제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

스마트워크 환경에서 스마트폰을 이용한 사용자 인증 기법 연구

변연상, 박대식, 곽진
순천향대학교 정보보호학과
e-mail : ysbyun@sch.ac.kr, dspark@sch.ac.kr, jkwak@sch.ac.kr

A Study on User Authentication Scheme Using the Smart Phone in the Smart work Environment

Yun-Sang Byun, Dae-Sik Park, Jin Kwak
Dept of Information Security Engineering, Soonchunhyang Univ.

요 약

최근 정보통신기술의 발달과 스마트기기 이용의 확산으로 인해 생활환경 및 업무 환경이 크게 변화되었다. 특히 스마트폰의 보급이 빠르게 확산되어 스마트폰을 사용해 업무처리가 가능한 스마트워크 환경에 관심이 증가하고 있다. 국내의 스마트워크에 대한 연구 및 기술개발은 초기단계이며 기업 내부 네트워크에 접근하기 위한 사용자 인증 기법 또한 부족한 실정이다. 따라서 본 논문에서는 스마트워크 환경에서 스마트폰을 이용하여 보안카드와 이미지 패스워드 기반의 사용자 인증 기법을 제안한다.

1. 서론

최근 정보통신기술의 발달과 스마트기기의 개발 및 이용이 빠르게 확산되어 사용자들의 업무환경이 크게 변화했다. 이동성이 높은 스마트폰, 태블릿을 이용함으로써 과거의 업무환경에서 나타난 공간의 제한이 없어지고 언제 어디서나 효율적으로 업무를 지속할 수 있는 스마트워크라는 신개념 업무환경이 주목받고 있다. 스마트워크는 다양한 디바이스를 이용하여 사무실 근무를 벗어나 스마트워크센터근무, 재택근무, 이동근무 등과 같은 방식으로 업무를 처리할 수 있다.

스마트워크 환경은 다양한 장소에서 기업 내부 네트워크에 접속하여 업무를 처리하기 때문에 내부 네트워크에 접속하는 사용자 인증이 중요하다. 또한 현재 스마트폰의 보급이 활성화되면서 대기업에서는 스마트폰을 이용한 스마트워크 환경을 구축 및 적용하고 있지만, 비인가 된 사용자가 스마트폰을 이용해 접근할 경우 기업의 중요한 정보가 유출될 가능성이 있다. 따라서 본 논문에서는 스마트폰을 이용한 사용자 인증 기법에 대해서 연구한다. 본 논문의 구성은 다음과 같다. 2장에서 스마트워크의 개념을 정리하고 3장에서는 본 논문에서 제안할 기법에 대한 관련연구를 서술한다. 4장에서는 문제점을 분석하고 5장에서는 스마트 폰을 이용한 사용자 인증 기법을 제안하고 6장에서는 결론을 맺는다.

이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No.2011-0007755).

2. 스마트워크의 정의

스마트워크는 기존 업무환경에 나타난 제한된 공간, 긴 출·퇴근거리 등 시간의 제약에서 벗어나 언제 어디서든 편리하게 업무를 처리할 수 있는 새로운 업무환경이다.

스마트워크는 업무를 처리하는 장소에 따라 스마트워크센터근무, 재택근무, 이동근무 등으로 구분되며, 원격근무(Teleworking)와 유사한 개념을 지닌 용어로 사용하고 있다. <표 1>은 스마트워크의 유형과 장점을 나타낸 것이다 [3].

<표 1> 스마트워크의 유형과 장점

유형	근무형태	장점
재택근무	- 자택에서 본사의 네트워크에 접속하여 업무수행	- 별도의 사무 공간 불필요 - 육아양육 문제 해결
이동근무	- 이동 가능한 디바이스를 이용한 현장 업무수행	- 잦은 외근, 현장 서비스와 같은 업무환경에 유리
스마트워크센터 근무	- 자택인근 원격사무실에서 업무 수행	- 회사와 유사한 업무환경 - 업무집중도 향상 가능 - 출·퇴근 시간 단축

2.1 스마트워크 국내 동향

스마트워크 국내 동향은 아직 초기단계이며, 현재 정부에서 2015년까지 공공기관에 50여개, 민간기관의 400여개의 스마트워크센터 구축을 목표로 추진되고 있다. 또한 전체 공무원의 30%, 전체 노동인구의 30%까지 스마트워크 근무비율을 증가시키겠다고 발표함에 따라 지속적으로 발전

할 것으로 예측된다[4].

2.2 스마트워크 국외 동향

스마트워크는 미국과 네덜란드와 같은 국외에서 활성화되어 있으며 다양한 형태로 각 국가에 맞게 적용되어 있다. <표 2>는 스마트워크 국외 동향을 나타낸다.

<표 2> 스마트워크 국외 동향

국가	내용
미국	· 인사 관리처, 일반 행정청을 중심으로 정책 추진, 활성화 연구 · 100개의 스마트워크센터를 건설하여 저탄소 업무환경 구축할 계획 발표 · 원격근무자의 비율이 '05년부터 지속적으로 증가
네덜란드	· 고용 규모가 큰 기업일수록 원격근무자의 비율이 높음 · 500명 이상의 고용인이 있는 경우 90%이상이 원격근무를 실시
일본	· 총무성을 중심으로 정책을 추진, 보완 및 개선 · 민간부문의 원격근무 도입 촉진을 위한 지원책이 마련

3. 관련연구

3.1 그래픽 기반 패스워드(Graphical Password)

일반적으로 패스워드는 어렵고 복잡하며 무질서도가 높은 패스워드를 사용하는 것을 권장하고 있지만 실질적으로 사용자들이 그렇게 사용하지 않기 때문에 다른 방식으로 이미지를 이용한 패스워드 방식인 그래픽 기반 패스워드(Graphical Password) 방식이 많이 연구되고 있다. 그래픽 기반 패스워드의 다양한 방식들 중에서 CA, Passfaces TM이 널리 사용되고 있으며 이는 다음과 같다.

o CA(Cognitive Authentication)

Weinshall이 2006년에 제안한 방식으로 다양한 종류의 이미지를 패스워드로 선택하고 이것을 이용하여 사용자 인증을 수행하도록 설계된 방식이다.

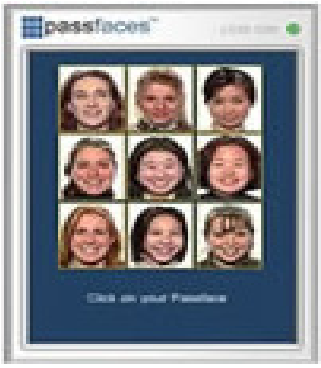
(그림 1) CA의 사용자 인증 화면

(그림 1)과 같이 다양하게 공개된 이미지를 선택을 하고 선택된 이미지를 비밀 이미지 집합으로 정의한다. 컴퓨터는 무작위로 이미지를 선택하여 화면에 그리드 형식으로 배열하고 왼쪽과 아래쪽에 각각의 행과 열에 맞추어 무작위로 일정한 범위 안의 숫자를 중복하여 배열하게 된다.

사용자는 왼쪽의 첫 번째 이미지가 본인이 선택한 비밀 이미지 집합에 속해 있을 경우 아래쪽으로 이동하고, 그렇지 않을 경우 왼쪽으로 이동하여 이미지를 보게 된다. 다음 이미지의 경우에도 같은 행동을 반복하여 마지막에 시선이 위치한 곳에 부여된 숫자를 입력하여 컴퓨터에 보내게 되는 방식이다. Weinshall이 작성한 논문에서는 저자들이 직접 사용자 실험에 참여하여 도출한 결과에서 1라운드에 약 20초를 소요하였으며, 200여일이 지난 시점에서도 90%이상 되는 성공률을 가지고 인증이 가능하다[4].

o PassfacesTM

PassfacesTM은 RealUser.com에서 개발한 인식기반의 이미지 인증 시스템이며 현재 스마트폰에서 사용되고 있는 방식이다. PassfacesTM의 사용자 인증화면은 (그림 2)와 같다.



(그림 2) PassfacesTM의
사용자 인증 화면

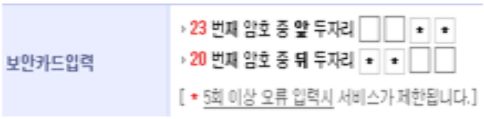
사용자는 초기 패스워드를 등록하기 위해 화면에 출력된 사람들의 얼굴 중에서 1~5개의 얼굴을 선택하여 패스워드로 등록하고, 인증단계에서 화면에 출력된 9개의 이미지 중에서 사용자가 앞서 패스워드로 등록한 이미지를 선택한다. 무작위로 출력되기 때문에 몇 번의 과정을 반복하여 이미지를 선택하고 사용자 인증이 이루어지게 된다[1][4].

3.2. 보안카드

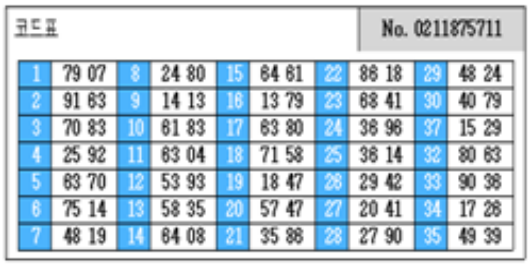
보안카드는 현재 금융권에서 많이 사용되고 있는 기법으로 금융 업무(송금, 결제 등)를 할 때 본인인증 수단으로 사용된다. 보안카드는 본인이 발급 기관에 방문하고 직접 본인인증 절차를 통해 발급받게 된다. 보안카드에는 1~30, 많게는 35개의 항목이 존재하고, 각 항목에 해당하는 4자리 숫자가 있다. 금융업무시 공인인증서를 통해 1차 인증을 수행하고, 2차적으로 보안카드에 적힌 무작위의 숫자를 요구하게 된다. 사용자는 요구된 항목의 숫자를 차례로 입력하여 인증을 받음과 동시에 금융 업무를 수행한다.

보안카드 발급은 발급 대상자마다 각각의 다른 숫자가 적힌 카드를 발급되며, 발급된 카드의 일련번호를 사용자

와 함께 서버에 등록함으로써 동기화가 진행된다.



(그림 3) 금융업무시 인증번호 요구 화면



(그림 4) 은행 보안카드

4. 보안 문제점 분석

스마트워크 환경에서는 다양한 디바이스를 이용하여 영업현장 및 자택, 스마트워크센터와 같은 곳에서 사내 네트워크에 접속하여 업무를 처리한다.

이동근무나 원격근무지에서 업무를 처리하기 위해 사용되는 다양한 디바이스에 대한 인증이 필요하지만 정확한 사용자 인증도 중요하다.

사용자 인증의 경우 다양한 사용자 인증 기술이 개발되어 있지만 기존의 기술들은 스마트폰을 이용한 스마트워크 환경에 적용시키기에는 적합하지 않다. 사용자가 다루는 정보들은 회사의 내부정보 등 기업에 큰 피해를 줄 수 있는 기밀자료도 있기 때문에 높은 보안 수준이 요구된다.

스마트워크 환경에서 스마트폰을 이용할 경우 발생할 수 있는 문제점 간단하게 요약해보면 아래와 같이 표현할 수 있다.

- 모바일 악성코드 감염 문제
- 기업 정보 및 기술의 무단 유출
- 단말기 인증 문제, 분실 문제
- 사용자 인증 문제

스마트워크는 다양한 환경에서 업무처리가 가능하기 때문에 시간적, 공간적 제약이 거의 없다. 하지만 그러한 환경 때문에 분실, 비인가 사용자의 접근 등과 같은 보안위협에 노출될 가능성이 있기 때문에 정확하게 사용자를 인증할 수 있는 기술이 필요하다. 따라서 본 논문에서는 스마트워크 환경의 이동근무, 원격근무에서 가장 널리 사용되는 디바이스인 스마트폰을 이용한 사용자 인증 기법에 대해서 제안한다.

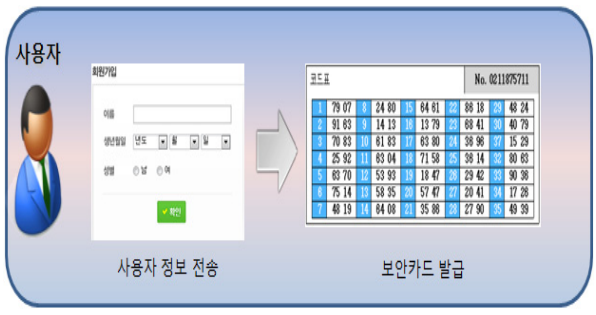
5. 제안 기법

스마트워크 환경에서는 재택근무, 스마트워크센터근무, 이동근무와 같은 다양한 형태가 존재한다. 그 중 이동근무는 스마트폰 보급의 확산으로 더욱 관심이 집중되고 있다. (그림 5)는 스마트워크 환경에서 스마트폰을 이용한 업무처리에 대하여 도식화하여 나타낸 것이다.

(그림 5) 이동근무를 통한 업무처리

스마트워크 환경에 적용할 수 있는 다양한 인증 기법에 대한 연구가 진행되고 있다. 본 논문에 제안 기법은 스마트워크 환경에서 사용자가 이동근무, 원격근무시 외부에서 스마트폰을 이용하여 기업 내부 네트워크에 접속하기 위해 사용자와 기업 내부 네트워크간 인증이 진행되는 방식으로 어플리케이션을 통한 보안카드와 이미지 기반 패스워드를 이용하는 기법을 제안한다.

사용자는 스마트폰으로 어플리케이션을 다운받아 실행시키게 되면 기업서버와 연결된 어플리케이션은 본인인증을 요구하고 사전에 기업서버에 등록한 정보와 본인인증시 입력한 정보가 일치하는 사용자에게 해당 스마트폰으로 모바일용 보안카드를 발급한다. 이때 보안카드 발급기관은 기업서버에서 해당 사용자의 정보를 전송받아 사용자가 입력한 개인정보와 일치여부를 확인한다. 사용자는 업무를 처리하기 위해 발급받은 보안카드를 이용하여 어플리케이션이 요구하는 보안카드의 숫자를 입력하고, 다음에 나오는 10*10 크기의 매트릭스에 입력한 숫자를 좌표로 활용하여 출력된 이미지에 해당되는 맵핑값을 다시 인증서버로 전송한다. 이와 같은 과정을 통해서 총 2번의 사용자 인증을 받게 된다. (그림 6)은 사용자 등록단계를 (그림 7)은 사용자 인증단계를 나타낸 것이다.



(그림 6) 사용자 등록단계

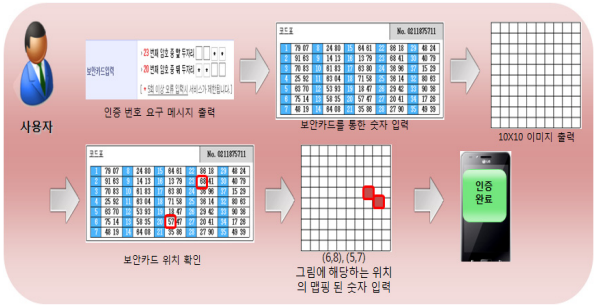
o 등록 단계

① 사용자는 개인정보를 인증서버에 전송하고 정당한 사용자임을 인증 받는다.

② 사용자는 업무에 필요한 어플리케이션의 이용하기 위해 보안카드 발급 기관에 단계 ①에서 입력한 개인정보를 전송하고 보안카드 발급을 요청한다.

③ 보안카드 발급기관은 인증서버로부터 사용자의 개인정보를 받고, 단계 ②에서 사용자가 직접 전송한 개인정보와 비교하여 정당한 사용자임을 확인한다.

④ 정당한 사용자로 판명되면 스마트폰으로 보안카드를 전송한다.



(그림 7) 사용자 인증 단계

o 사용자 인증 단계

① 사용자가 기업서버에 접속하게 되면 인증서버에서 사용자의 보안카드에 존재하는 숫자를 요구한다.

② 사용자는 등록단계에서 어플리케이션을 통해 다운받은 보안카드를 이용하여 각각에 해당되는 항목의 숫자를 입력한다.

③ 입력이 완료되면 이미지를 이용한 인증화면으로 전환되고, 10*10 크기에 해당하는 매트릭스에 서로 다른 이미지가 출력된다.

④ 사용자는 단계 ①에서 사용자에게 요구한 숫자를 좌표처럼 이용하여 해당되는 위치에 출력된 이미지를 선택한다.

⑤ 선택된 이미지에 맵핑되어 있는 숫자, 영문자가 출력되고 사용자는 다시 해당 맵핑값을 인증서버에 전송한다.

제시된 방법은 기업서버에서 인증서버로 제공하는 수많은 이미지들이 어플리케이션을 통한 접속을 할 때 마다 매번 다르게 출력된다. 또한 사용자는 어플리케이션을 통해 접속하여 요청받은 보안카드의 임의의 숫자를 입력하고, 그 해당 숫자를 좌표로 사용하여 화면에 출력된 이미지들 중 해당위치에 있는 이미지를 선택하여 해당하는 이미지에 맵핑된 숫자를 최종적으로 인증서버로 전송하여 인증을 완료한다.

스마트폰의 어플리케이션이 실행될 때 마다 인증서버와 통신하여 화면에 출력되는 이미지와 해당 맵핑값을 동기화한다. 이러한 과정에서 이미지 변조나 비인가 사용자에 대한 인증은 차단될 것으로 예상된다. 또한 보안카드는 1단계 인증에서 숫자를 통한 인증방식에 이용되고 2단계 인증에서는 이미지의 좌표 값을 나타내는 역할을 수행한다.

보안카드는 많은 사용자들에게 각기 다른 숫자가 적힌 보안카드가 전송되고 사용자들 마다 해당하는 이미지의 맵핑값은 어플리케이션을 통해 매 접속시 출력되는 이미지가 매번 다르기 때문에 똑같은 맵핑값의 입력이 불가능하다. 따라서 본인인증을 거친 사용자만 맵핑값을 입력할 수 있으며 정확한 사용자 인증을 받을 수 있다.

6. 결론

스마트워크 환경은 다양한 IT인프라를 이용한 혁신적인 업무 형태로 다양한 디바이스를 이용하는 스마트워크는 단말기 분실이나 사용자 인증, 단말기의 악성코드 감염을 통한 개인정보 및 기업 기밀정보 유출에 대한 보안 취약점이 있으며, 이와 같은 보안 취약점이 해결되지 않는다면 안전한 스마트워크 환경의 구축이 불가능하다.

외부에서 기업 내부 네트워크로 접속하는 스마트워크 환경에서는 디바이스에 대한 인증도 중요하지만 정확한 사용자 인증이 이뤄지지 않아 비인가 된 사용자가 내부 네트워크에 접속하여 기업 기밀정보를 유출 시킨다면 기업 입장에서는 큰 피해를 입을 것이다. 따라서 본 논문에서는 스마트폰을 이용한 스마트워크 환경에 접근하는 다양한 사용자들을 대상으로 보안카드와 이미지를 이용한 인증기법에 대해서 제안하였다. 이를 통해 외부에서 스마트워크를 이용하는 사용자들에 대하여 업무를 수행할 때 사용자별로 발급된 보안카드와 이미지를 이용한 맵핑값을 이용하여 비인가 된 사용자를 사전에 차단하고, 회사의 중요정보를 보호할 수 있을 것으로 기대되며 스마트폰을 이용한 스마트워크 환경에서 보안성 향상을 기대할 수 있다.

참고문헌

[1] Daphna Weinshall, "Connitive Authentication Schemes Safe Against Psyware", IEEE Symoisium on Security and Privacy, May 2006

[2] T, Valnetine, "An evaluation of the Passface personal authentication system", Technical Report, Goldsmiths College, University of London, 1999

[3] 이재성, 김홍식. "스마트워크 현황과 활성화 방안 연구", 한국지역정보화학회지, 제13권 제4호, pp.75-96, 2010

[4] 강전일, 양대헌, "인지 및 역할 기반 사용자 인증 기법"

[5] http://www.smartwork.go.kr