情報保護學會論文誌
第16卷 第6號, 2006. 12

사용자 프라이버시를 위한 안전한 GSM 사용자인증 프로토콜

박 미 옥,† 김 창 민‡
성결대학교

Secure GSM User Authentication Protocol For User Privacy

Mi-Og Park,† Chang-Min Kim‡
Sungkyul University

요 약

가장 대표적인 이동통신 표준의 하나인 GSM(Global System for Mobile communication)은 전 세계 70%이상의 사용자를 보유하고 있으며 사용자의 수도 지속적으로 증가하고 있다. 그러나 GSM 시스템은 사용자인증과정 중 MS(Mobile Station)을 유일하게 인증가능한 IMSI(International Mobile Subscriber Identity)값이 노출되어 사용자를 정상적으로 인증할 수 없는 문제를 가지고 있다. 본 고에서는 임시아이디와 암호화방식의 채택으로 안전성 향상과 사용자 프라이버시를 제공한다. 더욱이 기존의 GSM 사용자인증 프로토콜의 구조변경을 통해 빠른 사용자인증을 제공한다.

ABSTRACT

GSM(Global System for Mobile communications) that is the most popular standard for mobile phones, has more than 70% users in the world and the number of users increase continuously. However GSM system has the problem that cannot normally authenticate a user by the exposure of IMSI that is able to uniquely authenticate MS? during the user authentication procedure. In this paper? we provide security enhancement and user privacy by adopting a temporary id and an encryption scheme. Moreover we provide fast user authentication via architecture modification of the conventional GSM user authentication protocol.

Keywords : *User authentication protocol, Strong authentication, Anonymity, User privacy, GSM*

Ⅰ. GSM 사용자인증 프로토콜

GSM 시스템은 인증되지 않은 접근으로부터 네트워크와 사용자 프라이버시를 보호하기 위해 암호화 방식을 채택하였다. GSM의 사용자인증(그림 1)은 암호화키 분배과정과 함께 수행되며 *IMSI*가 네트워크에 알려지고, 채널이 암호화되기 전에 수행된다.

접수일: 2006년 7월 13일 ; 채택일: 2006년 11월 6일
† 주저자, mopark777@sungkyul.edu
‡ 교신저자, kimcm@sungkyul.edu

MS는 새로운 VLR(Visited Location Register)에게 *TMSI*(Temporary Mobile Subscriber Identity)와 *LAI*(Location Area Identity)를 전송하여 자신의 존재를 알린다. 새로운 VLR은 이전의 VLR에게 MS가 전송해온 *TMSI*와 *LAI*를 전송하여 MS의 *IMSI*값을 되돌려 받는다. 새로운 VLR은 MS의 신원을 검증받기 위해 *IMSI*를 HLR(Home Location Register)에 전송한다. HLR은 MS와의 비밀키 *Ki*와 난수 *RAND*를 입력으로 하는 A3알고리즘을 수행

하여 인증서명값 *SRES*와 암호화키 *Kc*를 계산한 후, n개의 인증파라미터 (*RAND*, *SRES*, *Kc*)를 새로운 VLR에 전송한다. 새로운 VLR은 이 n개의 인증파라미터 중에서 한 쌍의 triple을 선택하고, 이 triple에서 *RAND*값만 MS에게 전송한다. 새로운 VLR로부터 *RAND*를 전송받은 MS는 자신의 비밀키 *Ki*와 전송받은 *RAND*를 A3에 입력하여 생성된 *SRES*를 새로운 VLR에 전송한다. 새로운 VLR은 자신이 계산한 *SRES*와 MS로부터 전송받은 *SRES*를 비교하여 두 개의 값이 동일하면, MS를 정당한 개체로 인증하여 다음 서비스를 계속한다. 만약 값이 동일하지 않으면, MS 인증은 실패한 것으로서 세션을 종료한다[1,2]. 그러나 GSM 시스템은 무선채널상의 통신망에만 암호화방식을 채택하기 때문에, 제 3자는 HLR의 채널을 통해 *IMSI*와 같은 인증정보를 획득함으로써 다음과 같은 사용자인증 문제[3,4]를 발생시킨다.

- VLR/VLR간 그리고 VLR/HLR간의 통신에 암호화방식을 사용하지 않기 때문에, 사용자인증 정보인 *IMSI*가 노출되어 사용자인증, 위치갱신, 그리고 사용자 프라이버시 침해와 같은 문제들을 초래한다.
- GSM 시스템은 MS만을 인증하는 단일인증방식을 제공하기 때문에, VLR의 신분이 검증되지 않아 제 3자가 정당한 개체로 가장할 수 있다.
- VLR은 인증파라미터를 모두 소비할 경우, n개의 새로운 인증파라미터를 HLR에게 요청해야한다. 하나의 VLR안에 존재하는 모든 MS들은 n개의 인증파라미터를 가지고 있고, 이 인증파라미터들은 VLR에 저장되기 때문에 n개만큼의 저장공간 오버헤드가 발생한다.
- MS인증시, n개의 인증파라미터 전송 때문에 VLR/HLR간의 대역폭 소비가 발생한다.

Ⅱ. 향상된 사용자인증 메커니즘

1. 기본 원리

제안 메커니즘은 안전한 사용자인증과 프라이버시 보장을 위해 MS의 임시아이디 *TID*를 사용한다. *TID*는 *IMSI*대신 사용자인증 가능한 부가적인 파라미터로서, *IMSI*와 일대일로 매핑되며 HLR에서 유일한 값이어야 한다. *TID*는 안전한 의사난수생성기에 의해 랜덤하게 생성된다. 그러나 파라미터 *TID* 자체는 공개정보이다. *TID*의 생성은 HLR만이 가능하며, 사용자는 등록과정에서 비밀키 *Ki*, *IMSI*와 함께 *TID*를 제공받는다. 또한 제안 메커니즘에서는 MS/VLR간 상호인증, HLR에 의한 VLR로의 인증권한부여, 그리고 VLR의 신분을 검증한다. VLR은 MS인증권한을 부여받기위해 난수 $RAND_V$를 생성하여 자신의 인증서 *CertV* 계산을 위해 MS로부터 전송받은 *T*와 $RAND_V$를 XOR한 후, 자신의 비밀키 K_{VH}를 사용해 A3(K_{VH}, *T* XOR $RAND_V$)를 계산한다. 인증권한을 부여받은 후, VLR은 MS인증을 위해 HLR에서 생성한 비밀키 *Zi*를 사용한다. *Zi*는 HLR에서 생성한 난수 $RAND_H$와 *TIDn*, 그리고 전송받은 *T*를 XOR하여, 그 결과값을 HLR/MS와의 비밀키 *Ki*와 함께 A3(*Ki*, *T* XOR *TIDn* XOR $RAND_H$)로 입력함으로써 계산된다. 또한 인증권한을 부여받은 새로운 VLR은 MS가 새로운 VLR의 영역에 계속 머무르는 동안, MS인증을 위해 각각의 j번째 호를 위해 새로운 난수 *RANDj*만을 생성하면 된다.

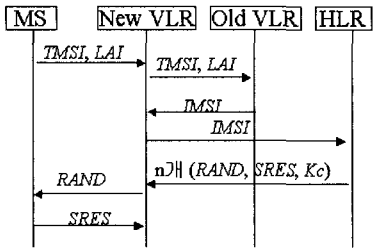
〔표 1〕 파라미터 정의

파라미터	기 능
T	타임스탬프(time stamp)
TIDo/*TIDn*	MS의 이전과 새로운 임시아이디
VLR_{ID}/HLR_{ID}	VLR과 HLR의 각 아이디
RANDi	각 개체가 생성한 난수들
Xv	*RANDv*와 *TIDn*의 XOR 연산값
K_{VH}	VLR과 HLR간의 공유비밀키
CertM	MS가 생성한 MS의 인증서
CertV	VLR이 생성한 자신의 인증서
CertHV	HLR이 생성한 VLR의 인증권한부여서

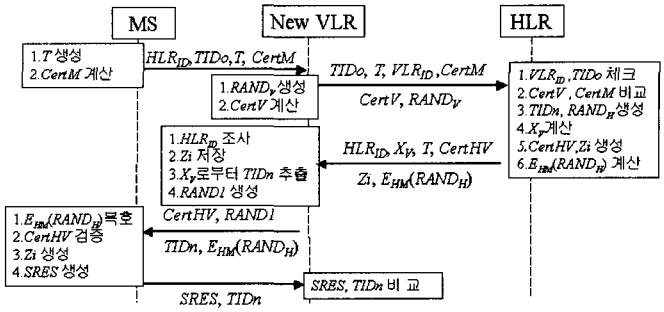
2. 제안 메커니즘의 동작원리

제안 메커니즘의 각 단계의 동작원리는 다음과 같다(그림 2).

단계 1) MS는 자신의 인증서 *CertM* 계산을 위해 자신이 생성한 타임스탬프 *T*, 현재의 임시아이디 *TIDo*, $RAND_H$, 그리고 *IMSI*를 XOR한 결과값과 비밀키 *Ki*를 A3(*Ki*, *T* XOR *TIDo* XOR $RAND_H$ XOR *IMSI*)에 입력



〔그림 1〕 GSM 사용자인증 프로토콜의 절차



〔그림 2〕 제안 메커니즘의 절차

한다. 이 결과값을 자신의 인증서 $CertM$로 사용하며, VLR에게 HLR_{ID}, T, $TIDo$, 그리고 $CertM$을 전송한다. 인증서 $CertM$ 계산에 사용된 난수 $RAND_H$는 MS인증단계에서 HLR이 생성하여 MS에게 전송해 준 비밀값으로서, MS가 새로운 VLR로 이동할 때 단 한번만 생성된다.

단계 2) 새로운 VLR은 자신이 생성한 난수 $RAND_V$와 전송받은 T를 XOR하여 그 결과값을 자신의 비밀키와 함께 A3에 입력함으로써 자신의 인증서 $CertV$를 계산한다. 그런 다음 $TIDo$, T, $CertM$, 자신의 아이디 VLR_{ID}, $CertV$, 그리고 $RAND_V$를 secure channel를 통해 HLR에게 전송한다. 만약 중복되는 $TIDo$가 존재하면 기존의 것은 그대로 두고 중복되는 두 번째 $TIDo$의 뒤에 숫자를 붙여 구별한다.

단계 3) HLR은 VLR_{ID}와 $TIDo$가 합법적인 ID인지 조사하여, VLR과 MS의 검증여부를 결정한다. 만약 일치하는 ID들이 없으면 세션을 종료하고, 일치하면 ID에 일치하는 VLR과 MS의 비밀키를 알 수 있기 때문에 $RAND_V$와 T를 사용하여 $CertV'$를 계산한다. 전송받은 $CertV$와 자신이 계산한 CertV′값이 동일하면, VLR을 정당한 개체로 신뢰하고, MS검증을 위해 전송받은 $TIDo$, T, 그리고 그에 일치하는 $IMSI$와 비밀키 Ki, $RAND_H$를 조사하여 $CertM'$를 계산한다. 전송받은 $CertM$과 자신이 계산한 $CertM'$의 계산결과가 다르면 세션을 종료하고, 동일하면 새로운 난수 $RAND_H$와 새로운 임시아이디 $TIDn$을 생성하여 T, VLR_{ID}와 XOR하여 MS의 비밀키와 함께 A3를 수행하여 VLR 인증권한부여서 $CertHV$ (A3(Ki, T XOR $TIDn$ XOR VLR_{ID} XOR $RAND_H$)를, $TIDn$, T, $RAND_H$를 XOR한 결과와 Ki를 A3에 입력하여 Zi를 계산한다. 마지막으로 HLR은 HLR_{ID}, X_V, $CertHV$, E_{HM} ($RAND_H$), 그리고 Zi를 새로운 VLR에게 전송한다. X_V는 전송받은 $RAND_V$와 새롭게 생성한 $TIDn$을 XOR한 결과를, $E_{HM}(RAND_H)$는 MS/HLR간의 암호화키로 암호화함을 나타낸다.

단계 4) 새로운 VLR은 HLR_{ID}를 확인하여 이 ID에 일치하는 비밀키 K_{VH}를 찾아낸 후, 전송받은 Zi를 저장한다. 일치하는 ID가 존재하면 VLR은 자신이 생성한 $RAND_V$를 알고있기 때문에 전송받은 X_V와 $RAND_V$를 XOR하여 $TIDn$값을 추출한다. $RAND_V$값이 변경되었다면 올바른 $TIDn$값을 얻을 수 없다. 동시에 VLR은 난수 $RAND1$을 생성하여 $VLR_{ID}, TIDn, CertHV, E_{HM}(RAND_H)$와 함께 MS에게 전송한다.

단계 5) MS는 VLR신분과 인증권한부여서의 정당성 검증을 위해 자신의 암호화키로 $E_{HM}(RAND_H)$를 복호화한다. 그런 다음 저장했던 T, $RAND_H$, VLR_{ID}, $TIDn$을 XOR하여, 자신의 비밀키 Ki와 함께 A3를 수행하여 $CertHV'$를 계산한다. 자신이 계산한 $CertHV'$과 전송받은 $CertHV$값이 동일하면, VLR을 정당한 개체로 믿고 VLR과의 비밀키 Zi를 계산하기 위해 $RAND_H$, $TIDn$, 그리고 T를 XOR연산 후 Ki와 함께 A3를 수행한다. Zi가 생성된 후, 전송받은 $RAND1$과 Zi를 A3로 입력하여 얻어진 결과값 $SRES$와 $TIDn$를 새로운 VLR에 전송한다. 새로운 VLR은 자신이 계산한 $SRES'$과 전송받은 $SRES$, 그리고 전송받은 $TIDn$과 저장해둔 $TIDn$를 각각 비교하여, 값이 모두 동일하면 MS를 정당한 개체로 인증하고, 그렇지 않으면 MS인증은 실패하여 세션을 종료한다.

Ⅲ. 비교 분석

제안 메커니즘의 안전성은 GSM의 보안 알고리즘 A3, A5, A8의 비도에 의존한다.

- 안전한 사용자인증

제안 메커니즘은 기존 메커니즘들과 달리 *IMSI* 값을 전송하지 않기 때문에, MS자체에서 이 값이 노출되지 않는한 안전한 사용자인증을 제공한다.

- 각 개체의 인증과 상호인증

MS와 VLR은 자신이 생성한 타임스탬프와 난수를 사용한 인증서 *CertM*과 *CertV*를 통해 HLR로부터 신분을 검증받는다. 또한 MS는 *CertHV*를 통해 HLR의 VLR 인증서를 다시 조사함으로써 새로운 VLR의 신분을 믿는다. GSM 시스템이나 기존의 다른 메커니즘들조차도 VLR을 인증하지 않거나 간단한 방식에 의해 곧바로 MS인증권한을 VLR에게 부여하기 때문에 시스템 전체의 안전성에 큰 문제를 야기할 수 있다. 제안 메커니즘에서는 *CertV*를 통해 HLR로부터 VLR의 신분을 인증하고, 인증이 성공한 경우에만 MS인증권한을 부여하여 네트워크상의 개체관리뿐만 아니라 정보관리의 안전성도 함께 제공해준다.

- ***TID*로부터의 *IMSI*의 안전성**

*TID*와 *IMSI*값의 일대일 매핑관계는 MS와 HLR만이 알고있으며 검증받은 정당한 VLR조차도 이 매핑관계를 알 수 없다. 또한 *TID*는 안전한 의사난수생성기에 의해 랜덤하게 생성되기 때문에, *TID*를 이용한 *IMSI*값의 유추공격에 안전하다. 또한, 임의의 한 VLR에 계속 머무를 경우 매번 HLR로부터 새로운 *TID*를 전송받는 것이 아니라 단 한번만 전송받기 때문에 매번 *TID*를 생성해야하는 계산과 전송의 대역폭 오버헤드를 줄일 수 있다.

- **VLR의 인증권한에 의한 *Ki*값의 안전성**

VLR은 HLR로부터 부여받은 인증권한을 위해 먼저 자신의 신분을 검증받은 후, HLR로부터 secure channel을 통해 전송받은 *Zi*를 MS/VLR간의 공유비밀키로 사용한다. 그러나 *Zi*의 생성은 비밀키 *Ki*로부터 유도되고, VLR은 *Ki*값과 MS의 *IMSI*값도 모른 상태에서 MS를 인증하기 때문에 *Ki*값의 노출위험은 없다.

- 강력한 인증기능

MS인증서 *CertM*은 난수 $RAND_H$, MS가 생성한 타임스탬프 *T*, 현재의 임시아이디 *TIDo*, 그리고 MS의 *IMSI*를 사용해 계산된다. $RAND_H$와 *TIDo*는 HLR이 생성한 파라미터들이고 *IMSI*는 HLR과 MS만이 알고있는 비밀인증 정보이다. 그러므로 *CertM*은 단순히 *T*나 MS가 생성한 난수만을 사용하는 방식에 비해 더 강력한 인증기능을 제공한다. VLR인증서와 인증권한부여서도 VLR에서 생성한 값과 자신의 아이디뿐만 아니라 MS에서 생성된 *T*를 인증서 계산에 같이 사용함으로써 MS 정당성과의 연계에 의해 VLR신분을 검증받기 때문에, 단순한 인증방식만을 사용하는 기존 메커니즘들에 비해 강력한 인증방식을 제공한다.

- 익명성

익명성을 거의 제공하지 않는 대부분의 기존 메커

〔표 2〕 기존 메커니즘들과의 특성비교

특성	GSM	제안메커니즘	[3]	[5]	[6]	[7]
MS/VLR간 상호인증	×	○	○	○	×	○
대역폭 사용량 축소	n	1	1	1	1	1
VLR 저장공간 축소	-	○	○	○	○	○
VLR간의 암호화필요성	-	×	○	○	○	○
VLR의 오버헤드	-	GSM과 난수생성 알고리즘	GSM과 난수생성 알고리즘	GSM과 난수생성 알고리즘	GSM과 난수생성 알고리즘	혼용
익명성	×	○	×	×	○	×
재생 공격	×	○	×	×	○	○
VLR의 IMSI사용	사용함	사용안함	사용함	사용함	사용함	사용함
인증단계 감소	7	5	7	6	7	7
강력한 인증기능	×	○	×	×	○	×
간단한 부인봉쇄	×	○	×	×	○	×

니즘들과 달리, 제안 메커니즘은 MS가 방문하는 VLR이 변경될때마다 새로운 *TIDn*과 HLR에게 검증받은 정당한 VLR일지라도 *IMSI*값을 전달받지 않기 때문에, MS와 HLR을 제외한 어느 개체에게도 *IMSI*값이 노출되지 않는다. 그러므로 익명성에 의한 사용자프라이버시를 안전하게 제공한다.

• 인증단계 감소

제안 메커니즘은 새로운 VLR이 이전의 VLR과의 통신단계를 없애고, HLR과 곧바로 통신함으로써 최소 7단계가 필요한 기존의 인증단계를 5단계로 감소시켰다. 그리하여 빠른 사용자인증과 함께 다음 서비스를 보다 빠르게 처리할 수 있다. 또한 이전 VLR과의 통신단계가 사라짐으로써, 그에 따른 프로세스 오버헤드가 사라졌다.

• 간단한 부인봉쇄

HLR이 생성한 $RAND_H$는 암호화되어 전송되기 때문에, 정당한 MS만이 $RAND_H$값에 대한 복호화가 가능하다. 그러므로 MS의 비밀키가 노출되지 않는 한, 어느 개체도 $RAND_H$값을 알 수 없어 MS의 간단한 부인봉쇄가 제공된다. 간단한 부인봉쇄는 공개키 방식에서의 부인봉쇄를 의미하지 않는다.

• $RAND_H$의 오버헤드

제안 메커니즘에서는 MS가 새로운 VLR에 방문하는 한번만 HLR로부터 한 개의 $RAND_H$를 전송받기 때문에, n개의 오버헤드가 1번으로 감소한다.

• 재생 공격

제 3자가 임의 정보를 획득하였다 할지라도 각 인증서 계산은 타임스탬프와 각 개체들이 생성한 난수들, 그리고 인증서생성 주체인 각 ID를 같이 사용하여 계산되기 때문에, 이전에 획득한 값들의 변경에 의해 현재의 인증서를 재사용할 수 없다. 각 인증서에 대한 공격에 성공하려면, HLR/MS간 그리고 HLR/VLR간의 각 비밀키를 분석해야만 한다.

Ⅳ. 결 론

본고에서는 불안전한 GSM 사용자인증 문제를 해결하고 안전한 사용자인증과 프라이버시를 보장하기 위해, MS의 임시아이디인 *TID*를 사용하였다. 또한 각 개체가 생성한 난수와 타임스탬프, 각 개체의 아이디, 그리고 HLR이 생성해준 난수 등을 가지고 각 개체가 인증서를 생성함으로써 개체의 강력한 인증방법을 제공하였다.

참 고 문 헌

[1] L. Chichun, C. Yujen, "Secure Communication Mechanism for GSM Networks," *IEEE Transactions on Consumer Electronics*, 45(4), pp. 1074-1080, November 1999.

[2] L. Chichun, C. Yujen, "Stream Ciphers of GSM," *Computer Communications* 24, pp. 1090-1096, 2001.

[3] Lee. C.C., Hwang. M.S., Yang. W.P., "Extension of Authentication Protocol for GSM," *IEE Proceedings. Communications*, 150(2), pp. 91-95, 2003.

[4] C. Yeongsub, C. Sangrae, C. Daeseon, J. Seunghun, C. Kyoil, P. Cheehang, "A Location Privacy Protection Mechanism for Smart Space," *WISA*2003, LNCS 2908, pp. 162-173, 2004.

[5] C. Youngjae, K. Soonja, "An Improvement on Privacy and Authentication in GSM," *WISA*2003, LNCS 3325, pp. 14-26, 2004.

[6] W.B. Lee, C.K. Yeh, "A New Delegation-Based Authentication Protocol for User in Portable Communication Systems," *IEEE Transactions on wireless communications*, Vol.4, No.1, pp. 57-64, 2005.

[7] O. Aydemir, A. A. Selcuk, "A Strong User Authentication Protocol for GSM," *14th IEEE Workshops on Enabling Technologies*: Infrastructures for Collaborative Enterprises(WETICE'05), Linkoping, Sweden, June 2005.