개인사용자 기반 스마트폰 원격관리 시스템 설계 및 구현

강성태* · 조인준**

Individual users based SmartPhone Remote Management System Design and Implementation

Sung-tae Kang* · In-june Jo**

요 약

최근 스마트폰 사용인구가 늘어나면서 휴대하기 쉽고, 각종 컨텐츠의 보관 및 이동이 쉬운 특성으로 인해 분실, 도난에 따른 개인 정보 유출뿐만 아니라 기밀 유출에 이르기까지 다양한 보안 위협 문제가 발생하고 있다.

본 논문에서는 고객을 대상으로 스마트폰의 다양한 보안 위협에 대응하기 위해 Mobile Device Management (MDM) 기술을 활용하여 사용자가 직접 관리가 가능한 스마트폰 원격관리 시스템을 설계하고 구현하였다. 이를 통해서 고객 스스로가 웹에서 스마트폰을 원격 관리하여 스마트폰의 분실, 도난에 따른 정보유출을 방지 할 수 있고, 사용제어 및 모니터링이 가능하다.

ABSTRACT

By increasing of the population that uses smartphones, problems such as the leakage of private and confidential information due to portable and easy to store and movement of diverse contents occur for a variety of security threats.

In this report,it provides helpful information to customers in order to respond various security threat by implementing and designing an remote administration system with using Mobile Device Management (MDM), technology. As a result, customers themselves can prevent information spill by managing remotely from WEB due to the lost and stolen. It is also possible to use control and monitoring.

키워드

모바일 단말관리, 원격관리, 스마트폰, 개인정보

Key word

Mobile Device Management (MDM), Remote Management, SmartPhone, Privacy

* 준회원 : 배재대학교 컴퓨터공학과(교신저자, stkang90@gmail.com)
** 정회원 : 배재대학교 컴퓨터공학과

접수일자 : 2012. 10. 15
심사완료일자 : 2012. 11. 04

Open Access http://dx.doi.org/10.6109/jkiice.2012.16.12.2675

Ⅰ. 서 론

최근 스마트폰 사용 인구가 늘어나면서 휴대하기 쉽고, 각종 컨텐츠의 보관 및 이동이 쉬운 특성으로 인해 분실, 도난에 따른 개인정보 유출뿐만 아니라 기밀 유출에 이르기까지 다양한 보안 위협에 대한 강화대책으로 관리의 필요성이 대두되면서 MDM 시스템이 스마트폰 보안의 핵심 요소가 되고 있다.[1][2]

MDM(Mobile Device Management)은 Over The Air (OTA)를 이용하여 언제 어디서나 모바일단말기가 켜진 상태로 있으면 원격에서 모바일 기기를 관리할 수 있는 통합시스템이다.[3]

현재 상용화 되어 있는 몇몇 MDM 솔루션을 살펴보면 기업이 자사의 고객 및 직원을 대상으로 중앙관리를 통해 스마트폰을 관리한다. 이러한 형태의 MDM에서 기업은 중앙관리를 통하여 많은 이점을 얻을 수 있지만 반면에 사용자들은 기업으로부터 사생활 침해라는 문제점이 발생한다. 사생활침해의 사례로 개인의 위치정보가 로그로 계속 쌓이고 있고, 관리자는 사용자의 동의 없이도 스마트폰을 원격 제어할 수 있다. 이는 스마트폰 사용자의 사생활이 침해당하는 문제를 지니고 있다.[4] 이러한 문제점을 해결하기 위하여 기업의 고객 및 직원뿐만 아니라 모든 스마트폰 사용자 스스로가 웹에서 스마트폰을 원격 관리하여 단말기의 분실, 도난에 따른 정보유출에 대비 하고 스마트폰 사용에 대한 제어와 모니터링을 할 수 있는 시스템이 요구되고 있다.

본 논문에서는 MDM을 활용하여 스마트폰 사용자 스스로가 원격으로 다양한 정보를 안전하게 얻고, 다양한 보안 위협에 대응할 수 있는 스마트폰 원격관리 시스템 설계 및 구현 방안을 제안하고자 한다.

Ⅱ. 국내 MDM 현황

스마트폰 보안이 중요시 되고 있는 만큼 국내 MDM 제품들도 다양한 보안기능들을 앞세워 시장을 선점하고 있다. 국내 대표적인 MDM 제품들은 모바일데스크(삼성), 모바일키퍼(지란지교소프트), 터치엔가드(루멘소프트) 등이 있다.

각 제품들의 운영정책과 관리시스템들은 달랐지만 서버구성은 MDM서버, 파일서버, 데이터베이스서버, WAS 등 공통된 구성을 갖고 있었다.

국내제품들의 관리시스템은 웹사이트에 접속해서 스마트폰의 정보, 기업 정보 등을 입력하여 회원가입하고 스마트폰에서 앱을 다운받아 로그인을 하면 각 기업의 관리자가 중앙 관리를 통해 자사의 고객 및 직원들을 관리해주는 시스템이다.

스마트폰 관리 방법은 스마트폰 분실을 예로 제품의 웹사이트에 접속하여 스마트폰에 로그인된 계정으로 로그인 한다. 로그인 후 MDM 서버에 접속하여 해당 스마트폰의 정보를 찾아 명령을 전송하고 수행 결과를 MDM서버에 저장하여 다시 웹사이트에서 확인 할 수 있다. 이외에도 기업의 관리자에게 요청하여 결과를 받아보는 방법도 있다.[5]

이 시스템의 단점은 서론에 언급한대로 사생활 침해 문제점이 발생한다. 제품에 따라 관리자가 관리 할 수 있는 기능을 제한하고 사용자가 관리할 수 있는 기능을 제한한 제품이 있는가 하면 관리자만 관리 할 수 있는 제품이 있기 때문에 모든 제품이 이러한 문제점을 갖는다고는 단정 지을 수 없다.

국내 MDM의 주요 기능을 정리하면 표 1-2 와 같다. 이들 내용을 요약하면 모바일 환경에서의 원격 또는 중앙 관리를 통해 단말기의 분실, 도난을 방지하고, 카메라 및 USB 등의 디바이스 제어를 통해 정보유출을 방지할 수 있는 통합 모바일 보안 기능들을 갖추고 있다.[5][6][7]

표 1. 모바일 보안 기능
Table. 1 Mobile Security Function

모바일 보안	
원격 데이터 보호	원격 데이터 백업
	데이터 삭제 및 공장초기화
	비밀번호 강제 설정
디바이스 제어	카메라, 녹음기 사용차단
	Wifi, 블루투스, 3G 차단
	USB 테더링, 메모리카드 제어
네트워크 보안	송수신 데이터 암호화
출입 통제 보안	GPS, 기지국, AP 위치
	사내 단말기 자동 통제
분실 도난 대비	원격 화면 잠금 제어
	단말기 위치추적
	비밀번호 오류 횟수 제한
	회수 요청 및 긴급통화

표 2. 모바일 관리 기능
Table. 2 Mobile Management Function

모바일 관리	
중앙관리	사용자 및 단말기 인증 및 조회
	Agent 설치 및 상태 조회
	사용자별, 그룹별 정책관리
	조직도 연동, S/W 배포관리
Application 관리	설치프로그램 현황 파악
	특정 APP 실행 차단
Back up 기능	중요데이터 백업 및 삭제
	원격 데이터 복원
리포트 및 통계	단말기분실 추적 리포트
	사용자, 단말기, 앱 사용현황

모바일 보안기능은 디바이스 제어와 네트워크 보안으로 모바일을 통한 자료 유출을 방지하며, 원격 데이터 보호, 분실 도난 대비 등을 통해 단말기 분실 시 타인에 의한 기업데이터 접근을 차단함으로써 안전하게 데이터를 보호 할 수 있다.

모바일 관리기능은 관리자만을 위한 기능으로 중앙관리를 통해 새로운 사용자를 추가하거나, 사용자별, 그룹별로 정책을 관리하고 사내 앱을 배포한다. 또 단말기 사용현황, 사용자, 앱, 에이전트 등에 대한 통합적인 관리 및 모니터링을 할 수 있다.

모바일 보안 기능, 모바일 보안 기능 대부분을 기업의 관리자가 관리하며 사용자가 직접 관리할 수 있는 부분은 극히 일부분이다.

Ⅲ. 스마트폰 원격관리 시스템 설계 및 구현

일반적으로 스마트폰 원격 관리시스템의 전체적인 구성도는 그림 1 과 같다. 그림의 순번은 서버와 스마트폰 간의 명령 전송 과정을 요약한 것이다.[8]

① 스마트폰 분실을 예로 사용자가 관리 웹사이트에 접속하여 서버에게 해당 디바이스에 위치요청을 한다.

② MDM 서버는 해당 스마트폰을 식별 후 위치요청 명령을 데이터베이스에 담는다.

③-④ 식별된 스마트폰에 명령이 있음을 알린다.

⑤-⑥ 스마트폰은 MDM서버에 접속하여 명령 목록을 가져와 실행하고 결과를 관리페이지에 반환한다.

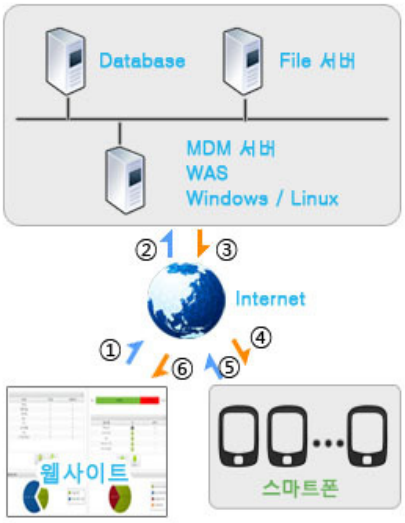

그림 1. 시스템 구성도
Fig. 1 System configuration

3.1. 서버 설계 및 구현

본 논문에서 설계하고 구현한 스마트 폰 원격관리 시스템의 서버는 MDM 서버, 파일서버, 데이버베이스서버 3개로 구성되어 있다. MDM 서버환경은 JAVA를 기반하여 설계하였다. 안드로이드 시스템의 기반이 JAVA로 이루어져 있기 때문에 SSL 통신 시 호환성을 위해 서버와 클라이언트 모두 JAVA를 기반으로 하였다.

MDM 서버의 구동 방법은 그림 2와 같은 플로 차트를 따른다.

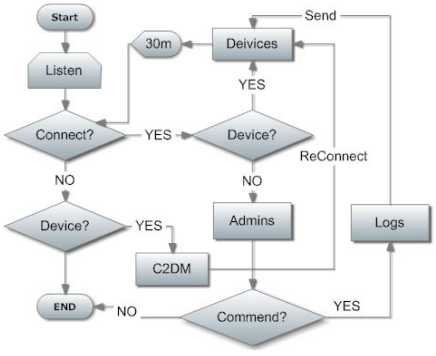

그림 2. MDM서버 플로차트
Fig. 2 MDM Server Flowchart

서버는 모바일 기기 및 사용자들의 아이디를 식별하여 연결을 관리하며 명령전송, 로그저장, 재연결 요구 등을 담당한다.

서버에 접속된 모바일 기기들은 30분마다 연결 체크를 한다. 연결 종료 시 구글의 푸시알림인 푸시 서버 C2DM(Cloud To Device Messaging)을 이용하여 재 연결을 요구한다.

스마트폰에 명령 전송 시에는 서버 접속 후 디바이스 아이디를 식별하여 데이터베이스에 명령로그를 남기며 명령이 담긴 데이터베이스 Table의 색인 값을 해당 스마트폰으로 전송한다. 색인 값을 받은 스마트폰은 다시 서버에 접속 후 자신의 디바이스 아이디로 식별되는 데이터베이스 Table에서 색인 값을 찾아 명령을 실행한다.

명령어 전송시 바로 스마트폰으로 명령을 전송하지 않고 데이터베이스를 거쳐 명령을 전송하는 이유는 명령 전송시 스니핑을 방지하고, 대용량의 데이터 전송 시 과부하로 인한 연결 지연문제를 방지하기 위한 목적이다. 또 모바일 단말의 전원이 종료되어있을 때 전송된 명령이 누락되므로 전원이 켜진 후에 전송되었던 명령들을 실행 할 수 있게 하기 위해서이다.

표 3 은 서버와 스마트폰 간의 전송된 명령을 간략히 정리한 것이다. AToMCmd#1269에서 AToMCmd는 관리자가 모바일에게 명령을 한다는 의미이고, 1269는 식별자로 자신의 디바이스 아이디 데이터베이스 Table 에서 1269번째 명령을 읽어 오면 된다. 명령은 LocationTrace #3G로 위치 추적을 의미하고 3G의 네트워크 위치를 요청했음을 의미한다. AToMCmd#1270은 위 명령의 응답을 의미한다.

표 3. 식별 색인 전송과 데이터베이스 로그
Table. 3 Identify Index and Database Log

명령어 전송	데이터베이스 로그
AToMCmd#1269	AToMCmd#LocationTrace#3G
MToACmd#1270	MToACmd#MtoALocationUpload#36.2 323054@126.9441184

파일서버는 웹 업·다운로드 방식으로 웹 서버를 통해 파일 백업 및 복원 시에 접근 할 수 있게 설계되었다.

데이터베이스 서버의 데이터베이스는 회원관리, 스마트폰 정보, 명령 로그 세 부분으로 나뉜다. 자세한 내용은 그림 3, 그림 4 을 통해 알 수 있다.

Field	Type	Key
num	int(11)	UNI
mDeviceId	varchar(45)	PRI
adminId	varchar(30)	
mAuthCode	varchar(15)	
mName	varchar(15)	
mPhone	varchar(15)	
mPushKey	varchar(300)	
mAppVer	varchar(10)	
mDeviceNetworkOperator	varchar(20)	
mRecentUpdateDate	varchar(25)	

그림 3. 스마트폰 정보 스키마
Fig. 3 Smartphone information schema

Field	Type	Key
num	int(11)	PRI
connectMode	varchar(5)	
deviceType	varchar(1)	
readCheck	varchar(1)	
mCmd	text	
actDate	varchar(25)	

그림 4. 명령 로그 스키마
Fig. 4 Commend log schema

구현된 서버의 모습은 그림 5와 같다. 접속한 사용자 및 모바일 기기들을 볼 수 있으며, 연결 체크 로그와 명령 전송 로그를 실시간으로 확인 할 수 있게 구현하였다.

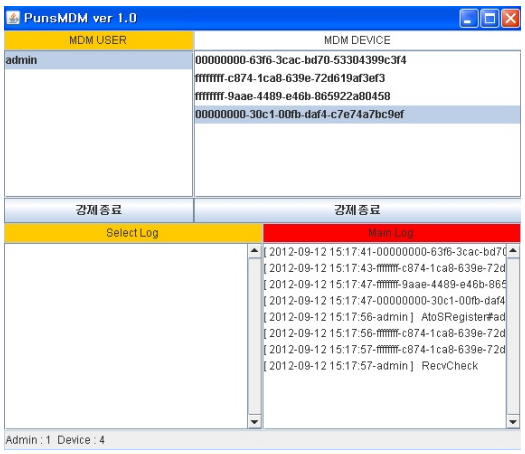

그림 5. MDM 서버 구현
Fig. 5 MDM Server Implementation

3.2. 클라이언트 설계 및 구현

스마트폰 원격관리 시스템의 클라이언트는 JAVA 기반의 안드로이드 SDK로 설계하였다. 사용자가 직접 실행해야 되는 어플리케이션과 달리 서비스 기반의 어플리케이션으로 처음 설치 시 간단한 등록절차를 제외하고는 자동으로 백그라운드에서 실행되어 서버와의 연결을 유지한다.

MDM 클라이언트의 구동 방법은 그림 6과 같은 플로차트를 따른다.

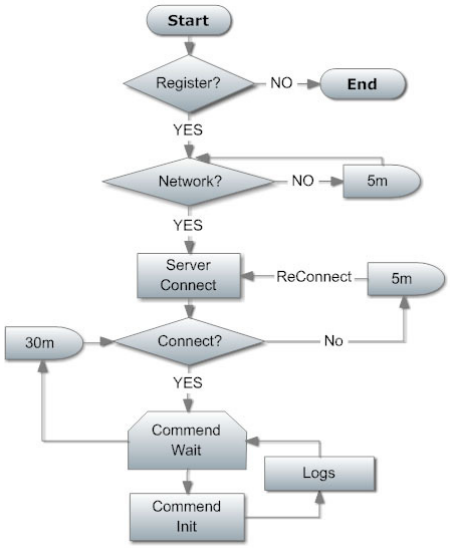

그림 6. MDM 클라이언트 플로차트
Fig. 6 MDM Client Flowchart

스마트폰은 3G, 4G, Wifi 등 인터넷과 연결 시에 서버에 자신의 디바이스 아이디를 등록하고 임의로 정해준 시간마다 패킷을 교환하며 서버와의 연결을 유지한다. 패킷 응답하지 않거나 지연될 경우 스마트폰이 재 연결을 할 때 까지 기다리는 것이 아니라 C2DM을 이용하여 재 연결을 요구하는 푸시 메시지를 전달한다.[9]

스마트폰과 웹사이트 간의 통신을 할 때 MDM서버를 통해 통신을 하면 빠른 속도의 양방향의 통신이 가능하고, 메시지의 손실률이 적다. 그러나 스마트폰의 인터넷 연결이 원활하지 않아 실시간으로 응답을 할 수 없을 경우 지연시간 동안 응답을 기다려야 한다는 단점이 있다. 이를 해결하기 위해 C2DM을 사용한다.

C2DM은 빠른 속도는 아니지만 단방향의 통신으로 지연시간 동안 응답을 기다리지 않고 MDM서버를 대신해 메시지를 전달해준다. 이외에도 C2DM은 스마트폰이 종료되어 서버에 연결되어 있지 않을 때도 MDM 서버대신 C2DM을 이용하여 메시지를 전달한다. 단방향 통신의 단점으로 웹사이트에서 결과를 볼 수는 없지만 원활한 인터넷 연결이 될 때 손실 없이 전송된 명령을 실행 할 수 있다.

두 통신 모두 SSL 통신으로 송수신 데이터를 암호화하서 전송하므로 모바일을 통한 자료유출을 방지 한다.

어플리케이션 상에서의 명령 메시지를 받고 동작하는 과정은 안드로이드 SDK의 레퍼런스만으로도 쉽게 설계 및 구현이 가능하였다. 안드로이드 SDK 에서는 개발자들이 쉽게 MDM을 개발하도록 대부분의 기능적 부분을 레퍼런스로 제공한다.

구현된 클라이언트는 서비스 기반의 어플리케이션으로 백그라운드에서 실행중임을 그림 7을 통해 알 수 있다. 사용자의 직접적인 실행은 불가능하고, 스마트폰 내에서 인터넷 연결을 체크하여 인터넷 사용이 가능할 때 자동으로 서버에 접속하여 연결 관리 및 명령을 수행한다.

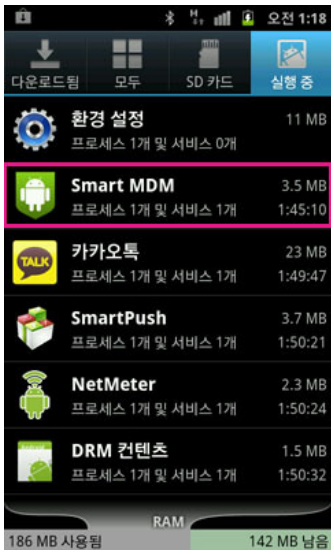

그림 7. MDM 클라이언트 구현
Fig. 7 MDM Client Implementation

3.3관리 웹사이트 관리 설계 및 구현

스마트폰 원격관리 시스템의 관리 웹사이트는 JAVA 기반의 MDM서버에 접속하기 위해 웹서버의 JSP(Java Sever Page)를 통해 접속하여 명령을 전송하고 결과를 받아와 보여준다.

관리 웹사이트의 구동 방법은 그림 8과 같은 플로 차트를 따른다.

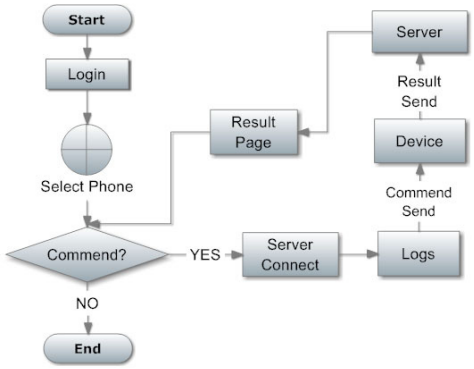

그림 8. 관리 웹사이트 플로차트
Fig. 8 Management Website Flowchart

관리 웹사이트는 간단한 로그인절차를 거친 후 등록된 스마트폰을 선택하고 사용자가 원하는 명령 전송 시에만 서버에 접속하여 명령 전송 후 결과를 받고 연결을 종료한다. 명령 전송시 매번 서버에 다시 접속하는 이유는 웹서버의 특성상 소켓 통신이 유지되고 있는 동안에는 다음 명령을 기다리고 있어 결과페이지를 보여줄 수 없기 때문에 연결 종료 후 결과페이지를 보여주기 위해서이다.

스마트폰을 관리하기 위해서는 기업의 관리자가 아닌 사용자 스스로가 직접 아래 표 4에 있는 기능 모두 사용하여 원격관리 할 수 있다.[10] 사용자 스스로가 관리자가 되어 스마트폰을 관리하므로 번거로울 수도 있지만 개인정보가 다른 사람을 거치지 않고 관리 할 수 있음으로 안전하게 사용이 가능하다. 또 기업의 직원 및 고객뿐만 아니라 모든 스마트폰 사용자가 사용이 가능하므로 기존 MDM의 사용 범위보다 더 넓어진다.[11]

표 4. 스마트폰 원격관리 시스템 기능
Table. 4 Smartphone Remote Management System Function

모바일 보안 기능	
원격 데이터 보호	내·외장 메모리 파일 다운로드
	내·외장 메모리 파일 삭제
	내·외장 메모리 파일 초기화
디바이스 제어	카메라, 녹음기 사용차단
	Wifi, 블루투스, 3G 차단
	디바이스 리소스 사용현황
디바이스 보안	강제 화면잠금
	강제 비밀번호 변경
	강제 공장초기화
분실 도난 대비	디바이스 추적 및 경로확인
	회수요청
	공장초기화
전화	부재중 전화기록 확인
	전화번호부
	전화번호부 백업
	전화번호부 삭제
메시지	읽지 않은 메시지 확인
	메시지 보내기
	메시지 전체 삭제
앱	최근사용앱 리스트
	실행 중 프로세스 종료
	설치된 앱 리스트 확인
알림	벨, 진동 울림
	무음, 진동, 벨 모드 전환

관리 웹페이지는 웹서버는 PHP와 JSP를 혼용하여 구현하였다. 웹 기반으로 구현되어 다양한 플랫폼에서 스마트폰 관리가 가능하다. 그림 9는 구현된 관리페이지로 스마트폰의 데이터를 백업하는 과정이다.

그림 9. 관리 웹사이트 구현
Fig. 9 Management Wetsite Implementation

V. 결 론

네트워크와 통신 서비스의 발전으로 점점 더 모바일 기기들이 복잡해지고 있고, 모바일 기기를 통해 제공되는 서비스도 다양해지고 있다. 사용자는 또한 편리함 속에서 안전하게 보호 받기를 원한다.

본 논문에서는 복잡하고 다양해진 모바일 단말을 기업에서 관리 받지 않고 사용자 스스로가 개인정보를 보호하면서 스마트폰을 관리하기 위한 방안으로 스마트폰 원격관리 시스템을 개발했다. 제안한 스마트폰 원격관리 시스템에서는 서버와 클라이언트 간의 보안 통신 환경을 개선하고, 타인에게 관리 받는 기존 MDM 관리 시스템을 보강하여 사용자 스스로가 직접 스마트폰을 관리 할 수 있게 함으로써 사용자의 개인정보를 보다 더 안전하게 보호 할 수 있도록 관리시스템을 개선하였다.

향후 연구로는 수집한 데이터를 분석 및 가공하여 사용자가 더욱 편리하게 사용하도록 최적화하여 사용자가 항상 최상의 환경에서 보다 더 안전하게 스마트폰을 관리할 수 있는 시스템을 구현할 것이다.

참고문헌

[1] 김기영, 강동호, “개방형 모바일 환경에서 스마트폰 보안기술”한국정보보호학회, 제 19권, 제5호, 2009. 10

[2] 박현아, 최재탁, 임종인, 이동훈, “모바일 환경에서의 개인정보 위협 분석 연구”, 정보보호학회지, 제 17권, 제 4호, pp.56-73, 2007. 8

[3] http://www.a3security.com

[4] 이호근, 이상훈, “정보 프라이버시의 향후 연구방향 도출을 위한 선행연구 분석”, 정보화정책, 제 16권, 제 2호, pp.3-26, 2009

[5] http://www.mobiledesk.co.kr

[6] http://www.mobilekeeper.co.kr

[7] http://touchen.lumensoft.co.kr

[8] Joon-Myung Kang, Hong-Taek Ju, Mi-Jung Choi, James Won-Ki Hong, and Jun-Gu Kim, ″ OMA DM-based Remote Software Fault Management for Mobile Devices″, International Journal of Network Management (IJNM), vol. 19, no. 6, pp. 491-511, Nov./Dec. 2009.

[9] 나사랑, 신수연, 권태경, “모바일 ID를 저장하여 관리 및 이용하고 있는 스마트폰의 사용자 인증 동향”, 정보보호학회지, 제. 21권, 제 4호, pp.22-31, 2011. 6

[10] 김상욱, “유비쿼터스 환경의 모바일 단발 보안 관리 기술 개발”, 정보보호학회지, 제 19권, 제2호, pp.74-81, 2009. 4

[11] http://www.puns.kr

저자소개

강성태(Sung-Tae Kang)

2013년 2월: 배재대학교 컴퓨터공학과 학사

※관심분야 : 시스템보안, 정보보호

조인준(In-June Jo)

1982년 2월: 전남대학교 계산통계학과 학사
1985년 2월: 전남대학교 전자계산학과 석사
1999년 2월: 아주대학교 컴퓨터공학과 박사
1983년 ~ 1994년: 한국전자통신연구원 선임연구원
1994년 1월 ~ 현재: 배재대학교 컴퓨터공학과 교수
※관심분야 : 정보보호, 컴퓨터 네트워크 보안, 전산조직응용