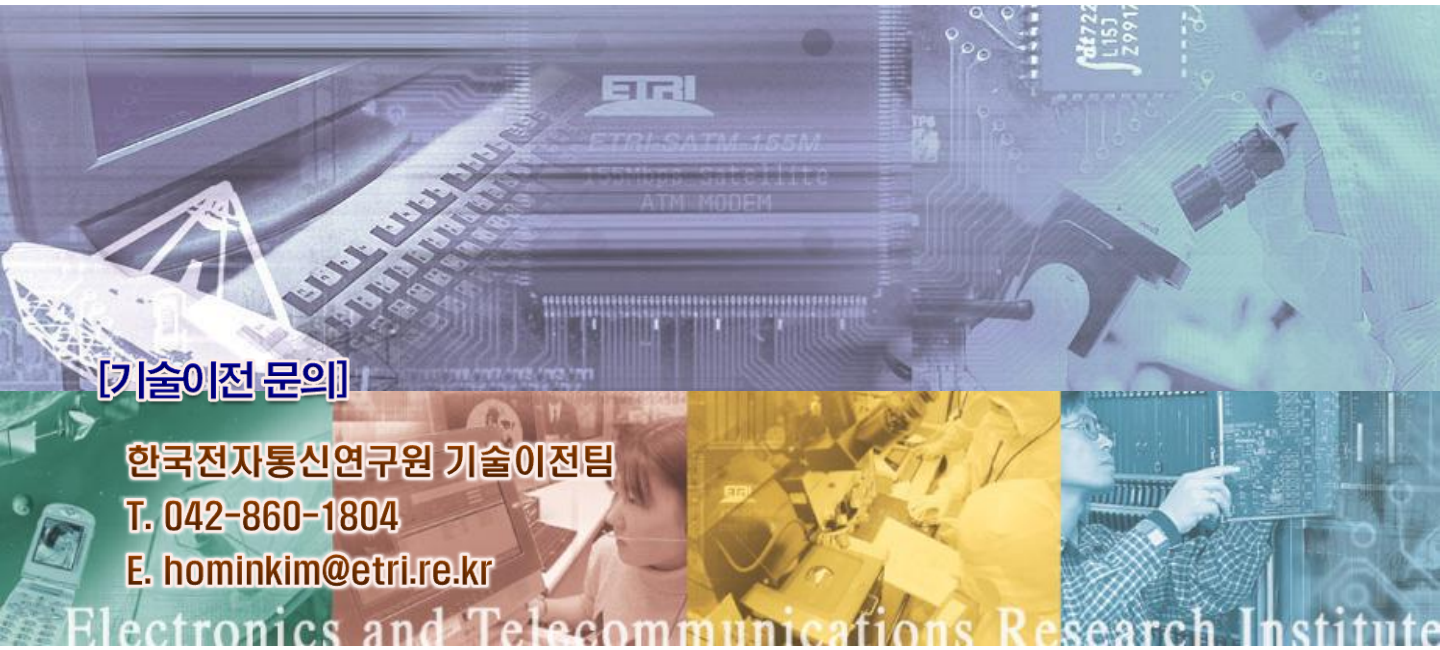
모바일 단말기용 자체방어 기술



[기술이전 문의]
한국전자통신연구원 기술이전팀
T. 042-860-1804
E. hominkim@etri.re.kr

Electronics and Telecommunications Research Institute

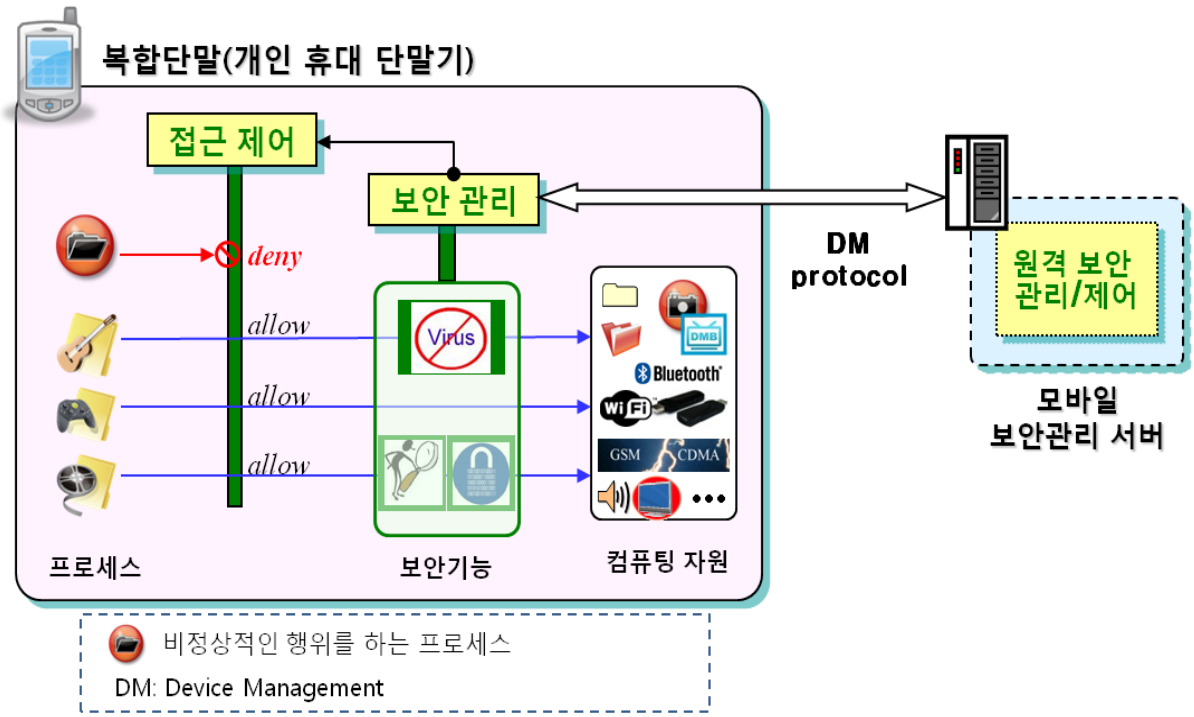
한국전자통신연구원

TECHNOLGY BRIEF 기술소개서

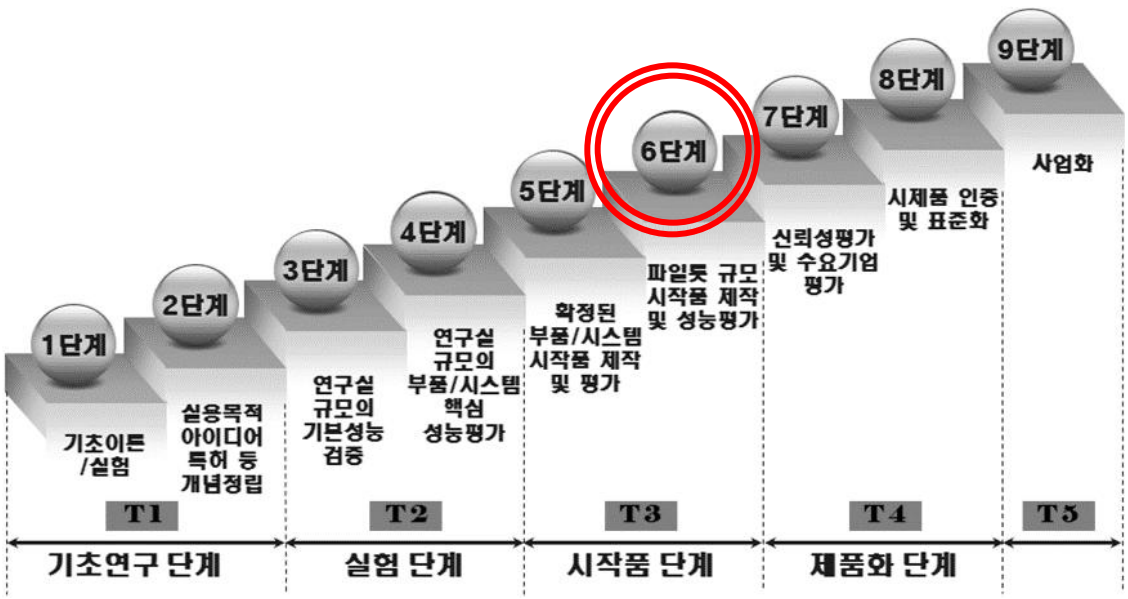
모바일 단말기용 자체방어 기술

기술개요

윈도우 모바일(Windows Mobile) 플랫폼을 기반으로 하는 PMP, PDA, 스마트 폰 등의 모바일 단말에 적용되며, 모바일 단말에 대한 바이러스 등의 외부 공격을 효과적으로 방어할 수 있는 접근제어 기능과 보안기능들을 효과적으로 관리/제어할 수 있는 보안관리기능을 제공하는 기술임



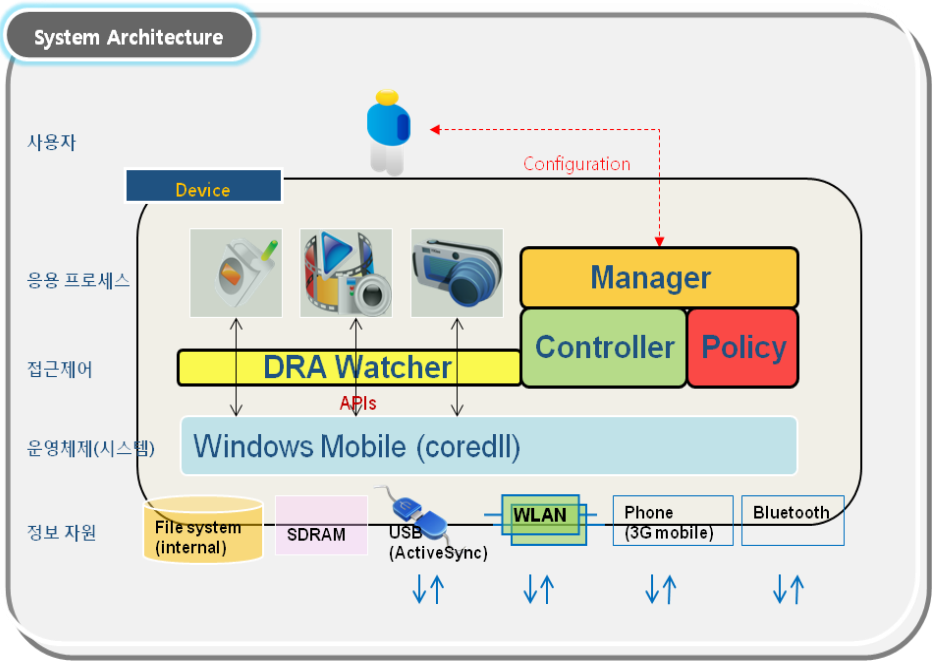
기술 개발 상태 : 6단계



TECHNOLGY BRIEF 기술소개서

모바일 단말기용 자체방어 기술

기술설명



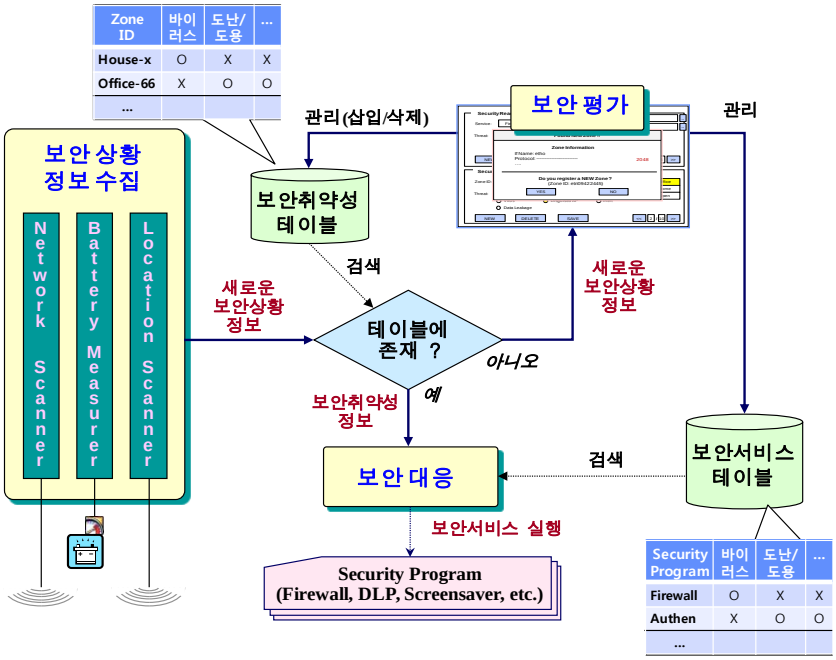
▶ 모바일 단말기용 접근제어기술

- 단말자원을 접근하는 프로세스 모니터링 기술 (단말자원: 파일, 프로세스, WiFi, SMS, Voice Cal, HSDPA, USB 등)
- 정책기반의 단말자원 접근제어 기술
- 접근제어 기술은 파일, 프로세스, 통신 인터페이스 (예, WiFi, USB, 3GPhone, SMS, HSDPA)와 같은 컴퓨팅 자원을 프로세스가 접근하는 것을 모니터링하고 제어함으로써 중요 데이터가 유출되는 것을 방지하고, 보안에 위협이 되는 비정상적인 접근행위를 탐지하고 차단하는 기능을 제공함. 접근제어 기술은 DRA(Dynamic Resource Access) Watcher, Controller, Manager 등 세 개의 컴포넌트로 구성됨

  - Watcher : 단말자원접근 감시 및 제어기능을 담당함. 모든 프로세스들이 단말의 정보 자원과 인터페이스에 접근할 때마다 Controller 에게 보고하고, Controller 의 명령에 따라서 단말자원접근을 허용/불허함

  - Controller : 전체 기능의 중심(main)으로서, Watcher로부터 수집한 정보와 Policy에 구축된 정책을 바탕으로 모든 제어 결정을 수행함. 또한 처리결과에 대한 보고, 모니터 및 로깅 기능도 담당함

  - Manager & UI : 주로 사용자 인터페이스 기능을 담당하여 Controller로부터 입출력 되는 정보를 사용자와 인터페이스 할 수 있는 기능을 제공함



▶ 모바일 단말기용 보안재구성 기술

- 상황정보 수집 및 보안상태 관리 기술 (상황정보: 모바일 단말의 현재 위치 및 접속한 네트워크 정보 등)
- 보안 상황기반의 보안서비스 자동구성 기술
- 위 그림은 보안관리기술에서 복합단말 보안재구성기능의 구조를 도시한 그림임. 세부적으로 **보안상황정보 수집과 보안평가 그리고 보안대응 모듈로 구성**됨. 보안상황정보수집 모듈은 모바일 단말이 접속한 네트워크, 위치 등의 상황정보를 수집하는 모듈이고, 보안평가 모듈은 새로운 상황정보가 발견될 때 사용자의 도움을 받아 그 상황에 대한 보안상태를 평가하는 모듈이며, 보안대응 모듈은 현재의 보안상태에 맞는 보안 기능을 재구성시키는 모듈임. 보안관리기술은 또한 프로토콜을 사용하여 복합단말의 보안기능을 원격에서 제어하고 관리하는 원격보안관리 기능을 제공함. **원격 보안관리기능은 복합단말이 도난 되거나 보안상황의 변경되었을 때, 정책을 기반으로 하여 복합단말의 접근제어 및 데이터소거 기능을 제어**함. 또한 암호화할 보호데이터와 보안상황정보 등의 보안정책을 원격으로 관리할 수 있음

▶ 모바일 단말기용 원격보안관리 기술

- 모바일 단말의 자원 (GSR, GPRS, 카메라, USB, WiFi 등)에 대한 원격제어
- 모바일 단말에 저장된 파일에 대한 원격 소거(Data Wiping)
- 정책기반의 보안재구성의 보안정책 구성

기술적 경쟁력

- 접근제어 기술은 독립적인 모듈로 제공하기 때문에, OS에 영향을 주지 않고, 윈도우 모바일 플랫폼 기반의 모바일 단말의 컴퓨팅 자원에 대한 접근을 모니터링하고 제어할 수 있는 범용 보안 모듈을 제공함
- 또한, 사용자 친화적인 기술로써, 접근제어 정책의 설정이 복잡한 기존의 기술과 차별성이 있음
- 보안관리 기술은 모든 보안 SW를 대상으로 자동구성 서비스를 지원하는 기술로써, 단일 보안 SW(예, 방화벽)의 자동구성만을 지원하는 기존의 기술보다 확장성에서 우수함
- 또한, 단말의 보안을 원격으로 관리할 수 있기 때문에 비즈니스용 복합 단말과 같이, 수준 높은 보안기능과 통합적인 보안관리를 요구하는 복합 단말의 요구사항을 완벽하게 충족시킬 수 있음

적용분야

▶ **PMP, PDA, 스마트 폰 등 개인 모바일 단말의 보안성 구축에 활용**

▶ **중요 데이터 유출 방지 및 비정상 행위 탐지를 제공함으로써 모바일 단말의 침해방지를 제공하는 보안 소프트웨어로써 활용**

▶ **모바일 단말에서 기 개발된 보안 프로그램(IDS, Firewall, Virus Scan, 인증 프로그램 등)의 효과적이고 효율적인 제어/관리를 위한 통합 보안 관리 소프트웨어로써 활용**

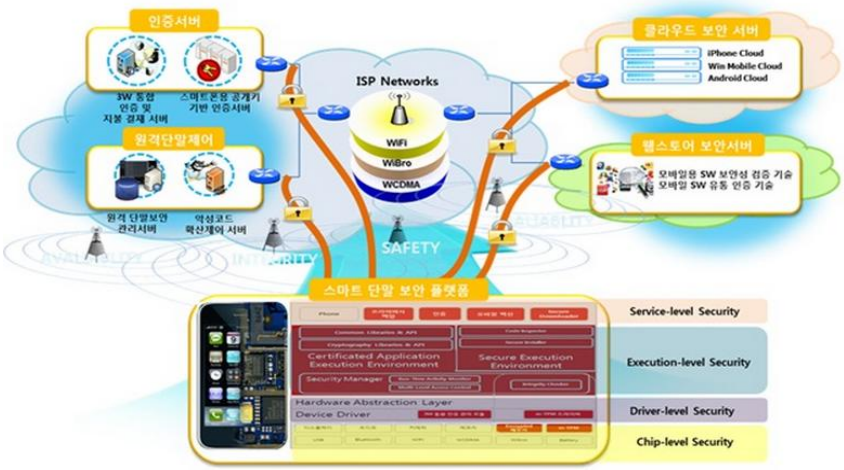
▶ **모바일 단말에서 사용자 편의성 제공을 위한 상황 기반의 응용 프로그램 자동 관리 소프트웨어로써 활용**

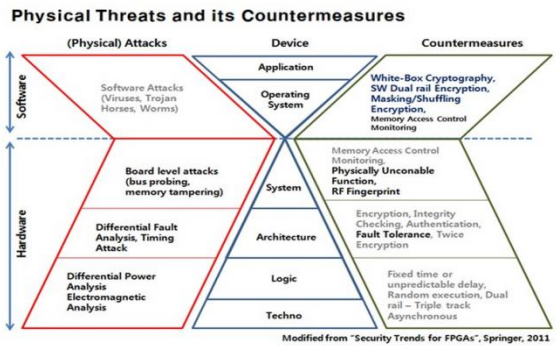
관련 지재권 현황

No.	국가	출원번호(출원일)	상태	명칭
1	KR	2007-0133405 (2007.12.18)	등록	개인용 컴퓨터에서 보호정보의 외부유출을 실용적으로 방지하는 방법 및 그 장치
2	KR	2008-0131564 (2008.12.22)	등록	모바일 통신 단말을 위한 보안 서비스 재구성 방법 및 그 장치
3	KR	2009-0117903 (2009.12.01)	등록	휴대용 컴퓨팅 단말의 시스템 자원 보안 장치 및 보안 방법
4	KR	2009-0117193 (2009.11.30)	공개	복수의 정보 영역을 포함하는 정보 단말 및 그것의 접근 제어 방법
5	US	12/571873 (2009.10.01)	공개	정보 단말기의 보안 관리 장치 및 방법

기술동향

각 앱스토어에 맞춰 개별적으로 진행되는 현재의 애플리케이션 개발작업이 2014년 경에는 대부분 사라지고 HTML5와 브라우저로 플랫폼에 구애받지 않는 개방적 웹앱 개발환경으로 전환





국내 기술

- **안티바이러스, 파이어월 등 대체 가능한 보안 제품은 존재**하나, 접근제어 보안 기술을 상용으로 제공하는 국내주도 벤더는 아직 없음. 모바일 단말에서 보안재구성 기술 및 원격보안관리기술을 개발하고 있는 국내 벤더는 찾아볼 수 없음

- 접근제어기술은 현재 주로 add-on 소프트웨어 형태로 제공할 수 있는 독립적인 보안 기능으로 개발되고 있기 때문에 **접근제어, 인증/인가, 암호화 등 최신 보안 요소 기술들을 유연하게 적용할 수 있음**. 국내의 접근제어기술은 구조상으로 OS 자체에서 제공되는 보안기능에 비하여 취약하며 OS기반 기술 부재로 인하여 적용성, 호환성이 낮음. 보안재구성기술 및 원격보안관리기술은 현재 초기연구 단계임

해외 기술

- 안티바이러스, 파이어월, 운영체제 등 대체 가능한 보안 제품이나 보안 기능을 일부 포함하는 완제품을 제공하는 벤더가 존재하나, **접근제어 보안 기술을 상용으로 제공하는 세계주도 벤더는 없음**. 보안재구성 기술을 개발하는 벤더로써 Check Point사가 있음. 원격보안관리 기술을 개발하고 있는 벤더로서 InnoPath와 Sybase가 있음

- 접근제어기술을 개발하고 있는 보안 업체는 주로 응용 계층의 보안 기능에 주력하고 있고, **OS보안 기술은 OS 주요 벤더들이 주력 제품의 요소기술로서 기술을 보유하고 있음**. 이동단말용 보안재구성기술에 대한 연구는 활발하지는 않지만 Check Point사에서 모바일 단말을 위한 방화벽 자동구성 기술을 개발함.

시장동향

모바일 단말 보안/데이터 보안 시장이 2008년 375억 달러, 2009년 515억 달러, 2011년에는 전세계적으로 957억 달러와 같이 급속도로 증가될 것으로 예측되고 있음

▶ **보안 인식 향상으로 인해 점차 OS 제품 자체의 보안성이 강화되고 있고, 응용 보안 기술인 안티바이러스 등의 제품들이 시스템 전체 보안을 제공하는 방식으로 시장 영역을 넓혀가고 있는 바, 접근제어 기술도 단순 소프트웨어 제품 형태가 아닌 통합된 보안 서비스를 제공하는 형태의 기술로 시장을 넓혀갈 것이라고 예상됨**

▶ **보안재구성 기술은 상황인식 기술에 해당하는데, 상황인식 기술은 U-헬스, 로봇, 홈 네트워크 등 매년 시장규모가 증가하고 있음. 보안재구성 기술도 또한 보안을 필요로 하는 모바일 단말(예, 비즈니스 모바일 단말)의 수요가 증가하고 있는 추세이기 때문에 본 기술에 대한 시장도 넓혀질 것으로 예상됨. 비즈니스용 모바일 단말의 수요가 증가함에 따라서 보안서비스 자동구성기술 및 원격보안제어 기술에 대한 시장규모가 증가할 것으로 예상됨**

(단위 : 백만불, 억원)

관련 제품/서비스	시장	1 차년도 (2010)	2 차년도 (2011)	3 차년도 (2012)	4 차년도 (2013)	5 차년도 (2014)
모바일 단말기용 자체방어 SW	해외	106	176	290	480	794
	국내	36	58	96	160	264

국내시장

▶ **가상화 기반 스마트 단말 보안기술은 소프트웨어 기반의 보안 플랫폼 기술로 비용 절감 및 확장성, 이식성이 우수하며, 실생활에 적용 가능한 우수한 보안 강도를 제공함**

• 가상화 기반 스마트 단말 운영환경 분리 및 보안기술을 연구/개발한다. 다양한 용도로 활용되는 스마트 단말의 운영환경을 “일반 도메인”과 “안전 도메인”으로 분리하여 “안전 도메인”에 대한 불법사용자의 접근을 차단하고, 스마트 단말 서비스의 안전성을 보장하기 위한 다양한 보안 기능을 연구/개발함

해외시장

▶ **Microsoft, Flask(Security Enhanced Linux), IBM(Brocade Advanced Security), Digital Equipment, HP Secure OS, SiliconGraphics(TrustedRIX),Unisys(Secure OS 2200 Systems) 보안제품이 존재함**

접근제어 관련 제품 및 서비스는 주로 OS 및 시스템 벤더가 OS, 서버시스템 등 대상 제품과 함께 완제품의 형태로 제공하며, 보안 기능 독립화 및 특성화가 어려운 단점이 있음

• 모바일 단말을 위한 보안재구성 제품으로는 Check Point사에서 개발한 Zone alarm 이란 보안 SW가 있지만, 방화벽 보안기능에 대한 재구성만을 제공함

관련기업

▶ **Microsoft, Flack, IBM, Check Point, Digital Equipment, HP secure OS, SiliconGraphics, Unisys**

수요처

기술 수요	보안, 소프트웨어 및 단말기 관련 기업
적용처	PMP, PDA, 스마트폰, 휴대 단말기

기술이전 내용 및 범위

▶ 소스 코드

- 윈도우 모바일(Windows Mobile) 플랫폼기반의 접근제어 모듈
- 윈도우 모바일(Windows Mobile) 플랫폼기반의 보안재구성 모듈
- 클라이언트 및 서버용 원격보안관리 모듈

▶ 문서

- 시스템 설계서 및 개발 문서
- 특허

예상 응용 제품 및 기대효과

▶ 기대효과

- 접근제어 기술은 보안정책을 기반으로 하여 파일, 프로세스, WiFi, SMS, Voice Cal, HSDPA, USB 등과 같은 단말자원에 대한 프로세스의 접근행위를 모니터링 함으로써 비정상적인 공격행위를 탐지/차단할 수 있음

- 보안 관리 기술은 모바일 단말기 자체적으로 현재의 보안 상태에서 가장 필요한 보안 서비스를 자동 제공함으로써 모바일 단말의 보안을 강화시키며, 보안 관리의 자동화를 제공함으로써 사용자 편의성 증대, 그리고 배터리 소모를 줄임으로써 자원 효율성을 극대화시키는 효과가 있음

- 보안 관리 기술은 단말기의 보안기능을 관리/제어할 수 있는 원격 보안관리 기능을 제공함으로써, 단말기의 도난/분실 등의 보안사고에 효과적으로 대처할 수 있을 뿐만 아니라 보안구성을 효과적으로 제공할 수 있음

▶ 예상 응용 제품 및 서비스

- 접근제어 관련 제품 및 서비스 : 주로 OS 및 시스템 벤더가 OS, 서버 시스템 등 대상 제품과 함께 완제품의 형태로 제공

▶ 테스트 방법

＊ 단말정보 전달 기능

- 모바일 보안서버를 실행(Web Aparch 구동)

- 복합단말을 부팅시킨 후 “DevSEC_Agent” 프로그램을 구동

- 모바일 보안관리 서버의 URL(즉, http://192.168.11.77/device_manager/request.php”)을 입력하고, 그 서버와 접속

- 복합단말의 IMEI(International Mobile Equipment Identity)와 전화번호정보, 그리고 zoneid 정보(복합단말이 위치한 장소 식별자)를 보안관리서버에게 제공

＊ 보안정책 전달기능

- 모바일 보안관리 서버는 접속된 복합단말로부터 zoneID 정보를 받으면, 그 zoneID에 해당하는 보안재구성정책을 복합단말에게 전달

- 사용자가 모바일 보안관리 서버의 GUI에서 “적용(enforcement)”를 클릭하면, 접근제어정책과 데이터소거 정책을 복합단말에게 전달

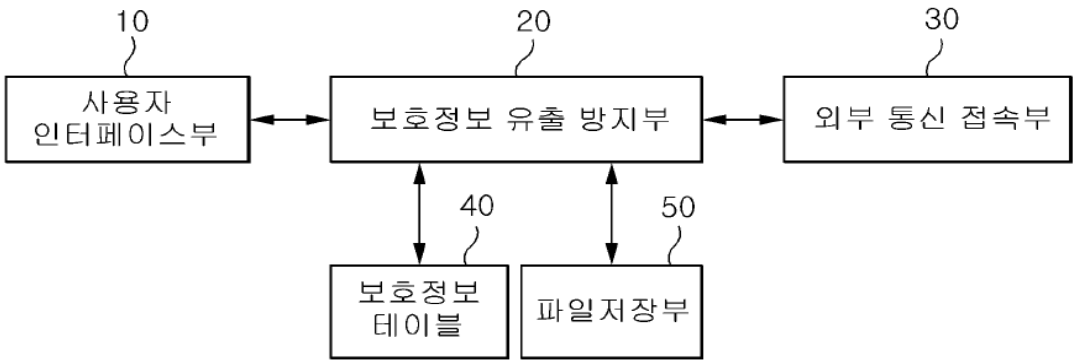
관련 특허 요약

발명의 명칭

개인용 컴퓨터에서 보호정보의 외부유출을 실용적으로 방지하는 방법 및 그 장치

기술 개요

개인용 컴퓨터에서 사용자가 중요하게 다루는 보호정보가 외부로 유출되는 것을 방지하는 보호정보의 외부유출을 방지하는 방법 및 그 장치에 관한 기술임



▶ **보호정보의 외부 유출 방지를 위한 장치의 구성**

- 개인용 컴퓨터에서 보호정보의 외부 유출 방지를 위한 장치는 사용자 인터페이스부(10), 보호정보 유출방지부(20), 외부통신 접속부(30), 보호정보 테이블(40) 및 파일저장부(50)로 구성됨
- 사용자 인터페이스부(10)는 사용자 인증을 통해 개인용 컴퓨터, 정보 저장 서버 등을 사용할 수 있도록 사용자의 사용 접속을 제공하는 인터페이스 역할을 수행함
- 보호정보 유출방지부(20)는 저장된 보호정보의 사용 및 외부로의 유출을 방지하는 역할을 수행하고, 파일 저장부(50)에 저장된 보호정보 파일이 외부통신 접속부(30)로 무단 유출되는 것을 방지하기 위하여, 보호정보 파일과 연관된 일반정보 파일의 속성을 보호정보로 연경하고, 보호정보 파일을 암/복호화함
- 보호정보 테이블(40)은 보호정보 및 일반정보를 구별하는 식별자 및 사용자 인터페이스부(10)를 통한 사용자에게 외부통신접속부(30)로의 접근 허용정도를 설정하는 외부정책을 저장하는 외부 접속제어 정책을 포함함

기술 특장점

▶ **보호정보 유출 방지**

- 일반 사용자가 일반정보 파일을 사용하여 보호정보 파일을 편집하는 것을 허용하기 때문에 사용자 편리성을 제공함
- 보호정보 접근동안 활성화된 모든 일반정보 파일의 속성을 보호정보로 변경하고 동시에 외부로의 보호정보 전송을 외부접근 제어 정책에 따라서 원천차단하므로 보호정보 유출을 방지함

대표 청구항 **전체 청구항 수 : 총 17항**

사용자 인증에 의한 보호정보를 포함하는 저장된 정보로의 접근을 제공하는 **사용자 인터페이스부**;
외부 통신을 제공하는 적어도 하나의 **외부통신 접속부**;
저장된 정보 중에서 보호정보 감지시 적어도 하나의 외부통신접속부로의 접근을 차단하도록 제어하는 **보호정보 유출방지부**; 및
보호정보를 구분하는 식별자를 포함하는 **보호정보 테이블**을 포함