http://dx.doi.org/10.5392/JKCA.2016.16.02.243

모바일 애플리케이션의 보안성 향상을 위한 App 제어 시스템 설계 및 구현

Design and Implementation of App Control System for Improving the Security of the Mobile Application

이유준*, 장영환**, 박석천**
제이컴정보통신*, 가천대학교 IT융합공학과**

Yu-Jun Lee(leeiami@naver.com)*, Young-Hwan Jang(jang0h@naver.com)**,
Seok-Cheon Park(scpark@gachon.ac.kr)**

요약

최근 모바일 기기를 소유한 사용자가 증가하면서 기업에서도 모바일 기기의 보안성이 보장된 관리 환경 구현이 가속화됨에 따라 기업은 개인의 기기를 통제하고 효율적 관리를 위해 MDM을 도입하였으나 기존 MDM의 App 관리 기능은 관리자가 해당 App을 등록하기 전까지 보안 위협을 막을 수 없다.

따라서 본 논문에서는 이러한 문제점을 해결하기 위해 보안성 향상을 위한 애플리케이션 제어 시스템을 제안한다. 제안 시스템을 설계하기 위해 MDM의 기능과 인증 기술을 분석하였고, 시스템 아키텍처를 정의하여 사내의 정보 유출을 방지할 수 있는 모바일 기반 응용 제어 시스템을 설계 및 구현하였다. 구현한 제어 시스템의 보안성을 평가하기 위해 국제공통평가기준의 보안성 평가 항목을 기준으로 테스트 시나리오를 작성해 테스트를 진행하였다. 테스트 결과 평균 40%의 보안성이 향상된 결과를 확인하였다.

■ 중심어 : | 모바일 애플리케이션 | 애플리케이션 보안 | 제어 시스템 |

Abstract

Recently, with the rise of the mobile device, from mobile devices the user who owns the security, speed up the implementation of the guarantee management environment as businesses and individual equipment for the effcient management of the existing system, but the introduction of the MDM MDM App management features administrators to register the App until you can't prvent the security threat.

Therefore, this paper addresses these issues in order to improve the security of your application for the control system. The proposed system is a function of the MDM authentication technology to design analysis, and system architecture to help prevent information disclosure within the design and implementation of Mobile-based application control system. Implementation of the control system to assess the security of the international common criteria security evaluation complete the test scenarios on the basis of the test items. An average of 40% of the test results to verify the results of this enhanced security.

■ keyword : | Mobile Application | Application Security | Control System |

접수일자 : 2015년 08월 20일
수정일자 : 2015년 10월 13일
심사완료일 : 2015년 10월 15일
교신저자 : 박석천, e-mail : scpark@gachon.ac.kr

I. 서 론

최근 정보화 수준이 고도화되고 대외 기술 교류가 활발해짐에 따라 기업은 정보 유출에 의한 피해사례가 급증하고, 자료 유출사례 중 전·현직 종사원인 내부자의 의해 발생되는 건이 80% 이상을 차지하고 있어 내부정보 유출 방지체계에 대한 구축이 절실히 요구되고 있다.

기존 모바일 기기 정책을 실행하는 방법인 MDM 시장은 빠르게 확대되고 있으나 MDM의 보안에 관한 연구는 심도 있게 이루어지지 않았다. MDM이 새로운 기술로서 시스템에 대한 위협, 보안 요구사항 등에 대한 연구가 부족하기 때문이다.

또한 기업에서는 개인의 모바일 기기를 사용하여 기업 내부 자료 접근이 용이하다는 부분을 문제로 삼고 있으나, 늘어나는 모바일 기기의 관리 비용을 감당할 예상과 인력이 부족하고, 보안에 대비하지 않은 채 다양한 개인용 모바일 기기의 사용을 허용할 경우 보안 위험성이 커지기 때문이다[1].

기존의 MDM은 애플리케이션을 관리하기 위해 먼저 사용자와 모바일 기기의 인증을 거친 뒤 관리자가 미리 등록한 비인가 애플리케이션의 패키지 목록을 가져오고 사용자 기기에 해당 애플리케이션이 있는지를 검색한 뒤 애플리케이션의 실행을 차단한다.

이러한 방식은 관리자가 비인가 애플리케이션의 패키지명을 등록하지 않으면 해당 기능의 통제가 이루어지지 않는다는 문제가 있다.

따라서 본 논문에서는 보안성 향상을 위해 관리자가 허가한 애플리케이션의 패키지 목록을 얻어오고 해당 애플리케이션이 아니면 모든 보안 위협 요소의 실행을 차단하는 방법을 제안한다.

또한 QR Code 인증 방식의 문제점인 코드 복제를 막기 위해 One Time QR Code 방식을 사용하므로 사용자와 모바일 기기 인증 시 실시간으로 코드를 생성하고 시간 값을 비교해 복제된 코드의 허위 인증을 보완한다.

보안성을 향상한 모바일 디바이스 제어기능과 QR Code를 활용하여 회사에 출근하게 되면 보안 서버를 통해 전화나 문자 등 모바일 기기의 기능을 유지하면서 관리자가 허용한 애플리케이션을 제외한 자료 유출이 가능한 모든 기능을 차단하게 된다.

또한 QR Code를 통해 출입 인증이 용이해짐에 따라 사내 출입시스템을 통합하여 관리의 효율성을 높이는 시스템을 설계 및 구현하였다.

본 논문의 구성은 1장 서론에 이어 2장에서는 MDM의 전반적인 기술 개요와 QR Code, 인증 기술에 대해 분석하였고, 3장에서는 보안성 향상을 위한 애플리케이션 제어 시스템을 설계하였다. 또한 4장에서는 설계한 제안 시스템을 알고리즘에 의거하여 구현 및 평가하고 마지막으로 5장에서 결론을 기술한다.

II. 관련 연구

1. MDM(Mobile Device Management)

MDM은 OTA(Over The Air)을 이용하여 언제 어디서나 모바일 기기가 Power On 상태로 있으면 원격에서 모바일 기기를 관리할 수 있는 시스템이다[2].

현재 글로벌하게 60여개 이상의 MDM 업체들이 활동하고 있으며, 제공하는 기능들의 공통 요소는 [그림 1]로 나타낸다[3].

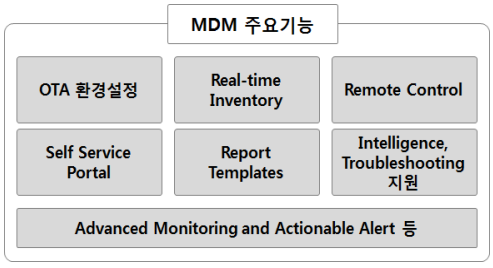


그림 1. 기존 MDM의 공통 주요기능

또한 Microsoft에서는 Architecture Guide for System Center Mobile Device Manager 2008이라는 문서를 통해 MDM 구성도에 대한 가이드라인을 제시해 놓았으며, Gateway Server, Device Management Server, Enrollment Server, DB가 필요하고 해당 모바일 기기는 게이트웨이 서버를 통하여 회사 네트워크의 MDM 관리 서버에서 제어가 이루어진다[4].

이러한 MDM은 짧은 서비스 타임과 최소의 비용으로 모바일 보안과 기능을 최적화시켜주는 시스템이었

으나 최근 보안 위협에 대한 강화 대책으로 관리의 필요성이 대두되면서 모바일 보안의 핵심 요소가 되고 있다[5].

2. QR Code(Quick Response Code)

QR Code는 빠른 응답이란 뜻을 가진 2차원 코드의 한 종류이며 바코드와 생긴 모양은 비슷하나 흑백 격자무늬 패턴의 사각형으로 만들어진 것으로서 1994년 도요타의 자회사인 덴소웨이브(Denso Wave)가 개발한 2차원 바코드 형식이다[6][7].

또한 구글에서 제공하는 오픈소스인 ZXing(Zevra Crossing)은 대다수가 QR Code 스캔 애플리케이션으로 활용하고 있을 정도로 널리 쓰이고 있으며 이러한 오픈소스를 통해 모바일 환경에서 손쉽게 임의의 QR Code를 생성할 수 있다[8][9]. ZXing의 컴포넌트 구성은 [그림 2]로 나타낸다.

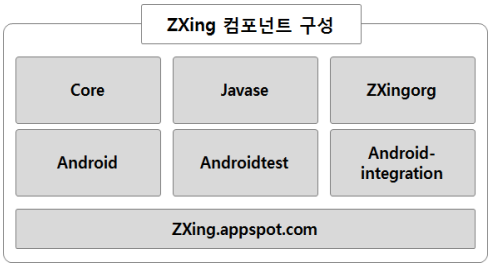


그림 2. ZXing 컴포넌트 구성

3. 인증 기술

여러 사람이 공유하고 있는 컴퓨터나 통신망의 경우 이를 사용하려는 사람이나 응용프로그램의 신분을 확인하여 불법적인 사용자가 들어올 수 없도록 시스템 보안을 유지하는 방법을 의미한다[10].

패스워드 방식 인증의 단점을 보완하기 위해 제시된 OTP(One Time Password)는 질의응답 방식, 시간 동기화 방식 등이 있으며, 질의응답 방식은 서버가 제시한 질의 값을 사용자가 알고리즘에 입력하여 응답 값을 얻고 해당 값을 서버에 전송하여 인증하는 방식이다.

시간 동기화 방식은 OTP 입력 값으로 비밀 키와 동기화 되는 시간을 사용하는 방식으로 기존 ID/PW 기반 인증 시스템에서 사용이 가능하고 질의응답 방식보다 간편한 장점을 지니고 있다[11][12].

III. 애플리케이션 제어 시스템 설계

1. 애플리케이션 제어 시스템의 개요

MDM의 애플리케이션 제어 기능은 사용자 기기에 해당 애플리케이션이 있는지 검색한 뒤 애플리케이션의 실행을 차단하는데 관리자가 비인가 애플리케이션의 패키지 명을 등록하지 않으면 해당 기능의 통제가 이루어지지 않는 단점이 있다.

따라서 본 논문에서는 보안성 향상을 위해 관리자가 허가한 애플리케이션의 패키지 목록을 얻어오고 해당 애플리케이션이 아니면 모든 보안 위협 요소의 실행을 차단하는 방법을 제안한다.

2. 제어 시스템 기능 블록다이어그램

본 논문에서는 자료 유출 가능성이 있는 모바일 애플리케이션을 통제하기 위해 MDM을 사용하였다.

MDM은 애플리케이션을 관리하기 위해 먼저 사용자와 모바일 기기의 인증을 거친 뒤 관리자가 미리 등록한 비인가 애플리케이션의 패키지 목록을 얻어온다.

또한 사용자 기기에 해당 애플리케이션이 있는지 검색한 뒤 실행을 차단하는 방법이지만 본 논문에서는 관리자가 허가한 애플리케이션의 패키지 목록을 얻어오고 해당 애플리케이션이 아니면 모든 보안 위협 요소의 실행을 차단한다. 제안 시스템의 블록다이어그램은 [그림 3]과 같이 설계하였다.

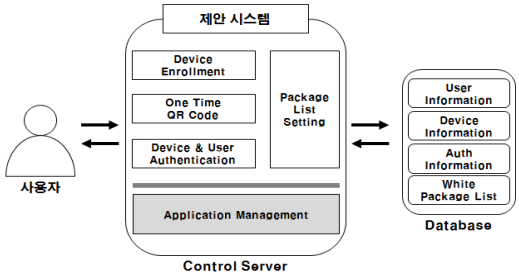


그림 3. 제어 시스템 기능 블록다이어그램

3. 애플리케이션 제어 시스템 DFD

시스템 내 데이터 흐름도를 이용하여 클라이언트와 서버의 전체적인 데이터 전송 주기를 정의한다.

데이터의 흐름은 사용자가 시스템 접속 시 One Time QR Code를 통해 인증하고 해당 사용자 정보를 사용자 DB에 저장하면 DB에서 패키지 목록을 획득한다.

획득한 애플리케이션 목록 기준으로 사용자 클라이언트 상태에 따라 동작, 해제 기능을 수행한다. 클라이언트는 요청받은 기능의 수행여부 결과를 DB에 저장하고 최종 결과를 출력한다. 설계한 DFD는 [그림 4]와 같다.

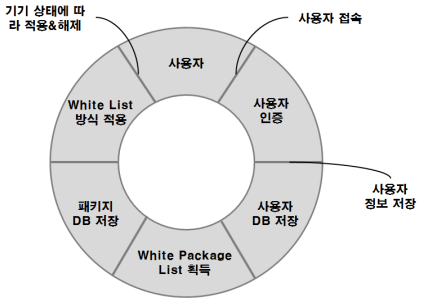


그림 4. 제어 시스템 DFD

4. 애플리케이션 제어 시스템 ERD

설계한 시스템은 사용자 정보 및 인증 DB와 관리자가 등록하는 임의의 패키지 목록 DB로 구성된다.

먼저 사용자 정보와 인증에 사용된 테이블 관계는 인증 여부에 따라 해당 사용자의 기기정보를 보유한다.

패키지 목록 테이블 간의 관계 역시 패키지 그룹에 따라 패키지명 목록을 보유하게 된다. 애플리케이션 제어 시스템 ERD는 [그림 5]로 나타낸다.

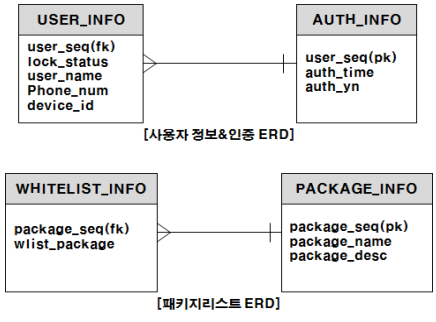


그림 5. 제어 시스템 ERD

5. 애플리케이션 제어 시스템 알고리즘

사용자가 클라이언트 실행 시 OTQ 방식의 사용자 인증을 한 뒤 사용자의 기기와 인증 정보로 인증 알고리즘과 애플리케이션 제어 알고리즘을 통해 해당 기기의 애플리케이션 실행 통제가 이루어진다. 애플리케이션 제어 시스템 알고리즘은 [그림 6]과 같이 설계하였다.

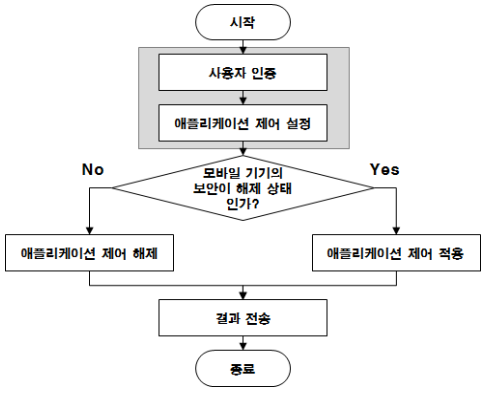


그림 6. 애플리케이션 제어 시스템 알고리즘

6. 사용자 인증 알고리즘

사용자 클라이언트 실행 시 실시간으로 코드 값을 생성하고 현재 시간과 비교 판별하여 인증을 수행한다. 정상 코드인 경우 인증 DB에 저장되고 일치하지 않는 경우 똑같은 과정을 반복 수행한다.

또한 저장된 결과를 통해 사용자의 인증 여부를 파악한다. 설계한 알고리즘은 [그림 7]로 나타낸다.

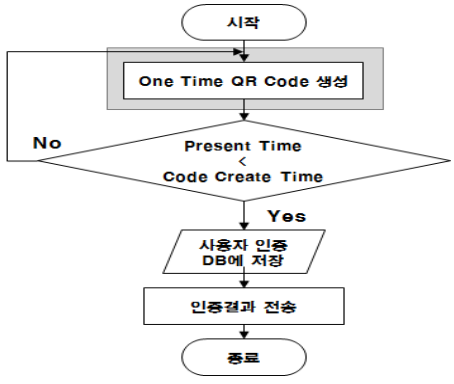


그림 7. 사용자 인증 알고리즘

7. 애플리케이션 제어 알고리즘

애플리케이션 제어기능 요청 시 패키지 목록 DB에서 허가된 패키지(White Package) 명들을 획득한다.

클라이언트는 실행하는 기능들의 패키지명과 일치하는 경우 정상 실행하고 일치하지 않는 경우 허가되지 않은 기능으로 판별하여 실행 통제 경고 후 해당 기능을 종료한다. 설계한 제어 알고리즘은 [그림 8]과 같다.

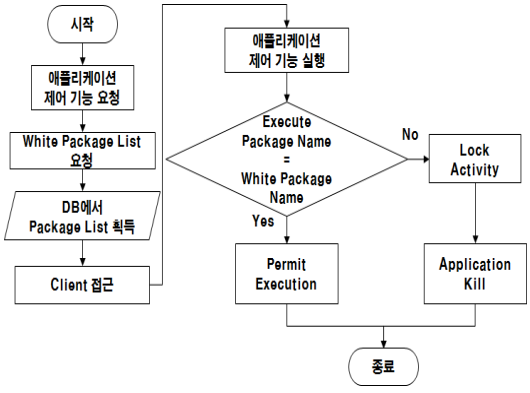


그림 8. 애플리케이션 제어 알고리즘

8. 애플리케이션 제어 시스템 순차다이어그램

제안하는 시스템은 사용자가 인증을 통해 기기를 등록하고 허가된 패키지 목록으로 보안 정책을 수립한다.

기기 상태에 따라 해당 클라이언트의 허가되지 않은 기능들을 통제하고 최종적으로 기능 수행 결과를 사용자에게 전송한다. 제안하는 제어 시스템의 순차다이어그램은 [그림 9]와 같다.

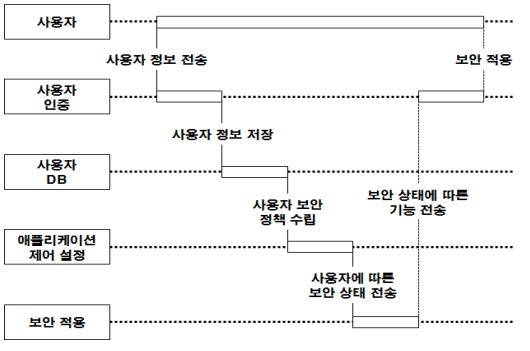


그림 9. 제어 시스템 순차다이어그램

8. 제어 시스템 프로그램 구조도

애플리케이션 제어 시스템은 사용자 클라이언트에서 OTQ를 통한 사용자 및 기기 인증을 통해 해당 기기의 보안 정책에 따라 모바일 기능의 실행을 통제한다.

관리자는 웹 서버를 이용해 등록된 기기의 정보를 확인할 수 있고 등록된 모바일 기기의 실행 통제 권한을 가진다. 또한 허용할 모바일 애플리케이션의 패키지명을 등록하여 보안정책을 수립한다.

사용자의 모바일 클라이언트를 통해 허가되지 않은 기능들의 실행을 제한한다. 제안 시스템의 프로그램 구조도는 [그림 10]으로 나타낸다.

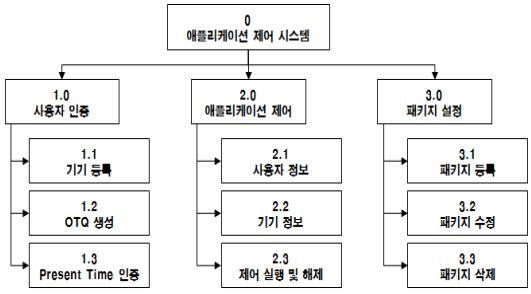


그림 10. 제어 시스템 프로그램 구조도

사용자 인증 기능은 클라이언트 실행 시 서버에 해당 기기의 최소한의 정보로 등록되고 ZXing 라이브러리를 사용하여 OTQ를 생성하고 현재 시간 값과 비교하여 인증 처리한다.

애플리케이션 제어 기능은 사용자의 허가되지 않은 모바일 애플리케이션을 통제하기 위해 해당 사용자의 기기 고유 ID를 통해 제어 기능을 실행 및 해제한다.

IV. 제어 시스템 구현 및 평가

1. 구현 환경

본 논문에서 구현한 애플리케이션 제어 시스템은 Windows 7 운영체제를 사용하였고, 개발 툴로 Eclipse와 Toad for Oracle을 사용하였으며, 화면 구성요소는 HTML, JavaScript로 구현하였다. 또한 모바일 클라이

언트는 Android 4.0을 사용하고 서버는 Spring과 iBatis Framework를 사용하였다.

2. 보안성 평가 및 분석

본 논문에서 제안한 애플리케이션 제어 시스템의 보안성 평가를 위해 국제공통평가기준(ISO/IEC) 관련 항목 테스트 방법을 통해 기존 시스템보다 보안성 향상을 검증하였다. 평가 항목은 [그림 11]과 같다.

그림 11. 보안성 평가 항목(ISO/IEC)

3. 애플리케이션 제어 시스템 구현

관리자 페이지는 로그인을 통해 등록된 관리자만 이용할 수 있다. 크게 모바일관리, 설정 메뉴로 구성되어 있으며 첫 화면은 모바일관리 페이지가 나오게 하였다.

모바일 관리 페이지는 등록된 사용자의 정보(이름, 휴대폰번호)를 볼 수 있고 해당 사용자의 모바일 기기를 제어할 수 있다. 구현한 관리 화면은 [그림 12]와 같다.

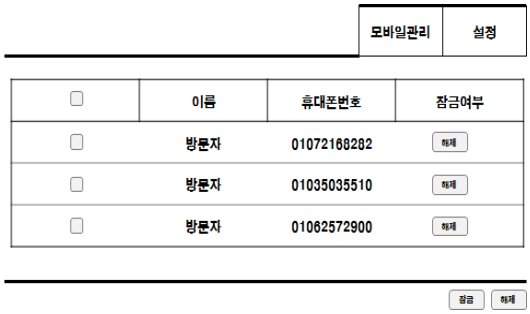


그림 12. 모바일 관리 화면

4. 모바일 클라이언트 구현

모바일 클라이언트는 모바일 애플리케이션 제어와 OTQ를 활용한 인증 기술을 적용하였다. 클라이언트는 서버와 GCM(Google Cloud Messaging) 푸시 서비스를 이용하여 데이터 교환을 하였다.

허가 기능 화면은 서버로부터 패키지 목록을 획득해 현재 허가된 기능을 사용자가 확인할 수 있도록 하였다.

애플리케이션 제어 기능이 동작되면 사용자가 허가되지 않은 기능들을 실행 시 “기능을 사용할 수 없습니다.” 문구가 있는 차단 액티비티가 호출되고 해당 기능은 강제로 종료되도록 하였다. 구현된 허가 기능화면은 [그림 13]으로 나타낸다.

그림 13. 허가 기능화면

5. 보안성 평가 및 분석

제안한 애플리케이션 제어 시스템의 보안성 평가를 위해 국제공통평가기준(ISO/IEC 15408) 관련 항목 테스트 방법 중 관련된 항목의 평가 방법을 통해 기존 시스템보다 보안성 향상이 되었음을 검증하였다. [표 1]은 보안성 평가 관련 항목이다.

표 1. 보안성 평가 관련 항목

특성	항목 명	평가항목의 목적	평가 방법
식별 및 인증	인증실패 처리	인증 실패를 탐지하고 대응행동을 수행하는지 평가	인증실패 시 대응 행동 수행 여부
	사용자 인증	행동을 허용하기 전에 사용자를 성공적으로 인증하는지 평가	사용자 인증 후에 행동이 허용되는지 여부
보안 관리성	보안기능 관리	인가된 관리자만 보안기능을 관리할 수 있게 제한하는지 평가	비인가자의 접근 차단 여부
	관리기능 수행	규정된 관리기능을 수행하는지 평가	규정된 관리기능 수행 여부
	보안역할 유지	보안기능이 인가된 역할을 유지하는지 평가	보안기능의 역할 유지 여부

관련 항목 평가를 통해 보안 취약점을 분석한 결과 기존 시스템은 두 항목에서 보안 취약점이 발생하였다.

사용자 인증 항목에서 카메라를 이용한 QR Code 복제 후 허위 인증이 가능하였고 관리기능 수행 항목에서 유해 애플리케이션의 패키지명을 수정하게 되면 비 허가 기능이 실행되는 보안 한계점이 발생하였다. 보안 취약점을 분석한 결과는 [표 2]로 나타낸다.

표 2. 보안 취약점 분석 결과

항목	취약점 분석	기존	제안
인증 실패 처리	인증 실패 시 대응 행동 수행	정상 작동	정상 작동
사용자 인증	QR Code 복제를 통한 허위 인증 여부	보안 취약	정상 작동
보안 기능 관리	관리자 계정을 통한 보안 설정	정상 작동	정상 작동
관리 기능 수행	유해 App 실행 여부	보안 취약	정상 작동
보안 역할 유지	클라이언트 삭제 시 보안 기능 유지	정상 작동	정상 작동

6. 보안성 평가 시나리오 시험 및 검토

설계 및 구현한 애플리케이션 제어 시스템이 정상적으로 기능을 수행하는지 보안성 평가 시나리오를 작성한 후 시나리오에 따라 평가를 진행하였다. 시스템의 평가 시나리오는 다음과 같다.

- 카메라로 QR Code 복제 후 인증 시도
- 비 허가 애플리케이션 패키지명 변경 후 동작 시도

보안성 평가 관련 항목 중 보안 취약점이 있는 사용자 인증과 관리기능 수행 항목을 나누고 사전 조건에 맞추어 테스트 절차를 진행하였으며 기대 결과를 얻고 정상적으로 동작함을 확인하였다.

테스트 결과 두 가지 항목의 보안성을 개선하여 기존 시스템보다 평균 40% 보안성이 향상된 결과를 확인하였다. 보안성 평가 결과는 [표 3]과 같다.

표 3. 보안성 평가 결과

항목	테스트 절차	기대 결과	결과
사용자 인증	-카메라로 QR Code 복제 -인증 시도	잘못된 코드경고, 인증 미처리	정상
관리 기능 수행	-패키지명을 변경한 유해 App 빌드 -제어 기능 실행 -유해 App 실행	차단 Activity 실행, 해당 기능 강제 종료	정상

V. 결 론

최근 모바일 기기를 소유한 개인 사용자가 급증하면서 기업 정보 유출에 의한 피해 사례가 급증하고, 자료 유출 사례 중 전·현직 종사원인 내부자에 의해 발생되는 건이 80% 이상을 차지하고 있어 내부정보 유출 방지체계에 대한 구축이 절실히 요구되고 있다.

이에 따라 기업은 MDM을 도입하였으나 MDM시스템은 사용자 기기에 해당 애플리케이션이 있는지 검색한 뒤 애플리케이션의 실행을 차단하는데 관리자가 비인가 애플리케이션의 패키지명을 등록하지 않으면 해당 기능의 통제가 되지 않는 단점이 있다.

따라서 본 논문에서는 보안성 향상을 위해 관리자가 허가한 애플리케이션의 패키지 목록을 얻어오고 해당 애플리케이션이 아니면 모든 보안 위협 요소의 실행을 차단하는 시스템을 설계 및 구현하였다.

제안하는 제어 시스템을 선계하기 위해 OTQ 인증 방식을 사용하여 사용자와 모바일 기기 인증 시 실시간으로 코드를 생성하고 시간 값을 비교하여 복제된 코드의 허위 인증을 보완하였다.

또한 모바일 기기의 기능을 유지하면서 관리자가 허용한 애플리케이션을 제외한 자료 유출이 가능한 모든 기능을 차단하여 비인가 애플리케이션 등록 전의 보안 사고를 예방하는 제어 시스템을 설계하였다.

본 논문에서 설계한 사용자 인증 알고리즘과 애플리케이션 제어 알고리즘을 토대로 보안성 향상을 위한 애플리케이션 제어 시스템을 구현하였다.

설계 및 구현한 제어 시스템의 보안성을 평가하기 위해 국제공통평가기준(ISO/IEC 15408)에서 관련 항목을

지표로 기존 시스템의 보안 취약점을 분석한 결과 기존 시스템의 보안 문제점 개선 및 정상 작동 확인을 통해 기존 시스템 대비 약 40% 보안성 향상을 검증하였다.

참 고 문 헌

[1] 김현홍, *스마트폰 환경에서 위치정보를 이용한 사용자 인증 기법 설계 및 구현*, 숭실대학교 석사학위논문, 2013.

[2] 이강현, 윤두식, "모바일보안을 위한 MDM의 효과적인 접근 방법," 정보보호학회논문지, 제23권, 제2호, pp.29-34, 2013.

[3] 유홍식, 선기현, 김성운, "공장 및 생산 자동화에 있어 안드로이드 기반의 보안성이 강화된 모바일 장비관리시스템 구현," 한국전자통신학회논문지, 제9권, 제7호, pp.779-789, 2014.

[4] Microsoft Corporation Architecture Guide for System Center Mobile Device Manager, 2008.

[5] 신숙조, 김선주, 조인준, "스마트폰에서 가상 디스크 플랫폼을 사용한 프라이버시 데이터 보호 방안," 한국콘텐츠학회논문지, 제13권, 제12호, pp.560-567, 2013.

[6] 이성권, 정창원, 주수종, "QR 코드를 이용한 의료정보 시스템 설계 및 구현," 한국인터넷정보학회논문지, 제16권, 제2호, pp.109-115, 2015.

[7] 조대제, 고재성, "QR 코드를 이용한 디지털 워터마크의 인식률 개선 방법 연구," 한국정보기술학회지, 제12권, 제10호, pp.173-179, 2014.

[8] 신동희, 장우성, "인터랙티브 마케팅커뮤니케이션 매체로써 QR코드 이용에 관한 연구 : 기술수용모델을 중심으로," 한국콘텐츠학회논문지, 제13권, 제3호, pp.76-86, 2013.

[9] 이상호, "QR코드 사용자의 수용 전, 후 행동에 영향을 미치는 요인," 한국콘텐츠학회논문지, 제11권, 제12호, pp.136-144, 2011.

[10] 허승표, 이대성, 김귀남, "모바일 환경에서 OTP 기술과 얼굴인식 기술을 이용한 사용자 인증 개선에 관한 연구," 정보·보안논문지, 제11권, 제3호, pp.75-84, 2011.

[11] 송성현, 김근욱, "국내외 OTP 표준화 동향", 정보보호학회논문지, 제22권, 제2호, pp.30-36, 2012.

[12] 한승진, "모바일 장치에서 OTP 기반의 바이오인식 보안을 위한 프레임워크," 한국컴퓨터정보학회논문지, 제17권, 제4호, pp.121-127, 2012.

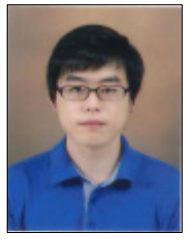
저 자 소 개

이 유 준(Yu-Jun Lee) 정회원

- 2015년 8월 : 가천대학교 모바일소프트웨어학과(석사)
- 2015년 8월 ~ 현재 : (주)제이컴정보

<관심분야> : 보안솔루션, 빅데이터, 모바일

장 영 환(Young-Hwan Jang) 준회원



- 2015년 8월 : 평생교육진흥원 멀티미디어학(공학사)
- 2015년 9월 ~ 현재 : 가천대학교 IT융합공학과 컴퓨터공학(석사)

<관심분야> : 모바일, 보안기법, 네트워크

박 석 천(Seok-Cheon Park) 정회원

- 1977년 2월 : 고려대학교 전자공학과(공학사)
- 1982년 2월 : 고려대학교 컴퓨터공학(공학석사)
- 1989년 2월 : 고려대학교 컴퓨터공학(공학박사)
- 1988년 ~ 현재 : 가천대학교 IT대학 컴퓨터공학과 정교수

<관심분야> : 네트워크, 모바일, 빅데이터