韓國컴퓨터情報學會 論文誌
第14卷 第7號, 2009. 7.

2009-14-7-3-4

다중체계 인증을 이용한 중요 시스템 보안 접근에 관한 연구

최 병 훈*, 김 상 근**, 배 제 민***

A Study of Authentication of Using Multi-factor

Choi, Byeong Hun *, Kim,Sang Geun **, Bae, Je Min ***

요 약

현재 인터넷에 대한 사고는 급증하는 추세이고, 대부분의 웹서버들이 해킹 및 스파이웨어 등의 방법을 통해 위협을 받고 있다. 많은 보안사고중 커다란 비중을 차지하고 있는 사고는 인증정보의 분실 및 인가되지 않은 내부의 사용자에 의해 이루어지고 있다. 또한 중요 정보시스템에 접근하여 작업을 하고자 할 때는 보안의 중요성이 더욱 강조되고 있다. 이에 많은 곳에서는 생체인증을 통하여 접근하는 방식을 사용하고 있다. OTP로 여러 시스템에 접근하고자 할 경우 여러 개의 디바이스를 지녀야 하며 생체인증의 경우 오인식율과 오거부율의 위험을 안고 있다. 또한 OTP를 분실하였을 경우 중요 정보시스템에 접근이 가능하여 보안 문제를 유발할 수 있다. 이에 본 연구에서는 모바일 RFID리더와 Tag, 접근자의 휴대폰을 분리하여 분실에 대한 위험을 감소시키고, 모바일 RFID리더와 Tag의 접촉으로 난수 인증키를 관리 시스템에서 발생하도록 하였다. 발생된 난수 인증키의 경우 미리 등록이 되어 있는 사용자의 휴대폰으로 전송하므로 기존의 ID, Password의 접속 방식보다 한 차원 높은 보안방식이다. 즉, 아직까지 보편화되지 않은 모바일 RFID를 중요 정보시스템에 접근하는 인증방식의 도구로 사용하는 방법에 대해 연구하였다.

Abstract

Internet accidents have skyrocketed every year. It always has been threatened by the methods such as hacking and Spyware. The majority of security accident is formed of the loss of authentication information, and the internal user who is not authorized. The importance of security is also emphasized when someone tries to do something accessing to the main information system. Accordingly, Biometrics has been used in many ways. OTP, however, must have a few devices accessing to several systems, and Biometrics involve some risk of mis-recognition rate and mis-denial rate. It also has the risk possible to access to the main information system when losing OTP. This research reduced risks about the loss as separating RFID leader for mobile, Tag and the accessor's cellular phone, and is about pseudo random validation key generated from the administration system through contact with RFID leader for mobile and Tag. As sending the key to

• 제1저자 : 최병훈
• 투고일 : 2008. 11. 18, 심사일 : 2009. 01. 29, 게재확정일 : 2009. 07. 22.
* CJ오쇼핑 ** 성결대학교 컴퓨터공학부 교수 *** 관동대학교 컴퓨터교육과 교수

user's cell phone which is already registered, security is strengthened more than existing connection methods through the ID and password. RFID for mobile not generalized to the present has been studied as a tool accessing to the main information system.

▸ Keyword : Mobile RFID, 방화벽, SSL VPN, 유비쿼터스, 보안인증

Ⅰ. 서 론

과거에 많은 기업들이 1차적 보안장비로 도입한 것이 방화벽이고, 현재는 더욱 강력한 보안장비를 도입하고 있다. U-포탈의 개념으로 각종 휴대용 장비를 이용한 중요정보 시스템(예: 영업지원시스템, 지원 Agent 시스템 등)과 최근 들어 SSL, VPN등의 보안통신장비를 통하여 기업 내의 보안을 강화하고 있다. 하지만 중요정보 시스템의 관리는 단순하게 ID와 Password를 이용한 1 Factor 인증만으로 이루어져 있다.

그러나 ID와 Password인 1Type의 보안대책으로 이루어져 있는 정보시스템은 외부 공격자로 하여금 각종 해킹 기법으로 인한 ID와 Password의 획득으로 기능을 상실하게 하며, 내부의 자원 및 정보 등이 위험에 노출되며[1], 개인정보 유출로 인한 금융사고 등과 같은 제 3의 범죄가 일어날 수 있다. 보안사고의 발생을 예방하고자 많은 기관 및 기업에서는 단순한 ID와 Password만을 사용하는 것을 지양하고 여러 가지 복합인증체계를 운영하고 있다. 이에 〈표 1〉과 같이 Type별 인증방식과 본 연구의 차이를 나타내었다.

표 1. 보안타입 및 종류
Table 1. Security Factor

인증구분	기 반	종 류
1Factor	지 식	ID, 패스워드
2Factor	소 유	스마트카드, OTP
3Factor	존 재	홍채, 지문
	행 동	음성, 서명
본 연구	지식+소유+행동	모바일 RFID

또한 정보유출 사고를 방지하고자 최근 중요정보 시스템 즉 회사의 영업비밀 및 연구정보 등을 운영하는 중요한 정보를 저장하는 시스템 접근시 개인 식별용으로 고정형 RFID등을 이용하는 곳이 점차 증가하고 있다. 이러한 고정형 RFID의 용도는 단순한 사용자인증 뿐만 아니라 사물에 대한 이력관리, 물류관리에 사용되고 있다. 이렇게 이력관리 및 물류관리에 사용되던 고정형 RFID를 보다 간편하고 사용하고자 모바일 RFID가 개발 되었다. 하지만 현제 모바일 RFID의 경우 상품정보 이력조회, 와인정보 조회 등의 기능 외에는 효율적으로 사용하는 사례가 거의 없다. 이렇듯 사용사례가 거의 없는 모바일 RFID을 이용하여 중요정보 시스템간의 인증이라는 보안적인 측면으로 연구하였다. 기존에는 ID, Password만을 이용하여 중요 정보시스템에 접속하였던 것에 비해 본 연구에서는 모바일 RFID를 통해 발생된 난수 인증키와 ID, Password의 입력으로 중요 정보시스템에 인증 받지 못한 내부 사용자들로부터 중요 정보시스템을 안전하게 보호하도록 구성하였다. 또한 OTP와 같이 하나의 디바이스를 이용한 인증도구의 분실로 비인가자의 접속을 효과적으로 대처하고자 휴대폰, 모바일 RFID리더와 Tag를 동시에 결합하여 난수 인증키를 생성하였다. 이렇게 생성된 인증키는 ID와 Password를 이용하여 중요 정보지원시스템을 안전하게 사용하도록 구성하였다.

Ⅱ. 관련 연구

2.1 보안사고 사례

최근들어 민간분야 및 공공분야의 보안사고가 잇따르고 있는데, 이는 외부로부터의 해킹보다는 내부사용자로 하여금 노출되는 경우가 많고 이로 인한 개인정보 및 기업정보의 유출은 급격히 증가하고 있다[2]. 심각한 점은 사고의 내용면에서 국가 중요정책은 물론 국가 안보와 관련된 외교 문건 및 군사기밀까지 유출될 가능성을 보여주고 있다는 점이다. 일반적으로 많은 회사의 보안사고는 회사직원 사칭 및 관련자외의 편리성을 도모하고자 ID와 Password를 공유하는 경우에 발생한다. 전문리서치기관인 영국의 BISS의 통계[3]에 따르면 보안사고의 원인은 보안솔루션이 도입되었음에도 불구하고 사용자의 보안인식 부족에서 발생한다고 지적하고 있다. 또한 보안사고의 원인 중 하나인 비인가자의 접근이다. 이러한 불법적인 사용자에 대한 접근이 강화되고 있다.

2.2 사용자 접근제어

인증정보의 유출로 인한 불법적인 접근이 나타날 경우 보안에 커다란 문제가 발생하므로 중요 정보시스템에 대해서는 사용자 접근제어기능이 요구된다. 특히 병원등과 같이 개인정보 및 기업의 중요한 데이터를 접근하는 곳에서는 불필요하거나 인가되지 않은 사용자의 접근에 대해 인증 및 제어의 중요성이 증가된다. 이에 중요한 정보를 다루는 곳의 정보시스템에는 사용자의 접근제어가 강화되는 추세이다. 이러한 사용자 접근을 통제하고자 ID, Password인증보다 강력한 사용자 인증도구를 사용하고 있다.

2.3 사용자 인증도구

중요 정보시스템의 접근에 있어 사용자 인증과정은 반드시 필요하다. 현재는 단순한 Password와 ID만을 사용한 1단계적인 인증을 대다수 사용하고 있으며 1단계 인증보다 강력한 인증이 필요한 경우에만 OTP 및 인증서등을 이용한 2단계적인 인증을 사용하고 있다. 또한 생체인증과 같은 3단계 인증을 사용하는 경우도 있으나 오인식율과 오거부율이 발생하여 중요정보 시스템의 접근에 사용하기보다는 중요 정보시스템이 보관되어 있는 장소 등과 같이 물리적 보안이 필요한 곳에서만 제한적으로 사용하고 있다. 이러한 인증도구에 대해 Ohkubo는 두개의 해시 체인을 사용하여 사용자의 프라이버시를 보호하는 기법을 제안하였으며[4], Henrici은 일 방향 해시 함수를 사용하여 추적될 수 있는 Tag의 ID를 변화시키는 기법을 제안하였다[5]. 그 외에도 중요정보시스템의 인증 무력화에 대한 DOS공격과 같은 특정 공격과 사용자의 프라이버시를 보호하는 안전한 기법들도 제안되었다[6][7]. 이러한 중요정보시스템 및 프라이버시를 보호하고자 모바일 RFID를 사용하였다.

2.4 모바일 RFID 기술

모바일 RFID의 경우 인식률이나 데이터 저장능력에 있어 여타 다른 매체에 비해 탁월하다. 또한 다른 인식 객체와 비교할 때 RFID기술은 현재 사용 중인 바코드에 비해 인식 속도가 빠르고, 바코드는 인식거리가 최대 50Cm인데 비해 RFID는 최대 27m까지 확장이 가능하며, 금속을 제외한 장애물 투과도 가능하다는 특징을 가지고 있다. 따라서 모바일 기술과 RFID를 이용하게 되면 바코드의 입지는 더욱더 좁아질 것이다[8][9]. 앞으로 모바일 RFID 리더기의 경우 RFID리더기가 휴대폰마다 내장되어 있으므로 동일 태그에 접속하는 리더기의 존재 확률이 가변적으로 변하게 되며, 반면에 태그는 정보를 제공하려는 위치에 고정되어 있는 경우(예; 미술관, 버스 정류장, 영화관 등)에 사용이 많아질 것이다[10].

III. 접근제어에 대한 프로토콜 설계

3.1 프로토콜 구성방법

본 논문에서 제안된 사용자 인증시스템은 모바일 RFID시스템과 기존의 보안장비를 연동하기 위하여 이동통신망을 이용하였다. <그림 1>의 경우 고정형 물류센터에서 사용되고 있는 RFID의 이용방법과 미술관에서 사용되고 있는 모바일 RFID를 이용하는 예를 나타내고 있다.

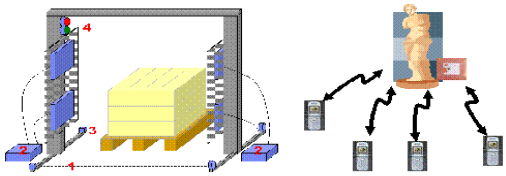

그림 1. 고정형 RFID와 모바일 RFID
Fig. 1. Fixed RFID and Mobile RFID

모바일 RFID를 통하여 인식된 Tag ID는 이동통신망을 통하여 난수 인증키 생성서버로 전송하였다. 이때 전송된 프로토콜은 http를 이용하였고 생성된 난수 인증키는 미리 등록된 사용자의 휴대폰으로 SMS를 통하여 전송한다. <그림 2>는 난수 인증번호를 받고자 하는 사용자가 입력단계부터 중요정보 시스템의 접근까지의 단계를 나타낸 전체 연계도이다.

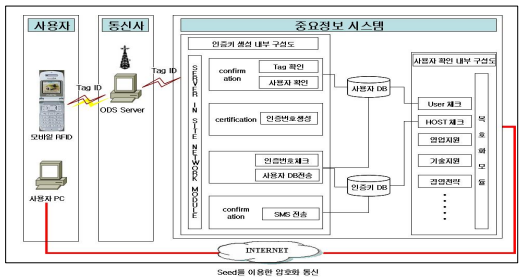

그림 2. 보안인증을 위한 시스템 구성도
Fig. 2. System configuration for Security authentication

3.2 주요 구성요소

1) 모바일 RFID 시스템

모바일 RFID는 착탈식으로 휴대폰을 리더기로 사용하였다. 휴대성이 편리하며 휴대형 리더기는 고정형 리더기가 존재하지 않는 특화된 지역에서 태그를 인식하는데 사용하게 된다. 〈그림 3〉은 본 연구에서 사용한 모바일 RFID 시스템으로 모바일 RFID 리더와 Tag, 휴대폰 등이 함께 존재해야 중요 정보 시스템에 접근이 가능하다.

그림 3. 모바일 RFID
Fig. 3. Mobile RFID

Tag의 경우 부착형으로 연구하였으나, 본 연구에서는 사원증 등으로 제작된 Tag를 사용하여 또 다른 개인 식별기능을 부여할 수 있도록 하였다. 즉, 모바일 RFID와 Tag가 접속하였을 경우 이동통신사는 난수 인증키 생성모듈에게 Tag ID만 전송시킨다.

2) 난수 인증키 생성모듈

모바일 RFID에서 보내온 Tag의 ID 및 관련정보 등은 이동통신사로 전송되며 이동통신사는 단순히 Tag ID를 중요정보시스템과 함께 위치하고 있는 인증키 생성시스템으로 전송한다. 난수 인증키의 중복 발생을 방지하기 위한 고유한 번호는 Tag ID, 휴대폰 번호, 휴대폰의 인증번호, 그리고 접속날짜 및 시간을 1/100초 단위 나누어 조합하여 난수 인증키를 발생하였다. Tag와 리더기를 접속한 시간을 1/100 형태로 전환하여 생성된 인증키는 동일한 시간대에 발생된 인증키의 중복여부를 DB에서 확인한 후 저장되며, 한번 사용된 인증키는 Host 체크모듈에서 사용자인증 후 삭제하므로 중복이 이루어지지 않는다.

3) SMS 전송모듈

사용자인증 모듈에서 생성된 고유한 난수 인증키를 미리 DB에 등록되어 있는 인가자의 휴대폰 및 PDA폰으로 전송하는 기능을 제공한다. SMS 전송모듈은 Tag ID를 기본 키로 보유하고 있는 Table에 입력하였다. 개인정보가 저장되어 있는 인사 DB에 사용자의 Tag ID 및 휴대폰의 인증번호, 휴대폰 번호 등을 비교하여 동일한 경우 사용자의 인사정보에 입력된 휴대폰 번호로 생성된 난수 인증키를 발송한다.

4) Host 체크모듈

모바일 RFID를 통하여 생성된 난수 인증키는 사용자의 SMS로 전송함과 동시에 인증 DB Table에 기록한다. 사용자로 하여금 중요정보 시스템에 접속과 동시에 인증키 값은 인증 DB에서 삭제하여 다른 위치에서의 동시 이중 로그인 하는 것을 원천적으로 차단한다. 〈그림 4〉와 같이 HOST 체크모듈을 통해 난수 인증키의 값이 다를 경우 로그인이 불가능하다.

그림 4. Host 체크를 위한 체크모듈
Fig 4. Check module for Host check

Ⅳ. 제안 프로토콜

사용자가 웹으로 중요 정보시스템에 접속을 시도하면 접속이 인가된 사용자의 인증여부는 모바일 RFID 리더기를 노트북 및 사원증으로 제작되어 있는 Tag와의 접촉을 시도한다. 모바일 RFID리더기로부터 인식된 Tag ID 및 휴대폰의 인증번호, 휴대폰번호는 이동통신망을 통하여 이동통신사로 전송된다. 이는 이동통신망을 통하여 장소 및 시간에 구애받지 않고 언제든지 사용가능하도록 하였다. 이동통신망을 통하여 전송된 Tag ID 및 휴대폰의 인증번호, 휴대폰번호는 이동통신

사와 규정된 난수 인증키 생성서버로 전송된다. 전송된 Tag ID 및 휴대폰의 인증번호, 휴대폰번호의 값은 난수 인증키 모듈을 통하여 난수 인증키가 생성되고, 생성된 인증키는 다시 등록된 사용자의 휴대폰으로 SMS를 통해 전송된다. 인증키를 전송받은 사용자는 ID, Password와 SMS를 통하여 전송받은 인증키로 접속을 시도한다. 이때 PC와 중요 정보시스템 사이에는 Seed 알고리즘과 개인키 기반인 대칭형 암호키 기법인 3DES를 이용하여 접속한다.접속된 웹 브라우저를 통하여 입력된 ID, Password, 인증키 정보를 암호화하여 중요 정보시스템으로 전송한다. 또한 접속의 시도와 접속여부가 DB화되어 내부의 사용자로 하여금 불필요한 접속에 관련된 추적이 가능하므로 보안에 더욱 강화하였다. 〈그림 5〉는 난수 인증키를 통한 접근절차를 나타낸다.

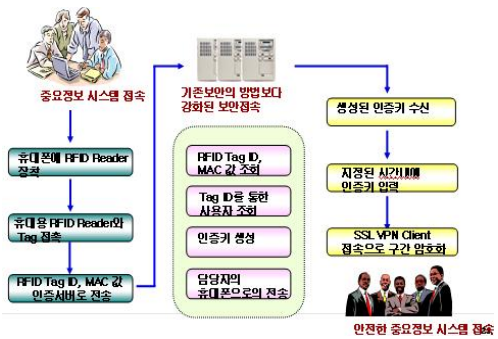

그림 5. 난수 인증키를 통한 접근절차
Fig 5. Process by Random-Number Authentication key

4.1 접속단계

접속단계에서 사용자는 모바일 RFID와 사원증으로 제작된 Tag를 접속하는 단계를 수행한다. 이때 Tag ID를 인식한 모바일 기기는 이동통신사에 Tag ID만을 전송한다. Tag ID를 전송받은 이동통신사는 중요 정보시스템 내에 설치되어 있는 Server in Site Network Module로 http프로토콜을 이용하여 Tag ID를 전송하는 단계를 수행한다.

4.2 Tag ID 확인단계

중요 정보시스템에서 전송받은 Tag ID는 사용자 확인모듈을 통하여 사용자 DB에 등록되어 있는 Tag ID인지 여부를 확인하는 단계를 실시한다. 등록되어 있지 않은 미인가 Tag ID의 경우 인증번호를 생성하는 난수 인증키 생성모듈로 전송되지 않는다.

1단계: Tag ID가 등록이 되어 있는지 Tag ID를 기본 키로 확인한다.

2단계: Tag ID가 존재하면 Tag ID로 등록되어 있는 사용자가 접속이 인가된 사용자인지 확인 후 필수필드인 휴대폰 번호의 여부를 확인한다.

4.3 난수 인증키 생성단계

난수 인증키를 생성하고 난수 인증키의 중복여부를 확인한 후 인증키를 SMS 전송할 수 있도록 DB에 저장한다.

1단계: Tag ID 및 사용자 확인을 마친 Tag ID는 난수 인증번호를 생성한다. 이때 난수 인증키를 생성하는 방식으로 사원번호 및 Tag ID, 현재시간을 1/100으로 환산하여 생성한다.

2단계: 생성된 난수 인증키는 중복되어 저장되어 있는지 사용자 DB 및 인증키 DB에서 중복여부를 확인한다. 중복여부가 확인되어 중복이 없을 경우 인증키 DB와 사용자 DB에 저장한다.

4.4 SMS 전송 및 HOST체크 단계

저장된 난수 인증키의 경우 SMS발송을 위해 인증키DB를 확인하며 인증키 DB에 난수 인증키가 입력됨과 동시에 사용자 DB에 저장되어 있는 사용자의 휴대폰으로 전송된다.

4.5 중요 시스템 접속단계

사용자가 난수 인증키로 중요 정보시스템에 접속을 시도할 때 Password와 인증키의 경우 Seed알고리즘을 이용한 암호화통신을 수행한다. 이때 암호화 모듈이 설치되지 않았거나 일정 접속시간이 초과하게 되면 생성된 난수 인증키는 사용자 DB와 인증키 DB에서 삭제된다. 또한 인가된 사용자가 중요 정보시스템에 접속하였을 때 실시간으로 사용자 DB에서 난수 인증키는 삭제되어 중복사용 위험성을 낮추었다.

V. 적용사례 및 분석

본 논문에서 연구된 사례는 다음과 같다. 중요 정보시스템에 접근을 하고자 하는 사용자는 모바일 RFID를 이용하여 난수 인증키를 생성하여 입력하므로 ID, Password와 별도로 난수 인증키를 통한 인증을 거치게 된다. 이는 모바일 RFID를 통하여 중복되지 않는 인증키를 보안담당자 및 인가된 사용자의 휴대폰으로 전송한다. 사용자의 접속 및 접속 시도 발생된 인증키는 DB로 남기게 되어 사용자의 접속시간 및 발행된 인증키의 로그를 남기게 된다.

이때 모바일 RFID 리더와 Tag, 휴대폰 등의 디바이스가

함께 존재하지 않으면 사용자는 중요 정보시스템에 접근 할 수 없다. 이는 모바일 RFID 리더와 Tag, 휴대폰 중 어느 하나라도 분실 시 중요정보 시스템에 절대로 접근이 불가능하여 비 인가된 사용자로부터 중요 정보시스템을 안전하게 보호할 수 있다. 허가되지 않은 사용자의 등록되지 않은 Tag로 발생되는 메시지는 〈그림 6〉과 같이 등록된 DB를 통하여 인증키를 발송하였다. 불법적으로 접속을 시도한 사용자로 인지된 경우 HOST 체크모듈이 동작하여 중요 정보시스템에 접속이 불가능하다. 이동통신사에서 모바일 RFID를 통해 전송된 Tag ID 및 휴대폰의 인증번호, 휴대폰번호의 값은 인증서버로의 수신된 Tag의 ID를 비교하므로 이는 발급된 인증키의 재사용을 방지하여 발생될 수 있는 위험요소를 미연에 방지할 수 있다.

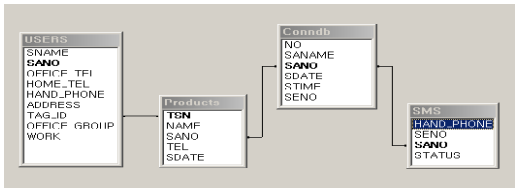

그림 6. 접근 및 SMS DB와의 관계
Fig 6. Relation between Access and SMS DB

중요 정보시스템의 관리자 화면에 발급현황이 입력됨과 동시에 SMS전송모듈로 인가된 담당자와 난수 인증키를 SMS 발송 DB로 입력된다. DB에 입력된 정보는 발송모듈을 통해 〈그림 7〉과 같이 인가된 사용자의 휴대폰으로 전송된다.

그림 7. 휴대폰으로 전송된 난수 인증키
Fig 7. Random-Number authentication key by SMS

중요 시스템에 접속하고자 하는 내부사용자가 해당 장비의 URL을 입력을 하면 〈그림 8〉과 같이 ID, Password외 추가로 모바일 RFID를 이용한 난수 인증키를 입력하는 페이지가 나타난다. 난수 인증키 및 ID, Password를 입력하면 Host 체크 모듈의 동작에 의해 ID, Password 및 난수 인증키가 성공적으로 인증이 될 경우 중요 정보시스템에 접속이 가능하다. 이는 ID, Password를 입력하였더라도 난수 인증키를 입력하지 않을 경우 접근제한의 메시지가 나타나므로 불법적인 사용자의 접근이 사전에 차단이 된다. 사례분석을 통해 다음과 같이 두 가지 사항을 확인할 수 있었다. 첫 번째, 내부인원에 대한 불필요한 접근을 근본적으로 차단할 수 있다. 두 번째, 난수 인증키를 생성시킬 경우 모바일 RFID리더 및 Tag, 휴대폰 등이 함께 있을 경우에만 난수 인증키가 생성되므로 불법적인 접근이 방지된다[11].

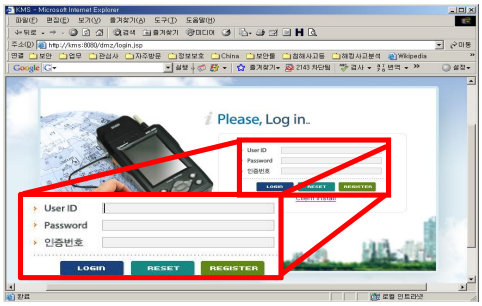

그림. 8 중요 정보시스템의 로그인 화면
Fig. 8 Log-In View of Information System

VI. 제안 프로토콜 평가

본 논문에서는 제시한 방법을 통하여 사용자 3명이 동시접속을 하여 발생된 난수 인증키와 접속 시 DB에서의 인증키 삭제 여부는 〈표 2〉과 같다. 즉, 유사한 시간대에 3명의 사용자로 하여금 난수 인증키를 5회 발급한 결과 중복된 난수 인증키의 발급과 로그인 접속 시 DB에서 인증키가 삭제됨이 나타났다. 이는 모바일 RFID와 Tag, 휴대폰을 통하여 인증키가 발급 되었으며 발급된 인증키를 이용하여 중요정보 시스템의 접속과 동시에 인증키의 정보를 DB에서 삭제하므로 재사용 하는 것이 방지되었다. 이와 유사한 접근방식으로 OTP와 Smart Card를 통한 접근방식이 있다. OTP의 경우 비용적인 측면에서 높은 구입비용과 높은 관리비용, 매년 라이선스 지불하고 있으며 도난 및 파손의 우려, 여러 개의 Token의 휴대해야 하며 별도의 서버/클라이언트 장치가 필요한 단점을 지니고 있다. 또 하나의 인증방법인 Smart Card의 경우 높은 구입비에 비해 잦은 고장으로 유지보수 비용이 매우 높다. 리더기의 경우 고정되어 있어 인하여 장소의 제약성을 크게 받는다. 또한 많은 인증방법 중에서 Smart Card가 지

표 3. 인증방법의 분류표
Table 3. Certification Table

기 술	보안 등급	재사용성	방 식	비 용	비 고
Username & Password	Low	의미 없음	단순 ID, Password만 기억	- 자체개발주류 - 비용 안듬	- Keyboard Spyware에 취약 - 중요 시스템의 보안에 매우 취약
OTP (Hard Tokens)	High	재사용 불가	Device 휴대	- 높은 구입비용 - 높은 관리비용 - 매년 라이선스 지불	- 도난 및 파손의 우려 - 여러 개의 Token의 휴대해야 할 가능성 - 서버/클라이언트 장치필요
Biometrics	High	재사용 불가	지문, 홍채 등 신체적 특징, 스캐닝 필요	- 높은 구입비용 - 높은 유지보수 비용발생	- 유인한 식별자로만 구별
Smart Card	High	재사용 불가	특별한 인식기가 설치된 곳만 사용가능	- 높은 구입비 - 높은 유지보수 비용	- 분실우려 - 잦은 고장우려
PKI	High	재사용 불가	설치가 되고 나면 사용용이	- 높은 구입비 - 높은 유지보수 비용	- 디바이스별로 특화 - 유동성이 불가능
본 연구	High	재사용 가능	모바일용 RFID리더 및 Tag, 휴대폰 필요	- 높은 구입비용 - 낮은 유지보수 비용 - 재사용이 가능하여 비용 절감	- 분실 시 보안의 문제가 없으며 디바이스별로 특화되지 않아도 됨 - 재사용이 가능하여 유지보수 비용절감 - PKI, OTP, UNP의 기능 혼합

나고 있는 가장 큰 단점은 분실을 통한 불법인증 및 불법적인 사용의 위험성을 지니고 있다. 이에 비해 모바일 RFID를 사용한 경우 높은 구입비용에 비해 낮은 유지보수 비용과 Tag 및 모바일 리더기의 재사용이 가능하여 비용 절감을 시키는 효과를 볼 수 있다. 또한 기존 OTP 및 Smart의 단점인 장소의 제약성을 모바일 RFID를 이용하므로 장소 및 시간에 구애받지 않고 효과적으로 사용할 수 있다. 분실 위험성의 경우 휴대폰, Tag, 모바일 RFID가 같은 공간, 같은 시간에 존재하여야만 인증키를 부여 받을 수 있으므로 분실로 인한 불법적인 접근 위험을 효과적으로 방지하였다.

표 2. 사용자에 따른 인증키 분배현황 및 접속시 인증키 삭제여부
Table 2. Random-Number authentication key sent to Mobile Phone

구 분		1회	2회	3회	4회	5회
사용자 A	인증키	1171436886429	1171436528951	1171436624458	1171436644475	1171436645998
	삭제	완료	완료	완료	완료	완료
사용자 B	인증키	1189496533223	1189496552987	1189496569457	1189496594023	1189496612584
	삭제	삭제완료	삭제완료	삭제완료	삭제완료	삭제완료
사용자 C	인증키	1165876508445	1165876515524	1165876519684	1165876529672	1165876524772
	삭제	완료	완료	완료	완료	완료

이는 스푸핑공격, Kill명령어 공격기법, Tag 위변조공격, 중복 및 재사용, 접속매체의 분실 등에 효율적인 것을 〈표 3〉과 같이 나타난다. 또한 20대 남녀 대학생의 패스워드 현황을 분석한 결과 6자리 이하의 패스워드를 이용하는 사용자가 64.5%에 이르고 있다. 또한 국내 은행, 국내 포털 등 103개의 웹사이트를 대상으로 조사한 결과 8자리 이상의 패스워드를 이용하는 웹사이트는 23%에 불과하며 조사대상 웹사이트의 99%는 패스워드 최소길이에 대한 제약이 약해서 안전하지 않은 길이의 패스워드 사용도 가능하다. 이는 6자리 이하의 패스워드를 알아내는데 필요한 시간은 약 8시간의 노력으로 가능하다[12]. 이에 본 연구는 최소12자리 이상의 난수를 발생하므로 안전한 인증번호를 통해 중요정보 시스템에 접근하므로 패스워드의 보안정책에 효율적이다.

Ⅶ. 결론 및 향후 연구과제

최근 고객의 정보가 입력되어 있는 노트북의 분실 시 해당 담당자의 책임 및 손해배상이 일어났다. 이는 노트북 및 접속 디바이스에 저장되어 있는 계정정보 등을 이용하여 중요 정보 시스템에 접근이 가능하며 한 기업의 보안사고로 이루어진다. 중요정보 시스템의 용이한 접근을 사전에 차단하고자 하는 것이 본 연구의 목적이다. 이에 본 연구는 모바일 RFID를 이용하여 난수 인증키의 생성 및 인가된 사용자에게 SMS를 통하여 인증키를 발송하여 기존의 ID와 Password만으로 사용되고 있는 보안장비의 접근의 보안을 한층 강화시켰다. 또한 RFID tag를 이용한 사원증 및 노트북에 부착하여 해당 담당

자가 사용하므로 접근의 제한 및 권한을 부여하였고 접근에 관련된 이력을 남김으로 작업의 내용을 확인하도록 연구하였다. 또한 인가된 ID, Password만 알고 있는 사용자라 할지라도 인증번호가 없으면 접속이 불가능하다. 이러한 접근 및 보안의 취약성을 모바일 RFID 시스템과의 연동으로 인하여 접근 권한을 제한함으로 보다 안정적인 시스템의 접근이 이루어진다. 또한 사용자의 인증과 동시에 접근에 필요한 난수 인증키를 생성하고자 할 경우 모바일 RFID리더 및 Tag, 사용자의 휴대폰이 함께 존재해야 하므로 어느 하나라도 분실 시 중요 정보시스템에 접근이 불가능하도록 하여 보안을 강화하였다.

향후에는 이동통신사와 인증키 생성시스템간의 데이터의 무결성 및 기밀성을 위한 IPSec VPN 또는 SSL VPN을 이용한 연구가 필요하다. 또한 휴대폰의 공통된 플랫폼을 통하여 다수의 이동통신사간의 연동으로 중요 정보시스템간의 네트워크의 확장과 자원의 공유 방법에 대한 연구가 필요하다.

참고문헌

〔1〕 숀 헤리스, 김 대경, "*Passport CISSP*," 정보문화사, pp. 54-70, 2004년.

〔2〕 정동기, "각급 기관 보안사고 근절대책", 전라남도 교육청, pp. 1, 2003년 11월

〔3〕 최원혁, "*기업정보 온라인유출 유형 및 사례 분석*", 국가사이버안전센터, pp. 3-4, 2005년 3월.

〔4〕 M. Ohkubo, K. Suzuki, and S.Kinoshita, "Efficient Hash-Chain Base RFID Privacy Protection Scheme", Ubcomp 2004 workshop

〔5〕 D. Henrici and Paul Muller, "Hash-Base Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers", PerSec'04 at IEEE perCom. pp. 149-153, 2004.

〔6〕 G. Avoine and Ph. Oechslin, "A Scalable and Provably Secure Hash-Base RFID Protocol", The 2nd IEEE International workshop on Pervasive Computing and Communication Security Society Press. Kauai Island Hawaii. USA, 2005. 2.

〔7〕 EPCglobal, "EPCTM Tag Data Standards Version 1.1 Rev1.24 Standard Specification 01". 04. 2004

〔8〕 Texas Instruments, *http://www.ti.com/tiris/*

〔9〕 Matrics Systems Corporation, "EPC and Radio Frequency Identification (RFID) Standards," pp.2~3, 2004.

〔10〕 장병준, "*모바일 RFID 기술 동향 및 주요 이슈*," ITFIND 주간기술동향, pp.3~4, 2005년 7월.

〔11〕 홍명선, "*2차원 바코드를 이용한 선불형 전자지급 휴대폰 결재 시스템의 기술구현* SK Review 제16권 2호, 2006년 4월.

〔12〕 Auto-ID Center, "860MHz-960MHz Class I Radio Frequency Identification tag Radio Frequency and Logical communication Interface Specification Proposed Recommendation Version 1.0.0. Technical Report MIT-SUTOID-TR-007", AutoID Center. MIT. 2002

〔13〕 한국정보보호 진흥원, "*당신의 패스워드는 얼마나 안전할까요?*", 정보보호 뉴스, 2007년 10월.

저 자 소 개

최 병 훈(Choi,Byeong Hun)

2001: 성결대학교 전산통계학과 공학사

2004: 숭실대학교 산업기술정보 대학원 산업정보시스템공학과 공학석사

현 재: CJ오쇼핑 감사팀 정보보안파트

관심분야: 정보보안, 유비쿼터스

김 상 근(Kim, Sang Geun)

1987: 중앙대학교 전자계산학과 이학사

1989: 중앙대학교 전자계산학과 이학석사.

1996: 중앙대학교 컴퓨터공학과 공학박사

현 재: 성결대학교 컴퓨터공학부 교수

관심분야: 정보보안, 유비쿼터스

배 제 민(Bae, Je Min)

1991: 중앙대학교 전자계산학과 이학사

1993: 중앙대학교 전자계산학과 이학석사

1998: 중앙대학교 컴퓨터공학과 공학박사

현 재: 관동대학교컴퓨터교육학과 교수

관심분야: 컴퓨터교육, 정보보안