일회용 패스워드 기반의 스마트지갑을 활용한 출입통제 시스템

최요한*, 서희석*

요약

출입통제시스템은 기업의 자산을 보호하기 위한 가장 기본이 되는 수단이다. 오늘날 대부분의 출입통제시스템은 RFID를 기반으로 이루어져 있다. 그러나 공격자의 공격방법이 고도화되면서 RFID는 더 이상 안전하지 않다. 본 논문에서는 스마트지갑을 활용한 일회용패스워드기반의 출입통제시스템을 제안한다. 기존의 스마트지갑은 스마트폰을 활용한 지불시스템으로 사용자인증을 위해서 단말장치와 페어링이 이루어진다. 하지만 페어링 과정이 단순하여 공격자의 공격에 취약하다. 본 논문에서는 스마트지갑의 페어링 과정의 보안을 강화하기 위해서 일회용 패스워드 시스템을 적용한다.

Access control system use of the smart wallet based on One-time password

Yo-Han Choi*, Hee-Suk Seo*

ABSTRACT

Access control is the primary means for security. in today, Key makes use of RFID for the most access control. But it is not safe more using RFID access control system As attackers develop technology. In this paper, we are vulnerable to cloning using RFID access control system as a solution for the one-time password-based access control system utilizing. Using smart wallet in order to perform user authentication process, the device requires pairing of smart phones. However, security procedures are applied only to the level of security strength is low. In this paper, a smart wallet's existing in order to increase the security of the pairing process, introduced a one-time password. Take advantage of it to apply to the access control system should provide the system configuration.

Keywords : Smart wallet, access control, user authentication, one-time password. Security

* 한국기술교육대학교 컴퓨터공학부(✉ahluiyoo@kut.ac.kr)
· 제1저자(First Author) : 최요한 · 교신저자(Correspondent Author) : 서희석
· 접수일(2011년 10월 28일), 수정일(1차 : 2011년 11월 25일), 게재확정일(2011년 11월 29일)

Ⅰ. 서 론

최근 수년간 산업 스파이에 의한 기밀문서 유출 사건 사고가 급증하면서 출입통제에 대한 관심이 부쩍 높아지고 있다. 그러나 해외 여러 다른 나라들에 비해 국내의 출입통제 시스템의 보안수준은 많이 뒤처지고 보안에 대한 경각심이 IT보안이나 영상 감시에 비해 상대적으로 부족한 상황이다. 출입통제 시스템은 전체 물리적인 보안 시스템과 IT 보안 시스템에 있어 필수적인 요소이고, 기본이 되는 보안 시스템으로 전체 시스템의 보안 레벨 향상 및 리스크 매니지먼트의 효율성에 미치는 영향이 크다.

다른 여려 산업과 마찬가지로 출입통제 시스템도 IT화 되고 있으며, 시장의 요구와 IT부품의 신뢰성 향상으로 IT화의 속도가 급 가속되고 있다. 이에 더불어서 보안시장에서도 점차 각각의 시스템의 통합화 바람이 불며 다양한 통합 솔루션이 나오고 있다.[1]

본 논문에서 활용하고자 하는 스마트지갑은 최근 사용자가 늘어나고 있는 스마트폰을 지불·결제 시스템으로 모바일지갑은 근거리 내 다양한 단말들과 무선통신을 통해 사용자 모바일ID정보 및 결제 관련 정보와 같은 개인정보를 송수신 할 수 있는 다양한 지능형사용자의 편의 제공 서비스이다.

본 논문에서는 기존의 출입통제 시스템의 한계와 스마트지갑의 취약성에 대해서 알아보고 이를 극복하기 위한 일회용 패스워드기반의 스마트지갑을 활용한 출입통제 시스템을 제시한다.

Ⅱ. 관련연구

2.1 RFID

현재 출입통제 시스템으로 가장 많이 활용되고 있는 방법은 근거리무선통신을 활용하여 이루어지고 있다. 대표적으로 RFID(Radio Frequency IDentification), IC칩, Bluetooth가 있으며 최근 NFC를 활용한 출입통제 시스템이 등장하였다.

RFID는 무선 주파수를 이용한 자동인식기술이다. 몇 년 전부터 기존의 바코드 시스템을 대체하기 위한 기술로서 주목받기 시작했지만 이제는 바코드 시스템의 활용도를 뛰어넘어 물류 및 유통뿐만 아니라 지급, 결제, 환자 관리 등 다양한 분야에 활용되고 있다. RFID를 출입통제 시스템과 접목하여 보안이 필요한 기관이나 업체들에서는 출입통제를 위해 수단으로도 활용하고 있다. RFID는 카드리더의 유효한 영역 안에 카드가 들어왔을 때 카드의 데이터(ID번호)를 리더에 전달하는 방식이다. 현재 가장 흔히 출입통제에 사용되고 있는 가장 흔한 방법이다. RFID카드의 ID번호를 등록하여 출입통제에 사용할 경우 출입통제 시스템과 통신을 하기 위해서 과거에는 시리얼 통신을 사용했으며, 최근에는 TCP/IP기반 통신 방식을 이용하여 출입통제 시스템과 통신을 하고 있다.[2]

또, 이러한 RFID는 전자여권으로도 활용되어 전자여권으로 여행객들에게 편의를 제공한다. 하지만 RFID의 복제 취약성으로 전자여권이 쉽게 복제되어 범죄에 악용되기도 한다.[3]

RFID를 이용한 출입통제시스템 역시 복제된 RFID 카드를 식별할 수 없어 출입통제 시스템으로서 제 역할을 수행하지 못한다.

2.2 IC 카드

스마트카드는 컴퓨터 칩이 내장된 신용카드 크기의 장치로 접촉식과 비 접촉식이 있다. 접촉식 스마트카드는 카드와 리더를 전기적으로 연결하는 커넥트가 있고, 비 접촉식 스마트카드는 RF 주파수를 사용하며 무선통신으로 리더에서 카드로 전원을 공급한다. 또한, 메모리 전용이나 마이크로 프로세스 기반 등의 스마트카드가 존재한다.

비접촉식 스마트카드는 다양한 보안 알고리즘, 특수키 사용, 암호화 기술, 상호인증 기술들을 사용할 수

있도록 함으로써 보안성이 크게 향상될 수 있게 되었고 다양한 어플리케이션이 카드와 리더 간에 구현되게 되면서 적용 가능한 어플리케이션이 많아지고 강력해졌다.

이러한 IC카드는 발급기관이 IC카드를 개인에게 제공할 때 카드에 전자사명 값이 카드번호, 사용자 이름, 주소 등과 같이 저장되며 카드가 단말기에 삽입된 후 발생자의 공개키에 대한 CA(인증기관)와 발행자의 공개키를 사용하여 서명값들을 검점함으로써, 카드에 대한 인증하는 방식을 취하고 있다.

이러한 방식은 단지 저장된 값만을 이용하므로 IC 카드 내에서의 공개키 암호 연상이 필요없다는 장점이 있는 반면 인증할 때마다 동일한 인증 정보를 사용하여 재사용 공격(replay attack)에 취약하다는 단점이 있다.

2.3 스마트지갑

모바일 지갑은 작게는 모바일 단말용 클라이언트 소프트웨어를 의미한다. 크게는 이를 지원하기위한 서버 제품군까지 포함되어 구성되는 시스템이다. 모바일 단말에 저장, 이용되는 개인 정보를 모바일 ID[4]라 한다. 모바일 ID를 구성하는 종류는 표 1과 같다.

표 1. 모바일 ID의 구성
Table 1. Mobile ID configuration

종류	내용
오프라인 ID	주민등록번호, 신분증, 시용카드번호
온오프라인 인증수단	출입증, ID, PW, 스마트키 등
정태적 개인정보	구매기록, 이동기록, 출입기록
퍼스널 컨텍스트	사용자 위치, 시간, 주변 환경
관심정보	선호도, 관심 분야

모바일 지갑 서비스의 개념은 다음과 같은 것들이 있다.

- 모바일 ID를 무선통신을 통해 모바일 단말에 발급받아 안전하게 저장, 관리
- 모바일 ID를 온오프라인 환경의 인증, 신원 확인, 지불에 안전하고 편리하게 사용
- 위 과정에서 자체 프로파일링된 동태적 개인정보를 개인에게 최적화된 서비스를 위하여 프라이버시를 보호하며 제공

스마트 지갑은 무선통신을 통해 인증정보, ID, 지불정보와 같은 모바일 자격정보를 발급받는다. 이러한 모바일 자격정보는 모바일 지갑의 부정사용방지 기능에 의해 안전하게 유지될 수 있다. 또한, 모바일지갑을 이용해 결제, 온오프라인 ID 증명 및 기타 다양한 사용자 편의 서비스들을 수행한다. 이때 무선통신을 통해 통신이 이루어진다. 모바일지갑 사용 과정의 개인 활동은 모바일지갑 내에 프로파일링되어 축적되고, 이렇게 축적된 개인정보는 개인화 서비스에 제공될 수 있다. 개인화 서비스의 예로는 이용자기반광고, 라이프스타일미디어, 네트워크 기반 IT서비스 등이 있다.

III. 스마트지갑의 사용자 인증방법

모바일지갑은 근거리 내의 단말과 페어링 과정을 거친 뒤 서비스가 제공된다. 모바일지갑의 페어링(Device pairing)기술에는 Diffie-Hellman(DH) 프로토콜[5]을 사용한다. DH프로토콜을 사용하는 페어링에는 세션확립이 중요하다. 세션확립 과정 중 중간자 공격 위협에 대한 노출문제가 존재한다. 페어링을 통해 확립된 세션키의 무결성을 검증하기 위해 OOB(Out-Of Band)채널을 활용하는 기술들이 제안되고 있다.

3.1 이미지 비교

페어링을 통해 양 단말 사이에 확립된 세션 키의 무결성을 확인하는 가장 확실한 방법은 OOB 채널을 통해 사용자가 직접 비교확인 하는 방법이다. 하지만 사용자가 직접 세션 키의 바이너리 값을 비교 판단하기에는 그 길이가 너무 길다.

따라서 세션 키의 해시를 통해 생성된 인증코드를 OOB 채널의 이미지로 출력하여 사용자의 시각을 통해 직접 양 단말 출력 이미지 사이의 동일 여부를 비교 판단하여 공개키의 무결성을 확인하는 기술들을 제안하였다. 하지만 세션 키의 해시 이미지에 대한 second pre-image[6]공격에 취약하다.

3.2 Seeing-is-Believing

초기 OOB 채널 인증 기법을 사용하는 페어링 방법들은 사용자가 인증 코드의 진위 여부를 결정하는 UC 기반이다. 하지만 UC 기반 페어링 방법은 사용자 판단 오류비율이 안전성에 영향을 미치는 한계가 있다. 따라서 Mccune, et al.[7]이 제안한 Seeing-is-Believing(SiB) 기술은 2차원 바코드로 인코딩된 인증코드를 수신 단말의 카메라가 그 값을 읽고, 인증 코드의 진위 여부를 단말 스스로 판단하는 DC 페어링 방법을 사용하였다. 바코드로 표현되는 인증코드는 공개키에 대한 해시 값을 사용한다. 이는 역시 second pre-image 공격에 취약하다. 하지만 SiB기술은 여러 개의 바코드를 사용하는 다중 바코드 방법과 DH 공개키에 대한 해시를 사용하는 방법을 제안하였다.

3.3 비주얼 채널 페어링

Saxena, et al.는 인증코드를 SiB의 바코드 대신 LED의 점멸로 표현하는 또 다른 비주얼 채널 페어링 기술을 제안하였다. 비주얼 채널 페어링 기술은 LED의 점멸 패턴 값을 수신하기위해 SiB 기술과 마찬가지로 카메라를 필요로 한다. 하지만 비주얼 채널 페어링 기술은 LCD 디스플레이 대신 하나의 LED만을 요구하므로 SiB 기술보다 송신 단말의 하드웨어 요구 조건이 낮다.

3.4 Loud and Clear

SiB와 비주얼 채널 페어링 기술에 필요한 카메라는 모바일 기기의 필수 요소가 아니며, 장착되어 있더라도 바코드를 인식하기 위해서는 촬영에 필요한 충분한 빛이 확보 되어야 한다. 따라서 SiB나 비주얼 채널 페어링에서 사용되는 비주얼 채널 대신, Goodrich, et al.는 오디오 채널 페어링 기술 Loud and Clear(L&C) [5]을 제안하였다. SiB 기술은 인증코드를 바코드로 표현한 반면 L&C 기술은 해당 데이터를 표현하는 단어들이 포함된 일련의 문장을 음성으로 들려주는 text-to-speech기법을 사용한다. 사용자는 양 단말의 스피커를 통해 출력되는 문장의 동일성 여부를 판단하거나 한 쪽 단말의 디스플레이를 통해 출력되는 문장과 다른 쪽 단말의 스피커를 통해 출력되는 문장의 동일성을 판단한다.

3.5 BEDA

Claudio Soriente, et al.에 의해 제안된 Button-Enabled Device Association(BEDA) [5]기술은 OOB채널로써 모바일 기기의 버튼 인터페이스를 사용한다. 따라서 기존의 다른 기술보다 하드웨어 요구사항이 가장 적다. BEDA 기술은 한 쪽 단말의 LED나 진동과 같은 출력을 사용자가 다른 쪽 단말의 버튼을 통해 입력하는 방법과 또는 사용자가 양 단말의 버튼을 동시에 누르고 때는 방법으로 비밀 값을 공유하게 된다. 이와 같이 양 단말 간에 공유된 비밀 값과 MANA-3 응용 프로토콜을 사용하여 안전하게 DH 공개키 값을 교환하고 세션 키를 확립한다.

3.6 HAPADEP

기존 페어링 기술들은 인증 기술에는 OOB 채널을 사용하는데 반해 DH 키 공유[4]는 WiFi 기반의

Ad-hoc연결을 사용한다. 이때 인증과정과 별개로 Ad-hoc 설정 과정은 사용자에게 사용성 측면에서 부담으로 다가올 수 있다. 따라서 Claudio Sorinete, et al.는 L&C 기술을 확장하여 키 공유 채널과 인증 채널 모두 오디오 채널을 사용하는 Human Assisted Pure Audio Device Pairing (HAPADEP)기술을 제안하였다. HAPADEP 기술의 DH 공개키 값은 fast codec으로 인코딩되어 공개키 교환 오디오 채널을 통해 빠르게 전송되고, 공개키 인증 코드는 slow codec으로 인코딩된 후 인증 오디오 채널로 전송되어 사용자의 정확한 공개키 인증을 돕는다. HAPADEP 기술의 인증 방법은 기존 L&C 기술과 같은 text-to-speech 비교 기법과 인증코드를 음계로 매핑한 멜로디 비교 기법을 제공한다.

3.7 Shake Well Before Use

OOB 채널을 통해 사용자가 세션 키 공유 과정에 직접 개입하는 페어링 방법들이 많이 연구되어오면서, 기존 OOB 채널을 사용하는 페어링 기술들의 사용성 분석에 대한 연구들과 함께 사용성 개선을 위한 연구가 계속되었다. Mayrhofer, et al.에 의해 제안된 Shake Well Before Use 기술은 양 모바일 단말을 함께 흔들어 줌으로써 가속 센서 값을 통해 비밀 값을 공유하고 이 비밀 값과 Interlock 프로토콜을 사용하여 안전하게 DH 공개키 교환 및 세션 키를 확립한다. 단순히 양 단말을 손에 들고 흔드는 동작만을 요구하므로 기존 페어링 기술들에 비해 사용성이 뛰어나다. 하지만 이와 같은 흔들기 페어링기법은 사람의 손으로 흔들기 무리가 없을 정도의 작은 크기의 모바일 단말 사이에서만 사용이 가능한 한계가 있다.

Ⅳ. 스마트폰과 OTP를 활용한 출입 통제 시스템

현재 사용되고 있는 스마트지갑의 인증방법은 단말과 사용자 이외에 인증과정에 대한 검증을 수행하기 위한 제 3자가 필요하다. 제3자가 개입하게 되면 출입통제 수단으로써 활용도가 낮아진다. 이러한 문제점을 해결하기 위해 기존의 스마트지갑에 일회용 패스워드 시스템을 도입한다.

일회용 패스워드[7] 기반의 스마트지갑를 활용한 출입통제 시스템은 기존의 근거리무선네트워크를 이용한 출입통제 시스템과 달리 출입통제를 위한 카드 형태의 인증수단을 사용하지 않는다.

4.1 출입통제 시스템 구성 요소

제시하는 출입통제 시스템의 구성은 크게 OTP생성을 위한 스마트폰, 출입통제를 수행하는 단말, 마지막으로 사용자의 모바일ID 인증과 사용자와 단말간의 통신을 제공하기 위한 인증서버로 구성된다.

OTP를 생성하기 위한 스마트폰은 사전에 인증서버에 등록하는 과정이 필요하다. 이때에 사용자의 모바일ID와 생성된 OTP를 검증하기 위한 OTP정보를 등록하게 된다.

사용자가 스마트폰을 분실했을 때, 습득자가 사용자의 출입 인증을 불법적인 사용을 방지하기 위해서 OTP를 생성하기 위한 패스워드를 통해 한 단계 더 사용자 인증을 수행한다.

스마트폰의 OTP생성화면은 다음과 같다. OTP를 생성하기 위해서는 사용자가 사전에 사용자가 등록한 패스워드와 단말정보를 입력하게 된다.

사용자의 출입통제를 직접 수행하게 되는 단말은 사용자가 스마트폰에서 생성된 OTP값을 입력하기 위한 키패드 혹은 터치패드가 필수적인 요소이다. 또한 사용자에게 단말 정보와 인증과정에 대한 정보를 제공하기 위한 디스플레이가 필요하다.

그림 1. 스마트지갑을 이용한 OTP생성하기 이전의 화면
Fig. 1. OTP generated using a smart wallet the previous screen

그림 2. 스마트지갑 에서의 OTP생성 화면
Fig. 2. OTP in a smart wallet creation screen

단말이 사용자에게 제공하는 단말 정보는 출입통제 시스템에 등록되어 있는 단말의 고유 ID를 이용하거나 TCP/IP를 통해서 출입통제 시스템과 통신을 할 경우 단말의 IP정보를 이용할 수도 있다.

사용자와 단말간의 통신을 연결해 주는 인증서버의 경우 출입통제 시스템 내에 있는 단말의 정보를 모두 파악하고 있어야 한다. 또한 사용자의 모바일ID와 OTP정보를 가지고 있기 때문에 높은 수준의 보안이 필요하다. 출입통제 시스템과 인증 서버를 같이 운영할 경우 인증서버와 단말 간의 통신에 소요되는 시간을 최소화 할 수 있을 것이다.

4.2 사용자 인증 절차

사용자가 출입통제 단말에 스마트지갑을 이용하여 출입통제를 하기 위한 절차는 다음과 같다.

스마트지갑을 이용하여 OTP를 생성하기 위해서 단말로부터 단말ID를 제공받는다. 제공 받은 단말ID와 사용자가 사전에 설정한 OTP비밀번호를 입력하여 OTP를 생성하게 된다.

OTP생성 시 인증서버로 사용자의 모바일ID와 단말의 정보가 전달되게 되고 인증서버는 전달받은 정보를 바탕으로 단말에서 사용자가 입력한 OTP에 대한 검증을 할 수 있는 해시값을 단말에게 제공한다.

출입통제 단말은 사용자가 입력한 OTP값을 해시함수를 통해 해시값을 얻는다. 이렇게 얻은 해시값과 인증서버로부터 제공받은 해시값을 서로 비교하여 사용자의 인증을 수행한다.

사용자의 인증 절차는 <그림 3>과 같다.

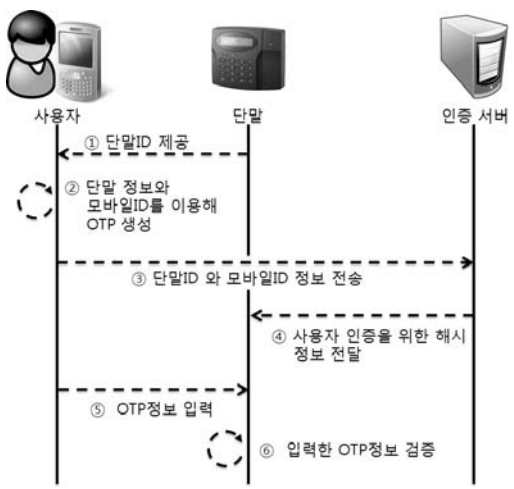

그림 3. 사용자 인증 절차
Fig. 3. User authentication process

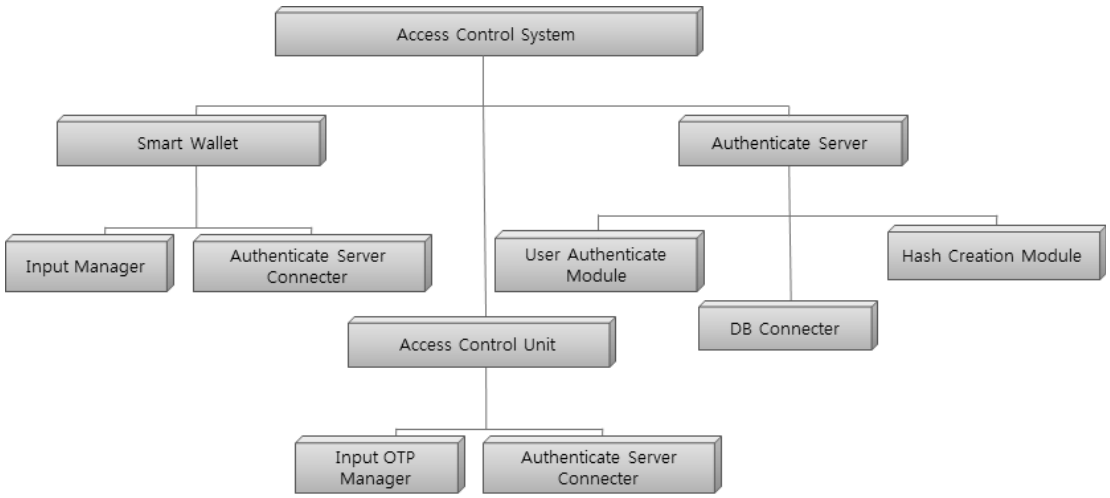

그림 4. OTP가 적용된 스마트지갑을 활용한 출입통제 시스템 구성
Fig. 4. Access control system use of the smart wallet applied on OTP

4.3 시스템 구조

OTP가 적용된 스마트지갑을 활용한 출입통제 시스템은 사용자가 출입통제 단말의 ID를 입력하고, 이를 인증서버에게 전달한다. 인증서버는 사용자로부터 받은 단말ID에 해당하는 출입통제 단말에게 사용자 인증을 위한 해시값을 전달한다. 그리고 출입통제 단말은 사용자로부터 입력받은 OTP번호에 대한 해시값을 구하고 인증서버로부터 제공받은 해시값과 비교하여 사용자 인을 수행한다. 이러한 출입통제 시스템의 구성은 <그림 4>와 같은 구조를 가진다.

OTP가 적용된 스마트지갑을 활용한 출입통제 시스템은 크게 Smart Wallet, Access control Unit과 Authenticate Server로 구성된다.

4.3.1 Smart Wallet

Smart Wallet은 출입통제 단말의 단말ID를 입력과 사용자가 사전에 설정한 OTP생성 비밀번호를 입력을 처리하기 위한 Input Manager를 갖는다.

사용자로부터 단말ID를 입력받으면 사용자의 모바일ID와 단말ID를 인증서버에 전달하기 위한 Authenticate Server Connecter로 구성된다.

4.3.2 Access control Unit

Access control Unit은 사용자 인증을 수행하는 출입통제 단말로서 사용자가 입력한 OTP를 관리하기 위한 Input OTP Manager와 인증 서버와의 통신을 위한 Authenticate Server Connecter로 구성된다.

Access control Unit에 포함되어 있는 Input Manager는 단순한 사용자의 입력을 관리하기 위한 Smart Wallet의 Input Manager와 달리 <그림 5>와 같은 구조를 가진다. 사용자로부터 입력받은 OTP를 이용해 해시값을 얻기 위한 OTP Hash Module도 포함되어 있다. 또한, OTP Hash Module을 통해서 얻은 해시값과 Authenticate Server로부터 제공받은 해시값을 비교하기 위한 Hash comparison Module을 포함하고 있다.

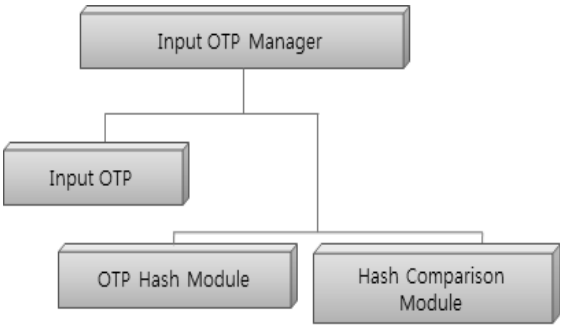

그림 5. Access control Unit의 Input Manager 구조
Fig. 5 Access control Unit of the Input Manager structure

4.3.3 Authenticate Server

Authenticate Server는 사용자가 정당한 출입 권한을 가지고 있는지 확인하는 수행 모델이다. 내부는 User Authenticate Module, DB Connecter 와 Hash Creation Module로 구성이 된다.

사용자를 인증할 수 있는 OTP정보가 네트워크를 통해 출입통제 단말에게 전송되어 비교를 수행하게 된다면 네트워크 전송 과정에서 스니핑을 통해 사용자가 입력한 패스워드를 도청 당할 경우를 대비하여 Hash Creation Module을 통해 사용자를 인증할 수 있는 정보를 일방향성 암호화를 진행한 뒤, 네트워크를 통한 전송과정 이전에 암호화 한다.

DB Connecter에서는 사용자가 정당한 출입권한을 가지고 있는지 확인하기 위해 필요한 모듈로서 DB에 저장된 출입허가자 목록에 접근하기 위해 사용되는 모듈이다.

User Authenticate Module은 DB Connecter를 통해서 DB에 접근하고 사용자가 정당한 권한을 가지고 있는지 확인하는 모듈이다. 사용자가 정당한 권한을 가지고 있다면 사용자의 OTP정보와 단말ID를 일방향성 함수를 통해서 해시 값을 구하고, 구한 해시 값을 사용자가 인증을 수행하려는 출입통제 단말에게 전달한다.

Ⅴ. 결론

본 논문에서는 일회용 패스워드 기반의 스마트지갑을 활용하여 출입인증을 하기 위한 방법을 제시하고 있다. 일회용 패스워드가 적용된ㄷ 스마트 지갑은 사용자 인증을 하기 위해서 바코드 스캐너등과 같은 추가 장비를 필요로 하지 않는다. 이러한 장점으로 인해 보안을 위해서 스캐너를 사용하지 못하는 연구소 및 정보기관의 출입인증을 위한 방법으로 활용 될 수 있다.

최근 출입인증 단말에 키패드 및 디스플레이가 포함되어 출시되고 있어, 일회용 패스워드 기반의 스마트지갑을 활용한 출입통제로 변경되기 위한 비용을 줄일 수 있을 것이다.

또한 복제에 취약한 RFID를 활용한 출입통제 시스템과 달리 OTP와 모바일ID을 활용하여 인증을 수행하기 때문에 출입통제 시스템보다 높은 수준의 보안성을 제공할 수 있다.

향후 일회용 패스워드 기반의 스마트지갑의 구성요소에서 발생할 수 있는 보안취약점을 분석하고 이를 보완하여 출입통제 시스템의 보안성을 향상 시킬 수 있는 방법에 대한 연구가 진행되어 질 것이다.

참고문헌

[1] 이철욱, "출입통제 시스템 및 스마트카드 솔루션의 현황 및 전망", 電子工學會誌 第36卷 第10號, 2009.10, page(s): 12-106

[2] 이근우, 원동호, 김승주, "RFID 활용 현황 및 보호대책", 정보보호학회지 제18권 제2호, 2008.4, page(s): 3-103

[3] 김주해, 최은영, 이동훈 "복제 공격 저항성을 갖는 전자봉인 보안 모델", 정보보호학회논문지 제17권 제5호, 2007.10, page(s): 3-153

[4] 박선영, 김주영, 송홍협, "표준 모델에서 안전한 Diffie-Hellman키 교환 프로토콜", 한국정보과학회, 정

보과학회논문지 : 정보통신, 제35권 제6호 2008.12, page(s): 465-473
[5] B.A. Forouzan, Cryptography and network security, 1th Ed., McGraw-Hill, 2008.
[6] J.M. McCune, A. Perrig, and M.K. Reiter, "Seeing-is-Believing: Using camera phones for human-verifiable authentication", IEEE Symposium on Security and Privacy, pp. 110-124, May 2005.
[7] 김기영, "일회용 패스워드를 기반으로 한 인증 시스템에 대한 고찰", 한국정보보호학회, 정보보호학회지, 제17권 제3호 2007.6, page(s): 26-31

저자소개

최요한(Yo-Han Choi)

2012년 2월 한국기술교육대학교 컴퓨터공학부 (공학학사)

2002년~현재 한국기술교육대학교 학사과정
※ 관심분야 : 악성코드, 네트워크, 모바일 보안

서희석(Hee-Suk Seo)

2000년 성균관대학교 산업공학과(학사)
2002년 성균관대학교 전기전자 및 컴퓨터공학과 (석사)
2005년 성균관대학교 전기전자 및 컴퓨터공학과 (박사)

2003년~현재 한국기술교육대학교 컴퓨터공학부 교수
※ 관심분야 : 모델링&시뮬레이션, 네트워크보안, 보안 시뮬레이션, USN