

스마트워크 환경에서 QR코드를 이용한 안전한 승인 인증 시스템

이광희, 김수현, 이임영
순천향대학교 컴퓨터소프트웨어공학과
e-mail: [success, kimsh, imylee]@sch.ac.kr

Secure authentication system using QRcode in Smart work environment

Kwang-Hee Lee, Soo-Hyun Kim, Im-Yeong Lee
Design of Computer Software Engineering, SoonChunHyang University

요 약

스마트워크란 시간과 장소의 제약 없이 업무를 수행하는 유연한 근무형태를 말한다. 스마트워크 근무 유형에는 가정에서 본사 통신망을 접속해 업무를 수행하는 재택근무와 주거지 인근 원격사무실에 출근하는 스마트워크 센터 근무, 그리고 스마트폰 등을 이용해 현장에서 업무를 수행하는 이동근무가 있다. 스마트워크를 통하여 기업들은 업무 효율과 생산성 향상시킬 수 있다. 또한 대도시 교통 혼잡을 줄이고 여성의 육아부담을 줄일 수 있어 정부에서 확대 지원하는 사업이다. 하지만 스마트워크의 특성상 원격으로 접속하여 업무를 처리하므로 공격자가 로그인 정보를 취득 시에는 위협이 존재한다. 또한 스마트워크 센터에서 사원 관리 취약성과 비인가자에 대한 접근이 용이하기 때문에 문제가 될 수 있다. 이에 따라 본 논문에서는 QR코드를 이용한 승인 인증 시스템을 제안하게 되었다.

1. 서론

스마트워크란 사무실에서 업무하는 것을 탈피하여 시간과 장소 제약 없이 어디서나 편리하게 근무함으로써 업무 효율성을 향상시킬 수 있는 미래 지향적인 업무환경을 의미한다. 스마트워크 환경에는 스마트워크 센터를 이용한 근무방식과 스마트폰으로 이용하는 근무방식이 있다. 이미 미국과 일본 네덜란드 등 선진국에서는 오래 전부터 스마트워크를 도입해 시행하고 있다.

이러한 흐름으로 정부는 스마트워크 환경을 통하여 교통비 절감과 탄소 배출량 감소, 출퇴근 피로 감소로 인한 업무효율성과 같은 경제적 효과를 예상하였다. 2015년까지 전국에 50개의 스마트워크 센터를 구축하고 전체 공무원 30%가 활용하게 할 방침이다[1].

업무 환경이 스마트워크 환경으로 빠르게 변하고 있지만 보안에 대해 많이 미흡하다. 특히 스마트워크 센터 보안 위협으로는 비인가자에 대한 접근 문제와 사원 관리가 취약하다는 점, 그리고 로그인 정보 취득 시 문제라는 것이다. 본 논문에서는 이와 같은 위협을 줄이기 위해 QR코드를 이용한 승인 인증 시스템을 설계 및 구현하게 되었다.

2. 요구사항

본 논문에서 제안하고자 하는 시스템은 스마트워크 센

터의 보안 위협으로부터 QR코드를 이용하여 승인 인증하는 것이다. 정당한 사용자를 증명하는 사용자 인증을 통하여 위협으로부터 최소한 줄이기 위해 다음과 같은 요구사항이 필요하다.

2.1 사용자 인증

스마트워크 센터 PC클라이언트는 비인가자에 접근을 차단하며 정당한 사용자만 접근해야 한다. 그러므로 정당한 사용자라는 것을 증명하는 사용자 인증이 있어야 한다.

2.2 기밀성

승인 인증을 위한 어플리케이션 사용 시 정당한 사용자만이 어플리케이션을 사용해야 하며 로그인 정보 및 QR코드 값이 노출되지 않아야 한다.

2.3 무결성

스마트워크 센터 PC클라이언트로 송신되는 QR코드와 인증 서버로 송신되는 로그인 정보 값, QR코드 값은 인증을 위해 변조되지 않아야 한다.

2.4 상호작용성

사용자와 서버간의 원활한 통신이 이루어져야 하며 사용자는 서버로부터 받은 데이터를 이용함으로써 시스템

사용에 영향을 줄 수 있어야 한다.

2.5 즉시연결성

사용자는 시·공간의 제약 없이 단말기를 이용하여 서버와 통신이 가능해야 하며, 서비스를 원활히 제공 받을 수 있어야 한다. 모바일 콘텐츠의 가장 큰 장점이라고 할 수 있는 즉시연결성을 만족함으로써 항상 최신 데이터를 보유하여 적절한 시기에 올바른 서비스를 제공 받을 수 있어야 한다.

3. 제안방식

본 연구에서 제안하는 시스템은 사원이 본사의 컴퓨터에 접속하기 위해서 초기 ID/PW를 입력하는 것이 아니라 화면안의 QR코드를 회사만의 어플리케이션을 통하여 촬영을 한다. 그 이후 QR코드 값을 검사한 후 값이 일치하였을 경우에만 로그인 화면을 출력하고 사원이 로그인을 하게 되면 본사의 컴퓨터와 접속을 하는 방식이다. 이를 통하여 기존 시스템보다 안전한 로그인 시스템과 기밀문서 보안을 제공한다.

3.1 시스템 계수

- *:참여 객체
- K_{sa*} : 어플리케이션과 인증 서버간의 암호화와 복호화에 사용될 대칭키
- K_{sc*} : 인증 서버와 PC클라이언트간의 암호화와 복호화에 사용될 대칭 키
- id: 사원의 ID
- pwd: 사원의 패스워드
- qrValue: QR코드 값
- Pv: PC클라이언트의 잠금 해제 승인 값
- $E_*[]$: *의 대칭키로 암호화
- $D_*[]$: *의 대칭키로 복호화

3.2 어플리케이션과 인증 서버간의 사용자 인증

본 시스템은 어플리케이션과 인증 서버가 대칭키를 분배 받은 것으로 가정한다. 초기 어플리케이션이 로그인 정보와 QR코드 값을 대칭키로 암호화하여 인증 서버로 전송한다. 인증 서버는 전송 받은 값을 대칭키로 복호화하여 로그인 정보 및 QR코드 값을 검증하고 승인 인증을 한다.

step 1. 어플리케이션은 대칭키를 통하여 id와 pwd 그리고 qrValue를 암호화하여 인증 서버로 전송한다.

$$E_{K_{sa*}}[id||pwd||qrValue]$$

step 2. 인증 서버는 PC클라이언트로부터 전송 받은 값을 대칭키로 복호화하여 id, pwd, qrValue를 검증하여 승인 인증을 한다.

$$D_{K_{sa*}}[E_{K_{sa*}}[id||pwd||qrValue]] =? id||pwd||qrValue$$

3.3 인증 서버와 PC클라이언트간의 잠금 해제

초기 인증 서버와 PC클라이언트만이 사용할 대칭키를 분배한다. 인증 서버는 승인 값을 생성하여 대칭키를 이용하여 암호화하고 PC클라이언트로 전송한다. PC클라이언트는 전송 받은 값을 복호화 하여 검증하고 PC잠금을 해제 한다.

step 1. 인증 서버는 승인 값인 Pv를 생성하고 PC클라이언트와의 대칭키를 이용하여 암호화를 한 뒤 PC클라이언트로 전송한다.

$$E_{K_{sc*}}[Pv]$$

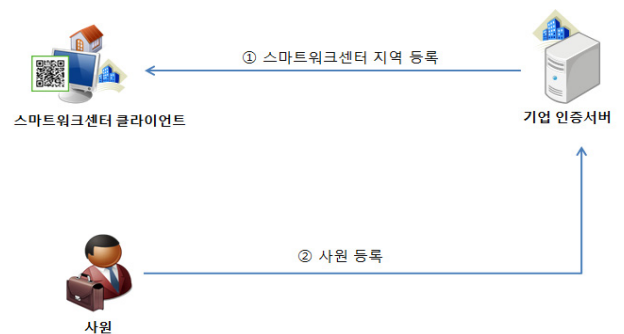
step 2. PC클라이언트는 인증 서버로부터 전송받은 값을 대칭키를 사용해서 복호화 하여 Pv를 검증하여 컴퓨터 잠금을 해제한다.

$$D_{K_{sc*}}[E_{K_{sc*}}[Pv]] =? Pv$$

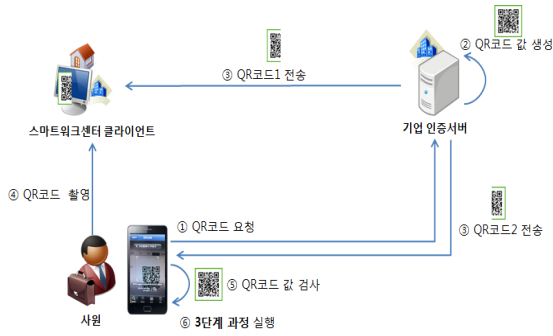
3.4 시나리오

본 프로그램은 기존 스마트워크 시스템에서 로그인 기능만을 제공하기 때문에 기존보다 안전한 로그인 인증 시스템을 제공하기 위하여 QR코드를 결합한 것이다. 초기 인증 서버는 지역 스마트워크 센터를 등록하고 또한 사원은 사원 등록을 한다(그림 1 참조). 사용자는 어플리케이션을 통하여 해당 지역의 QR코드를 요청한다. 그에 따라 인증 서버는 해당 지역의 QR코드를 생성하고 이미지를 1/2로 분할하여 스마트워크 PC클라이언트와 어플리케이션으로 각각 전송하게 된다. 사원이 PC클라이언트의 QR코드를 촬영하면 어플리케이션은 QR코드 값을 검사를 하고 로그인 화면으로 전환한다(그림 2 참조).

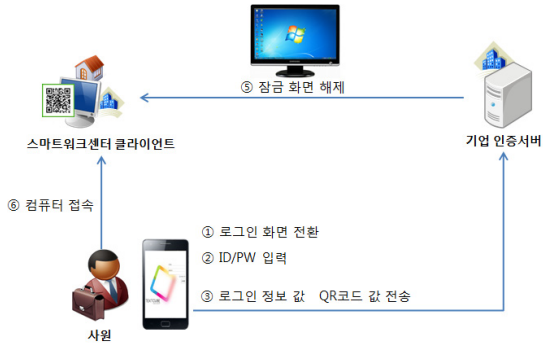
사용자가 로그인을 성공하게 되면 어플리케이션은 인증 서버에게 로그인 정보와 QR코드 값을 전송한다. 인증 서버는 완성된 QR코드 값과 로그인 정보를 정당한 사용자 인지를 판별하기 위해 저장된 DB정보 값과 비교 검사를 한다. 그 뒤 결과 값이 일치하게 되면 스마트워크 센터 모니터화면의 잠금 상태를 해제하여 사용자가 사용할 수 있게 된다(그림 3 참조).



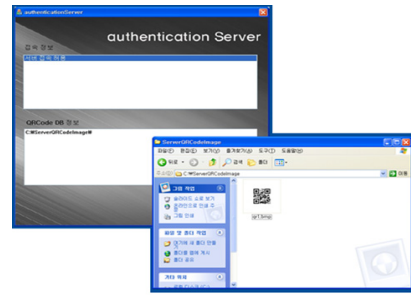
(그림 1) 근무지역 및 사원 등록



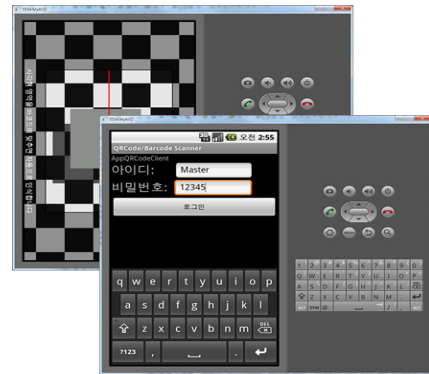
(그림 2) QR코드 생성 및 QR코드 검증



(그림 3) PC클라이언트 잠금 해제



(그림 5) 인증 서버



(그림 6) 어플리케이션

4. 제안방식 구현

제안 시나리오를 기반으로 QR코드를 이용한 승인 인증 시스템을 구현하였다.

4.1 스마트워크 센터 PC클라이언트

클라이언트는 비인가자에 대한 사용을 제한하기 위하여 키보드 잠금 및 QR코드 출력을 담당하고 있다(그림 4 참조).

4.2 인증 서버

인증 서버는 로그인 정보와 QR코드 값을 검사하며 QR코드 생성을 담당한다(그림 5 참조).

4.3 어플리케이션

어플리케이션은 QR코드 촬영 및 검사를 하여 인증 서버로 로그인 정보 및 QR코드 값을 전송을 담당한다(그림 6 참조).



(그림 4) 스마트워크 센터 PC클라이언트

5. 제안방식 분석

본 연구의 제안방식은 다음과 같은 보안 요구사항을 충족함으로써 다음과 같은 이점을 제공한다. 본 장에서는 2장에서 언급한 요구사항에 따라 분석한다.

5.1 사용자 인증

사용자 인증방식은 PC클라이언트의 QR코드 정보와 어플리케이션의 로그인 정보, QR코드 정보를 기반으로 QR코드 및 ID&Password 방식을 사용한다. 그러므로 기존 시스템의 로그인 방식보다 QR코드를 통하여 인증을 한 번 더 하게 된다.

5.2 기밀성

어플리케이션은 초기 스마트워크 센터 사용 등록 시 설치하는 것이므로 정당한 사용자만 QR코드 및 로그인 정보를 인증 서버로 전송할 수 있으므로 비인가자는 전송할 수 없어 기밀성을 제공한다.

5.3 무결성

어플리케이션은 해쉬 함수를 이용하여 값을 얻고 인증 서버로 전송한다. 인증 서버는 해쉬 값을 통하여 데이터가 변조 되지 않았음을 검증하게 되므로 무결성을 제공한다.

5.4 상호작용성

사용자는 QR코드 인증을 간단한 조작만으로 인증 서버로부터 인증 할 수 있게 된다. 인증 서버는 인증을 하기 위하여 QR코드를 생성하고 분할하여 PC클라이언트와 어플리케이션으로 각각 전송하게 된다.

5.5 즉시연결성

QR코드 승인 인증 시스템은 어플리케이션에서 QR코드를 요청 시 인증 서버와 통신하여 QR코드를 수신한다. 그 이후 즉각 반응하여 QR코드 촬영 화면으로 전환하고 QR코드 이미지를 출력한다. 또한 어디서나 어플리케이션 업데이트가 가능함으로써 보안에 대한 취약을 낮추게 된다.

6. 결론 및 향후 연구 방향

본 논문은 취약점이 많은 기존 스마트워크 센터 환경에 비해 강력한 보안을 기대할 수 있다. QR코드를 이용하여 비인가자 접근을 차단할 수 있으며 공격자가 로그인 정보를 취득하더라도 전체 QR코드 값을 취득할 수 없으므로 기존 로그인방식보다 안전하다. 또한 QR코드를 생성할 때 지역 특정 값으로 생성하고 이미지를 분할하여 스마트워크 센터와 사원에게 각각 보낸다. 그러므로 해당 지역 스마트워크 센터에서만 인증할 수 있으므로 기업 입장에서 불 때 사원 관리를 할 수 있는 강점이 있다.

이와 같은 특성으로 인하여 본 논문의 제안 방식을 제안할 경우 스마트워크 센터에서 비인가자 접근을 차단하여 기업의 기밀문서 유출되는 사건사고의 피해를 감소할 것이다.

스마트워크 환경이 지속적으로 성장하고 있으므로 향후 모바일 스마트워크 보안 프로그램을 개발하는데 집중적인 연구가 필요할 것이라고 사료된다.

참고문헌

- [1] 김지선, "스마트워크 정보보안이 핵심", 디지털타임스 2011. 7.27
- [2] 최용락, 소우영, 이재광, 이임영, "컴퓨터 통신보안 3rd Edition", 도서출판 그린, 2005. 8. 20.
- [3] 김승연, "열혈강의 JAVA PROGRAMMING" 도서출판 프리텍, 2006. 09. 01.
- [4] 남궁서, "JAVA의 정석(2ND EDITION)", 도서출판 도우출판, 2010. 01. 20.
- [5] 셰인 콘더, 로런 다시, "시작하세요 안드로이드 프로그래밍", 도서출판 위키북스, 2009. 11. 26
- [6] 에드 버넷, 한정민, "헬로, 안드로이드: 구글의 모바일 개발 플랫폼 소개하기", 도서출판 ITC, 2009. 03. 18.
- [7] 건호랩(devstory), "웹에서(java/jsp) zxing 를 이용한 qrcode(qr코드) 생성하기"
- [8] 자바API, "www.javastudy.co.kr/api/api1.5/index.html "
- [9] 성윤정, "Visual C++ MFC 윈도우 프로그래밍", 도서출판 INFINITY BOOKS, 2009. 10. 26.
- [10] 최호성, "열혈강의 Visual C++2008 MFC 윈도우 프로그래밍" 도서출판 프리텍, 2009. 8. 15
- [11] 김용성, "Visual C++6 완벽가이드 2nd Edition", 도서출판 영진닷컴, 2007. 9. 1