情 報 保 護 學 會 誌
第17卷 第3號, 2007. 6

유비쿼터스 환경에서의 보안 서비스 제공을 위한 OTP 적용 구조 설계

황지온*, 엄윤식*, 남승민*, 박세현**

요 약

미래 정보사회로 의미가 확대된 유비쿼터스 환경은 글로벌 컴퓨팅 환경에 기반한 유비쿼터스 인프라에서의 최적 보안 서비스 제공을 위한 지속적인 정보보호 기술이 요구되고 있다. 이와 같이 보안 서비스는 사용자에게 유비쿼터스 사회에서의 안전성, 신뢰성, 건전성을 제공하기 위한 다양한 수단을 포괄하는 개념으로, 개인의 프라이버시 침해 및 컨텍스트의 무분별한 사용이라는 문제점에 대응할 수 있어야 한다. 현재의 ID/Password를 사용한 인증 단계에서 발생되는 여러 문제들에 대한 대응 방안으로 OTP(One Time Password)가 부각되고 있다. OTP는 다양한 어플리케이션으로의 적용 및 유연한 사용자 권한 설정이 가능한 장점을 통해 다른 사용자 인증 방식에 비해 유비쿼터스 환경으로의 효율적인 적용이 가능하다. 하지만 OTP에 대한 인식의 부족 및 사용자 인증에 대한 중요성 인지 미흡으로 인하여 OTP 활용을 위한 시스템과 구조 연구가 부족하고, 제한적인 서비스에 OTP가 활용되고 있다.

본 논문에서는 사용자를 위한 보안 서비스를 제공하고자 유비쿼터스 환경에서의 보안 요소 강화를 위한 OTP의 보안 요구사항을 분석하고, OTP를 이용한 다양한 적용 방안을 고려한다. 이와 같은 연구를 통해 OTP의 효율적 관리 방안과 다양한 서비스 및 환경에서의 적용 방안 연구를 통하여, 기존 인증 방식보다 보안성이 강화된 인증 체계의 구현과 다양한 보안 서비스 제공이 가능할 것으로 기대 된다.

Ⅰ. 서 론

유비쿼터스 환경은 사용자에게 맞춤형 서비스를 제공해줌은 물론 효율적인 정보 제공이 가능하다. 그러나 사용자 프로파일과 주변 컨텍스트에 기반한 서비스 제공은 아직까지 보안 요소 기술 측면에서 개인 정보 유출, 중간자 공격 등의 위험이 존재한다.

유비쿼터스 환경은 UNI(Ubiquitous Network Infrastructure)에서 USDI(Ubiquitous Service Domain Infrastructure)을 기반으로 하는 서비스 제공 형태로 변화되고 있으며, 사용자에게 동적으로 찾아가는 서비스로 이동이 된다는 것을 의미한다. 따라서 유비쿼터스 환경에서의 사용자 정보 관리 및 사용자 권한 설정, 인증, 보안 등급 설정 등은 필수불가결한 요소이다.

최근 들어 정보 보안 솔루션의 한계성이 대두되면서 정보 중심적(Information-centric) 보안이라는 새로운 패러다임이 등장하고 있으며, 특히 사용자에 대한 인증을 기반으로 서비스와 정보를 제공해주는 방안이 중요한 쟁점으로 부각되고 있다.

이러한 보안의 중요성을 기반으로 사용자 인증을 위한 다양한 연구가 진행되어 왔다. 손쉽게 사용자가 사용 가능한 ID/Password, 패스워드를 암호화 하는 등의 다양한 방식으로의 암호화를 적용하는 Digest Authentication, 인증서를 통한 인증 방식, 생체 인증 방식 등이 연구되었다. 그러나 기존의 다양한 연구는 복잡성이 높은 사양으로 인한 확장성 제한, 사용자 신체정보에 대한 Privacy 노출, 인증절차의 복잡성에 의한 문제점이 존재한다. 이러한 문제점의 해결 방안으로써 OTP [1][2]가 제시되고 있으며, OTP는 익명성, 확장성, 휴대성의 특징으로 사용자 정보의 저장으로 인한 사용자 정보유출

* 중앙대학교 전자전기공학부 홈네트워크 연구센터
** 중앙대학교 전자전기공학부 홈네트워크 연구센터 센터장
본 연구는 정보통신부 및 정보통신연구진흥원의 대학IT연구센터(중앙대학교 홈네트워크연구센터) 지원사업의 연구결과로 수행되었음.

의 사전 방지가 보장되고 실시간 접근 제어가 가능하다. 또한, OTP는 확장성과 휴대성이 우수하여 Push Service에서 사용자에게 편의성을 제공하는 면에서 효과적인 인증의 방안으로 대두되고 있다. OTP는 Smart Card [3][4][5][6][7] 등의 응용분야에 적용시킴으로써 유비쿼터스 환경의 다양한 서비스와 도메인에서 안정된 방법으로 사용자를 인증 할 수 있는 시스템 구축이 가능하다.

따라서 본 논문에서는 유비쿼터스 서비스 환경에서의 OTP를 활용한 시스템 구조를 설계하고 서비스에 대한 적용 방안을 연구하고자 한다. 본 논문의 2장에서는 기존 연구와 OTP 적용 사례[8][9]에 대해 분석한다. 3장에서는 OTP에서의 보안 요구사항을 분석하고, OTP를 기반으로 한 구조의 설계 및 유비쿼터스 환경에서의 적용 방안을 제안한다. 마지막으로 4장에서는 결론 및 향후 연구방향을 제시한다.

Ⅱ. Related Work

기존의 단순 정보 제공이나 기본적인 인터넷 상에서의 서비스는 사용자의 인증[10]을 간단하게 함으로써 사용자의 편의성에 중점을 두었으나, 유비쿼터스 환경에서의 지식 기반, 사용자 중심 서비스에서는 사용자 및 중요한 정보를 기반으로 서비스가 제공되기 때문에 사용자의 인증은 중요한 보안 요소로 인식된다. 따라서 유비쿼터스 환경에서 적합한 사용자 인증을 구현하기 위해서는 사용자의 편의성뿐만 아니라 확장성과 안전성, 효율성이 고려되어야 한다. 따라서 기존의 연구에 대한 분석을 통해 유비쿼터스 환경에서의 적합한 인증 방식 및 구조의 구현 방안을 고려해야 한다.

사용자에게 편의성을 제공함은 물론 효율적인 인증 서비스 구현, 다양한 서비스 및 환경으로의 확장성, 차별화된 사용자 권한 설정 방식의 적용을 위한 다양한 사용자 인증 방식이 연구되고 있다. 그러나 사용자 인증을 위한 방식들은 특정 상황이나 환경에 적합하도록 구현되거나 특징적 성격에 중점이 맞춰진 상태로 구현되었기 때문에 유비쿼터스 환경으로의 적용에는 문제가 존재한다. 그리고 사용자 인증의 확장을 위해서는 특정 인증 방식을 적용하고 다양한 도메인 간의 연동을 위한 전반적인 네트워크 구조[11][12][13]의 구현이 필요하다. 기존의 연구되고 적용된 사용자 인증의 대표적인 방식[17]은 다음과 같다.

• Basic ID/PWD

HTTP 방법을 이용해 ID와 패스워드로 사용자를 인증한다. 이 인증 방법은 HTTP, HTTPS 프로토콜을 사용하는 경우 사용자가 입력한 ID와 패스워드가 네트워크를 통해 전송된다. 사용자가 사용하기에는 손쉬우나 보안적으로 가장 취약한 방법이다.

• Digest Authentication

Digest Authentication 방법을 이용해 ID와 패스워드로 사용자를 인증한다. 이 인증방법은 Basic ID/Password 인증보다 향상된 보안 서비스를 제공하지만, 패스워드가 저장될 때 반드시 패스워드 원본으로 저장돼야 하기 때문에 서버에서의 패스워드 관리에 각별한 주의가 요구된다.

• Form Based Authentication

Customized Form을 이용해 사용자를 확인한다. 사용자 ID/Password 이외의 다른 정보 등을 추가적으로 포함해 사용할 수 있다. 전달되는 정보의 암호화를 위해서는 HTTPS 프로토콜이나 기타 암호 제품을 사용할 수 있다.

• X.509 Client Certificate over SSL

HTTPS 프로토콜의 사용자 인증서 인증 프로토콜을 이용해 인증한다. 인증서의 폐기 여부 확인을 위해 CRL 검증과 OCSP 검증 방법을 사용할 수 있다.

• 생체 인식

사용자의 지문이나 홍채 등을 이용해 사용자를 인증한다. 아직은 널리 사용되고 있지 않으나 지문 인식의 경우 그 영역이 확대되고 있는 추세이다.

기존 기술에서는 정보의 중요성에 따라 보안의 강조와 사용자의 편의성에 대해 고려하였다. 그리고 일반적인 인터넷 사용에서는 주로 사용자의 편의성이 강조된 ID/Password의 사용 및 암호화된 패스워드를 사용하는 방식 등이 활용되었으며, 다양한 현금 상거래 및 금융 관련 업무에서 인증서를 활용한 방법이 적용되었다. 또한 실용화 전단계로 현재 연구로써 진행의 주체가 되고 있는 생체 인식이 존재한다. 그러나 여전히 이러한 기존 기술은 사용자 편의성 및 보안성, 확장성의 측면에서 부족한 부분이 존재한다.

사용자 인증은 방식뿐만 아니라 적용되는 서비스 및

방안도 다양하다. 기존의 인증에 비해 어플리케이션이 다양하며 유연한 사용자 권한 설정, 사용자 권한 설정에 기반한 차별적 제공, 다양한 인증 기능을 통해 최근 많은 서비스와 분야에서 제공되고 있는 OTP의 활용은 다음과 같다.

• 전용 하드웨어 OTP 토큰

OTP를 자체 생성할 수 있는 연산 기능, 암호 알고리즘 등을 내장하고 있는 OTP 토큰이다. 시스템 적용이 용이하여 많이 사용되고 있다. 그러나 사용자가 별도의 토큰을 휴대해야 하는 불편함과 토큰 구입비용에 대한 부담 등의 취약점을 안고 있다.

• 모바일 OTP

OTP 생성알고리즘이 소프트웨어 모듈로 휴대폰에 탑재된 형태를 가지고 있다. 별도의 OTP 토큰을 휴대할 필요가 없고 전용 토큰 구입 비용 절감에 대한 장점이 있다. 그러나 텔레뱅킹 서비스나 모바일 뱅킹 서비스에서는 이용할 수 없다.

• 디스플레이형 OTP 생성카드

이 OTP 토큰은 IC 카드 앞면에 디스플레이 창이 있다. 장점으로는 휴대가 간편하여 다양한 전자금융 서비스에서 이용 가능하다. 그러나 구입비용 높아서 현재 전용 VIP용 OTP 카드로 사용하고 있다.

• 보이스 OTP

IC 카드에 오디오 기능이 있는 OTP 생성 카드이며, 장점으로는 휴대성이 간편하다. 단점으로는 사용시 마이크 장치가 필요하여 시스템 환경이 복잡하고 구입비용이 높다.

기존 OTP의 생성 매체를 분류하여 각 특징에 대해 살펴봤다. 본 논문에서는 기존의 문제점을 해결하기 위해 사용자 인증/권한/서비스 측면에서 OTP 기반의 구조를 설계하고 OTP에 대한 효율적인 관리 방안, 다양한 서비스와 환경에서의 적용 방안을 제시한다.

Ⅲ. 본 론

OTP는 등록 후 다른 서비스 도메인에서 사용자의 정보를 저장하거나 볼 수 없어 사용자 정보 유출에 대한 방지가 가능하며, 익명성이 요구되는 응용 분야에서 실시간 접근 제어가 가능하다. 또한 네트워크 기반의 통합된 관리[14][15]로 편리성이 우수하고 유비쿼터스 환경에서 Push Service로 사용자에게 편의성을 제공할 수 있는 장점으로 인해 유비쿼터스 환경에서의 적용성이 높다. 따라서 본 논문에서는 유비쿼터스 환경에서의 효과적이고 확장성이 높은 사용자 인증을 위해 OTP 개념을 이용한 OTP의 요구사항의 분석을 통해 활용 모델을 제시한다.

3.1. 유비쿼터스 환경에서의 OTP 시스템 요구사항

유비쿼터스 환경에서의 네트워크 접속은 시간, 공간과 관계없이 이루어지게 된다. 이러한 개방형 네트워크에서 사용자의 비밀 정보를 안전하게 보호하며 원하는 서비스를 효율적으로 수행하기 위해서는 물리적인 보안뿐 아니라 추가적인 인증방식이 필요하다. 특히, 유비쿼터스 환경에서는 기존의 컴퓨팅 환경에 비하여 더욱 더 많은 사용자 정보를 수집하게 되고 사용자의 위치를 추적하면서 사용자를 인지하여 서비스를 제공하기 때문에 보안이 취약할 경우 기존 컴퓨팅 환경보다 더 큰 문제들을 발생시킨다.

이에 따라 유비쿼터스 환경에서의 보안 강화를 위해 OTP를 사용함에 있어 다음과 같은 기능이 요구된다.

- 상호인증을 제공해야 한다.
- 동적인 키를 사용해야 한다.
- 사용자의 이동에 따른 무선 구간 키 교환 기법을 제공해야 한다.
- 장치를 분실 및 도난당했을 경우 사용자에 대한 인증이 필요하다.
- 안전적인 협약이 필요하다.
- 편리한 사용자 접근 제어가 필요하다.
- 사용 중인 그룹웨어 등 어플리케이션과 호환을 제공하여야 한다.
- 사용자의 익명성을 보장하여야 한다.
- 사용자의 기밀성을 보장하여야 한다.

3.2. 유비쿼터스 서비스 적용을 위한 OTP 활용 모델

특정 도메인과 서비스에서 적용하는 OTP에서 유비쿼터스 환경에서의 적용으로 확대하기 위해서는 다양한 네트워크와 서비스 도메인 간의 정보 연동이 가능해야

하며, 사용자 인증 정책에 기반한 차등적인 서비스와 정보 제공이 필요하다. 따라서 유비쿼터스 환경에서 사용자 중심의 서비스 제공을 위해서는 사용자 인증에 대한 관리 방안과 다양한 도메인 간의 정보 관리, 서비스 및 사용자에 대한 정책적인 분류 방안이 적용된 전체 구조의 구현이 요구된다. 따라서 본 논문에서는 전체 구조를 설계하고 이를 기반으로 OTP를 통한 사용자 인증 및 인증 정보의 관리와 도메인 간의 연동 방안을 제안하고 유비쿼터스 환경에서의 적용 가능한 서비스를 제시하고자 한다.

3.2.1. 유비쿼터스 환경에서의 안전한 서비스 제공을 위한 OTP 기반의 구조 설계

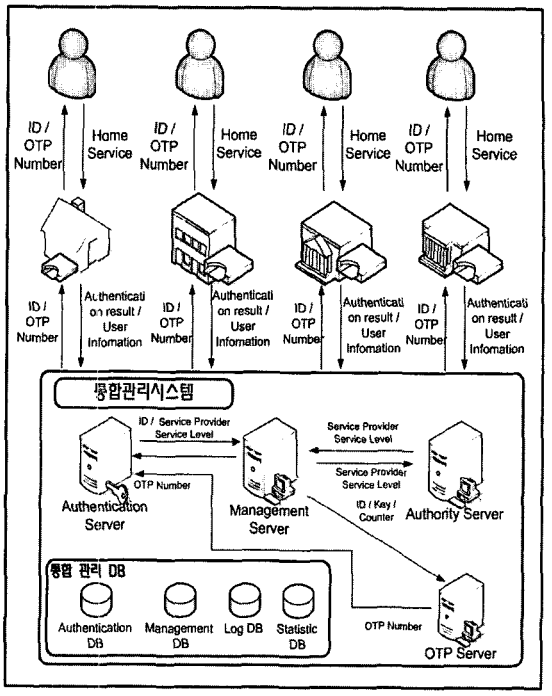
사용자는 서비스를 제공 받기 위해 서비스 제공자로부터의 인증을 필요로 하게 된다. 사용자 인증을 위해 사용자는 자신의 OTP Client에서 지문인식을 통한 인증을 받은 후 생성된 OTP Number를 서비스 제공자에게 ID와 함께 제시한다.

사용자의 ID와 OTP Number를 제공 받은 서비스 제공자는 사용자의 정보를 제공 받기 위해 검증된 통합 인증센터에 자신의 보안 등급과 제공하려는 서비스 등급을 알려주고, 사용자의 ID/OTP Number를 전송한다.

통합 인증센터에서는 Management 서버를 통해 사용자의 ID를 인지하고 Key와 Counter 값을 OTP Server에 전달하고 OTP Server를 통해 OTP Number를 생성한 후 인증 서버를 통해 인증하게 된다. 또한, 사용자와 서비스 제공자간의 상호인증을 위해 서비스 제공자의 보안 등급을 확인 후 서비스 제공자에게 사용자의 정보를 제공하게 된다.

본 논문에서 제안하고 있는 OTP 시스템 구조는 유비쿼터스 시대의 서비스에서의 인증 시 익명성의 보장을 위하여 기존에 사용하고 있던 ID와 Password에 대한 기밀성, 무결성, 네트워크 보안의 강화를 위하여 OTP를 적용하고자 한다.

유비쿼터스 서비스에서 사용자의 익명성 및 프라이버시 보호를 위하여 사용자의 요청 및 선택 후에 정보를 수집할 수 있어야 하며 위치 별 제공 서비스 통제가 가능하여야 한다. 이를 위해 사용자는 위치 별 서비스를 요청 할 때 사용자의 신상정보나 위치정보 등의 프라이버시 정보가 아닌 ID/OTP Number를 서비스 제공자에게 제공함으로써 사용자의 익명성 및 프라이버시를 보호할 수 있게 된다.



〔그림 1〕 유비쿼터스 서비스 적용을 위한 OTP 시스템 구성도

서비스 제공자는 사용자의 정보 수집을 위해 통합관리 시스템으로부터 인증을 받은 후 서비스 제공자의 Level에 따라 사용자의 정보를 제공받게 된다.

3.2.2. OTP Client

• 현재 사용되고 있는 OTP 하드웨어의 문제점

현재 여러 분야에서 사용되고 있는 OTP를 생성하는 여러 하드웨어들은 2-Factor[16] 인증 제공 방식을 사용하여(지식기반 + 소유기반) 사용자를 인증하고 있다. 이러한 현재의 OTP 하드웨어 들은 OTP의 도난에 취약점을 가지고 있다. 유비쿼터스 환경에서는 보안의 중요성이 더욱 부각됨에 따라 장치를 분실 및 도난당했을 경우에도 안전할 수 있는 새로운 인증 방안이 필요하다.

본 논문에서는 이러한 문제점을 해결할 수 있는 Biometrics를 이용한 3-Factor OTP 방식을 제안하고자 한다.

• 3-Factor OTP Card

본 논문에서 제안하는 Portable Biometric OTP Card는 카드의 지문인식 시스템을 통해 디바이스에서 사용자를 인증한 후, 그에 맞는 OTP Number를 생성하는 방식으로 Card 내에 저장되어 있는 사용자의 지문과 사

용자의 요청으로 인한 OTP 입력 시 입력되는 지문이 일치할 때만 OTP Number를 Display 하게 된다.

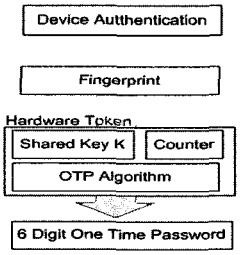
위에서 제시한 3-Factor OTP Card (지식기반 + 소유기반 + 생체정보)의 사용으로 인증절차의 복잡성을 줄이고, 3-Factor Authentication을 실현함으로써 보다 강화된 인증이 가능하게 된다.

사용자는 자신의 신체정보나 신상정보 등의 프라이버시 정보를 서비스 제공자에게 노출하지 않음으로서 익명성을 보장받게 되는 이점이 있다.

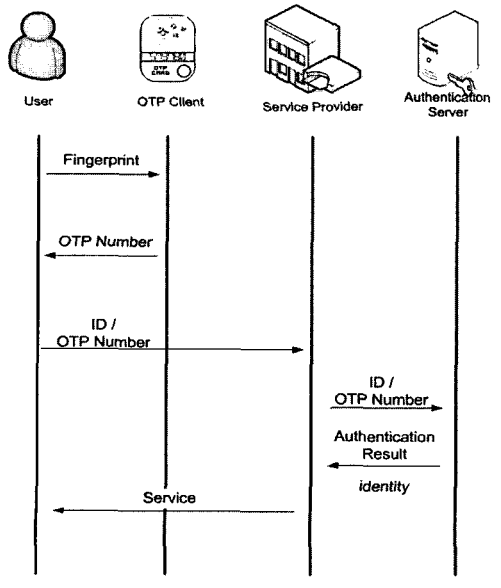
3.2.3. 차등적 등급에 따른 Profile 및 Service 구성

서비스 제공자는 OTP 통합인증 센터로부터 사용자의 정보를 제공받게 될 때, 미리 정해진 등급에 따라 차등된 사용자의 정보를 제공 받을 수 있게 된다.

이로 인해 사용자가 원하지 않는 정보의 누출을 보호



〔그림 2〕 OTP Client 동작 원리



〔그림 3〕 OTP 기반의 시스템 흐름도

〔표 1〕 차등적 등급 분류에 따른 사용자 정보 제공의 예

	조회 등급		서비스 항목
Level 0 (Guest Mode)	Personal	Name, Age, Gender	기본적인 안내 서비스
	Device	Mobile Type, Power Management Type	
Level 1 (Single Mode)	Personal	Limited information, E-Mail Address, Preferred Service Type	위치 안내 서비스 - 주차장, 상품
	Device	Defined Max Data Rate, Memory size, Computation Ability	
Level 2 (Interm ediate Mode)	Personal	Birthday, Cellular Number, Interest information	친구 찾기 서비스, 광고 서비스
	Device	Minimum latency and throughput, device address	
Level 3 (Master Mode)	Personal	Home address, Phone number, Schedule, 생활 반경	성인 인증 생활 정보 서비스
	Device	Power Status, Mac Address	

하면서 인증이 가능하게 된다.

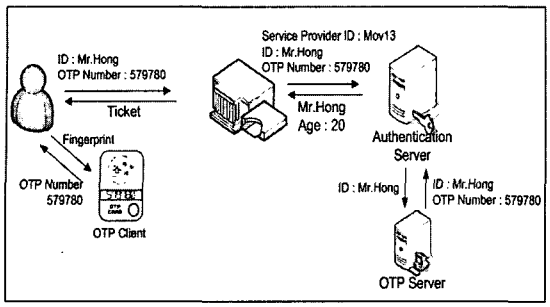
3.3. 유비쿼터스 서비스 적용 방안

본 논문에서 제안하는 OTP 기반의 구조는 사용자 인증에 따른 차등적인 서비스 및 정보 제공이 가능하다. 본 절에서는 유비쿼터스 서비스에서 앞에서 언급한 OTP 시스템 모델을 적용 방안과 서비스를 제시 한다.

3.3.1. 극장 내 사용자 성인인증 시스템

사용자가 19세 관람불가 영화를 관람하기 위해 티켓을 구매할 때 현재의 극장에서는 신분증을 제시함으로써 원하지 않는 프라이버시까지 노출되고 있다. 이러한 개인의 프라이버시 침해 및 컨텍스트의 무분별한 사용이라는 문제점에 대한 대응방안으로 본 논문에서 제시하는 OTP 시스템을 이용할 수 있다.

OTP를 적용한 시스템 방안에 대한 성인인증 시나리오는 기본적으로 3단계로 나누어져 있다. 첫 번째, OTP 카드 사용자가 영화상영관의 티켓을 예매하기 전에 영



〔그림 4〕 서비스 흐름도

화 관람 등급에 의한 사용자 인증이 필요하다. 두 번째로 사용자는 티켓 예매를 위한 인증 요청을 받으면 사용자의 ID와 인증암호를 제시하다. 인증암호는 OTP카드를 통해 확인을 한다. 세 번째, 극장 내에 있는 통합인증시스템을 통해 티켓예매소 데스크의 서비스제공자에게 인증 확인한 결과를 전송한다. 사용자는 성인인증을 위해 데스크에 ID를 제시하고 자신의 OTP Number 확인을 위해 OTP Client로부터 인증을 받는다. 이후 OTP Number를 데스크에 제시하면, 데스크에서는 OTP 통합인증 센터와 연결된 단말을 통해 사용자를 인증하고 나이 등의 필요한 정보만을 전송 받는다.

사용자는 OTP 시스템을 사용함으로 인해 서비스에 필요한 정보만을 제공할 수 있어 프라이버시의 보호를 받을 수 있게 되고, 익명성을 보장 받게 된다.

또한, 서비스 제공자는 검증된 인증센터로부터 사용자의 정보를 입력받아 보다 신뢰적인 서비스를 제공할 수 있게 된다.

3.3.2. 세미나장에서의 관계자출입시스템

세미나장과 같이 개인정보에 대한 위치정보와 출입허가증이 필요한 장소에서는 또 다른 보안 단계가 적용돼야 한다. 첫 번째, 사용자가 세미나장으로의 출입을 했을 때, 서비스 제공자는 출입 허가 여부 확인을 위해 ID와 OTP로 인증 확인을 한다. 두 번째, OTP인증 후 서비스 제공자를 통해 중앙 서버의 통합인증시스템에서 출입허가 시스템으로 출입권한(이름, 직책, 소속기관 등)을 전송 받는다. 마지막으로 통합된 출입통제 시스템에서 인증을 확인한 다음에 사용자는 세미나장의 출입허가를 받아서 출입을 한다. 사용자는 한 번의 인증 과정으로 개인정보를 공개하지 않고 출입 인증 가능하다.

지금까지 OTP 카드 적용 시나리오에 대해 살펴보았다. 유비쿼터스 서비스가 제공되는 곳에서는 사용자 인증이 필요 요소이며, OTP카드의 활용도는 매우 크다.

Ⅳ. 결 론

사용자 인증에 대해 기존의 ID/Password 방식에서의 정보 노출이나 위험성에 대한 해결 방안으로 제시가 되었던 생체 인증, OTP 등의 방식을 적용하기 위한 다양한 연구가 진행되었다. OTP는 사용상의 이점을 기반으로 여전히 존재하는 보안적 취약성에도 불구하고 금융권, 게임 등에 적용되고 있다.

그러나 여전히 OTP에 대한 인식의 부족, 사용자 인증에 대한 중요성 인지 미흡으로 OTP를 활용하기 위한 시스템과 구조 연구가 부족하여 특정 환경과 서비스에 제한적인 활용만이 이루어지고 있다.

본 논문에서는 유비쿼터스 환경에서 보안 요소의 강화를 위한 OTP의 보안 요구사항을 분석함으로써 OTP의 다양한 적용 방안을 고려하였다. 그리고 OTP의 다양한 서비스로의 확대를 위한 전체 구조와 사용자 인증 방안을 분석 및 연구했다. 이러한 구조를 기반으로 한 서비스를 제안함으로써 OTP의 활용 방안을 모색했다.

여전히 OTP의 적용을 위해서는 OTP 솔루션의 생성 방식에 대한 구체적인 협의와 구조에 기반한 네트워크 구성, 사용자 보안에 기반한 차등적 서비스의 제공을 위한 환경 구성 등의 문제점들이 산재해 있다. 그러나 유비쿼터스 환경에서의 안전한 서비스 제공을 위해서는 사용자 인증이 필요 요소이며, 이것에 대한 대안으로써의 OTP의 활용도는 매우 크다. 따라서 OTP 솔루션의 적용을 위한 구조를 기반으로 환경 구성과 OTP에 대한 효율적인 관리 방안, 다양한 서비스와 환경에서의 적용 방안을 연구함으로써 효율적인 인증 체계의 구현과 다양한 보안 서비스의 제공이 가능할 것으로 기대된다.

참고문헌

〔1〕 Akihiro SHIMIZU, "A One-Time Password Authentication Method", *Kochi University of Technology Master's thesis*, January 2003.

〔2〕 T. Tsuji, T. Kamioka, and A. Shimizu, "Simple and secure password authentication protocol" ver.2 (SAS-2)", *IEICE Technical Report, OIS2002-30*, vol.102, no.314, September 2002.

〔3〕 Narn-Yih LEE and Jung-Chic CHEN, " Impro-

vement of One-Time Password Authentication Scheme Using Smart Cards" *IEICE Trans. Commun.*, vol, E88-B, pp. 3765-3767, 2005.

[4] T.C. Yeh, H.Y. Shen, and J.J. Hwang, "A secure one-time password authentication scheme using smart cards" *IEICE Trans. Commun.*, vol. E85-B, no.11, pp.2515-2518, Nov. 2002.

[5] W.C. Ku, H.C. Tsai, and M.J. Tsaur, "Stolen-verifier attack on an efficient smartcard-based one-time password authentication scheme" *IEICE Trans. Commun.*, vol.E87-B, no.8, pp.2374-2376, Aug. 2004.

[6] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards" *IEEE Transactions on Consumer Electronics,* Vol. 46, No. 1, 2000, pp. 28-30.

[7] H. M. Sun, "An efficient remote use authentication scheme using smart cards" *IEEE Transactions on Consumer Electronics,* Vol. 46, No. 4, 2000, pp.958-961.

[8] M.H. Lin and C.C. Chang, "A secure one-time password authentication scheme with low-computation for mobile communications" *ACM SIGOPS Operating Systems Review*, vol.38, no.2, pp.76-84, April 2004.

[9] T. Tsuji and A. Shimizu, "Cryptanalysis on one-time password authentication schemes using counter value" *IEICE Trans. Commun.*, vol.E87-B, no.6, pp.2756-2759, June 2004.

[10] L. Lamport, "Password Authentication with Insecure Communication", *Communications of the ACM 24.*11 (November 1981), pp.770-772.

[11] D.L. McDonald, R.J. Atkinson, C. Metz "One-Time Passwords in Everything (OPIE): Experiences with Building and Using Strong Authentication" *In Proc. of the 5th USENIX UNIX Security Symposium,* June 1995.

[12] Vipul Goyal, Ajith Abraham, Sugata Sanyal and Sang Yong Han, "The N/R One Time Password System", *Proceedings of the International Conference on Information Technology: Coding and Computing* (ITCC'05)

[13] P. Mackenzie and R. Swaminthan, "Secure network authentication with password identification", *IEEE P1363 Working Group,* 1999.

[14] J. Archer Harris, "OPA: A One-time Password System", *Proceedings of the International Conference on Parallel Processing Workshops (ICPPW '02)*

[15] Neil Haller, Neil, and Metz, Craig, "A One-Time Password System", RFC 1938, May 1996.

[16] Matt Bishop "Computer Security: Art and Science", *Addison-Wesley Professional,* 2002.

[17] EAM·SSO 기술과 표준화 동향, 강신범

〈著者紹介〉

황 지 온 (Zion Hwang)
2003년 2월 : 중앙대학교 정보 시스템학과 졸업
2005년 2월 : 중앙대학교 전자전기공학부 석사
2005년 9월~현재 : 중앙대학교 전자전기공학부 박사과정
관심분야 : 홈네트워크, 지식기반 서비스 아키텍처 등

엄 윤 식 (Yoonsik Uhm)
2004년 2월 : 중앙대학교 전자전기공학부 졸업
2006년 2월 : 중앙대학교 전자전기공학부 석사
2006년 3월~현재 : 중앙대학교 전자전기공학부 박사과정
관심분야 : 홈네트워크 미들웨어, 지식기반 서비스 아키텍처, 홈네트워크 보안 등

남 승 민 (SeungMin Nam)
2007년 2월 : 상명대학교 컴퓨터시스템공학과 졸업
2007년 3월~현재 : 중앙대학교 전자전기공학부 석사과정
관심분야 : 홈네트워크, 홈네트워크 보안

박 세 현 (Sehyun Park)
정회원
1999년 3월~현재 : 중앙대학교 부교수
2004년 8월~현재 : 홈네트워크 연구센터 센터장
관심분야 : 홈네트워크, 유비쿼터스 컴퓨팅, 인터넷 보안 및 정책 관리 등