(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년05월29일
(11) 등록번호 10-1148889
(24) 등록일자 2012년05월16일

(51) 국제특허분류(Int. Cl.)
H04W 12/06 (2009.01) *H04W 88/02* (2009.01)
H04L 9/32 (2006.01)
(21) 출원번호 10-2011-0032328
(22) 출원일자 2011년04월07일
심사청구일자 2011년04월07일
(56) 선행기술조사문헌
KR1020070046012 A
KR1020060114482 A
US20030233580 A1

(73) 특허권자
주식회사 정보보호기술
서울특별시 서초구 반포대로 89, 4층 (서초동, 유민빌딩)
(72) 발명자
류동주
경기도 남양주시 와부읍 덕소로97번길 101, 동부센트레빌 112동 1901호
문길종
서울특별시 동작구 사당로8나길 9, 302호 (사당동)
(뒷면에 계속)
(74) 대리인
특허법인다울

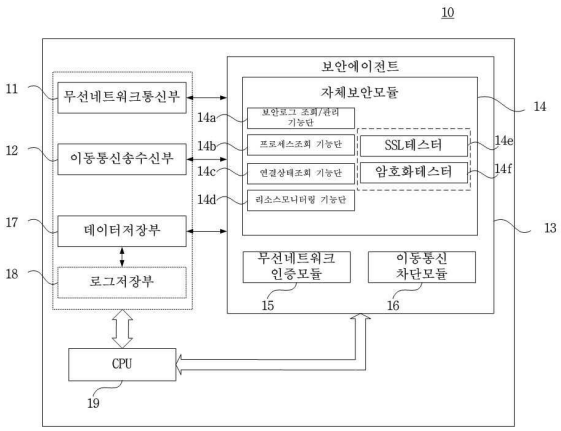
전체 청구항 수 : 총 15 항 심사관 : 장상배

(54) 발명의 명칭 **자체보안기능을 구비한 모바일터미널 및 이의 보안강화방법**

(57) 요 약

본 발명은 자체보안기능을 구비한 모바일터미널 및 이의 보안강화방법에 관한 것이다. 본 발명은, 초기화에 따른 모바일터미널의 장비 인증을 실행하는 보안서버; 및 상기 장비 인증과 무선AP와의 구간에 대한 IP네트워크 구간 인증 완료에 따라 사용자 기반의 자체보안기능을 웨이크-업(Wake-Up) 하며, 상기 웨이크-업에 따라 이동통신네트워크와의 연결을 차단하는 모바일터미널을 포함한다.

대 표 도 - 도2



(72) 발명자

노봉남

광주광역시 광산구 첨단중앙로181번길 88-21, 대우아파트 108동 503호 (월계동)

이형효

전라북도 전주시 완산구 서신동 965-3 대우대창아파트 101동 504호

박진모

전라남도 완도군 보길면 예송로278번길 57-1

이동수

광주광역시 동구 중앙로 347-1 (계림동)

김성호

광주광역시 서구 상무버들로 15, 버들마을 2단지 211동 402호 (유촌동)

이 발명을 지원한 국가연구개발사업

과제고유번호	07첨단도시A01
부처명	국토해양부
연구사업명	첨단도시개발
연구과제명	U-Eco City 인프라 통합보안 기술 개발
주관기관	삼성 sds
연구기간	2008.08.22 ~ 2013.04.29

특허청구의 범위

청구항 1

초기화에 따른 모바일터미널의 장비 인증을 실행하는 보안서버; 및

상기 장비 인증과 보안AP와의 구간에 대한 IP네트워크 구간 인증 완료에 따라 사용자 기반의 자체보안기능을 웨이크-업(Wake-Up) 하며, 상기 웨이크-업에 따라 이동통신네트워크와의 연결을 차단하는 모바일터미널; 을 포함하는 것을 특징으로 하는 자체보안기능을 구비한 모바일터미널.

청구항 2

청구항 1에 있어서, 상기 보안서버는,

상기 모바일터미널과 상기 보안서버에 저장된 인증서가 동일한 인증기관(CA)이 발행한지 여부를 인증하며, 상기 보안서버에 저장된 서버 인증서와 서버 개인키를 통해 인증에 따른 유효성을 확인하는 보안모듈; 을 포함하는 것을 특징으로 하는 자체보안기능을 구비한 모바일터미널.

청구항 3

청구항 2에 있어서, 상기 모바일터미널은,

사용자의 선택적 요청에 따라, 기저장된 클라이언트 인증서를 상기 보안서버로 전송하여 상기 보안서버의 유효성 확인에 따라 유효성이 확인된 경우, 상기 보안서버와의 세션을 유지하는 보안에이전트; 를 포함하는 것을 특징으로 하는 자체보안기능을 구비한 모바일터미널.

청구항 4

청구항 3에 있어서, 상기 모바일터미널은,

유저인터페이스 화면 구성을 위한 자체보안모듈;

상기 모바일터미널을 구성하는 구성요소들이 기록하는 데이터를 저장하며, 로그정보 추출기능을 구비하는 데이터저장부; 및

상기 데이터저장부로부터 추출된 로그정보를 분리하여 저장하는 로그저장부; 를 더 포함하는 것을 특징으로 하는 자체보안기능을 구비한 모바일터미널.

청구항 5

청구항 4에 있어서, 상기 자체보안모듈은,

상기 모바일터미널을 구성하는 상기 구성요소들이 기록하는 데이터 중 로그정보를 추출하여 상기 로그저장부에 별도로 저장하며, 사용자의 요청에 따라 상기 로그저장부 저장된 로그정보를 나타내는 보안로그 조회/관리 기능단;

사용자의 요청 또는 자동으로 실행되고 있는 프로세스 정보를 출력하는 프로세스조회 기능단;

상기 보안AP를 통한 IP네트워크와의 연결상태, 상기 이동통신네트워크와의 연결 상태와 수신감도를 나타내는 연결상태조회 기능단;

상기 모바일터미널의 중앙처리장치(CPU)의 현재 사용량, 상기 데이터저장부와 상기 로그저장부의 메모리 사용량, 외부에 대한 패킷 전송률을 나타내는 리소스모니터링 기능단;

상기 보안에이전트가 정상적으로 상기 IP네트워크와의 통신이 수행되고 있지를 나타내는 SSL테스터; 및

상기 IP네트워크 구간 인증에 따라 상기 보안에이전트가 정성적으로 상기 보안AP와의 데이터 송수신에 있어 암호화 기능을 테스트하는 암호화테스터; 를 포함하는 것을 특징으로 하는 자체보안기능을 구비한 모바일터미널.

청구항 6

청구항 3에 있어서, 상기 보안에이전트는,

상기 IP네트워크 구간 인증을 수행하도록 상기 보안AP와 신호 및 데이터를 송수신하도록 제어하는 무선네트워크인증모듈; 을 더 포함하는 것을 특징으로 하는 자체보안기능을 구비한 모바일터미널.

청구항 7

청구항 3에 있어서, 상기 보안에이전트는,

상기 모바일터미널의 장비 인증과 상기 IP네트워크 구간 인증이 완료되어 상기 자체보안기능이 웨이크-업(Wake-UP)되면, 상기 이동통신네트워크로 신호 및 데이터가 송수신되는 것을 차단하는 이동통신차단모듈; 을 더 포함하는 것을 특징으로 하는 자체보안기능을 구비한 모바일터미널.

청구항 8

청구항 3 내지 청구항 7 중 어느 하나에 있어서, 상기 보안서버는,

기저장된 클라이언트 개인키를 이용해 상기 클라이언트 인증서를 검증하며, 상기 클라이언트 개인키는 공개키이며, 상기 클라이언트 인증서는 PKI 방식의 인증서인 것을 특징으로 하는 자체보안기능을 구비한 모바일터미널.

청구항 9

청구항 1 내지 청구항 7 중 어느 하나에 있어서, 상기 모바일터미널은,

상기 보안AP를 통해 IP네트워크에 접속하는 과정에 있어서, 상기 보안AP와 EAP-TLS 프로토콜 기능을 이용해 상기 IP네트워크 구간 인증을 수행하는 것을 특징으로 하는 자체보안기능을 구비한 모바일터미널.

청구항 10

보안서버가, 초기화에 따른 모바일터미널의 장비 인증을 실행하는 제 1 단계;

상기 모바일터미널이, 보안AP와의 구간에 대한 IP네트워크 구간 인증을 수행하는 제 2 단계; 및

상기 모바일터미널이, 자체보안기능을 웨이크-업(Wake-Up) 하며, 이동통신네트워크와의 연결을 차단하는 제 3 단계; 를 포함하는 것을 특징으로 하는 자체보안기능을 구비한 모바일터미널의 보안강화방법.

청구항 11

청구항 10에 있어서, 상기 제 1 단계는,

상기 보안서버가, 상기 모바일터미널과 상기 보안서버에 저장된 인증서가 동일한 인증기관(CA)이 발행한지 여부를 인증하는 동일성 인증단계; 및

상기 보안서버가, 상기 보안서버에 저장된 서버 인증서와 서버 개인키를 통해 인증에 따른 유효성을 확인하는

서버인증단계; 를 포함하는 것을 특징으로 하는 자체보안기능을 구비한 모바일터미널의 보안강화방법.

청구항 12

청구항 11에 있어서, 상기 서버인증단계 이후에 수행되는,

상기 보안서버가, 상기 모바일터미널의 선택적 요청에 따라 상기 모바일터미널에 저장된 클라이언트 인증서를 수신하여 유효성을 확인하여 유효성이 확인된 경우, 상기 모바일터미널과의 세션을 유지하는 클라이언트인증단계; 를 더 포함하는 것을 특징으로 하는 자체보안기능을 구비한 모바일터미널의 보안강화방법.

청구항 13

청구항 12에 있어서, 상기 클라이언트인증단계는,

상기 보안서버가, 상기 클라이언트 인증서의 유효성이 확인되지 않은 경우, 상기 모바일터미널과의 세션을 단절하는 것을 특징으로 하는 자체보안기능을 구비한 모바일터미널의 보안강화방법.

청구항 14

청구항 12에 있어서, 상기 클라이언트인증단계는,

상기 보안서버는, 기저장된 클라이언트 개인키를 이용해 상기 클라이언트 인증서를 검증하며,

상기 클라이언트 개인키는 공개키이며, 상기 클라이언트 인증서는 PKI 방식의 인증서인 것을 특징으로 하는 자체보안기능을 구비한 모바일터미널의 보안강화방법.

청구항 15

청구항 10에 있어서, 상기 제 2 단계는,

상기 모바일터미널이, 상기 보안AP를 통해 IP네트워크에 접속하는 과정에 있어서, 상기 보안AP와 시드 블록암호 알고리즘 또는 아리아 알고리즘을 이용해 상기 IP네트워크 구간 인증을 수행하는 것을 특징으로 하는 자체보안기능을 구비한 모바일터미널의 보안강화방법.

명 세 서

기 술 분 야

[0001] 본 발명은 네트워크상의 보안 강화 기술에 관한 것으로, 보다 구체적으로는, 모바일터미널에 대한 기밀성, 무결성, 그리고 특정서버로의 접근 통제를 확보하는 자체보안기능을 구비한 모바일터미널 및 이의 보안강화방법에 관한 것이다.

배 경 기 술

[0002] 일반적으로, 인터넷 및 네트워크 관련 기술의 발달로 인하여 각 개인은 필요로 하는 정보를 인터넷 환경 내에서 자유롭게 취득하거나 전달할 수 있게 되었고, 각 기업체에서도 원거리 상에 위치되어 있다 하더라도 인터넷을 통해 각종 정보 자료의 공유가 가능하게 되었다.

[0003] 이러한 통신 및 네트워크 기술의 발달에 따라 최근의 네트워크 환경은 동축 케이블 또는 광케이블과 같은 유선 매체를 이용하는 유선 네트워크 환경으로부터 다양한 주파수 대역의 무선 신호를 이용하는 무선 네트워크 환경으로 변해가고 있다.

[0004] 무선 네트워크는 유선 네트워크와 달리 데이터 전송 경로가 물리적으로 고정되어 있지 않으므로, 무선 네트워크는 유선 네트워크에 비하여 통신의 보안성이 취약하다.

[0005] 한편, 악의적인 사용자들에 의해서 무선 네트워크의 공격 기법은 다양해지고 있으며, 해킹 기법의 발달로 자동화, 지능화된 해킹 툴이 공개적으로 유포되어 국내외 해킹 발생 빈도는 급격히 증가하고 있는 추세이다.

[0006] 특히, 네트워크의 취약점이 지속적으로 증가하고 있으며 웜바이러스와 같은 치명적인 공격에 의해 네트워크 서비스를 마비시킬 수 있는 서비스 거부(DDoS) 공격이 급증하고 있는 가운데 무선 네트워크상에서의 보안을 강화하기 위한 방법이 필요한 실정이다.

[0007] 이에 따라 해당 기술분야에 있어서는 모바일터미널 단에서 보안을 강화하고, 보다 강화된 기능을 갖는 모바일터미널상에서의 기밀성, 무결성, 그리고 외부 서버로의 접근 통제를 확보하기 위한 기술개발이 요구되고 있다.

발명의 내용

해결하려는 과제

[0008] 본 발명은 상기의 문제점을 해결하기 위한 것으로, 종래의 인증모듈(SIM(Subscribe Identity Module), USIM(Universal Subscribe Identity Module), UIM(User Identity Module))과 홈위치레지스터(HLR) 및/또는 방문자위치레지스터(VLR)에 의한 인증과 차별화된 자체 저장된 클라이언트 인증서 전송을 통해 모바일터미널의 장비 인증을 수행하는 모바일터미널의 유효성 확인 과정을 수행하는 자체보안기능을 구비한 모바일터미널 및 이의 보안강화방법을 제공하기 위한 것이다.

[0009] 또한, 본 발명은 모바일터미널의 장비 인증, IP네트워크 구간 인증, 그리고 IP네트워크와의 세션 연결 후 이동통신네트워크로의 신호 및/또는 데이터 송수신을 차단하며, 이와 동시에 자체보안기능 구현에 따라 모바일터미널의 보안을 관리하기 위한 자체보안기능을 구비한 모바일터미널 및 이의 보안강화방법을 제공하기 위한 것이다.

[0010] 또한, 본 발명은 모바일터미널과 보안서버에 저장된 인증서가 동일한 인증기관의 발행여부, 서버 인증서와 서버 개인키를 통한 검증, 그리고 PKI 방식의 클라이언트 인증서와 공개키인 클라이언트 개인키를 통한 검증의 순차적 장비 인증을 통해 기밀성, 무결성 및 접근 통제를 확보하는 자체보안기능을 구비한 모바일터미널 및 이의 보안강화방법을 제공하기 위한 것이다.

[0011] 그러나 본 발명의 목적들은 상기에 언급된 목적으로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0012] 상기의 목적을 달성하기 위해 자체보안기능을 구비한 모바일터미널은, 초기화에 따른 모바일터미널의 장비 인증을 실행하는 보안서버; 및 상기 장비 인증과 무선AP와의 구간에 대한 IP네트워크 구간 인증 완료에 따라 사용자 기반의 자체보안기능을 웨이크-업 하며, 상기 웨이크-업에 따라 이동통신네트워크와의 연결을 차단하는 모바일터미널; 을 포함한다.

[0013] 상기 보안서버는, 상기 모바일터미널과 상기 보안서버에 저장된 인증서가 동일한 인증기관(CA)이 발행한 지 여부를 인증하며, 상기 보안서버에 저장된 서버 인증서와 서버 개인키를 통해 인증에 따른 유효성을 확인하는 보안모듈; 을 포함한다.

[0014] 상기 모바일터미널은, 사용자의 선택적 요청에 따라, 기저장된 클라이언트 인증서를 상기 보안서버로 전송하여 상기 보안서버의 유효성 확인에 따라 유효성이 확인된 경우, 상기 보안서버와의 세션을 유지하는 보안에이전트; 를 포함한다.

[0015] 상기 모바일터미널은, 유저인터페이스 화면 구성을 위한 자체보안모듈; 상기 모바일터미널을 구성하는 구성요소들이 기록하는 데이터를 저장하며, 로그정보 추출기능을 구비하는 데이터저장부; 및 상기 데이터저장부로부터 추출된 로그정보를 분리하여 저장하는 로그저장부; 를 더 포함한다.

[0016] 상기 자체보안모듈은, 상기 모바일터미널을 구성하는 상기 구성요소들이 기록하는 데이터 중 로그정보를 추출하여 상기 로그저장부에 별도로 저장하며, 사용자의 요청에 따라 상기 로그저장부 저장된 로그정보를 나타내는 보안로그 조회/관리 기능단; 사용자의 요청 또는 자동으로 실행되고 있는 프로세스 정보를 출력하는 프로세스조회 기능단; 상기 보안AP를 통한 IP네트워크와의 연결상태, 상기 이동통신네트워크와의 연결 상태와 수신감도를 나타내는 연결상태조회 기능단; 상기 모바일터미널의 중앙처리장치(CPU)의 현재 사용량, 상기 데이터저장부와 상기 로그저장부의 메모리 사용량, 외부에 대한 패킷 전송률을 나타내는 리소스모니터링 기능단; 상기 보안에이전트가 정상적으로 상기 IP네트워크와의 통신이 수행되고 있는지를 나타내는 SSL테스터; 및 상기 IP네트워크 구간 인증에 따라 상기 보안에이전트가 정성적으로 상기 보안AP와의 데이터 송수신에 있어 암호화 기능을 테스트하는 암호화테스터; 를 포함한다.

[0017] 상기 보안에이전트는, 상기 IP네트워크 구간 인증을 수행하도록 상기 보안AP와 신호 및 데이터를 송수신하도록 제어하는 무선네트워크인증모듈; 을 더 포함한다.

[0018] 상기 보안에이전트는, 상기 모바일터미널의 장비 인증과 상기 IP네트워크 구간 인증이 완료되어 상기 자체보안기능이 웨이크-업 되면, 상기 이동통신네트워크로 신호 및 데이터가 송수신 되는 것을 차단하는 이동통신차단모듈; 을 더 포함한다.

[0019] 상기 보안서버는, 기저장된 클라이언트 개인키를 이용해 상기 클라이언트 인증서를 검증하며, 상기 클라이언트 개인키는 공개키이며, 상기 클라이언트 인증서는 PKI 방식의 인증서이다.

[0020] 상기 모바일터미널은, 상기 보안AP를 통해 IP네트워크에 접속하는 과정에 있어서, 상기 보안AP와 EAP-TLS 프로토콜 기능을 이용해 상기 IP네트워크 구간 인증을 수행한다.

[0021] 상기의 목적을 달성하기 위해 자체보안기능을 구비한 모바일터미널의 보안강화방법은, 보안서버가, 초기화에 따른 모바일터미널의 장비 인증을 실행하는 제 1 단계; 상기 모바일터미널이, 무선AP와의 구간에 대한 IP네트워크 구간 인증을 수행하는 제 2 단계; 및 상기 모바일터미널이, 자체보안기능을 웨이크-업 하며, 이동통신네트워크와의 연결을 차단하는 제 3 단계; 를 포함한다.

[0022] 상기 제 1 단계는, 상기 보안서버가, 상기 모바일터미널과 상기 보안서버에 저장된 인증서가 동일한 인증기관(CA)이 발행한 지 여부를 인증하는 동일성 인증단계; 및 상기 보안서버가, 상기 보안서버에 저장된 서버 인증서와 서버 개인키를 통해 인증에 따른 유효성을 확인하는 서버인증단계; 를 포함한다.

[0023] 그리고 상기 서버인증단계 이후에 수행되는, 상기 보안서버가, 상기 모바일터미널의 선택적 요청에 따라 상기 모바일터미널에 저장된 클라이언트 인증서를 수신하여 유효성을 확인하여 유효성이 확인된 경우, 상기 모바일터미널과의 세션을 유지하는 클라이언트인증단계; 가 더 포함된다.

[0024] 상기 클라이언트인증단계는, 상기 보안서버가, 상기 클라이언트 인증서의 유효성이 확인되지 않은 경우, 상기 모바일터미널과의 세션을 단절한다.

[0025] 상기 클라이언트인증단계는, 상기 보안서버는, 기저장된 클라이언트 개인키를 이용해 상기 클라이언트 인증서를 검증하며, 상기 클라이언트 개인키는 공개키이며, 상기 클라이언트 인증서는 PKI 방식의 인증서이다.

[0026] 상기 제 2 단계는, 상기 모바일터미널이, 상기 보안AP를 통해 IP네트워크에 접속하는 과정에 있어서, 상기 보안AP와 시드 블록 암호 알고리즘 또는 아리아 알고리즘을 이용해 상기 IP네트워크 구간 인증을 수행한다.

발명의 효과

[0027] 본 발명의 실시예에 따른 자체보안기능을 구비한 모바일터미널 및 이의 보안강화방법은, 자체 저장된 클라이언트 인증서 전송을 통해 모바일터미널의 장비 인증을 수행하여 종래의 방식과 다른 방식에 의한 모바일터미널의 유효성 확인 과정을 수행한다.

[0028] 또한, 본 발명의 다른 실시예에 따른 자체보안기능을 구비한 모바일터미널 및 이의 보안강화방법은, 모바일터미널의 장비 인증, IP네트워크 구간 인증, 그리고, IP네트워크와의 세션 연결 후에는 이동통신네트워크와의 신호 및/또는 데이터 송수신을 차단하며, 이와 동시에 자체보안기능 구현에 따라 모바일터미널의 보안을 관리할 수 있는 효과를 제공한다.

[0029] 뿐만 아니라, 본 발명의 다른 실시예에 따른 자체보안기능을 구비한 모바일터미널 및 이의 보안강화방법은,

모바일터미널과 보안서버에 저장된 인증서가 동일한 인증기관의 발행여부, 서버 인증서와 서버 개인키를 통한 검증, 그리고 PKI 방식의 클라이언트 인증서와 공개키인 클라이언트 개인키를 통한 검증의 순차적 장비 인증을 통해 기밀성, 무결성 및 접근 통제를 확보하는 효과를 제공한다.

도면의 간단한 설명

[0030] 도 1은 본 발명의 실시예에 따른 자체보안기능을 구비한 모바일터미널을 포함하는 보안시스템을 나타내는 도면이다.

도 2는 도 1의 모바일터미널(10)의 구성을 나타내는 도면이다.

도 3은 도 1의 보안시스템 중 보안서버(40)에서의 함수 동작 흐름을 나타내는 도면이다.

도 4는 도 1의 보안시스템 중 모바일터미널(10)에서의 함수 동작 흐름을 나타내는 도면이다.

도 5는 도 1의 모바일터미널(10)에서 보안에이전트(13)가 실행된 경우의 초기 유저인터페이스 화면을 나타내는 도면이다.

도 6은 도 5의 모바일터미널(10)에서 보안에이전트(13)가 실행된 뒤 메뉴상태로 이동된 것을 나타내는 유저인터페이스 화면을 나타내는 도면이다.

도 7은 도 6의 메뉴로 이동된 유저인터페이스 화면에서 보안로그 조회 및 관리 기능 선택된 초기 상태를 나타내는 도면이다.

도 8은 도 7의 보안로그 조회 및 관리 기능 상태에서 로그 세부 사항이 출력된 상태(a) 및 관리(b)를 나타내는 도면이다.

도 9는 도 6의 메뉴로 이동된 유저인터페이스화면에서 프로세스 조회 기능이 선택된 상태를 나타내는 도면이다.

도 10은 도 6의 메뉴로 이동된 유저인터페이스화면에서 연결 상태 조회 기능이 선택된 상태를 나타내는 도면이다.

도 11은 도 6의 메뉴로 이동된 유저인터페이스화면에서 리소스 모니터링 기능이 선택된 상태를 나타내는 도면이다.

도 12는 도 6의 메뉴로 이동된 유저인터페이스화면에서 SSL 테스트 기능 및 암호화 테스트가 선택된 상태를 나타내는 도면이다.

도 13은 도 1의 모바일터미널(10) 상에 보안에이전트(13)가 실행된 경우의 이동통신네트워크에 대한 통신 차단 기능이 실행된 것을 나타내는 유저인터페이스 화면 구성을 나타낸다.

도 14는 본 발명의 실시예에 따른 자체보안기능을 구비한 모바일터미널의 보안강화방법을 나타내는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0031] 이하, 본 발명의 바람직한 실시예의 상세한 설명을 첨부된 도면들을 참조하여 설명할 것이다. 하기에서 본 발명을 설명함에 있어서, 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다.

[0032] 본 명세서에 있어서는 어느 하나의 구성요소가 다른 구성요소로 데이터 또는 신호를 '전송'하는 경우에는 구성요소는 다른 구성요소로 직접 상기 데이터 또는 신호를 전송할 수 있고, 적어도 하나의 또 다른 구성요소를 통하여 데이터 또는 신호를 다른 구성요소로 전송할 수 있음을 의미한다.

[0033] 도 1은 본 발명의 실시예에 따른 자체보안기능을 구비한 모바일터미널을 포함하는 보안시스템을 나타내는 도면이다. 도 1을 참조하면, 보안시스템은 자체보안기능을 구비한 모바일터미널(10, 이하 모바일 터미널), 보안 AP(20), IP네트워크(IP NETWORK, 30), 보안서버(40), 게이트웨이(50), 기지국(60) 및 이동통신네트워크

(MOBILE RADIO COMMUNICATION NETWORK, 70)를 포함한다.

[0034] 모바일터미널(10)은 저장된 클라이언트 인증서를 보안AP(20)의 접속을 통해 IP네트워크(30)와 연결된 보안서버(40)로 전송하여 인증을 수행한다(P1). 여기서 클라이언트 인증서는 PKI(public key infrastructure) 방식의 인증서이다.

[0035] 모바일터미널(10)은 보안AP(20)를 통해 IP네트워크(30)에 접속하므로, 네트워크 구간인 모바일터미널(10)과 보안AP(20) 구간의 인증을 수행한다(P2).

[0036] 좀 더 구체적으로 살펴보면, 모바일터미널(10)은 보안AP(20)와 EAP-TLS 프로토콜 기능을 이용해 보안AP(20)과 모바일터미널(10) 구간에 대한 암호화를 수행한다.

[0037] 본 발명의 다른 실시예로, 모바일터미널(10)은 시드 블록 암호 알고리즘(SEED 알고리즘) 또는 아리아 알고리즘(ARIA 알고리즘)을 이용해 보안AP(20)과 모바일터미널(10) 구간에 대한 암호화를 수행한다. 이 경우 암호화 시에 신뢰도를 높이기 위해 종래의 WPA 방식의 인증과 임시 키 무결성 프로토콜(TKIP)이 아닌 자체 개발된 SEED 알고리즘 또는 ARIA 알고리즘을 이용하는데 기술적 특징이 있다.

[0038] IP네트워크 구간 인증(P2)이 완료됨에 따라, 모바일터미널(10)이 보안에이전트(13)를 실행시키면, 보안에이전트(13)는 기지국(60)을 통한 이동통신네트워크(70)에 연결된 타 단말, 서버, 그 밖의 시스템(미도시)과의 통신을 차단한다.

[0039] 여기서, 보안AP(security access point, 20)는 IP네트워크(30)에 접속되어 모바일터미널(10)과 게이트웨이 역할을 담당하며 부가적으로 라우팅과 보안기능을 갖추고 있으며, IP네트워크(30)는 대용량, 장거리 음성 및 데이터 서비스가 가능한 대형 통신망의 고속 기간 망이며, 예컨대, 인터넷(Internet)이 될 수 있다.

[0040] 또, IP네트워크(30)는 ALL IP(Internet Protocol) 기반의 고속의 멀티미디어 서비스를 제공하기 위한 차세대 유선 망일 수 있으며, 보안AP(20)와 연결된 모바일터미널(10), 보안서버(40) 그 밖의 시스템 상호 간의 신호 및 데이터를 상호 전달하는 역할을 한다.

[0041] 보안서버(40)는 자체적인 인증과 모바일터미널(10)의 인증을 수행하는 보안모듈(41)을 구비한다. 보안모듈(41)은 모바일터미널(10) 장비 인증 목적으로 실행한다(P1).

[0042] 보안모듈(41)은 제 1 보안단계로 모바일터미널(10)과 보안서버(40)에 저장된 인증서가 동일한 인증기관(Certificate Authority, CA)이 발행한 것인지를 인증한다.

[0043] 제 2 보안단계로, 보안모듈(41)은 보안서버(40)에 저장된 서버 인증서와 서버 개인키를 통해 유효성 확인을 수행에 따른 초기화를 성공적으로 완료한다.

[0044] 이후, 제 3 보안단계로, 보안모듈(41)은 모바일터미널(10)의 선택적 요청에 따라 모바일터미널(10)에 저장된 클라이언트 인증서를 수신하여 검증을 수행하여 결과에 따라 세션을 유지 여부를 결정한다.

[0045] 보안모듈(41)은 보안서버(40)에 기저장된 클라이언트 개인키를 이용해 클라이언트 인증서를 검증하며, 클라이언트 개인키는 공개키인 것을 특징으로 한다.

[0046] 한편, 도시된 게이트웨이(G/W, 50)는 프로토콜 변환기의 하나이며, 이동통신네트워크(70)와 IP네트워크(30)를 통해 접속하는 단말 간의 데이터 송수신을 가능하게 한다. 게이트웨이(50)는 왑게이트웨이(WAP Gateway)로서, 모바일터미널(10)이 이동통신네트워크(70)를 통해 보안서버(40)에 액세스하기 위한 프로토콜 스택을 포함할 수 있다.

[0047] 기지국(60)은 모바일터미널(10)이 이동통신네트워크(70)에 접속할 수 있는 무선 접속링크를 제공하며, 사용자의 인터넷 데이터가 이동통신네트워크(70)을 통하여 송수신될 수 있도록 하는 역할을 수행한다.

[0048] 이동통신네트워크(70)는 동기식 이동 통신망일 수도 있고, 비동기식 이동 통신망일 수도 있다. 비동기식 이동통신망의 일 실시 예로서, WCDMA(Wideband Code Division Multiple Access) 방식의 통신망을 들 수 있다.

[0049] 이 경우 도면에 도시되진 않았지만, 이동통신네트워크(70)는 RNC(Radio Network Controller), 및 비동기식 MSC(Mobile Switching Center)를 포함할 수 있다. 한편, WCDMA망을 일 예로 들었지만, 3G LTE망, 4G망 등 차세대 이동통신망으로 변경될 수 있음은 주지의 사실이다. 이동통신네트워크(70)는 모바일터미널(10)과 상대단말, 그 밖의 시스템 상호 간의 신호 및 데이터를 상호 전달하는 역할을 수행하며, 특히 음성 통화 및 화상 통화의 송수신을 수행한다.

[0050] 도 2는 도 1의 모바일터미널(10)의 구성을 나타내는 도면이다. 도 1 및 도 2를 참조하면, 모바일터미널(10)은 무선네트워크통신부(11), 이동통신송수신부(12), 보안에이전트(13), 데이터저장부(17), 로그저장부(18) 및 중앙처리장치(CPU, 19)를 포함한다.

[0051] 무선네트워크통신부(11)은 보안AP(20)와의 IP네트워크 구간 인증에 따라 IP네트워크(30)를 거쳐 보안서버(40)와 데이터 송수신을 수행한다.

[0052] 이동통신송수신부(12)는 기지국(60)을 통해 이동통신네트워크(70)를 거쳐 다른 단말, 서버, 그 밖의 시스템(미도시)과 데이터 송수신을 수행한다.

[0053] 본 발명에서, 이동통신송수신부(12)는 보안에이전트(13)의 자체보안모듈(14)이 활성화되면, 자체보안모듈(14)에 의해 송수신기능이 차단되는 것을 특징으로 한다.

[0054] 보안에이전트(13)는 보안서버(40)와의 데이터 송수신을 통해 도 1에서 설명한 모바일터미널(10)의 장비 인증(P1)을 수행하며, 이를 위해 PKI 방식의 클라이언트 인증서가 데이터저장부(17)에 저장되어 있다. 한편, 보안에이전트(13)는 다양한 기능을 구현하기 위해 자체보안모듈(14), 무선네트워크인증모듈(15) 및 이동통신차단모듈(16)을 포함한다.

[0055] 그리고 본 명세서에서 모듈이라 함은, 본 발명의 기술적 사상을 수행하기 위한 하드웨어 및 상기 하드웨어를 구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미할 수 있다. 예컨대, 상기 모듈은 소정의 코드와 상기 소정의 코드가 수행되기 위한 하드웨어 리소스의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된 코드를 의미하거나, 한 종류의 하드웨어를 의미하는 것은 아님은 본 발명의 기술분야의 평균적 전문가에게는 용이하게 추론될 수 있다.

[0056] 자체보안모듈(14)은 보안에이전트(13)에 의해 모바일터미널(10)에 대한 장비 인증(P1), 그리고 후술할 무선네트워크인증모듈(15)에 의해 IP네트워크 구간 인증(P2)이 완료되어, 자체보안기능이 웨이크-업 되면, 추가적인 기능을 구현한다. 이를 위해 자체보안모듈(14)은 보안로그 조회/관리 기능단(14a), 프로세스조회 기능단(14b), 연결상태조회 기능단(14c), 리소스모니터링 기능단(14d), SSL테스터(14e) 및 암호화테스터(14f)를 포함한다.

[0057] 보안로그 조회/관리 기능단(14a)은 모바일터미널(10)의 전체 구성요소들(보안에이전트(13), 자체보안모듈(14), 무선네트워크인증모듈(15), 이동통신차단모듈(16) 및 중앙처리장치(CPU, 19)를 포함)이 기록하는 데이터 중 로그정보를 추출하여 로그저장부(18)에 별도로 저장한다. 이후, 보안로그 조회/관리 기능단(14a)은 사용자의 요청에 따라 로그저장부(18)에 저장된 로그정보를 출력해 주며, 이에 대한 구현화면의 일 예는 후술할 도 7 및 도 8에 도시되어 있다.

[0058] 프로세스조회 기능단(14b)은 모바일터미널(10)에서 사용자의 요청 또는 자동으로 실행되고 있는 프로세스 정보를 출력하며, 이에 대한 구현화면의 일 예는 후술할 도 9에 도시되어 있다.

[0059] 연결상태조회 기능단(14c)은 현재 연결 상태 정보를 나타낸다.

[0060] 보다 구체적으로, 연결상태조회 기능단(14c)은 WiFi방식에 의해 보안AP(20)를 통한 IP네트워크(30)와의 연결상태, 그리고 3G와 같은 이동통신네트워크(70)와의 연결 상태와 수신감도를 나타내며, 현재 연결된 주소와 연결된 포트 및 열린 포트 정보도 출력한다.

[0061] 한편, 이에 대한 구현화면의 일 예는 도 10에 도시되어 있다.

[0062] 리소스모니터링 기능단(14d)은 사용자의 요청에 따라 모바일터미널(10)의 중앙처리장치(CPU, 19)의 현재 사용량, 데이터저장부(17) 및 로그저장부(17)의 메모리 사용량, IP네트워크(30)와 연결된 외부로의 패킷 전송률을 출력하며, 이에 대한 구현화면의 일 예는 도 11에 도시되어 있다.

[0063] 여기서 중앙처리장치(CPU, 17)는 모바일터미널(10)의 일반적인 기능을 수행하는 것으로 이에 대한 상세한 설명은 생략하도록 한다.

[0064] SSL테스터(14e)와 암호화테스터(14f)는 보안에이전트(13)가 정상적으로 실행되는지 테스트해 볼 수 있는 기능으로, 각각이 보안에이전트(13)의 통신 기능과 암호화 기능을 테스트하기 위한 구성으로, 이에 대한 구현화면의 일 예는 도 12에 도시되어 있다.

[0065] 무선네트워크인증모듈(15)은 IP네트워크 구간 인증(P2, 도 1참조)을 수행하도록 보안AP(20)과 신호 및 데이터를 송수신하도록 무선네트워크통신부(11)를 제어한다.

[0066] 이동통신차단모듈(16)은, 모바일터미널 장비 인증(P1, 도 1 참조)와 IP네트워크 구간 인증(P2)이 완료되어 자체보안기능이 웨이크-업 되면, 이동통신송수신부(12)가 작동하지 못하도록 이동통신송수신부(12)를 제어한다. 한편, 이동통신차단모듈(16)에 의해 구현된 화면의 일 예는 도 13에 도시되어 있다.

[0067] 데이터저장부(17)는 보안에이전트(13)의 각 세부구성에서 기록하는 데이터를 저장하며, 로그정보 추출을 수행하는 보안로그 조회/관리 기능단(14a)의 일부 기능을 수행 가능하다.

[0068] 데이터저장부(17)는 비휘발성 메모리(Non-volatile memory, NVM)로써 전원이 공급되지 않아도 저장된 데이터를 계속 유지하며 삭제되지 않으며, 플래시 메모리(Flash Memory), MRAM(Magnetic Random Access Memory), PRAM(Phase-change Random Access memory: 상변화 램), FRAM(Ferroelectric RAM: 강유전체 램) 등으로 구성될 수 있다.

[0069] 이에 따라, 로그저장부(18)는 보안에이전트(13)의 각 세부구성에서 기록하는 데이터 중 로그정보가 데이터저장부(17)에 의해 추출되어 저장된다.

[0070] 도 3은 도 1의 보안시스템 중 보안서버(40)에서의 함수 동작 흐름을 나타내는 도면이다. 도 3을 참조하여, 보안서버(40)의 보안모듈(41)에서 구현되는 함수 동작에 대해 설명한다. s_init()함수는 보안서버(30)의 초기화 기능을 수행한다(S11). 여기서, 사용되는 인자는 리스닝 할 포트 번호, 인증서버(40)에 저장된 CA인증서 파일 위치, 서버 인증서 파일의 위치, 서버 개인키 파일의 위치이며, 여기서 해당 각 위치는 저장된 디렉토리 정보를 의미한다.

[0071] 보안서버(40)의 초기화가 정상적으로 성공되면, 1이 반환되고 s_accept() 함수를 실행할 수 있다. s_accept() 함수는 클라이언트인 모바일터미널(10)로부터 연결을 기다리고 접속이 요청되면 모바일터미널(10)과 협상을 통해 세션을 형성한다(S12).

[0072] 단계(S13)에서 s_accept() 함수는 세션이 맺어지면 소켓 식별자를 반환한다.

[0073] s_read() 함수와 s_write() 함수는 소켓 식별자를 이용하여 클라이언트인 모바일터미널(10)과 통신이 가능하다(S13, S14). get_peer_infor() 함수는 보안서버(40)와 세션이 연결된 모바일터미널(10)의 정보를 가져온다(S15).

[0074] 보안서버(40)는 모바일터미널(10)과의 모든 통신이 마무리되면 s_close() 함수를 통해 세션을 종료시킬 수 있다(S16).

[0075] 도 4는 도 1의 보안시스템 중 모바일터미널(10)에서의 함수 동작 흐름을 나타내는 도면이다. 도 4를 참조하면, 모바일터미널(10)은 보안서버(40)에 접속하기 위해서 2가지 함수를 사용할 수 있다.

[0076] secure_open() 함수는 보안서버(40)에 모바일터미널(10)의 인증서를 전송하지 않고 보안서버(40)의 인증서(예컨대, CA인증서, 서버 인증서)만을 검증한다(S21).

[0077] 다른 함수인 secure_open_cert() 함수는 보안서버(40)에게 모바일터미널(10)의 인증서를 전송하여 검증을 받은 후 세션을 유지하게 된다(S22).

[0078] 세션 유지 후, 핸들 값을 이용하여 secure_read() 함수와 secure_write() 함수를 통해 보안서버(40)와 통신이 가능하다(S23, S24).

[0079] 모아일터미널(10)은 보안서버(40)와의 통신이 완료되면 secure_close() 함수를 통해 통신을 종료한다(S25).

[0080] 한편, 하기의 표 1은 모바일터미널(10)에 저장되는 인증서의 예시이며, 표 2는 보안서버(40)에 저장되는 인증서들의 예시이다.

표 1

[0081]

NAME	설명
caert.crt	CA인증서
test3.crt	클라이언트 인증서

표 2

[0082]

NAME	설명
caert.crt	CA인증서
server.crt	서버 인증서
serverkey.pem	서버 개인키
key.pem	클라이언트 개인키

[0083] 표 1 및 표 2를 참조하면, 모바일터미널(10)에 저장되는 CA인증서와 보안서버(40)에 저장되는 CA인증서는 동일한 것을 사용합니다. 한편, 도 1에서 상술한 동일한 인증기관에서 발행된 인증서 여부를 판단하기 위해 모바일터미널(10)의 CA인증서와 보안서버(40)의 CA인증서는 인증기관의 인증서이며, 모바일터미널(10)의 클라이언트 인증서와 보안서버(40)의 서버 인증서가 동일한 인증기관(CA)이 발행한 것인지를 인증한다.

[0084] 보안서버(40)의 서버 인증서와 서버 개인키는 상술한 secure_open() 함수에 의해 클라이언트가 보안서버(40)의 인증서의 유효성 확인을 할 경우 사용된다.

[0085] 상술한 secure_open_cert() 함수에 의해 연결될 경우 모바일터미널(10)의 클라이언트 인증서는 보안서버(40)로 전송되어 보안서버(40)에 저장되어 있는 CA인증서에 의한 검증을 수행된다.

[0086] 한편, 도 3 및 도 4의 각 함수들을 리눅스 시스템을 기반으로 설명하였으나, 반드시 리눅스 시스템에 국한되지 않으며 다른 운영체제 또는 시스템에서도 변형하여 사용가능하다.

[0087] 도 5는 도 1의 모바일터미널(10)에서 보안에이전트(13)가 실행된 경우의 초기 유저인터페이스 화면을 나타내는 도면으로, 보안에이전트(13)의 시작 화면을 나타낸다. 시작 화면 중 불특정 영역을 클릭하면 도 6의 메뉴 액티비티로 이동된다.

[0088] 도 6은 도 5의 모바일터미널(10)에서 보안에이전트(13)가 실행된 뒤 메뉴상태로 이동된 것을 나타내는 유저인터페이스 화면을 나타내는 도면이다.

[0089] 도 6와 같이, 보안에이전트(13)는, 상술한 시작 기능과 메뉴 기능 화면을 구현하는 기능 외에 "보안로그 조회 및 관리", "프로세스 조회", "연결 상태 조회", "리소스 모니터링", "SSL 테스트", "암호화 테스트" 기능을 구현하며, 구현된 기능은 모바일터미널(10)의 사용자에 의해 선택될 수 있다.

[0090] 도 7을 참조하면, 보안로그는 보안에이전트(13)를 포함하는 모바일터미널(10)의 각 구성요소들이 기록하고자 하는 데이터 중 로그정보를 추출하여 로그저장부(18)에 별도로 저장된 것으로, 보안로그 조회기능은 로그저장부(18)에 저장된 로그정보를 출력해주는 것이다.

[0091] 로그정보는 "타입정보"(Type: Success 또는 Failed), 이벤트가 일어난 "시간정보"(Time), 인증서버(40)를 포함하는 외부단말의 IP주소(IPv4 또는 IPv6)인 "외부연결정보"(Remote)를 포함한다.

[0092] 도 8은 도 7의 보안로그 조회 및 관리 기능 상태에서 로그 세부 사항이 출력된 상태(a) 및 관리(b)를 나타내는 도면이다.

[0093] 도 8(a)를 참조하면, 출력된 로그정보 중 하나를 클릭하면 추가로 무선네트워크통신부(11)를 통해 통신을 시도한 애플리케이션 명칭(보안AppName)과 행위에 대한 설명(Description)을 나타내는 항목이 추가된 화면이 출력된다. 한편, 로그 세부 사항에서 삭제 버튼을 누르면 현재 선택된 로그는 삭제가 된다.

[0094] 한편, 도 8(b)를 참조하면, 도 7의 상태에서 "타입정보(Type)", "시간정보(Time)" "외부연결정보(Remote)" 중 어느 하나를 클릭하면, 각 항목에서의 분류기준에 따라 정렬이 이뤄진다. 여기서는 시간정보(Time)에 따라 시간의 선후에 따라 정렬된 타임 컬럼 정렬상태를 나타내다.

[0095] 도 9는 도 6의 메뉴로 이동된 유저인터페이스화면에서 프로세스 조회 기능이 선택된 상태를 나타내는 도면이다. 도 9를 참조하면, 프로세스 조회 기능은 모바일터미널(10)에서 실행되고 있는 프로세스 정보를 보여준다. 한편, 모바일터미널(10)은 안드로이드 운영체제를 사용하나 반드시 이에 한정되는 것은 아니다.

[0096] 프로세스 조회기능에서 제공되는 정보는 실행유저(USER), 프로세서 인식자(Process IDentifier: PID), 프로세스 명칭(NAME)를 포함한다.

[0097] 도 10은 도 6의 메뉴로 이동된 유저인터페이스화면에서 연결 상태 조회 기능이 선택된 상태를 나타내는 도면이다. 도 10을 참조하면, 연결 상태 조회 기능은 IP기반의 WiFi 방식 등을 이용해 보안AP(20)를 통한 IP네트워크(30)와의 연결상태, 그리고 3G, 4G와 같은 이동통신네트워크(70)와의 연결 상태와 수신감도를 나타내며, 현재 연결된 주소와 연결된 포트 및 열린 포트 정보를 표시한다.

[0098] 보다 구체적으로, 수신 감도 정보는 현재 연결된 보안AP의 수신 강도를 나타내는 것이고, Wi-Fi 연결 상태 정보는 Wi-Fi 활성화 여부를 보여준다. 또한 네트워크분석 정보(netstat)는 현재 열린 네트워크 상태 정보를 보여준다.

[0099] 도 11은 도 6의 메뉴로 이동된 유저인터페이스화면에서 리소스 모니터링 기능이 선택된 상태를 나타내는 도면이다. 도 11을 참조하면, 리소스 모니터링 기능은 중앙처리장치(CPU, 19)의 현재 사용량, 데이터저장부(17) 및 로그저장부(18)를 포함하는 모바일터미널(10)의 메모리 사용량, 패킷 전송률을 출력한다.

[0100] 리소스 모니터링 기능은 각 사용량들을 1초마다 갱신하여 실시간으로 표시하며, CPU 점유율에서는 자체보안기능을 구비한 모바일터미널 CPU의 전체 사용량을 보여주고, 메모리 사용률에서는 전체, 사용중, 여유 메모리 양을 보여준다. 패킷 전송량은 1초를 주기로 갱신되며, 매 초당 패킷량을 보여준다.

[0101] 도 12는 도 6의 메뉴로 이동된 유저인터페이스화면에서 SSL 테스트 기능 및 암호화 테스트가 선택된 상태를 나타내는 도면이다. 도 12를 참조하면, SSL 테스트 기능과 암호화 테스트는 보안에이전트(13)가 정상적으로 실행되는지 테스트해 볼 수 있는 기능으로, 각각이 보안에이전트(13)의 통신 기능과 암호화 기능을 테스트할 수 있다.

[0102] 도 12(a)는 테스트 화면을 나타내며, 도 12(b)는 테스트 성공화면을 나타낸다. 도 12(b)와 같이 테스트가 성공하면, 도 12(a)의 공백부분([ ])에 Success가 표시되고, 에디터 박스에는 정상적으로 문자열을 받은 모습(Your Message: Send Message)를 보여준다.

[0103] 도 13은 도 1의 모바일터미널(10) 상에 자체보안기능이 활성된 경우의 이동통신네트워크에 대한 통신 차단 기능이 실행된 것을 나타내는 유저인터페이스 화면 구성을 나타낸다. 도 13을 참조하여 설명의 편의상 이동통신네트워크(70)를 3G망으로 설정하면, 3G 통신 차단 기능은 보안에이전트(13)가 실행되는 동안 3G 통신을 차단하는 기능을 한다. 보안에이전트(13)가 실행되는 동안에 3G 통신을 사용하고 있는지 확인하여 3G 통신을 사용하고 있다면 3G 통신을 차단하고, 3G 통신이 차단되었음을 사용자에게 알려준다.

[0104] 그리고 자체보안기능을 수행하는 자체보안모듈(14)이 종료된 경우, 다시 3G 통신 연결을 복구시키고, 3G 연결 복구를 사용자에게 알려준다.

[0105] 도 14는 본 발명의 실시예에 따른 자체보안기능을 구비한 모바일터미널의 보안강화방법을 나타내는 흐름도이다. 도 1 내지 도 14를 참조하면, 모바일터미널(10)의 액세스 요청에 따라 보안서버(40)는 모바일터미널(10)의 인증을 시작한다(S100).

[0106] 보안서버(40)는 자체적인 인증과 모바일터미널(10)의 인증을 수행하는 보안모듈(41)을 실행시켜 모바일터미널(10) 장비 인증을 실행한다. 먼저, 보안모듈(41)은 모바일터미널(10)과 보안서버(40)에 저장된 인증서가 동일한 인증기관(CA)이 발행한 것인지를 확인한다(S110).

[0107] 단계(S110)에 따라 동일 인증기관이 발행된 경우, 보안모듈(41)은 보안서버(40)에 저장된 서버 인증서와 서버 개인키를 통해 검증을 수행에 따른 초기화를 완료한다(S120).

[0108] 단계(S120)에 따라 초기화가 성공적으로 완료되면, 단계(S130)에서 보안모듈(41)은 모바일터미널(10)의 선택적 요청이 있는 경우, 모바일터미널(10)에 저장된 클라이언트 인증서를 수신하여 유효성 확인을 수행하여 결과에 따라 세션을 유지 여부를 결정한다(S140).

[0109] 여기서, 보안모듈(41)은 보안서버(40)에 기저장된 클라이언트 개인키를 이용해 클라이언트 인증서를 검증하며, 클라이언트 인증서는 상술한 바와 같이, 보안서버(40)가 공개키인 클라이언트 개인키를 이용해 유효성 확인을 수행하는 PKI(public key infrastructure) 방식의 인증서인 것에 본 발명의 특징이 있다. 이러한 방식은 종래의 SIM, USIM, UIM과 같은 인증모듈을 이용한 본인 인증과 차별화된다.

[0110] 단계(S130) 또는 단계(S140) 이후, 모바일터미널(10)은 IP네트워크 구간 인증을 수행한다(S150).

[0111] 모바일터미널(10)은 보안AP(20)를 통해 IP네트워크(30)에 접속하는데, 보안AP(20)로의 접속을 통해 EAP-TLS 프로토콜 기능을 이용해 보안AP(20)과 모바일터미널(10) 구간에 대한 암호화를 수행한다.

[0112] 단계(S160)에 따른 IP네트워크 구간 인증이 완료되면, 모바일터미널(10)은 도 5 내지 14와 같이 동작하고 구현되는 자체보안기능을 웨이크-업하면, 자체보안모듈(14)는 자체보안기능이 실행되는 동안 기지국(60)을 통한 이동통신네트워크(70)에 연결된 타 단말, 서버, 그 밖의 시스템과의 통신을 차단한다(S170).

[0113] 또한, 단계(S100) 내지 단계(S170)의 단계를 거친 모바일터미널(10) 만이 상술한 도 5 내지 도 14와 같은 메뉴 구성을 통한 동작이 구현가능한 것을 특징으로 한다.

[0114]

[0115] 본 발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.

[0116] 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기테이프, 플로피 디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어, 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다.

[0117] 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술 분야의 프로그래머들에 의해 용이하게 추론될 수 있다.

[0118] 이상과 같이, 본 명세서와 도면에는 본 발명의 바람직한 실시예에 대하여 개시하였으며, 비록 특정 용어들이 사용되었으나, 이는 단지 본 발명의 기술 내용을 쉽게 설명하고 발명의 이해를 돕기 위한 일반적인 의미에서 사용된 것이지, 본 발명의 범위를 한정하고자 하는 것은 아니다. 여기에 개시된 실시예 외에도 본 발명의 기술적 사상에 바탕을 둔 다른 변형 예들이 실시 가능하다는 것은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 자명한 것이다.

부호의 설명

[0119]

10: 모바일터미널	11: 무선네트워크통신부
12: 이동통신송수신부	14: 보안에이전트
14a: 보안로그 조회/관리 기능단	14b: 프로세스조회 기능단
14c: 연결상태조회 기능단	14d: 리소스모니터링 기능단

14e: SSL테스터

14f: 암호화테스터

17: 데이터저장부

18: 로그저장부

20: 보안AP

30: IP네트워크

40: 보안서버

41: 보안모듈

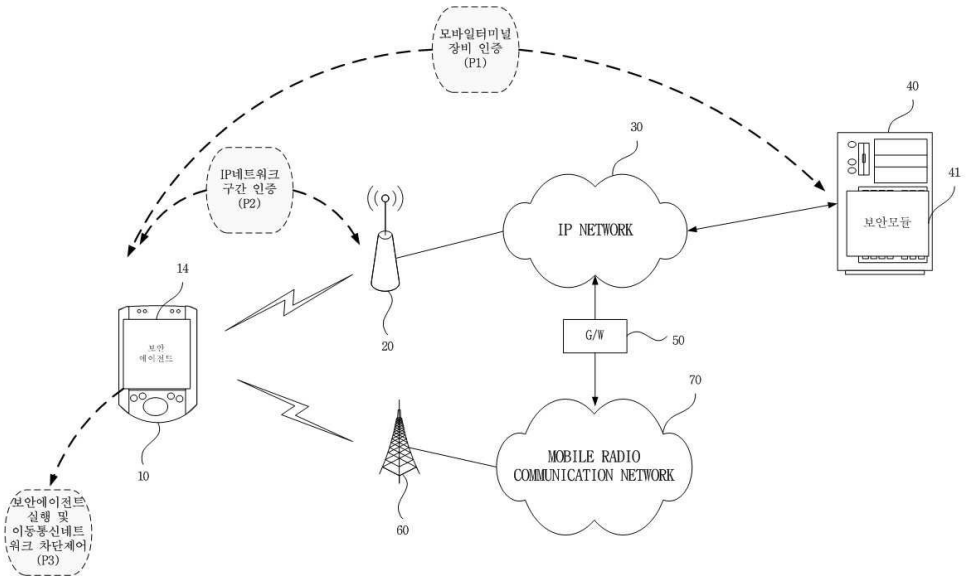
50: 게이트웨이

60: 기지국

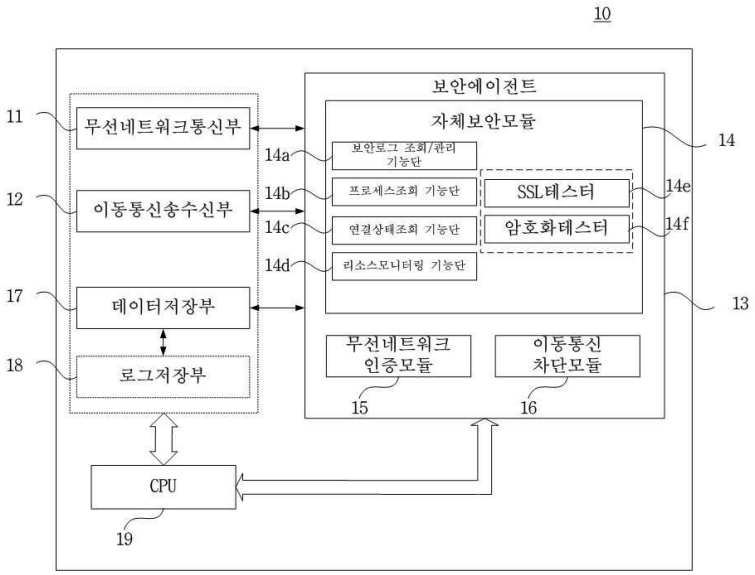
70: 이동통신네트워크

도면

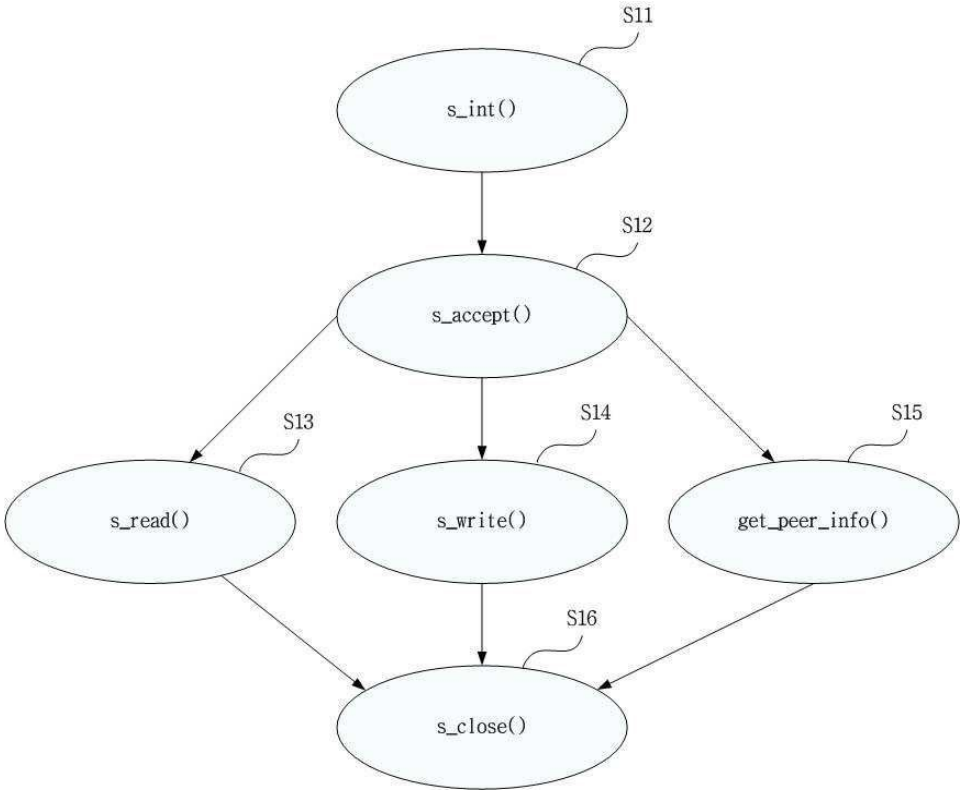
도면1



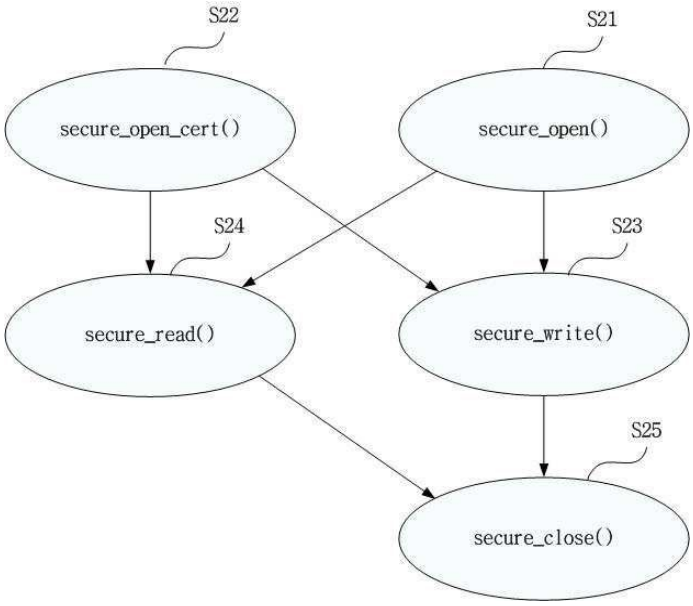
도면2



도면3


S11
s_int()
S12
s_accept()
S13
s_read()
S14
s_write()
S15
get_peer_info()
S16
s_close()

도면4

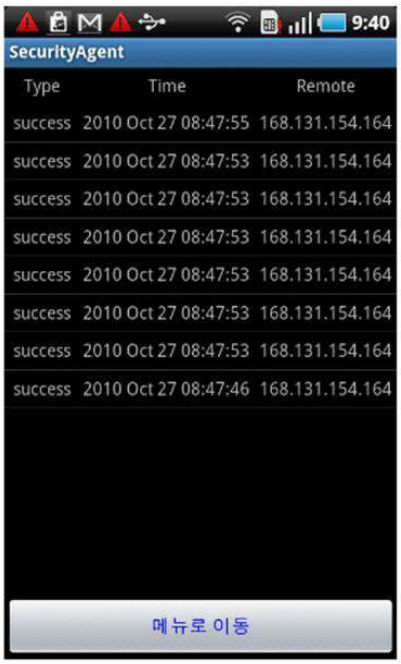

S22
secure_open_cert()
S21
secure_open()
S24
secure_read()
S23
secure_write()
S25
secure_close()

도면5

Security Agent

도면6

도면7


9:40
SecurityAgent
Type Time Remote
success 2010 Oct 27 08:47:55 168.131.154.164
success 2010 Oct 27 08:47:53 168.131.154.164
success 2010 Oct 27 08:47:53 168.131.154.164
success 2010 Oct 27 08:47:53 168.131.154.164
success 2010 Oct 27 08:47:53 168.131.154.164
success 2010 Oct 27 08:47:53 168.131.154.164
success 2010 Oct 27 08:47:53 168.131.154.164
success 2010 Oct 27 08:47:46 168.131.154.164
메뉴로 이동

도면8


9:44
SecurityAgent
Type Time Remote
로그 세부 사항
AppName : SecurityAgent
Type : success
Time : 2010 Oct 27 08:47:53
Remote : 168.131.154.164
Description : Connected to the Server Successfully
삭제
닫기
메뉴로 이동
9:46
SecurityAgent
Type Time Remote
success 2010 Oct 27 08:47:46 168.131.154.164
success 2010 Oct 27 08:47:53 168.131.154.164
success 2010 Oct 27 08:47:53 168.131.154.164
success 2010 Oct 27 08:47:53 168.131.154.164
success 2010 Oct 27 08:47:53 168.131.154.164
success 2010 Oct 27 08:47:53 168.131.154.164
success 2010 Oct 27 08:47:53 168.131.154.164
success 2010 Oct 27 08:47:55 168.131.154.164
메뉴로 이동

(a) (b)

도면9


9:49
SecurityAgent
USER PID NAME
root 1 /init
root 2 kthreadd
root 3 ksoftirqd/0
root 4 watchdog/0
root 5 events/0
root 6 khelper
root 7 async/mgr
root 8 suspend
root 9 sync_supers
root 10 bdi-default
root 11 kblockd/0
root 12 kmmcd
root 13 bluetooth
메뉴로 이동

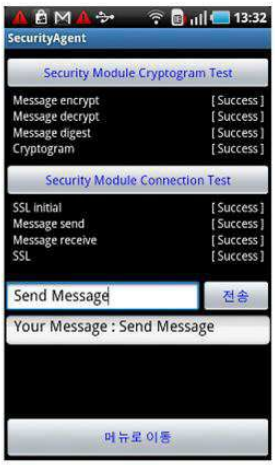
도면10


15:00
SecurityAgent
수신 감도
불량
양호
Wi-Fi 연결 상태
WiFi 사용 중
netstat
Proto Local Foreign State
tcp 127.0.0.1:5037 0.0.0.0:* LISTEN

도면11

도면12

(a)



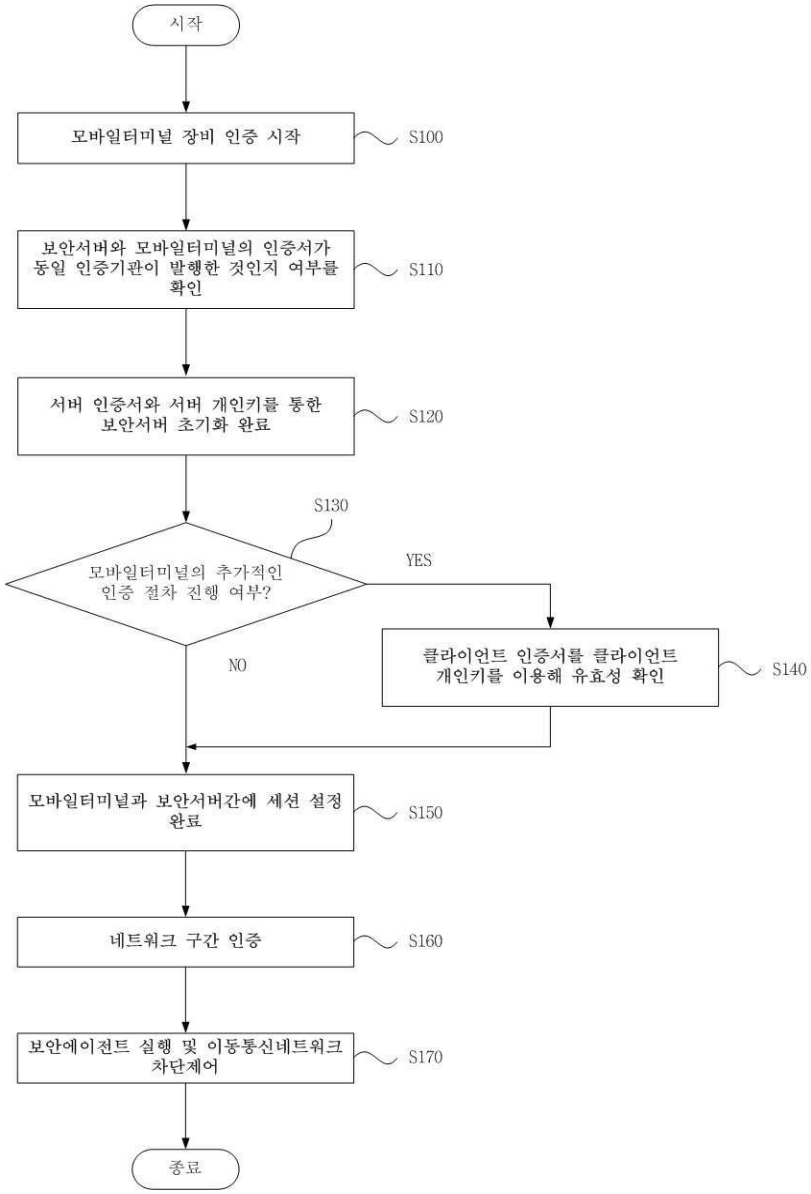
(b)

도면13

(a)

(b)

도면14


시작
모바일터미널 장비 인증 시작
S100
보안서버와 모바일터미널의 인증서가 동일 인증기관이 발행한 것인지 여부를 확인
S110
서버 인증서와 서버 개인키를 통한 보안서버 초기화 완료
S120
S130
모바일터미널의 추가적인 인증 절차 진행 여부?
YES
NO
클라이언트 인증서를 클라이언트 개인키를 이용해 유효성 확인
S140
모바일터미널과 보안서버간에 세션 설정 완료
S150
네트워크 구간 인증
S160
보안에이전트 실행 및 이동통신네트워크 차단제어
S170
종료