情報保護學會論文誌
第18卷 第2號, 2008. 4

OTP를 활용한 UICC(Universal IC Card) 기반의 인증 메커니즘에 관한 연구*

강 수 영†, 이 임 영‡
순천향대학교 컴퓨터학부

A Study on UICC(Universal IC Card)-based Authentication Mechanism using OTP*

Soo-Young Kang†, Im-Yeong Lee‡
Division of Computer, Soonchunhyang University

요 약

IT 기술의 발전으로 유비쿼터스 환경이 구축되고 있으며, 많은 서비스의 제공 환경이 모바일 환경으로 전환되고 있다. 또한 기존에 집이나 회사 등 고정된 위치에서 제공받았던 서비스들이 모바일 단말기의 발전에 따라 이동성이 부여되어 사용자가 이동하면서도 서비스를 제공받도록 요구되고 있다. 휴대 인터넷은 모바일 단말기를 이용하여 이동하면서도 서비스를 제공받을 수 있으며, 모든 네트워크에서 인증이라는 요구 사항이 반드시 제공되어야 하듯이 휴대 인터넷에서도 UICC와 AAA 인증 서버 간에 인증이 제공될 경우에만 서비스가 제공된다. 하지만 UICC에서 AAA 인증 서버에게 초기 인증 요청을 할 때 UICC의 식별 정보가 평문으로 노출되어 모바일 단말기의 프라이버시 노출의 문제점이 제기되고 있다. 이를 보완하기 위하여 모바일 단말기에서 발생한 OTP(One-Time Password)를 이용하여 단말기의 식별 정보를 가변하게 생성하고 프라이버시를 보호할 수 있는 방안에 대하여 제안한다. 또한 OTP 프레임워크로부터의 인증을 제공함으로서 사용자에게 안전한 서비스를 제공하고 OTP 통합 인증을 구체화할 수 있는 메커니즘에 관하여 제안한다.

ABSTRACT

Ubiquitous environment is constructed by development of an IT technology, offer environment of many service changed to mobile environment. Also, existed service offered at fixed position like home or company, but according to development of mobile device, user require service as moving. Wibro can offer as user moving using mobile device. As requirement should be included authentication, in case of authentication between UICC and AAA authentication server is offered in Wibro, service is available. However, when UICC requires initial authentication to AAA authentication server, identification information of UICC expose as plaintext, so privacy infringement of mobile device occurs. Therefore, identification information of terminal generate randomly using OTP(One-Time Password) that generated in mobile terminal, and we proposed mechanism of privacy protection. Also, we proposed mechanism that offer secure service to user as offer authentication from OTP framework, and offer OTP combination authentication detailedly.

Keywords : OTP(One-Time Password), UICC(Universal IC Card)

접수일: 2008년 12월 17일; 채택일: 2008년 2월 13일

* 본 논문은 사단법인 금융보안연구원에서 주최한 제 1회 금융보안 OTP 활용 우수논문 공모전 수상작입니다.

† 주저자, bbang814@sch.ac.kr
‡ 교신저자, imylee@sch.ac.kr

Ⅰ. 서 론

최근 정보통신 기술의 발전에 따라 모든 서비스의 제공이 모바일 환경으로 전환되고 있다. 우리나라 인구 4,500만 명 중 휴대폰 가입자의 수가 4,000만 명에 육박하는 것은 모바일 환경으로의 전환을 보여주고 있다. 모바일 환경에서 서비스를 제공받기 위해서는 모바일 단말기를 소지해야 하며, 그 종류로는 휴대폰, PDA (Personal Digital Assistants), 노트북, 스마트 폰 등이 있다. 또한 모바일 환경에서는 사용자들의 정당성을 검증하기 위한 식별과 인증이 요구되고 있다. 정보통신부와 TTA 프로젝트 그룹 PG302에서는 국내 휴대 인터넷 접속과 인증에 관련되어 UICC(Universal IC Card)를 기반으로 인증을 제공하고 있다. 모바일 단말기에서 제공받을 수 있는 확장 서비스로 휴대 인터넷, 금융거래 그리고 개인 정보 관리 등이 있다. 이러한 서비스들은 사용자의 정당성이 검증된 후 서비스 제공 및 거래가 가능하기 때문에 인증이 필수 요소로 꼽히고 있다. 따라서 모바일 단말기에서 정당한 사용자가 올바른 서비스를 제공받기 위해서는 UICC 기반의 인증이 제공이 되어야 한다[5, 6].

기존의 인터넷 환경에서는 인증의 수단으로 ID와 패스워드 기술을 기반으로 인증을 제공하였다. 포털 사이트에 로그인을 할 때 ID와 패스워드를 입력하여 ID에 해당하는 패스워드를 입력한 사용자만이 서비스를 제공받을 수 있다. 하지만 고정된 패스워드는 불법적인 제 3자에게 노출되었을 때 정당한 사용자로 위장하여 서비스를 제공받거나 패스워드를 변경하여 정당한 사용자가 서비스를 제공받지 못하도록 서비스 거부 공격을 할 수 있다[1]. 또한 고정된 패스워드는 사용자가 자신이 외울 수 있는 정보, 즉 자신의 개인 정보 등을 이용하여 패스워드를 설정하기 때문에 사전 공격 및 패스워드 추측 공격이 가능할 수 있다. 이를 보완하기 위하여 일회성을 가지는 OTP에 대한 연구가 진행되고 있으며, 특히 금융 거래에 있어서 이체 한도가 5천만 원 이상인 자는 의무적으로 OTP 토큰을 발급 받아 사용하고 있다. 하지만 토큰의 휴대성이 불편하여 사용자의 모바일 단말기에서 OTP가 생성되는 mOTP(mobile OTP)에 대한 사용도 늘고 있는 추세이다.

따라서 본 논문은 UICC 기반 인증 방식에서 발생하는 단말기의 식별 정보 평문 노출의 문제점을 해결하고 모바일 단말기에서 OTP를 생성하여 OTP 프레임워크로부터 인증을 받은 후 휴대 인터넷 서비스를 제공받는 방안에 관하여 제안한다. 또한 인증 제공 객체가 AAA(Authentication, Authorization, Accounting) 인증 서버가 아닌 OTP 프레임워크로서 기존에 사용하고 있는 금융권과 마찬가지로 하나의 OTP 토큰을 발급받고 휴대 인터넷 및 금융 거래 등 많은 서비스를 사용할 수 있도록 유연성을 제공한다. 본 논문의 2장에서는 보안 위협 및 요구 사항에 대하여 기술하고 3장에서는 관련 연구, 4장에서는 2장에서 도출한 보안 위협에 안전하고 요구 사항들을 만족하는 제안 메커니즘에 대하여 기술한다. 5장에서는 각 방식을 분석하고 6장에 결론을 끝으로 논문을 마치고자 한다.

Ⅱ. 보안 위협 및 요구 사항

모바일 환경은 사용자가 모바일 단말기를 통하여 이동성에 따른 인증과 끊임없는 서비스를 제공해야 한다. 하지만 무선 통신 채널에서 발생할 수 있는 위협 요소는 점차 증가하고 있으며 이를 해결하기 위하여 아래의 요구 사항을 만족할 수 있어야 한다.

2.1. 보안 위협

사용자의 모바일 단말기에서 발생하는 OTP는 OTP 프레임워크로부터 인증을 받아야 하며, 인증을 받은 사용자만이 서비스를 제공받을 수 있다. 하지만 무선 통신 채널은 불안전한 채널로써 불법적인 제 3자의 공격이 가능하다. 다음은 모바일 환경에서 OTP 인증을 제공하는데 있어서 발생할 수 있는 보안 위협이다.

◈ 스니핑(Sniffing) : 모바일 환경에서 전송되는 값들은 불법적인 제 3자에게 노출될 수 있으며, 악의적인 제 3자가 통신 내용을 엿들을 수 있다.

◈ MITMA(Man-In-The-Middle Attack) : 불법적인 제 3자는 정당한 통신 객체들 사이에서 전송되는 값들을 가로채서 정당한 객체에게 전송함으로써 정당한 객체로 위장할 수 있고 획득한 값을 분석하여 중요 값을 획득하거나 생성하여 사용할 수 있다.

◈ 재전송 공격(Replay Attack) : 불법적인 제 3자는 정당한 통신 객체들 간에 전송되는 값들을 획득하여 정당한 객체에게 재전송함으로써 정당성을 검증받거나 중요 값을 획득하여 정당한 객체로 위장할 수 있다.

◈ 서비스 거부 공격(Denial of Service Attack) : 불법적인 제 3자가 전송되는 데이터를 위조 및 변조하여 정당한 객체가 인증 받지 못하도록 하거나 정당한 사용자에게 지속적인 서비스를 제공하지 못하게 할 수 있다.

2.2. 요구 사항

모바일 환경에서 OTP를 사용하는데 있어서 사용자의 정당성이 제공되어야 하며 전송되는 데이터의 위조 및 변조가 불가능하도록 해야 한다. 또한 OTP 사용에 있어서 입력 값이 동기화 된 값으로서 동기화를 제공해야 하며 다음의 요구 사항들을 만족해야 한다.

◈ 인증(Authentication) : 사용자의 모바일 단말기에서 발생한 OTP는 OTP 프레임워크로부터 인증을 받아야 하며 올바른 OTP를 생성한 사용자만이 정당성을 검증 받을 수 있다.

◈ 기밀성(Confidentiality) : 통신에 사용되는 비밀 값은 정당한 객체들만이 공유해야 하며 불법적인 제 3자에게 노출되지 않아야 한다.

◈ 무결성(Integrity) : 통신 데이터는 전송되는 도중 위조 및 변조되지 않아야 하며 이를 확인할 수 있어야 한다. OTP에 사용되는 해쉬 함수는 각 정당한 객체들이 동일한 해쉬 함수를 사용해야 하며 동일한 입력 값을 사용했을 경우 동일한 결과 값이 출력되어야 한다.

◈ 동기화(Synchronization) : OTP 생성 입력 값으로 사용되는 시간 및 이벤트 값은 동기화 되어 있어야 하며 모바일 환경에서 전송되는 도중 비동기화가 발생하지 않도록 해야 한다.

Ⅲ. 관련 연구 동향

OTP 기술은 동기화 여부에 따라 비동기화 방식과 동기화 방식으로 나눌 수 있다. 비동기화 방식은 서버가 일정한 개수의 패스워드를 생성하고 클라이언트와 공유한다. 그 후 인증할 때마다 패스워드를 차례대로 비교하여 인증하는 방식으로 Challenge- Response의 형식의 인증 방식이다[2, 3, 8, 10]. 동기화 방식은 입력 값(시간, 이벤트 값 등)에 따라 Time Sync 방식, Event Sync 방식, Time Event Sync 방식으로 나뉠 수 있다. 각 방식들은 일반적으로 토큰에서 사용되지만 휴대의 간편함을 제공하기 위하여 사용자의 모바일 단말기에서 발생하는 OTP도 많이 사용되고 있다. 본 장에서는 동기화 OTP 방식에 관하여 기술하고 각 방식의 장점 및 단점에 관하여 분석한다. 또한 국내 휴대 인터넷에서 사용자 인증 모듈을 탑재하여 인증을 수행하는 UICC 표준과 UICC에서 인증을 제공하기 위한 EAP-AKA (Extensible Authentication Protocol-Authentication and Key Agreement)메커니즘에 관하여 기술한다.

3.1. 동기화 OTP 인증 기술

동기화 방식의 OTP는 입력 값에 따라 Time Sync 방식, Event Sync 방식, Time Event 조합 Sync 방식으로 분류된다[14]. 본 절에서는 각 방식에 대한 설명과 장/단점을 기반으로 분석한다.

3.1.1 Time Sync

본 방식은 토큰 안에 내장되어 있는 타이머에서 생성된 시간 값과 서버의 시간을 동기화 시키고 사전에 안전하게 공유된 비밀키를 기반으로 OTP를 생성하는 방식이다. 일반적으로 정해진 시간(보통 1분)마다 OTP가 생성되며 시간을 설정하는 것은 OTP 토큰을 개발하는 업체에 따라 다르게 설정되어 있다. 불법적인 제 3자가 이전 세션의 OTP를 스니핑 했을 경우 제한된 시간(보통 1분) 안에 사용하지 못하면 그 패스워드는 폐기되고 다른 OTP가 생성되므로 기존의 고정된 패스워드에 비하여 강력한 보안을 제공하고 있다. 서버와 클라이언트 간에 발생할 수 있는 비동기 현상을 줄이기 위하여 오차 범위(보통 ±3분)를 두고 있지만 인증에 실패할 경우 다음 OTP가 생성되기까지 일정 시간을 대기해야하는 불편함을 가지고 있다.

3.1.2 Event Sync 방식

본 방식은 서버와 클라이언트 간에 동기화된 이벤트 값과 사전 안전하게 공유된 비밀키를 기반으로 OTP를 생성하는 방식이다. 이벤트 값은 토큰에 있는 버튼을 눌러 1씩 증가시키며 서버는 인증 제공 시 1씩 증가하는 방식이다. 최근에는 휴대의 간편함을 위하여 카드 OTP를 사용하며 카드에 버튼을 만들어 Event Sync 방식을 사용하고 있다. 하지만 사용자의 사용 미숙이나 타인의

실수로 버튼이 잘못 눌려질 경우가 비일비재하여 비동기에 대한 문제가 가장 큰 문제로 제시되고 있다. 본 방식도 Time Sync 방식과 마찬가지로 비동기화에 대응하기 위한 오차 범위(보통 +16회)를 두고 있지만 사용자 인증에 대한 폭이 넓어짐에 따라 불법적인 제 3자의 인증이 제공될 수 있다. 또한 오차 범위에 해당하는 OTP를 모두 생성해서 비교해야 하므로 서버의 부하량에 대하여 비효율적인 단점을 가지고 있다.

3.1.3 Time Event Sync 조합 방식

본 방식은 방식의 이름에서도 알 수 있듯이 Time Sync 방식과 Event Sync 방식의 단점을 보완하기 위하여 두 방식을 조합한 방식이다. Time Sync 방식에서 정해진 일정 시간 안에서도 인증 실패 시 대기 시간을 줄이기 위하여 이벤트를 발생시켜 OTP를 생성할 수 있는 방식이다. 입력 값으로는 동기된 시간과 이벤트 값 그리고 비밀키가 사용되며 이 값을 해쉬하여 나온 출력 값 중 6~8자리의 OTP를 추출하기 위하여 Truncation 함수를 통하여 짧은 비트수로 해쉬 값을 잘라낸다. 일반적으로 일정 시간 안에 6회의 이벤트를 발생시킬 수 있어 일정 시간 안에 6개의 OTP가 생성될 수 있어 강력한 보안 및 인증 실패 시 대기 시간을 줄여 편의성을 제공하고 있다. 하지만 시간과 이벤트 값을 모두 동기화 시키는 것이 가장 큰 문제가 되고 있으며 오차 범위로 인한 서버 부하량이 증가할 수 있다.

3.2. UICC 기반 인증 기술 - EAP-AKA 인증 메커니즘

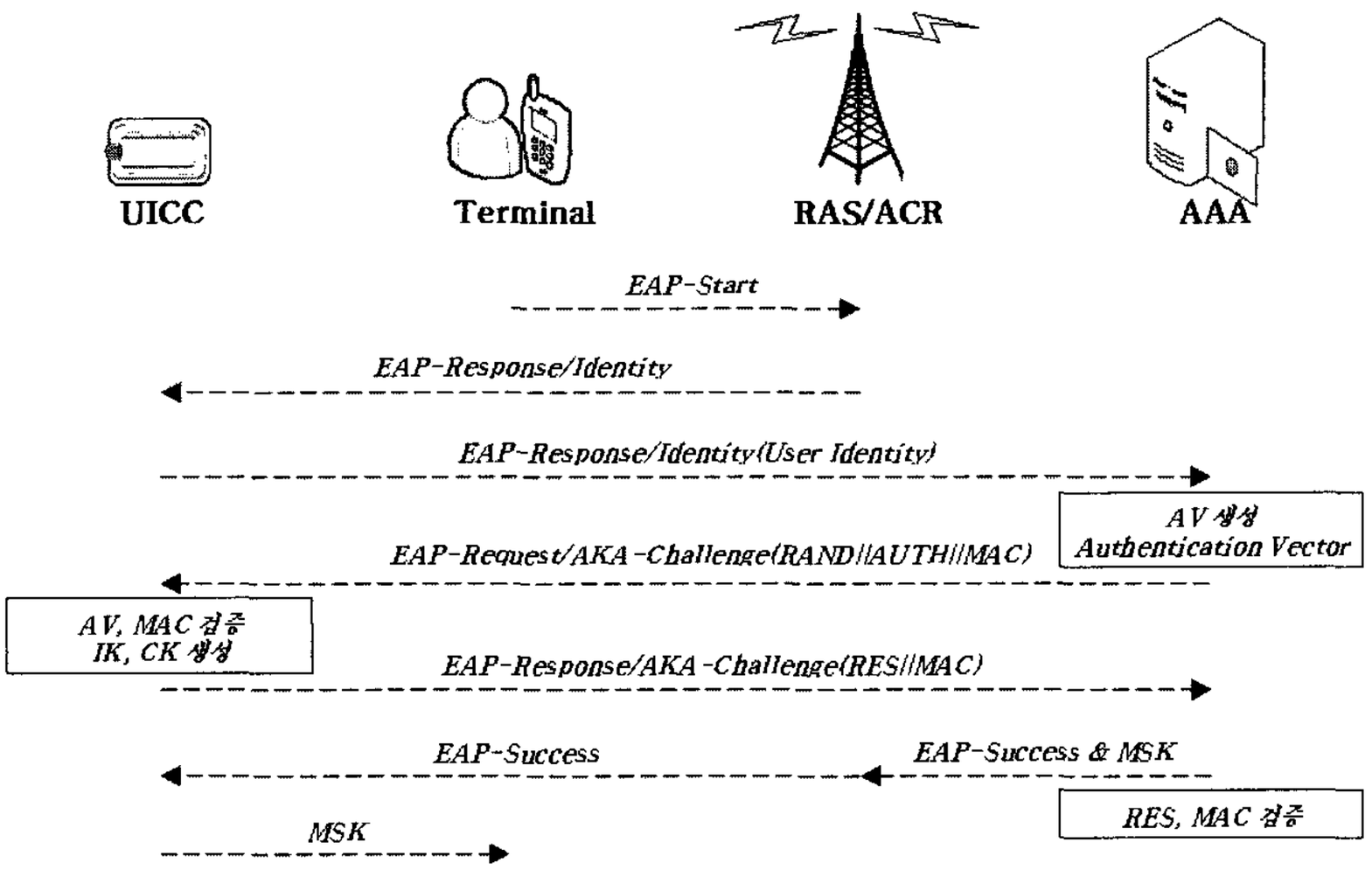
정보통신 기술의 발전으로 모바일 환경으로의 전환이 진행되고 있으며 이동성에 따른 인증 기술이 요구되고 있다. 국내는 모바일 환경의 차세대 기술인 휴대 인터넷에서 인증을 제공하기 위하여 UICC 기반의 EAP(Extensible Authentication Protocol) 인증 방식을 채택하고 AKA(Authentication and Key Agreement) 인증 메커니즘을 결합한 EAP-AKA 인증 메커니즘을 사용하고 있다[4]. 본 장에서는 EAP-AKA 메커니즘에 관하여 기술한다.

3.2.1 UICC

UICC는 휴대 인터넷의 안전한 네트워크 접속을 위한 가입자 인증과 다양한 통신 및 부가 서비스를 제공하는 다기능 스마트카드 이다. 휴대 인터넷을 지원하는 PDA, 노트북, 스마트 폰 등에 장착되어 사용자들이 안전하게 휴대 인터넷 망에 접속할 수 있도록 하며, 인증 받은 사용자가 다양한 서비스를 이용할 수 있도록 한다. UICC는 휴대 인터넷 가입자 인증 모델을 탑재한 세계 최초의 사용 카드로써 가입자 인증 모듈 탑재를 통한 WCDMA (Wideband Code Division Multiple Access) 접속 인증을 지원할 수 있다. 또한 글로벌 플랫폼인 개방형 표준을 지원하여 금융 관리, 보안 관리, 개인 정보 관리 등의 부가 서비스를 지원한다[7, 11]. UICC 관련 표준은 ISO/IEC(International Organization for Standardi zation/ International Electrotechnical Commission), ETSI (European Telecommunications Standards Institute), 3GPP(3rd Generation Partnership Project) 등 기관에서 정의되며, 키 및 인증관련 규격은 IEEE(Institute of Electrical and Electronics Engineers), IETF(Internet Engineering Task Force), TTA(Telecommunication Technology Association) 등의 표준단체에서 정의하고 있다[15].

3.2.2 UICC기반 EAP-AKA 인증 메커니즘

모바일 단말기에서 휴대 인터넷 및 서비스 제공을 위하여 UICC 기반의 메커니즘이 사용되고 있다. 휴대 인터넷에서는 인증 및 키 관리를 위하여 PKM(Privacy and Key Management) 메커니즘을 사용하고 있으며 PKM 메커니즘은 초기에 사용된 방식으로 RSA(Rivest Shamir Adleman) 기반 인증을 제공하는 PKMv1과 PKMv1의 단점을 보완하여 RSA와 EAP 기반 인증을 제공하는 PKMv2가 있다. PKMv1은 단방향 인증을 제공하고 가변적인 값이 사용되지 않아 재전송공격에 취약하여 PKMv2를 사용하고 있으며 표준 메커니즘으로 EAP-MD5, EAP-TLS, EAP-AKA 등이 사용되고 있다. 이 중 EAP-AKA는 3GPP에서 제안한 인증 메커니즘으로 GSM(Global System for Mobile Communications)와 호환성을 제공하여 세계적인 시스템으로 확장하는데 기반이 되고 있다. EAP-AKA 인증 메커니즘은 사용자의 모바일 단말기가 Identity를 인증 서버에게 전송하여 인식된 후 난수(RAND), 인증 벡터(AUTH), RES (Result Part), IK(Integrity Key), CK(Cypher Key)등을 생성하여 인증을 수행한다. EAP-AKA 인증 메커니즘



〔그림 1〕 EAP-AKA 인증 메커니즘

의 동작은 [그림 1].과 같으며 각 단계를 기술한다[15].

EAP-AKA 인증 메커니즘은 다음과 같은 단계로 동작한다.

단계 1. 사용자의 단말기는 서비스를 제공받기 위하여 기지국에 EAP 프로토콜 개시 메시지를 전송한다.

단계 2. 기지국은 EAP 프로토콜 개시 메시지에 대한 응답 메시지인 EAP-Response 메시지와 어떠한 사용자가 인증을 요청하는 것인지 판별하기 위하여 단말기의 식별 정보를 요구하는 메시지를 전송한다.

단계 3. UICC는 사용자의 식별 정보를 인증 서버에게 전송하고 인증 서버는 인증이 가능한 사용자인지 식별한다. 식별 후 사용자에 대한 인증 벡터를 생성하고 인증 벡터가 없을 경우 인증 센터로부터 새로운 인증 벡터를 검색하여 설정한다.

단계 4. 인증 서버는 보안 제공 키들을 생성하고 RAND와 AUTH를 UICC에게 전송한다.

단계 5. UICC는 RES와 보안 제공 키들을 생성하고 AUTH를 검증하여 인증 서버를 인증한다. 그리고 RES와 MAC을 인증 서버로 전송한다.

단계 6. 인증 서버는 RES와 MAC을 검증하고 MSK (MaSter Key)를 기지국으로 전송하고 기지국은 성공 여부를 UICC로 전송한다. UICC는 성공 여부 메시지를 받고 사용자의 단말기에 MSK를 저장하여 키를 안전하게 공유한다.

EAP-AKA 인증 메커니즘이 동작하는데 있어서 PKMv1에서의 일방향 인증과 재전송 공격의 취약성을 난수와 MAC 검증으로 인한 보완을 하였으나 기지국이 단말기에게 요청한 식별 정보를 평문으로 인증 서버까지 전송하여 사용자 프라이버시가 침해될 수 있다.

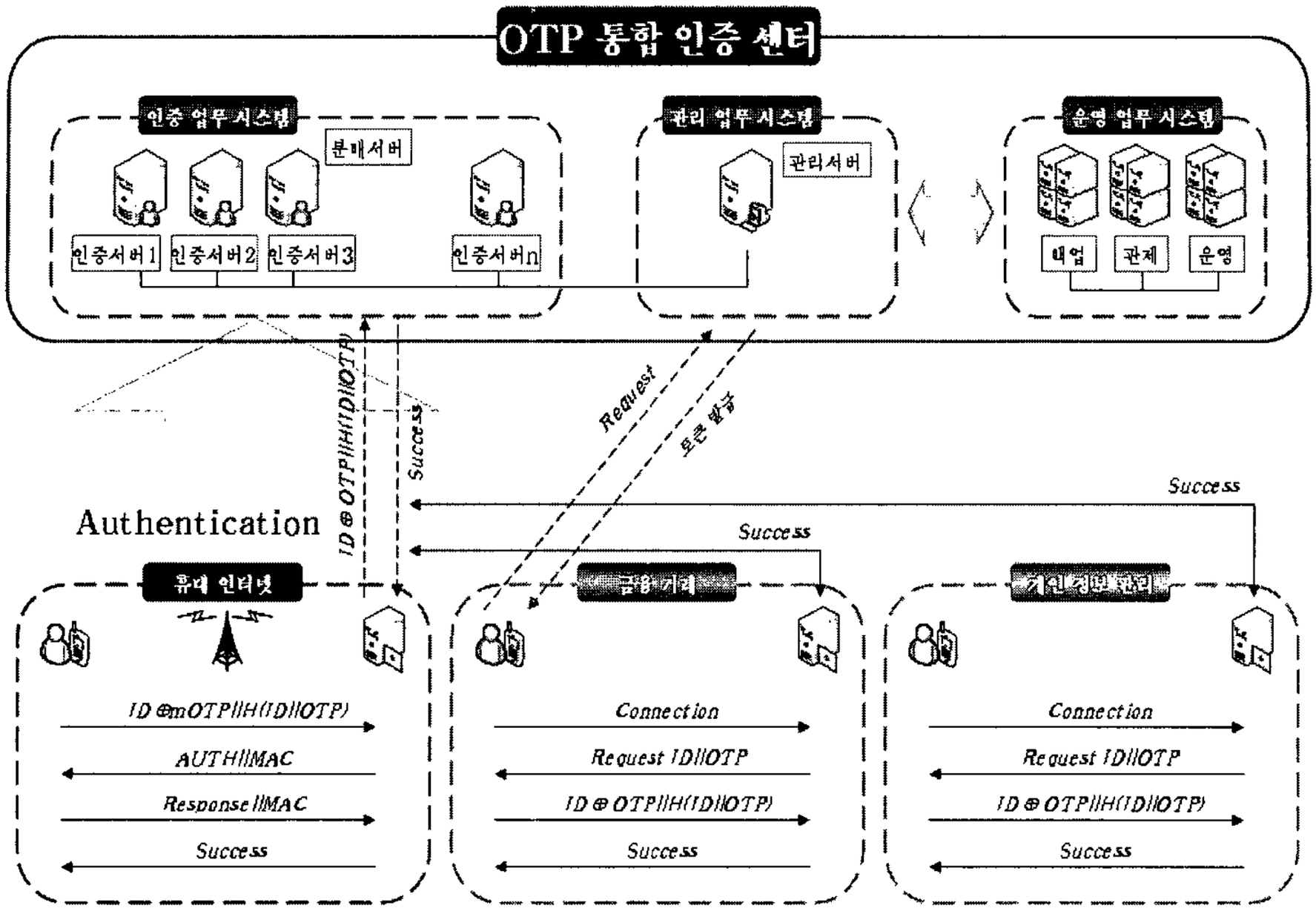
Ⅳ. UICC 기반 OTP 사용자 인증 메커니즘

본 장에서는 2장에서 도출한 보안 위협 사항에 안전할 수 있으며, 요구 사항을 만족할 수 있는 인증 메커니즘에 관하여 제안한다.

4.1. 인증 시나리오

UICC 기반의 모바일 단말기는 모바일 환경에서 인증을 제공하기 위하여 EAP-AKA 인증 메커니즘을 사용하고 있다. 하지만 사용자 식별 값이 평문으로 노출되며 휴대 인터넷 인증 과정 시 프라이버시 침해 문제가 발생하고 있다. 현재 사용되고 있는 많은 서비스들이 모바일 단말기에서 제공되는 환경으로 전화되어가는 시점에서 식별 정보 노출은 큰 문제가 되고 있다. 이러한 문제를 현재 금융 보안에 가장 많이 사용되고 있는 OTP를 이용하여 인증을 제공하고자 한다.

OTP 프레임워크에서는 현재 금융권의 OTP를 통합 관리하고 있다[13]. 공인인증서와 같이 한 은행에서 발급받은 공인인증서를 다른 은행의 인터넷 뱅킹에도 사용할 수 있도록 하고 있다. 이와 같이 OTP도 한 은행에



〔그림 2〕 UICC 기반 사용자 인증 메커니즘 구성도

서 발급받고 다른 은행에서도 사용할 수 있도록 OTP 프레임워크를 두어 통합 관리하고 있다. 이것은 하나의 서비스만을 위해 OTP 토큰을 발급받는 것이 아니라 범용성을 제공하기 위한 OTP 시스템을 구축하는 것이다.

모바일 환경에서 많은 서비스가 제공되고 있는 지금 OTP는 금융권뿐만 아니라 모바일 단말기에서 제공되는 서비스들에 적용될 수 있다. 모바일 단말기에서 제공될 수 있는 휴대 인터넷, 금융 거래, 개인 정보 관리 등 많은 서비스들은 한번 OTP S/W를 모바일 단말기에 다운로드 받아 설치하고 각각의 서비스를 제공받는데 사용할 수 있다. [그림 2].와 같이 OTP 프레임워크로부터 OTP S/W를 다운로드 받아 설치하고 금융 거래와 개인 정보 관리를 할 경우에도 모바일 단말기에서 생성되는 OTP를 통해 인증 받고 서비스를 제공받을 수 있다.

본 제안 방식은 난수를 이용하여 식별 정보를 가변적이게 생성하여 사용자 프라이버시를 보호하고 자동 생성 카운터를 입력 값으로 하는 OTP를 사용함으로써 비동기화를 완화시켜 사용자를 인증하는 방식이다. 기존의 금융권에서 사용되고 있는 OTP 통합 인증 방식과 동일하게 향후 모바일 단말기에서 제공되는 많은 서비스들을 하나의 모바일 OTP를 이용하여 통합 인증할 수 있도록 AAA 인증 서버뿐만 아니라 OTP 프레임워크로부터 인증을 제공받도록 하였다.

4.2. 시스템 계수

본 인증 메커니즘은 다음의 시스템 계수를 사용한다.

◈ *PSS(Portable Subscriber Station)* : 서비스를 이용하기 위한 사용자의 단말기

◈ *RAS(Radio Access Station)* : 단말과 통신하는 기지국

◈ *ACR(Access Control Router)* : 부가 서비스를 담당하는 제어국

◈ *AAA(Authentication, Authorization, Accounting)* : 인증, 인가, 과금을 제공하는 인증 서버

◈ *AC(Authentication Center)* : OTP를 통합 관리하는 OTP 프레임워크

◈ *ID(IDentification)* : 사용자의 고유한 식별 정보

◈ *metaID* : 사용자의 고유한 식별 정보로

◈ *AK(Authentication Key)* : PSS와 AAA 간에 안전하게 사전 공유된 인증키

◈ *SK(Secret Key)* : PSS와 AC 간에 안전하게 사전 공유된 비밀키

◈ *r(Random number)* : AAA의 R.N.G(Random Number Generator)에서 생성한 난수

◈ *ACT(Auto CounTer)* : OTP 입력 값인 이벤트 값으로 PSS와 AC 간에 동기되어 있으며 10초에 1씩

증가하여 동기화를 제공하는 자동 카운터[9, 12]

◈ *RV_1(Random Value 1)* : 난수가 포함된 가변적인 값 1로 AK⊕r

◈ *RV_2(Random Value 2)* : 난수가 포함된 가변적인 값 2로 ID⊕r

◈ *ACV_1(Auto Counter Value 1)* : ACT가 포함된 가변적인 값 1로 ID⊕ACT

◈ *ACV_2(Auto Counter Value 2)* : ACT가 포함된 가변적인 값 2로 H(ID)⊕ACT

◈ *HV_1(Hash Value 1)* : 해쉬 값 1로 H(r)

◈ *HV_2(Hash Value 2)* : 해쉬 값 2로 H(AK||r)

◈ *RES(Response)* : PSS의 최종 응답 값으로 *H(AK||ACT)*

◈ *OTP_1(OTP 1)* : PSS와 AC 간에 상호 인증을 위한 One-Time Password로 PSS에서 생성한 Event Sync 방식의 OTP 값 *H(SK||ACT||r)*

◈ *OTP_2(OTP 2)* : PSS와 AC 간에 상호 나인증을 위한 One-Time Password로 AC에서 생성한 Event Sync 방식의 OTP 값 *H(SK||ACT)*

◈ *H( )* : 충돌성이 없는 안전한 해쉬 함수(MD5, SHA-1...)

◈ ⊕ : Exclusive OR 연산

4.3. 인증 메커니즘

모바일 환경에서 UICC 기반의 사용자 단말기를 가지고 휴대 인터넷 및 금융 거래를 이용하려는 요구가 증가하고 있다. UICC 기반의 사용자 인증을 제공하기 위하여 휴대 인터넷에서는 EAP-AKA 인증 메커니즘을 채택하고 있다. 하지만 식별 정보가 평문으로 노출되기 때문에 불법적인 제 3자에 대한 프라이버시 침해가 발생할 수 있다. 본 제안 방식은 OTP 프레임워크의 구축에 따라 모바일 단말기에서 발생하는 OTP를 이용하여 단말기와 OTP 프레임워크 간의 인증을 제공하고자 한다. 사용자 인증을 제공했을 경우 휴대 인터넷, 금융 거래, 개인 정보 관리 등을 모바일 단말기에서 안전하게 서비스 받고 프라이버시 보호가 제공된다. [그림 3].에서는 제안 인증 메커니즘의 전체 흐름도를 나타내며 각 단계에 대하여 기술하겠다.

단계 1. 사용자의 단말기 PSS는 AAA 인증 서버에게 서비스 제공을 위한 인증을 요청하면 AAA는 난수 r을 생성하고 AK와 XOR 연산하여 RV_1을 생성한다. 그리고 난수의 무결성 검증을 위한 H_1을 생성하여 PSS에게 전송한다.

$$RV_1 = AK \oplus r$$
$$H_1 = H(r)$$
$$RV_1 \| H_1$$

단계 2. PSS는 RV_1에 AAA와 사전 공유된 AK를 XOR 연산하여 r'을 획득하고 r'를 해쉬한 값과 전송된 H_1을 비교하여 두 값이 일치하면 난수의 무결성을 검증한다. r이 전송되는 도중 위조 및 변조로부터 안전했을 경우, 사용자는 자신의 ID를 PSS에 입력하고 ID와 자동 생성 카운터 ACT를 XOR 연산하여 ACV_1을 생성한다. ID를 입력하는 것은 모바일 단말기를 잊어버렸을 경우 제 3자가 사용하지 못하도록 하기 위하여 단말기 사용자의 ID가 올바르게 입력되었을 경우에만 패스워드가 생성된다. 또한 ID와 r을 XOR 연산한 RV_2와 ID, SK, AC, 난수를 해쉬하여 생성한 OTP_1을 AAA에게 전송한다.

$$RV_1 \oplus AK = r'$$
$$H_1 = H(r')$$
$$ACV_1 = ID \oplus ACT$$
$$RV_2 = ID \oplus r$$
$$OTP_1 = H(ID \| SK \| ACT \| r)$$
$$ACV_1 \| RV_2 \| OTP_1$$

단계 3. AAA는 RV_2에 r을 XOR 연산하여 ID'를 획득하고 데이터베이스에 저장되어 있는 식별 정보인지 확인한다. ID'가 있을 경우 사용자를 식별하고 ACV_1에 ID'를 XOR 연산하여 AC'를 획득한다. 그리고 전송된 ACV_1, RV_2, OTP_1을 AC에게 전송한다.

$$RV_2 \oplus r = ID'$$
$$ACV_1 \oplus ID' = ACT'$$
$$ACV_1 \| RV_2 \| OTP_1$$

단계 4. AC는 인증 서버에 ACV_1과 동일한 값이 있는지 확인하고 값이 있을 경우 PSS를 인증한다. ACV_1을 통해 사용자의 ID'를 획득하고 RV_2와 XOR 연산하여 r'를 획득한다. 그리고 SK와 ACT, r을 해쉬하여 생성된 값과 OTP_1을 비교하여 두

값이 일치하면 ACT와 r의 무결성을 검증하고 SK를 통해 PSS를 인증한다. 그 후 ID를 해쉬하여 저장해 놓은 $metaID$와 ACT를 XOR 연산하여 ACV_2를 생성하고 인증을 위한 OTP_2를 $metaID$, SK와 ACT를 사용하여 생성한 뒤 AAA에게 전송한다.

$$ACV_1 = ?ACV_1$$
$$RV_2 \oplus ID' = r'$$
$$OTP_1 = ?H(ID \| SK \| ACT \| r')$$
$$ACV_2 = metaID \oplus ACT$$
$$OTP_2 = H(metaID \| SK \| ACT)$$
$$ACV_2 \| OTP_2$$

단계 5. AAA는 ACV_2에 단계 3에서 획득한 ACT'를 XOR 연산하여 $metaID'$를 획득하고 ID를 해쉬한 값과 비교한다. 두 값이 일치하면 AC를 인증하고, AK와 r을 해쉬하여 생성한 H_2를 OTP_2와 함께 PSS로 전송한다.

$$ACV_2 \oplus ACT = metaID'$$
$$metaID' = ?H(ID)$$
$$H_2 = H(AK \| r)$$
$$H_2 \| OTP_2$$

단계 6. PSS는 AAA와 공유한 AK를 r과 해쉬한 값을 생성한 뒤 H_2와 비교하여 두 값이 일치하면 AAA를 인증한다. 그리고 AC와 공유한 SK를 ACT와 해쉬한 값을 생성한 뒤 OTP_2와 비교하여 두 값이 일치하면 AC를 인증한다. AAA와 AC에 대한 인증이 완료되면 인증 응답 값을 생성하기 위하여 AK와 ACT를 해쉬하여 RES를 생성하고 그 값을 AAA에게 전송한다.

$$H_2 = ?H(AK \| r)$$
$$OTP_2 = ?H(metaID \| SK \| ACT)$$
$$RES = H(AK \| ACT)$$

단계 7. AAA는 AK와 ACT를 해쉬한 값이 RES와 동일할 경우 PSS를 인증한다.

$$RES = ?H(AK \| ACT)$$

V. UICC 기반 OTP 사용자 인증 메커니즘 분석

본 장에서는 2장에서 도출한 보안 위협과 요구 사항에 대한 만족 여부에 관하여 분석한다.

5.1. 보안 위협에 따른 분석

사용자 인증 메커니즘에 대한 안전성은 2장에서 도출한 보안 위협에 대하여 안전해야 제공될 수 있으며 모바일 환경에서의 보안 위협으로는 스니핑, MITMA, 재전송 공격, 서비스 거부 공격 등이 있다. 본 장에서는 보안 위협에 따라 제안 메커니즘을 분석한다. ([표 1]. 참조)

◈ 스니핑(Sniffing) : 모바일 환경에서 전송되는 값들이 불법적인 제 3자에게 노출되지 않기 위하여 AAA에서 생성한 r과 AC와 동기화된 ACT를 사용하여 가변적인 값을 통해 값이 노출되어도 그 값을 통하여 중요 값을 추측하거나 획득할 수 없다.

◈ MITMA(Man-In-The-Middle Attack) : 본 인증 메커니즘에서 사용되고 있는 중요 값들은 AK, SK, ID 등 정당한 객체들 간에 안전하게 사전 공유되어 있으며, 불법적인 제 3자가 통신 데이터를 획득하더라도 무결성 검증을 위한 해쉬 값을 함께 보냄으로써 위조 및 변조할 수 없다.

◈ 재전송 공격(Replay Attack) : 통신 데이터들은 사전에 공유된 인증키와 비밀키에 의존하고 있으

〔표 1〕 제안 메커니즘 분석

보안 위협	공격 방지 여부	공격 방지 요소	요구 사항	요구 사항 제공 여부	요구 사항 제공 요소
스니핑	방지	r, ACT	인증	제공	OTP1, OTP2
MITMA	방지	⊕, H( )	기밀성	제공	AK, SK
재전송공격	방지	r, ACT	무결성	제공	H( )
서비스거부	방지	ID, ⊕, H( )	동기화	제공	ACT

며 r과 ACT를 통하여 가변적인 값을 생성함으로써 재전송 공격으로부터 안전하다.

통신이 불안전하게 종료됐을 때, 불법적인 제 3자가 통신 데이터를 획득하여 정당한 객체에게 재전송을 했을 경우 AAA의 R.N.G에서는 다른 난수가 생성되며 ACT는 자동으로 증가하기 때문에 인증 받을 수 없다.

◈ 서비스 거부 공격(Denial of Service Attack) : 불법적인 제 3자는 통신 데이터 획득은 가능하지만 XOR 연산과 무결성 제공을 위한 해쉬 값이 항상 함께 전송되므로 데이터를 위조 및 변조할 수 없으며, 정당한 객체들 간에 비밀 값을 공유함으로써 정당한 객체로의 위장이 불가능하며 서비스 거부 공격에 성공할 수 없다. 또한 정당한 객체에게만 서비스를 제공하기 위하여 올바른 ID를 입력할 때에만 올바른 OTP를 생성할 수 있다.

5.2. 요구 사항에 따른 분석

모바일 환경에서 OTP를 사용하는데 있어서 휴대 인터넷 및 금융 거래 서비스, 개인 정보 관리 서비스 등을 이용하기 위해서는 정당한 사용자 검증 과정이 필수적이며 반드시 사용자에 대한 인증이 필요하다. 또한 안전하지 않은 통신 채널을 고려했을 경우 데이터의 위조 및 변조가 불가능해야 한다.

◈ 인증(Authentication) : OTP 프레임워크는 PSS가 생성한 ACV_1이 데이터베이스에 저장되어 있으면 PSS를 인식하고 SK와 AC를 기반으로 한 OTP_1을 생성하여 사용자에 대한 인증을 제공한다. 또한 RV_2를 통해 획득한 난수를 입력 값으로 사용하여 생성한 OTP_1이 정상적으로 생성되었을 경우 AAA의 정당성을 검증한다.

AAA는 AC로부터 전송된 ACV_2에 AC를 XOR 연산하여 $metaID$를 획득하고 ID를 해쉬한 값과 비교한다. 두 값이 일치하면 AC를 인증하고, PSS로부터 최종 응답 값으로 전송된 RES와 자신이 생성한 $H(AK||AC)$가 동일할 경우 PSS를 인증한다. PSS는 AAA로부터 전송된 H_2와 자신이 생성한 $H(AK||r)$을 비교하여 두 값이 일치하면 AAA를 인증하고, AC로부터 전송된 OTP_2와 자신이 생성한 $H(SK||AC)$를 비교하여 두 값이 일치하면 AC를 인증한다. 따라서 각 객체에 대한 상호 인증이 제공된다.

◈ 기밀성(Confidentiality) : PSS는 AAA와 AK를 사전 공유하고, AC와 SK를 사전 공유하며, 사용자의 ID는 AAA, AC 모두 공유하고 있다. 비밀 값과 식별 정보는 정당한 객체들 간에 공유되어 있으며 XOR 연산과 해쉬 함수를 통하여 불법적인 제 3자에게 노출되지 않도록 기밀성을 제공한다.

◈ 무결성(Integrity) : 통신 데이터는 전송되는 도중 위조 및 변조로부터 안전했는지에 대하여 검증되어야 하며 본 메커니즘에 사용된 값들은 , 뿐만 아니라 해쉬 함수를 통해 생성된 One-Time Password OTP_1과 OTP_2도 데이터의 무결성을 제공한다.

◈ 동기화(Synchronization) : 본 메커니즘에 사용된 OTP 방식은 Event Sync 방식으로 일정 시간마다 1씩 증가하는 자동 카운트 ACT를 기반으로 OTP를 생성한다. OTP 프레임워크와 동기되어 있고 조작이 필요 없이 자동 생성되므로 동기화를 제공할 수 있으나 모바일 환경에서 불안전한 세션 종료 시 비동기화가 발생할 수 있다.

◈ 효율성(Efficiency) : 입력 값으로 사용되는 ACT는 사용자의 모바일 단말기 안에서 자체 생성되는 값으로서 오차 범위는 Time Sync 방식과 동일한 ±3분을 가지며, 30초마다 1씩 증가하는 카운트를 사용하므로 1분에 최대 2개의 OTP가 생성된다. 기존의 Time Sync 방식은 1분에 1개의 OTP가 생성되며 Event Sync 방식은 최대 6번의 이벤트를 발생할 수 있기 때문에 6개의 OTP를 생성하고, 조합 방식은 1분에 1개씩 가 생성되고 6번의 이벤트를 발생할 수 있기 때문에 최대 7개의 OTP를 생성할 수 있다. 생성된 검증을 위하여 Time Sync 방식은 오차 범위 6분 동안에 1개씩 생성되는 를 검증하기 위하여 최대 6개의 OTP를 생성해야 검증이 가능하고, Event Sync 방식은 16회의 오차 범위로 인하여 최대 17개의 OTP를 생성해야 검증이 가능하다. 조합 방식은 두 방식의 도차 범위를 합하여 각 분마다 17개씩의 OTP를 ±3분 오차 범위에 따라 119개를 생성해야 검증이 가능하다. 하지만 ACT를 사용할 경우 서버에서 2개씩, ±3분의 오차 범위로 인하여 14개의 OTP만을 생성해도 검증이 가능하여 단말기의 효율성 및 서버의 효율성을 제공할 수 있다. ([표 2]. 참조)

〔표 2〕 OTP의 입력 값인 ACT 분석

	Time Sync	Event Sync	Time Event Sync	ACT(Auto-CounTer)
오차 범위	±3분	16회	±3분, 16회	±3분
1분에 생성되는 OTP 개수(Client)	1개	최대 6개	최대 7개	최대 2개
1분에 생성되는 OTP 개수(Server)	최대 7개	최대 17개	최대 7x17개 =119개	최대 7x2개 =14개
비동기화	보통	빈번	빈번	완화
효율성	높음	높음	낮음	높음

Ⅵ. 결론 및 향후 연구 방향

정보통신 기술의 발전은 모바일 환경으로의 서비스 전환을 가져오게 되었다. 이러한 환경에서 사용자에게 서비스를 제공하기 위해서는 인증이 반드시 필요하며 사용자를 인증하는 방안에 대한 연구가 활발히 진행되고 있다. 특히 이동성이 제공되는 차세대 이동통신 기술 휴대 인터넷은 UICC를 기반으로 하여 사용자를 인증하고 있으나 식별 정보가 쉽게 노출되어 프라이버시 침해가 발생할 수 있다. 따라서 본 연구에서는 사용자의 모바일 단말기에서 발생한 OTP를 이용하여 단말기의 식별 정보를 가변하게 생성함으로서 프라이버시를 보호하고, OTP 프레임워크로부터 인증을 받음으로서 사용자가 안전하게 서비스를 제공받을 수 있는 방안에 관하여 연구하였다. 본 메커니즘은 자동 생성 카운트를 입력 값으로 이용하여 비동기화를 완화 시키고 가변 식별 정보를 이용한 프라이버시 보호를 제공하는 등 많은 장점을 가지고 있다. 하지만 모바일 단말기에서 생성한 OTP를 기반으로 통합 인증이 제공되는 것이 현재 구현되지 않으며 서비스 사업자와 통신 사업자들 간의 협약 문제가 야기될 수 있다. 또한 입력 값으로 사용되는 자동 생성 카운트는 기존의 방식들에 비하여 비동기화를 완화시킬 수는 있지만 불안전한 네트워크 통신 채널에서 동기화를 제공하는 데에는 아직도 많은 문제가 발생할 것이다. 따라서 이를 보완하기 위하여 OTP의 동기화를 제공하여 사용자를 정확하게 인증할 수 있는 방안에 대하여 지속적인 연구가 필요할 것이며, 안전한 OTP 사용으로 인한 활용 분야가 확대되어야 할 것으로 사료된다.

참고문헌

[1] Anita K. Jones, “Password Authentication with Insecure Communication”, *Communications of the ACM*, 1981

[2] Chang Y.F, Chang C.C, Kuo J.Y, "A Secure One-time Password Authentication Scheme using Smart Cards without Limiting Login Times", *Operating Systems Review*, Vol. 38, No. 4, 2004

[3] Haller, N.M, "The S/KEY One-time Password System" *RFC 1760*. 1995.02

[4] Inn-yeal Oh, Hyung Joon Jeon, “The Verification of Linearizer for Wibro PAM”, *ICCSA 2006*, pp 974-981, 2006.08

[5] Jun-Cheol Jeon, Kee-Won Kim, and Kee-Young Yoo, "Non-group Cellular Automata Based One Time Password Authentication Scheme in Wireless Networks", *Verlag Berlin Heidelberg 2006*, pp. 110-116, 2006.05

[6] Kyu Ouk Lee, Jin-Ho Hahm, Young Sun Kim, "Operator's QoS Policy in WiBro Implementation", *NEW2AN 2006*, pp. 143-147, 2006.05

[7] Lee, N.Y., Chen, J.C., "Improvement of One-time Password Authentication Scheme Using Smart Cards" *IEICE Trans. Commun.* Vol. E88-B. No. 9. 2005.09

[8] Mitchell, C.J., Chen, L., "Comments on the S/KEY User Authentication Scheme", *ACM Operating Systems Review*. Vol. 30. No. 4.

[9] Soo-Young Kang, Im-Yeong Lee, Doo-Soon Park, "A Study On Improved OTP Authentication Scheme Using Synchronization Scheme", *MITA 2007*, pp. 210-213, 2007.08

[10] Yeh, T.C., Shen, H.Y., Hwang, J.J. "A Secure

One-time Password Authentication Scheme Using Smart Cards", *IEICE Trans. Commun.* Vol. E85-B. No. 11. 2002.11

[11] 강수영, 이임영, "향상된 S/Key 방식을 이용한 안전하고 효율적인 OTP 인증 방안에 관한 연구", *한국멀티미디어학회 춘계학술대회*, Vol.10, No.1, 2007.05

[12] 강수영, 이임영, "동기화 방식을 이용한 향상된 일회용 패스워드 인증 방안에 관한 연구", *한국정보보호학회 춘계학술대회* Vol.17, No.1, 2007.05

[13] 서승현, 강우진, "OTP 기술현황 및 국내 금융권 OTP 도입사례", *정보보호학회지*, 제 17권 제 3호, pp. 18-25, 2007.06

[14] 최동현, 김승주, 원동호, "일회용 패스워드(OTP: One-Time Password) 기술 분석 및 표준화 동향", *정보보호학회지*, 제 17권 제 3호, pp.12-17, 2007.06

[15] 정보보호진흥원, "와이브로 정보보호 보안 기술 해설서", 2006.08

〈著者紹介〉

강 수 영 (Soo-Young Kang) 학생회원

2006년 2월 : 순천향대학교 정보기술공학부 졸업

2006년 3월~현재 : 순천향대학교 전산학과 석사 과정

<관심분야> RFID 보안, OTP 보안

이 임 영 (Im-Yeong Lee) 종신회원

1981년 8월 : 홍익대학교 전자공학과 졸업

1986년 3월 : 오사카대학 통신공학전공 석사

1989년 3월 : 오사카대학 통신공학전공 박사

1989년 1월~1994년 2월 : 한국전자통신연구원 선임연구원

1994년 3월~현재 : 순천향대학교 컴퓨터학부 교수

<관심분야> 암호이론, 정보이론, 컴퓨터 보안