$을 복호화한 값을 비교하여 일치한다면 단말이 *SK*를 소유하였음을 확인할 수 있으므로 단말을 인증한다. 이러한 상황에서 단말이 VLR_2로 이동하였을 때 기존의 3GPP AKA에서는 VLR_1과 VLR_2사이의 응답-요청을 통하여 VLR_1이 보호되지 않는 채널로 단말의 AV를 VLR_2에게 전송하는 방식을 정의하였다. 본 논문에서는 보

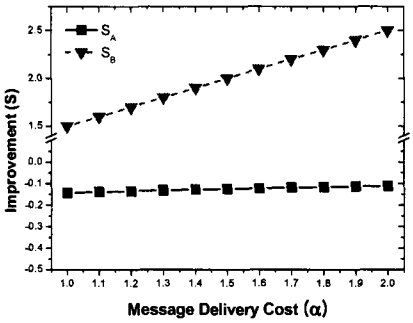
호되지 않는 채널로 VLR 간의 인증정보의 교환이 없는 핸드오버 인증 기법으로 (그림 2)에서 보듯이 메시지 (8)과 메시지 (9)를 제시하였다. 메시지 (1)에서 메시지 (7)를 통해 핸드오버 할 VLR에 대한 *TICKET*을 미리 수신할 수 있다. 지연이 적은 핸드오버를 위해, 이웃 Access Point(AP)에게 인증정보를 사전 분배하는 매커니즘이 다수 연구되고 있다[6]. 따라서 Kerberos-AKA에서 핸드오버를 위해 *TICKET*를 사전 분배하는 것은 reasonable 하다고 말할 수 있다.

	3GPP AKA	Kerberos-AKA
MS 연산량	5H+1X	2E
VLR 연산량	-	2E
HLR 연산량	5H+1X)×m	2E
단말-VLR대역폭	128×4bits	128×6bits
VLR-HLR대역폭	(128×5)×m bits	128×3bits

(표 1) 연산량 비교

		3GPP AKA	Kerberos-AKA
Full Auth.	단말-VLR	4	5
	VLR-HLR	2	2
Handover Auth.	단말-VLR	3	2
	VLR_1-VLR_2	2	-

(표 2) 메시지 교환횟수 비교



(그림 3) Kerberos-AKA의 성능향상정도

(표 1)은 연산량 면에서 3GPP AKA와 Kerberos-AKA를 비교 분석한 결과이다. 3GPP AKA의 경우 HLR이 *XRES, CK, IK, MAC, AUTN* 마다 해쉬함수 연산을 하고, *SQN*를 *AK*와 XOR하기 때문에 5H+1X의 연산량이 필요하다. 또한 이러한 작업을 AV[1..m]개 마다 반복하기 때문에 AV의 개수 m을 고려하였다. 반면 Kerberos AKA에서는 HLR에서는 TICKET을 k_v로 암호화하여 생성하고 다시 k_m으로 암호화하는데 2E의 과정이 필요하다. (표 2)는 메시지 교환횟수면에서 3GPP AKA와 Kerberos-AKA를 비교 분석한 결과이다. 단말과 VLR의 메시지 교환 Cost를 1 unit으로 가정하고 VLR과 HLR간 및 VLR과 VLR간의 메시지 교환 Cost를 α unit으로 가정한다. 또한 인증시나리오를 고려하여 Full authentication을 *A*, Handover authentication을 *B*라 정의한다. 이에 대해 Kerberos-AKA의 성능향상을 S_A, S_B라고 표기하고 이를 (그림 3)에 나타내었다. 메시지 교환 Cost인 α가 증가함에 따라 성능향상의 정도는 증가한다. 이처럼 제안한 인증기법은 핸드오버 과정에서 인증시간을 단축시켰다. 기존에 3GPP AKA에서 VLR 간에 인증정보를 교환하던 방식을 지양하고, 단말이 VLR에게 바로 핸드오버 인증을 요청하는 방식을 제안하였다. 이로써 핸드오버 인증 전체 과정에서 사용되는 메시지의 개수가 5개에서 3개로 감소하였고, 특히 VLR 간 메시지 교환을 없애 높은 성능향상을 보였다.

참고문헌

[1] Third Generation Partnership Project, Technical Specification Group SA, 3G Security, "Security Architecture, version 4.2.0, Release 4", 3GPP, TS 33.102, 2001

[2] Muxiang Zhang, Yuguang Fang, "Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol", *IEEE Transactions on Wireless Communications*, Vol.4, No.2, March 2005

[3] Wen-Shenq Juang, Jing-Lin Wu, "Efficient 3GPP Authentication and Key Agreement with Robust User Privacy Protection", *IEEE Wireless Communications and Networking Conference*(WCNC), March 2007

[4] Charlie Kaufman, Radia Perlman, Mike Spenciner, "Network Security; Private Communication in a Public World", *Prentice Hall*, 2nd edition, 2002

[5] Chung-Ming Huang, Jian-Wei Li, "Authentication and Key Agreement Protocol for UMTS with Low Bandwidth Consumption", *The 19th International Conference on Advanced Information Networking and Applications* (AINA), March 2005

[6] Chanil Park, Junbeom Hur, Chanoe Kim, Young-joo Shin, and Hyunsoo Yoon, "Pre-authentication for Fast handoff in Wireless mesh networks with mobile APs", *The 7th International Workshop on Information Security Applications (WISA 2006)*, August 2006