화자인증을 이용한 GSM 사용자 인증모델

박미옥*, 김은환*, 전문석*
*숭실대학교 컴퓨터학과
e-mail:mopark@kingdom.ssu.ac.kr

A GSM User Authentication Model using Speaker Verification

Mi-Og Park*, Eun-Hwan Kim*, Moon-Seog Jun*
*Dept of Computer Science, Soong-Sil University

요약

GSM(Global System for Mobile Communications) 표준은 전송되는 데이터를 암호화하여 사용하는 안전한 모바일 폰 시스템을 위해서 디자인되었다. 하지만, GSM이 더 이상 안전하지 않다는 것이 입증되고 있다. 그래서, 본 고에서는 GSM 이동통신상의 전자상거래 이용자들에게 보다 편리하고 안전한 서비스를 제공하기 위해서 새로운 모델을 제안한다.

본 고에서 제안하는 모델은 GSM의 사용자 인증을 개선하기 위해서 화자인증을 결합한 더 안전한 사용자 인증 방법을 제안하였고, 이 인증방법을 기반으로 하여 사용자인증 서비스를 어디에서 제공해 주느냐에 따른 모델에 대한 분석을 제시한다.

1. 서론

2002년 현재 IT 업계의 화두는 단연 움직이는 인터넷 서비스, 즉 모바일 인터넷이며 디지털 이동통신의 대표적인 것이 바로 GSM(Global System for Mobile communications)이다. GSM 방식 단말기는 현재 세계 전체 이동전화의 55%, 디지털 셀룰러의 64%를 점유하고 있으며 142개국에서 2억5천만 이상의 가입자를 확보하고 있지만[1], GSM 보안이 더 이상 안전하지 않다는 사실이 보고되고있다[2],[3]. 그래서, 본 논문은 급속히 증가하는 이동통신상에서의 전자상거래 사용자들에게 보다 안전한 GSM 보안을 제공하기 위해서 화자인증 기술을 이용하여 사용자에게는 편리함을 제공하고, 사용자를 인증하는 보안에 있어서는 더 강력한 보안성을 제공하는 새로운 모델을 제안한다.

본 논문의 구성은 2장에서 기존의 GSM 보안을 살펴보고, 3장에서는 전자상거래 상에서 보다 안전한 사용자 인증을 위한 새로운 모델의 개념과 동작원리, 그리고 장단점 등을 통해서 제안한 모델이 편리성과 함께 더 강력한 사용자 인증을 제공한다는 사실을 기술하고, 그에 대한 효율성을 보인다. 마지막으로 4장에서는 제안한 모델의 향후 과제와 결론을 내린다.

2. GSM Security

GSM 표준에서의 인증은 가입자 식별정보와 인증용 알고리즘 및 키가 내장된 스마트 카드를 단말기에 넣고 네트워크와의 인증을 행하는 것이 특징이다. 인증 프로토콜은 IMSI 또는 TMSI 정보를 이용한 가입자 확인이 선행되어 이루어지는 것으로 먼저 가입자 A가 통화 요구를 네트워크 측에 TMSI 정보를 전송함으로써 네트워크 측의 인증센터가 가입자의 인증용 키를 데이터 베이스로부터 수령하여 준비된 상태가 되면 프로토콜을 시작한다. 프로토콜의 절차는 3단계로 이루어지며 [그림1]과 같다[4],[5].

[단계 1] 인증센터는 가입자 A로부터의 통화 요구가 있을 경우 먼저 난수 RAND(Challenge R)를 발생하여 가입자 A에게 전송한다

[단계 2] 가입자 A는 수신한 RAND를 사용하여 자신의 인증키 Ki를 인증 알고리즘인 A3에 입력하여

출력 SRES를 계산하고 인증센터에 이 SRES 값을 전송한다.

[단계 3] 인증센터는 가입자 A의 인증키 Ki와 자신이 발생한 난수를 입력으로 한 A3 알고리즘의 출력값과 수신한 SRES 값을 비교한다. 이 값이 일치하면 인증센터는 사용자를 정당한 사용자로 판단하고 그 다음 절차인 A8 알고리즘과 A5 알고리즘을 순서대로 실행한다.

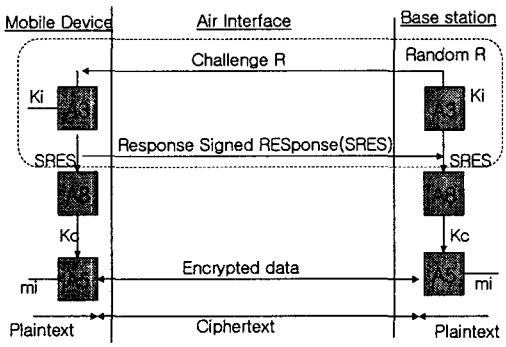

그림 1 GSM 보안 모델

3. 제안한 모델

사용자 인증 알고리즘(A3), 세션키 생성알고리즘(A8), 데이터 암호알고리즘(A5)을 순서대로 사용하는 GSM은 역추적공격에 의해 이미 해독 가능한 것으로 보고되고있다. 또한, 차세대 이동통신 보안에 대한 연구는 활발히 진행되고 있는 반면에, 현재 사용중인 이동통신보안에 관한 연구는 활발히 이루어지지 않고 있는 실정이다. 그래서, 본 고에서는 이러한 문제점을 해결하여 기존의 수많은 이동통신 사용자들에게 보다 더 안전한 통신을 제공하고, 특히 이동통신을 이용한 전자상거래 사용자들에게 더 안전한 보안과 편리성을 제공하기 위한 목적으로 새로운 GSM 사용자인증 모델을 제안한다.

전자상거래의 서비스를 안전하게 사용하기 위해서는 무결성, 비밀성, 인증, 부인방지의 네 가지 기능을 지원해야 하며, 전자상거래는 이 네 가지 기능 중에서도 전자상거래라는 특성상 사용자 인증부분에 많은 중요성을 두고 있다. 그 이유는 전자상거래 상에서 빈번히 발생할 수 있는 도난과 같은 문제점은 정당한 사용자뿐 아니라 서비스를 제공해주는 측에게도 많은 피해를 주기 때문이다.

3.1 제안한 모델의 동작원리

본 고에서는 전자상거래를 사용하는 이동 단말기 사용자들에게 보다 안전한 인증과 부인방지 서비스를 제공하기 위해서 화자인증 방법을 GSM에 사용하는 방법을 제안한다. GSM의 사용자인증 방법과 화자인증 방법을 새롭게 구축하는데는 여러 가지 방식이 존재할 수 있는데, 본 고에서 제안하는 모델은 기존의 GSM 사용자인증과 화자인증을 병렬로 수행하는 방안을 제안한다. 병렬로 수행된 두 개의 사용자 인증알고리즘의 결과는 AND 연산으로 연결하여 결과가 모두 참일 경우에만 사용자인증이 성공하도록 모델을 만든다. 이 사용자 인증과정이 성공하면 그 다음 단계는 기존의 GSM 사용자 인증방식과 동일하게 세션키를 생성하는 과정을 실행하고 그 다음 단계인 데이터를 암호화하여 전송하는 단계로 진행하는 방식이다. 본 고에서는 제안한 화자인증과 기존의 GSM 사용자 인증알고리즘을 결합하여 병렬로 수행하는 새로운 방식의 사용자 인증방법을 병렬 사용자 인증모델이라 칭하기로 하고, 그에 대한 그림은 다음 [그림2]에서 볼 수 있다.

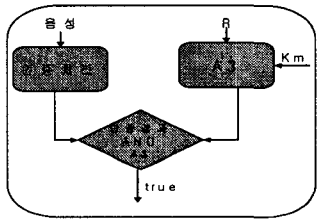

그림 2 병렬 사용자 인증모델

새롭게 제안한 병렬 사용자 인증모델은 사용자를 어디에서 인증해주느냐에 따라서 세 가지 모델로 다시 나누어진다. 세 가지 모델로 분류하여 제안하는 이유는 사용자인증을 어디에서 서비스해주느냐에 따라 각자 다른 장점과 단점을 가질 수 있기 때문이며, 이러한 관점에서 제안한 첫 번째 모델은 이동단말기에서만 병렬 사용자 인증서비스를 제공해주는 방법을 사용하고, 두 번째 모델은 서버 측에서만 병렬 사용자 인증서비스를 제공하는 방법을 사용한다. 제안한 병렬 사용자인증 방법을 사용하지 않는 측에서는 기존의 GSM 사용자 인증방식을 그대로 이용하여 기존의 구조를 변경하거나 하는 부담이 전혀 없게 새로운 모델을 구성한다. 마지막으로, 세 번째 모델은 이동단말기와 서버 측 모두에서 사용자를 인증하는 방법을 사용한다.

사용자 인증을 위해 새롭게 이용하는 화자인증 방법은 생체인식의 한 종류로서 각 사용자마다 독특한 성문(voice print)을 가지고 있다는 것을 이용하

여 정당한 사용자인지 아닌지를 인증하는 방법이다. 그래서, 화자인증 방법을 기존의 GSM 사용자 인증 방법과 새롭게 결합하여 사용할 경우, 사용자들은 단순히 말만하면 자신을 인증 받을 수 있기 때문에 사용자에게는 편리함을 제공하고, 그와 동시에 생체인식시스템의 특성상 사용자 인증을 하는데 있어서는 더 강력한 보안성을 제공하여 본 고에서 이동 단말기를 이용한 전자상거래 상에서의 사용자 인증과 부인방지를 위한 모델에 더 효율적이라는 것을 알 수 있다.

3.2 제안한 모델의 고찰

본 절에서는 새롭게 제안한 병렬 사용자인증 방법에 대한 장단점을 설명하고, 이 인증방법을 기반으로 하여 어디에서 인증처리를 하느냐에 따라 달라지게 되는 또 다른 세 개의 제안 모델에 대한 동작원리와 장단점을 살펴보면서 제안한 모델의 효율성을 언급한다.

먼저, 새롭게 제안한 사용자인증 모델은 기존의 GSM 사용자 인증과 화자 인증 부분을 병렬로 수행하고 두 개의 사용자인증 결과를 AND로 연결하기 때문에 결과가 모두 참일 경우에만 그 다음 단계를 진행하도록 모델화하였다. 두 개의 인증과정을 병렬로 수행하는 이유는 속도에 있어서 기존의 사용자 인증 방법과 화자인증 방법을 직렬로 수행하는 것보다 더 빠른 응답속도를 내기 때문이다. 이동단말기는 그 사용하는 환경이 PC와 같은 고정된 환경이 아니고 메모리나 배터리의 제한적인 특성 등을 고려해 볼 때 이동단말기 사용자들에게는 속도가 훨씬 느리고, 공중파의 특성들도 사용자에게 더 느린 속도를 제공할 수 있는 이유가 되기 때문에 될 수 있으면 이동단말기 사용자들에게 빠른 응답속도를 제공하기 위해서 병렬은 최적의 방법이다. 그래서, 새로운 사용자인증 모델은 두 개의 인증방법을 병렬로 처리하여 그 속도의 효율성을 제공하여 이동단말기 사용자들과 전반적인 속도를 향상시키는 새로운 모델의 기반을 만든다.

제안한 병렬 사용자 인증모델의 보안측면을 살펴보면, 화자인증을 사용한 장점과 AND 연산을 사용한 장점이 사용자 인증에 대한 보안성을 훨씬 강력하게 만든다는 것을 알 수 있다. 그 이유는 화자인증의 특성상 사용자의 성문(voice print)은 고유하고 독특한 것이기 때문에 제 3자가 목소리를 흉내내거나 정당한 사용자의 목소리를 녹음하여 정당한 사용자인 것처럼 흉내내는 등의 문제점을 화자인증 방법이 해결할 수 있기 때문이다. 만약, 기존의 GSM 사용자 인증이 노출되었다고 하더라도 새롭게 접목한 화자인증 방식이 유일한 비밀키의 역할을 충분히 해주기 때문에 안전하며, 화자인증의 보안성이 강력하다는 여러 보고들에 의해서도 화자인증 방법의 보안성이 기존의 다른 암호방식을 사용한 보안 방법보다 더 안전하다는 것을 알 수 있다. 그래서, 기존의 GSM 사용자인증이 노출되었다 하더라도 화자인증에서 강력한 사용자 인증을 충분히 제공해 줄 수 있기 때문에 사용자 인증이 더 강화되며, 더 강화된 사용자 인증은 전체적인 보안도 강력하게 해주는 장점을 지니게 된다.

병렬 사용자인증 모델에 대한 편리성의 측면을 살펴보면, 기존의 GSM 사용자 인증부분은 그대로 사용되고 새롭게 결합된 부분이 화자인증 부분이기 때문에 새롭게 제안한 병렬 사용자 인증모델을 사용하는 사용자는 자신이 누구인지를 인증 받기 위해서 어떤 비밀정보를 새롭게 암기한다거나 잊어버리거나 기록해야하는 등의 부담이 전혀 없이 간단히 몇 마디의 말만하면 자신을 인증 받고 서비스를 계속해서 받을 수 있기 때문에 새로운 사용자 인증부분이 추가되었다 하더라도 제안한 모델을 이용하는 사용자는 임의의 부담이 없어 굉장한 편리함을 제공한다고 할 수 있다. 기존의 사용자인증만 사용할 때는 말을 하는 부분은 없지만, 그 대신에 사용자 인증 부분이 안전하지 못한 기존의 방법을 그대로 사용하는 것보다는 몇 마디의 간단한 말을 함으로써 사용자 인증을 더 강력하게 해서 날로 증가하는 이동단말기 전자상거래 사용자들에게 사용의 편리성과 함께 강력한 보안성을 제공한다.

다음은 병렬로 수행되는 새로운 사용자 인증모델을 바탕으로 사용자 인증을 어느 쪽에서 수행하느냐에 따른 또 다른 세 가지 모델에 대해 설명한다. 먼저, 첫 번째 제안모델은 이동단말기 측에서만 제안한 병렬사용자 인증모델을 사용하여 사용자 인증을 수행한다. 이 첫 번째 모델의 장점을 살펴보면, 이동단말기 측에만 화자인증 알고리즘을 사용하기 때문에 GSM 네트워크 측인 서버 쪽에서는 기존의 데이터를 변경한다거나 새로운 서버를 구축해야 하는 등의 부담이 전혀 없다. 첫 번째 모델에서의 경제적인 부담은 더 강력한 사용자 인증을 위해 화자인증 알고리즘을 이동단말기에 심는 경제적인 부담만 존재하며, 이러한 경제적인 부담은 기존의 제품을 볼 때

다른 생체인식 제품에 비해서 월등히 저렴하다는 특성을 가지고 있기 때문에 다른 방식을 사용할 경우보다 경제적인 부담이 훨씬 적다. 속도의 측면은 병렬 사용자인증 모델에서 언급했던 것처럼, 병렬로 사용자를 인증하기 때문에 속도에 있어서도 크게 늦어지지 않고 빠른 속도를 제공할 수 있다.

두 번째 모델은 네트워크 측에서만 병렬사용자 인증모델을 사용하는 경우이다. 이 모델의 가장 큰 단점은 네트워크 측에서 사용자 인증을 해야하기 때문에 네트워크 측을 새롭게 수정하는 것이다. 이것은 첫 번째 모델에 비해 네트워크 전체를 수정하는 경제적인 부담이 존재한다. 또한, 네트워크 측에서는 서비스를 요청하는 각자의 사용자를 모두 인증할 수 있어야하기 때문에 많은 사용자들의 성문에 대한 데이터베이스를 더 추가해야 한다. 하지만, 임의의 한 사용자의 성문을 저장하기 위해 필요한 메모리는 아주 작기 때문에 많은 사용자를 위한 성문을 저장하는 메모리도 그에 따라 축소되게된다. 또한, 사용자들의 성문에 대한 데이터베이스는 다른 비밀 정보와 함께 노출이 되지 않도록 안전하게 보관하고 관리해야한다. 데이터베이스를 안전하게 보관, 관리하는 측면은 이미 기존의 방식들에서도 사용하고 있기 때문에 이에 대한 부가적인 부담은 들지 않는다. 사용자 인증방법을 서비스해줄 수 있는 처리능력 측면을 고려해보면 첫 번째 모델에서는 이동단말기의 특성상 메모리나 배터리의 환경이 제한적이지만, 서버측에서는 이러한 제한적인 환경이 거의 없기 때문에 사용자를 인증하는 처리능력이 뛰어나고 결국 전체적인 부담이 크지 않는다는 것을 알 수 있다.

마지막으로 세 번째 모델은 이동단말기와 서버 측 모두에서 병렬 사용자 인증모델을 이용하여 사용자를 인증하는 방법이다. 이 모델은 첫 번째와 두 번째 모델을 결합한 방식으로서 사용자를 인증하는 관점에서 볼 때 이동단말기와 서버 측 모두에서 사용자를 인증하기 때문에 다른 두 개의 모델에 비해 가장 강력한 사용자인증을 제공해준다. 그래서, 가장 안전한 전자상거래를 지원하는 사용자 인증에서 효율적으로 사용할 수 있다. 이 모델의 경제적인 측면을 살펴보면, 첫 번째 모델의 부담과 두 번째 모델의 부담을 합한 만큼의 부담을 가진다. 하지만, 여기서 주목해야 할 사항이 새롭게 화자인증 서비스를 구축하는데 드는 비용은 들지만, 이러한 비용은 정당한 사용자가 아닌 제 3자에 의해 결과적으로 발생할 수 있는 정당한 사용자들의 피해와 서버 측의 피해를 막아주는 것이기 때문에 이러한 면을 고려해 볼 때, 새로운 사용자 인증 방법을 구축하는데 드는 부담은 미래에 있을 피해를 미리서 막아줌으로써 더 경제적일 수 있다는 것을 고려해야 한다. 세 번째 모델은 제안한 두 개의 모델에 비해 가장 많은 경제적인 부담은 들지만, 점차 증가하는 전자상거래의 이동단말기 사용자들과 그에 따른 피해를 고려해 본다면, 가장 안전하고 강력하게 사용자를 인증해 줄 수 있는 방법이다. 또한, 사용자 인증방법이 기존의 암호알고리즘을 사용할 경우에 발생할 수 있는 새로운 비밀키를 암기한다거나, 비밀정보를 잊어버린다거나, 비밀키를 임의 장소에 기록했다가 노출되는 위험성 등과 같은 문제점이 없고 사용자의 목소리를 이용한 인증 방식으로서 사용자에게 편리함을 제공하여 부담이 되지 않고, 화자인증의 특성인 강력한 보안을 동시에 제공해 줄 수 있어 전자상거래에서 보다 강력한 보안성과 편리함을 제공하는 모델이라는 것을 알 수 있다. 속도측면을 살펴보면 병렬로 사용자를 인증하기 때문에 그 속도도 빠르다는 것을 알 수 있다.

4. 결론

본 고에서는 현재 점차 증가하고 있는 이동단말기의 전자상거래 사용자들에게 보다 안전하고 편리한 사용자 인증을 제공하기 위해서 화자인증 기술을 기존의 GSM 사용자 인증과 결합한 새로운 사용자 인증 모델을 기반으로 한 세 가지 인증서비스 모델을 제안하였다. 이 세 가지 모델은 기존의 사용자 인증보다 더 강력한 인증을 할 뿐만 아니라, 화자인증을 사용했기 때문에 사용자에게는 사용의 편리성을 제공하는 특성을 가진다. 본 고의 향후과제로는 제안한 모델의 시뮬레이션을 통한 비교분석이 수행되어야하겠고, 데이터의 암호화를 담당하는 A5 알고리즘을 개선하여 전반적으로 더 안전한 GSM 보안 모델을 구성하는 연구가 필요하겠다.

참고문헌

[1] http://www.com-world.co.kr/

[2] http://iol.ie/~kooltek/gsmhack.html

[3] http://tta.or.kr/StdInfo/jnal/jnal69/10-6.htm

[4] 박춘식, "디지털 이동통신을 위한 안전대책", 한국전자통신연구소

[5] Uyless Black, "MOBILE and WIRELESS NETWORKS", p.176-209, Prentice-Hall, 1996