(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.[6]
H04Q 7/32

(45) 공고일자 2005년06월07일
(11) 등록번호 10-0492840
(24) 등록일자 2005년05월24일

(21) 출원번호 10-1999-7001850
(22) 출원일자 1999년03월04일
번역문 제출일자 1999년03월04일
(86) 국제출원번호 PCT/US1997/015311
국제출원일자 1997년09월05일
(65) 공개번호 10-2000-0068467
(43) 공개일자 2000년11월25일
(87) 국제공개번호 WO 1998/10611
국제공개일자 1998년03월12일

(81) 지정국

국내특허 : 알바니아, 아르메니아, 오스트리아, 오스트레일리아, 아제르바이잔, 보스니아 헤르체고비나, 바르바도스, 불가리아, 브라질, 벨라루스, 캐나다, 스위스, 중국, 쿠바, 체코, 독일, 덴마크, 에스토니아, 스페인, 핀란드, 영국, 그루지야, 헝가리, 이스라엘, 아이슬랜드, 일본, 케냐, 키르키즈스탐, 북한, 대한민국, 카자흐스탄, 세인트루시아, 스리랑카, 리베이라, 레소토, 리투아니아, 룩셈부르크, 라트비아, 몰도바, 마다가스카르, 마케도니아공화국, 몽고, 말라위, 멕시코, 노르웨이, 뉴질랜드, 슬로베니아, 슬로바키아, 타지키스탄, 투르크맨, 터어키, 트리니아드토바고, 우크라이나, 우간다, 우즈베키스탄, 베트남, 폴란드, 포르투칼, 루마니아, 러시아, 수단, 스웨덴, 싱가포르, 세르비아 앤 몬테네그로, 짐바브웨, 시에라리온, 가나,

AP ARIPO특허 : 케냐, 레소토, 말라위, 수단, 스와질랜드, 우간다, 가나, 짐바브웨,

EA 유라시아특허 : 아르메니아, 아제르바이잔, 벨라루스, 키르키즈스탐, 카자흐스탄, 몰도바, 러시아, 타지키스탄, 투르크맨,

EP 유럽특허 : 오스트리아, 벨기에, 스위스, 독일, 덴마크, 스페인, 프랑스, 영국, 그리스, 아일랜드, 이탈리아, 룩셈부르크, 모나코, 네덜란드, 포르투칼, 스웨덴, 핀란드,

OA OAPI특허 : 부르키나파소, 베닌, 중앙아프리카, 콩고, 코트디브와르, 카메룬, 가봉, 기니, 말리, 모리타니, 니제르, 세네갈, 차드, 토고,

(30) 우선권주장 08/706,574 1996년09월05일 미국(US)

(73) 특허권자 에릭슨 인크.
미합중국 27709 노쓰 캐롤라이나주 리써치 트라이앵글 파크다비스 드라이브 511

(72) 발명자 오스본,윌리엄,알.
미국27513노쓰캐롤라이나주캐리웨이크워털루스태이션드라이브107

(74) 대리인 주성민
안국찬

심사관 : 김지강

(54) 전자 메모리 탬퍼링을 방지하는 시스템

요약

셀룰러 전화 등의 전자 장치내의 메모리를 탬퍼링하는 것을 방지하는 방법 및 장치에 관한 것이다. 메모리 및 처리 수단을 갖는 전자 장치는 장치의 메모리 내용에 대하여 단방향 해시 계산을 실행하기 위해 사용되는 로직을 포함하여, 그러한 내용의 감사 해시값 또는 서명이 구해진다. 감사 해시값은 인증된 메모리 내용에서 구한 인증된 유효 해시값과 비교된다. 감사 해시값과 유효 해시값 사이의 차는 메모리 탬퍼링을 나타낸다. 본 발명의 다른 국면에 따르면, 전자 장치 메모리 내용

은 메모리 내용에 대한 액세스가 허용되기 전에 인증되는 데이터 전송 장치에 의해 갱신될 수 있다. 데이터 전송 장치 인증은 공개/개인 키 암호화 방식의 사용을 수반한다. 데이터 전송 장치가 전자 장치와 인터페이스하여 메모리 액세스를 요구할 때, 데이터 전송 장치를 인증하기 위한 처리가 개시된다.

대표도

도 5

색인어

데이터 전송 장치, 셀룰러 전화, 전자 장치, 공중 교환망, 전자 메모리

명세서

배경기술

본 발명은 전자 메모리 조작(electronic memory manipulation)을 방지하는 시스템에 관한 것으로, 특히 전자 장치(electronic device)에서 바람직하게 안전한 메모리 내용의 허가안된 조작을 방지하는 방법 및 장치에 관한 것이다.

본 명세서에 기재된 발명은 그의 메모리 내용이 안전한 또는 바람직하게는 변경되지 않은 상태로 유지되어야 하는 전자 장치에 관한 것이다. 그러한 요구는 셀룰러 전화 메모리의 부정 조작을 방지하는 등의 보안(security) 이유 또는 항공기 제어 또는 의료 기계 조작 등의 중요한 애플리케이션에 있어서 전자 장치 동작의 완전성을 유지할 목적으로 필요하게 된다. 본 명세서에 기재되고 설명되는 바와 같이, 본 발명의 예시적인 국면은 셀룰러 전화내의 하나이상의 전자 메모리를 안전하게 하는 시스템 및 방법에 대하여 설명된다. 또한, 본 명세서에 기재된 것은 전자 메모리를 액세스하는 것이 허용되기 전에 인증 처리(authentication process)를 받은 데이터 전송 장치를 사용하여, 전자 장치내의 하나이상의 전자 메모리를 액세스하고 그것의 조작을 허용하는 시스템이다. 또한, 셀룰러 전화 애플리케이션의 문맥 상에서 시스템도 설명된다. 본 명세서에 기재된 본 발명의 예시적인 실시예가 안전한 셀룰러 전화 메모리 및 셀룰러 전화에서 메모리 내용을 안전하게 액세스하고 변경하는 수단에 대하여 설명되지만, 당분야의 통상의 기술자라면 본 발명에 따른 시스템이 그의 내용이 변경되지 않고 유지되어야하는 하나이상의 메모리를 갖거나 또는 그의 메모리가 인증된 수단에 의해서만 액세스되어야 하는 전자 시스템에도 적용될 수 있다는 것을 용이하게 이해할 것이다. 따라서, 본 발명의 범위는 본 명세서에 기재된 예시적인 실시예에 의해 제한되는 것이 아니고 그보다는 첨부 특허청구범위 및 그것과 동등한 것에 의해 제한된다.

미국에서는 1995년에 셀룰러 전화 부정 행위(fraud)로 인한 손실이 600 밀리언 달러로 산출되었다. 그에 따라, 제조 업자, 서비스 제공자, 미국 연방 통신 위원회(the Federal Communications Commission : FCC) 및 산업 무역 그룹은 그러한 부정 행위를 제거하기 위해 노력하는 다수의 기술을 연구하였다. 미국에서 행해지는 대부분의 셀룰러 전화 부정 행위는 셀룰러 전화가 통신을 확립하기 위해 제공해야만 하는 셀룰러 전화의 전자 일련 번호(electronic serial number : ESN)를 변경하는 메모리 조작의 형태를 수반한다. 따라서, FCC에 의한 규정은 고려하여, 하나의 부정 행위 방지 기술은 셀룰러 전화 제조 업자에게 모든 마이크로프로세서 코드 및 ESN을 변경불가능하게 할 것을 요구하는 것이다. 본 발명을 수용하는 시스템에 의해 제기되는 관련 문제 및 셀룰러 원격 통신 동작 환경의 설명을 돕도록 기본적인 셀룰러 통신의 백그라운드가 이하에 제공된다.

셀룰러 통신 시스템의 단순화된 레이아웃이 도 1에 도시되어 있다. 이동 전화(mobile telephone) M1-M10은 셀룰러 기지국 B1-B10과 무선 신호를 송수신하는 것에 의해 공중 교환망의 고정부와 통신한다. 또한, 셀룰러 기지국 B1-B10은 이동 교환 센터(Mobile Switching Center : MSC)를 거쳐 공중 교환망에 접속된다. 각각의 기지국 B1-10은 대응 영역 또는 "셀" C1-C10내에서 신호를 송신한다. 도 1에 도시한 바와 같이, 기지국의 이상적인 배치는 최소량의 중복을 갖고, 이동 전화 통신이 보통 발생하는 영역(예를 들면, 대도시 영역)을 실질적으로 커버하도록 조직된다.

사용자가 셀내에서 이동 전화를 기동할 때, 이동 전화는 이동 전화의 존재를 나타내는 신호를 셀의 기지국으로 송신한다. 이동 전화는 각 기지국에 의해 연속해서 감시되는 지정된 셋업 채널 내에서 그의 ESN을 구비할 수 있는 신호를 송신한다. 기지국이 이동 전화의 신호를 수신할 때, 셀내에 이동 전화의 존재를 등록한다. 이 처리는 이동 전화가 다른 셀로 이동하는 경우에 적절히 등록되도록 주기적으로 반복될 수 있다.

이동 전화 번호가 다이얼될 때, 전화 회사 중앙부는 그 번호를 이동 전화로서 인식하고 콜(call)을 MSC로 전송한다. MSC는 현재 등록 정보 및 다이얼된 이동 전화 번호에 따라 페이징 메시지(paging message)를 특정 기지국으로 송출한다. 하나 이상의 기지국이 그의 셋업 채널로 페이지(page)를 송신한다. 다이얼된 이동 전화는 그 셋업 채널상의 그의 식별(identification)을 인식하고, 기지국 페이지에 응답한다. 또한, 이 이동 전화는 할당된 음성 채널에 동조하기 위해 명령에 따른 후 링잉(ringing)을 개시한다. 이동 사용자가 통신을 끝낼 때, 신호 톤(singnaling tone)은 기지국으로 송신되고, 양측은 음성 채널을 해제한다.

상술한 동작에 있어서, 이동 전화는 고정된 네트워크에 영구히 접속되지 않지만 그 대신 소위 "에어 인터페이스(air interface)"를 거쳐 기지국과 통신한다. 물론, 이것은 통신 시스템에 물리적으로 연결하는 제약없이 사용자가 이동 전화를 용이하게 운반할 수 있으므로, 셀룰러 통신 시스템의 유연성을 제공한다. 그러나, 이것과 동일한 특징도 셀룰러 전화 시스템을 거쳐 송신되는 정보를 안전하게 하는 것에 대해서 어려움을 발생시킨다.

예를 들면, 통상의 유선 전화 시스템에서, 중앙 부처 교환국은 물리적으로 부착되어 있는 통신 라인에 의해 설정된 전화 사용에 대하여 특정 가입자를 식별하여 계산서에 기입할 수 있다. 따라서, 가입자 계정의 부정 사용은 통상 물리적 접속이 가입자의 라인에 대하여 이루어질 것을 요구한다. 이것은 자칭 부정 사용자에게 발견될 위험성을 준다.

한편, 셀룰러 원격 통신 시스템은 에어 인터페이스를 거쳐 통신하므로, 자칭 부정 사용자에 대한 접속 문제를 갖지 않는다. 프로텍션이 없는 방식에서는 부정 사용자가 통신을 확립하고 유지하기 위해 여러번 이동 전화에 의해 네트워크로 송신되는 가입자의 전자 일련 번호(ESN)를 액세스함으로써 다른 가입자의 계정을 사용할 수 있다.

표준 셀룰러 접속을 확립함에 있어서, 2개의 식별 코드가 이동 전화에 의해 시스템으로 송신된다. 이들은 이동 식별 번호(Mobile Identification Number : MIN) 및 ESN이다. MIN은 가입자를 식별하고, ESN은 가입자에 의해 사용중인 실제 하드웨어를 식별한다. 따라서, 새로운 기기를 구입하는 가입자로 인해, 특정 ESN에 대응하는 MIN이 시간이 지남에 따라 변하는 것이 기대된다. MIN은 10디지트 디렉토리 전화 번호에서 구해진 34비트 2진 숫자이고, ESN은 이동 전화를 유일하게 식별하는 32비트 2진 숫자이다. ESN은 통상 이동 전화 제조 업자에 의해 설정된다.

예를 들면, 어드밴스드 이동 전화 시스템(Advanced Mobile Phone System : AMPS)에서 통신을 셋업하는 데 사용되는 종래 인증 방법은 도 2에 도시된 흐름도에 의해 설명된다. 이 방법에 따르면, 블록(200)에서 기지국은 이동 전화로부터 ESN과 MIN을 모두 수신한다. 이들 식별 코드는 그들이 그 이동 전화로부터 수신되는 것을 나타내기 위해 ESN_m 및 MIN_m으로 지정된다. 이어서, 블록(202)에서, 기지국은 시스템 메모리에서 MIN_m에 대응하는 ESN_{sys}를 검색한다. 그 후, 블록(204)에서, ESN_{sys}는 ESN_m과 비교된다. 두 개의 일련 번호가 동일하면, 처리는 블록(206)으로 진행하고 시스템 액세스가 허용된다. 그렇지 않으면, 블록(208)에서 시스템 액세스는 거부된다.

이 시스템의 문제점중 하나는 부정 사용자가 에어 인터페이스상에서 또는 다른 소스로부터 엿듣는 것(eavesdropping)에 의해 유효 MIN/ESN 조합을 조립하는 것이 비교적 단순하다는 것이다. 이 종래 시스템에 따른 액세스는 이동 전화로부터 수신된 MIN 및 ESN이 시스템 메모리에 저장된 것에 대응하면 유효라고 추정되므로, 부정 액세스를 위해 필요한 모든 정보가 전자 엿듣기(electronic eavesdropping)에 의해 얻어질 수 있다.
부정 사용을 방지하기 위한 다른 기술이 제안되었다. 예를 들면, 서비스 캐리어에 의해 개인 통신 단말의 식별 번호를 등록하는 방법을 기술하고 있는 미국 특허5,386,486호가 있다. EP 0 583 100 A1은 휴대 전화내 번호 할당 모듈의 불법적 설정을 방지하는 휴대 전화용 번호 할당 모듈을 기술하고 있다.

유럽 GSM 규격(Global System for Mobile Communication), 미국 TIA/EIA/IS136 규격 및 일본 퍼스널 디지털 셀룰러 규격 무선 통신 시스템하에서 동작하는 시스템에 있어서, 엿듣기에 기인하는 부정 행위는 챌린지-응답 방법(challenge-response method)을 사용하여 방지된다. 챌린지-응답 방법에 따르면, 각각의 이동 전화는 그 이동 전화 및 네트워크내 데이터베이스에 저장된 유일한 기밀 키(unique secret key)와 관련된다. 시스템 고유의 알고리즘은 각각의 이동 전화 및 소망 네트워크 노드에 저장된다. 콜이 셋업될 때, 인증이 요구되는 것에 의해, 네트워크는 이동 전화에게 챌린지(난수)를 보낸다. 수신된 챌린지 및 저장된 기밀 키에 따라, 이동 전화는 알고리즘을 사용하여 응답을 계산하고 그 응답을 네트워크로 송신한다. 그와 동시에, 네트워크는 동일한 챌린지 및 네트워크저장 기밀 키에 따라 "기대(expected)" 응답을 계산한다. 그 후, 네트워크는 이동 전화의 계산된 응답을 수신하고, 이동 전화의 계산된 응답과 네트워크의 계산된 응답을 비교한다. 불일치가 발생하면, 적절한 동작이 발생하고, 예를 들면 액세스가 거부되거나 또는 경고 플래그가 설정된다. 이동 무선 시스템에 있어서 기지국과 이동 전화사이에서 인증 검사를 실행하는 방법은 P. Dent 등에게 허여된 미국 특허 제5,282,250호에 기재되어 있다.

AMPS 등의 종래 아날로그 시스템에 있어서, 대부분의 부정 행위는 유효 가입자를 "클론(clone)"한 부정 사용자가 유효 MIN/ESN쌍을 획득하고 그 쌍을 사용하여 셀룰러 전화를 리프로그램하는 것에 의해 방해된다. 더 정교하게 클론으로 되는 구성에 있어서, 셀룰러 전화의 소프트웨어는 몇 개의 MIN/ESN쌍, 실제로 소위 "텀블링(tumbling)"을 사용할 수 있도록 리프로그램된다. 텀블링 루틴에 의해 프로그램된 셀룰러 전화는 MIN/ESN 쌍을 랜덤하게 스크롤하고 선택하여 콜을 개시한다. 부정 행위가 서비스 제공자 또는 가입자에 의해 식별될 때, MIN/ESN쌍은 무효로 된다. 콜 시도시 무효 MIN/ESN쌍과 마주칠 때, 텀블링 루틴은 그 MIN/ESN쌍을 단순히 삭제하고 유효 MIN/SEN쌍을 찾을때까지 스크롤링을 계속한다. 셀룰러 전화에 프로그램된 모든 MIN/ESN쌍이 무효로 된후, 통상 전화 사용자는 셀룰러 전화에 프로그램되는 MIN/ESN 쌍의 새로운 세트를 갖도록 클로너(cloner)로 복귀한다.

대부분의 셀룰러 부정 행위는 몇 단계의 메모리 조작을 수반한다. 이것은 종래 셀룰러 전화 메모리 및 프로세서 구성의 블록도를 도시한 도 3을 참조하여 설명된다. 컨트롤러(300)는 메모리 버스(308)를 사용하여 ROM 또는 플래쉬 프로그램 메모리(320), EEPROM(310) 및 랜덤 액세스 메모리(RAM)(330)와 통신한다. 프로그램 메모리(320)는 셀룰러 전화의 일반적 동작을 위해 사용되는 대부분의 코드를 저장하기 위해 사용되는 불휘발성 판독/기록 메모리이다. EEPROM(310)은 MIN/ESN쌍(314, 316) 및 사용자 프로파일 정보(312)(예를 들면, 스피드 다이얼링 번호)를 저장하기 위해 사용되고, RAM은 스크래치패드 메모리를 판독/기록하기 위해 사용된다. 클로너는 플래쉬 메모리(320) 또는 EEPROM(310)에 저장된 정보를 바이패스 또는 수정하기 위해 사용되는 정보를 모으기 위해 메모리와 컨트롤러(300)사이에서의 메시징을 감시하는 것으로 알려져 있다.

대부분의 일반적인 전화 부정 행위 방법은 ESN을 변경하기 위해 전화 서비스 및 수리를 의도하는 테스트 커맨드의 위법 사용이었다. 그러나, 더욱 최근에 생산된 전화는 그러한 탬퍼링에 강하고, 이러한 공격 방법을 효과적으로 제거한다. 따라서, 클로너는 더욱 정교한 공격 모드에 의존한다.

그러한 기술중 하나는 ESN(314)을 포함하는 원래의 EEPROM(310)을 제거하고 그것을 교환하는 것을 수반한다. 그의 제거에 이어서, EEPROM은 그의 내용을 해독하기 위해 연구된다. 그 후, 해독된 내용은 유효 사용자의 계정으로부터 교체 EEPROM을 유용된(misappropriated) ESN/MIN쌍으로 프로그램하도록 사용된다. 이 기술은 클로너가 하나의 ESN을 한번 변경하기만 원한다면 클로너에게 매력적일 수 있다. 그러나, 이 기술은 큰 노동력을 요하므로, 기술이 형편없는 클로너는 극도로 조심하지 않으면 인쇄 회로를 손상시킬 수 있다.

클로닝 정교화에 있어서 큰 단계는 전화의 마이크로프로세서 프로그램 코드를 해석하고 그 코드의 하나 이상의 부분을 재기입하여 셀룰러 기지국으로 부정한 신원(identity)(ESN/MIN 쌍)을 송신하는 것을 수반한다. 이것은 때때로 전화 하드웨어 디자인의 역 엔지니어링부를 수반하고, 매립된 소프트웨어 디자인의 상당한 이해를 요구한다. 그러나, 이 방법의 명백한 이점은 일단 수정이 완료되면, 필요에 따라 새로운 신원으로 전화를 리프로그램할 수 있는 것이다.

대부분의 정교한 공격은 하드웨어 수정과 조합하여, 상술한 바와 같은 셀룰러 전화의 마이크로프로세서 코드의 변경을 결합한다. 이러한 기술의 일예는 셀룰러 전화가 처음으로 켜질 때 부트-업(boot-up) 처리중에만 실행하는 종래 메모리 확인 루틴에 의한 검출을 방지하기 위해 소위 "셰도우 메모리(shadow memory)"를 사용하는 것이다. 부트-업 처리는 컨트롤러(300)내에 포함된 작은 부분의 부트 코드(304)(도 3 참조)에 따라 실행된다. 부트-업 처리는 셀룰러 전화를 서비스중 상태로 형성하고, 마이크로프로세서(301)내의 프로그램 카운터를 플래쉬 메모리(320)내의 적절한 위치에 설정한다. 이 처리가 완료될 때, 컨트롤러(300)는 사용자에게 전화가 서비스중임을 나타내기 위해 LED(318)(또는 다른 등가의 신호)를 켤 수도 있다. 클로너는 다음에 더욱 상세히 설명하는 바와 같이 플래쉬 메모리(320)내의 정상 동작 코드의 실행을 전복(subvert)하기 위해 컨트롤러(300)와 LED(318)사이의 접속(306)을 감시할 수 있다.

전형적인 최근 셀룰러 전화에 포함된 플래쉬 메모리(320)는 512K의 어드레스가능한 용량을 갖는다. 클로너는 플래쉬 메모리(320)를 제거하고, 그 플래쉬 메모리(320)의 내용을 1024K 셰도우 메모리(322)의 첫 번째 512K에 복사한후 원래의 플래쉬 메모리를 1024K 셰도우 메모리(322)로 교체한다. 부트-업중, 프로그램 메모리에 대한 액세스는 플래쉬 메모리(320)의 첫 번째 512K에 있어서 성공적으로 지시된다. 그 후, 클로너는 셰도우 메모리(322)에 대한 모든 장래 프로그램 메모리 액세스를 전환하기 위해, 부트 처리가 완료된 것(LED 신호(306) 등)을 나타내는 전화에서 유용한 신호를 감시할 수 있다. 그 후, 셀룰러 전화는 텀블링 루틴 코드 및 대응 MIN/ESN쌍을 포함하도록 프로그램될 수 있는 셰도우 메모리(322)에서 찾을 수 있는 명령에 따라 동작한다.
메모리 탬퍼링을 방지하기 위해 여러 가지 시도가 이루어지고 있다. 예를 들면, WO 91/09484는 이동 무선 전화내 메모리 영역의 액세스가 ROM에서 페치된 CPU 명령에 의해서만 허용되는 보안 기술을 기재하고 있다. FR 2 681 965는 특정 이벤트 발생시 기록되는 것에 대하여 메모리를 보호하는 시스템을 기재하고 있다. 부정 사용 및/또는 탬퍼링에 대한 다른 시스템은 셀룰러 전화 프로그래밍을 탬퍼링하고 하가안된 액세스를 숨기는 셀룰러 전화의 원격 액세싱 시스템을 기술하고 있는 미국 특허5,046,082호 및 휴대 객체의 처리 회로에 의해 계산된 서명이 원래의 메시지 서명과 비교되는 프로그램 또는 데이터의 완전성 검사를 기술하고 있는 미국 특허5,442,645호에 기재되어 있다.

대부분의 셀룰러 부정 행위가 몇 단계의 메모리 조작에 기초하므로, 미국 연방 통신 위원회(FCC)는 셀룰러 전화 부정 행위의 이러한 국면에 관한 솔루션을 현재 고려하고 있다. 이 솔루션은 FCC 규칙 §22.219에 수용되어 있다. 현재 기재되어 있는 바와 같이, §22.919는 이동 전화의 운영 소프트웨어가 변경가능으로 되는 것을 금지하고, ESN이 공장에서 설정되어 어떠한 방식으로든 변경, 이동, 제거 또는 조작될 수 없는 것을 요구하고, 제조 업자를 포함하여 관계자가 셀룰러 전화의 ESN, 시스템 로직 또는 펌웨어를 제거, 탬퍼 또는 변경을 시도하면 이동 송신기가 동작불능으로 될 것을 요구한다.

소비자의 관점에서, 제조 업자 또는 그의 공장의 허가된 서비스 대리인이 셀룰러 전화를 프로그램하는 현재의 능력은 적절히 동작하지 않는 셀룰러 전화의 교체를 용이하게 한다. 예를 들면, 가입자의 셀룰러 전화가 적절히 동작하고 있지 않으면, 가입자는 공장의 허가된 대리인으로부터 새로운 장치를 얻고 이전 장치와 동일한 전자 "퍼스널리티(personality)"를 포함하도록 그것을 프로그램할 수 있다. 셀룰러 전화의 전자 퍼스널리티는 ESN뿐만아니라 개인 및/또는 상용 전화 번호 등의 가입자에 의해 장치에 프로그램되는 상당한 양의 정보 및 사용자 프로파일도 포함한다. 셀룰러 전화에 대하여 ESN 및 다른 메모리를 신속하고 용이하게 바꾸는 수리/교체 프로그램 및 기술은 그들의 가입자가 불완전한 단말에 의해 불편하게 되는 것을 원하지 않는 셀룰러 서비스 제공자의 주장에 있어서 개발되었다.

FCC §22.919하에서, 상술한 상황에 있는 가입자는 그들의 이전 장치가 결점이 있으면 새로운 이동 장치를 여전히 얻을 수 있을 것이다. 그러나, 새로운 고정된 ESN이 새로운 장치와 관련되므로, 새로운 ESN 정보는 그것을 그들의 데이터베이스에 프로그램해야 하는 셀룰러 캐리어에게 전달되어야 한다. 이것은 가입자가 서비스를 갖지 않는 장시간을 요할 수 있다. 또한, 가입자는 그들의 셀룰러 전화를 개인 또는 상용 전화 번호로 리프로그램해야 한다. §22.919에 의한 더 많은 중요한 문제는 셀룰러 서비스 제공자가 그들의 셀룰러 전화를 프로그램 또는 리프로그램하는 것에 의해 그들의 가입자에게 시스템 업그레이드를 제공하는 능력에 대하여 가질 수 있는 반대 효과이다.

§22.919의 실제 효과는 다음에 설명하는 시스템을 업그레이드하는 셀룰러 산업의 능력에 대한 것이다. 예를 들면, TIA/EIA/IS-136 규격에 규정된 바와 같은 디지털 제어 채널의 사용은 셀룰러 캐리어가 단문 메시지 서비스 등의 새로운 확장 서비스를 제공하게 하는 것이다. 캐리어, 제조 업자 또는 허가된 대리인에게 셀룰러 전화의 소프트웨어 및/또는 펌웨어를 변경하는 것이 허용되면, 그러한 서비스는 단말의 소프트웨어 업그레이드를 통하여 신속하고 효과적으로 가입자에게 유용하게 될 수 있다. §22.919(그의 현재 형태)하에서, 제조 업자, 제조 업자의 허가된 서비스 대리인 뿐만 아니라 셀룰러 캐리어도 그러한 소프트웨어 변경을 할 수 없다. 캐리어가 가입자에게 시스템 향상을 제공할 수 있는 유일한 방법은 가입자에게 새로운 셀룰러 전화를 구입할 것을 요구하는 것뿐이다.

가입자뿐만 아니라 제조 집단에 관하여 §22.919의 효과를 향상시키기 위해, FCC는 이 규칙이 초기 종류 수용(type acceptance)을 위한 애플리케이션이 1995년 1월 1일이후 제출된 셀룰러 전화에 적용가능하다고 진술한다. 실제로, FCC는 1995년 1월 1일이전 제출된 종류 수용을 위한 애플리케이션에 따라, 현재 동작중인 2천만 셀룰러 전화뿐만 아니라 1995년 1월 1일이후 서비스중인 수백만 셀룰러 전화를 규칙에서 제외하였다. 불법을 목적으로 전자 정보가 조작될 수 있는 수많은 셀룰러 장치가 이미 시장에 있다는 사실은 §22.919가 부정 행위 문제에 대하여 매우 적은 영향을 갖는 다는 것을 의미한다. ESN의 불법적 탬퍼링에 의해 부정 행위를 저지르는 실체는 §22.919 제약을 받지 않는 수백만 단말을 사용하는 것에 의해 계속 그렇게 할 수 있다.

상기로부터 알 수 있는 바와 같이, 안전한 메모리를 갖는 셀룰러 전화의 공급이 매우 요망되고 있다. 현재, 셀룰러 전화를 탬퍼링에 저항하도록 개장하는 솔루션은 출현하지 않고 않다. 또한, 인증된 액세스만 보장하도록 전자 장치 메모리에 갱신을 제공하는 방법 및 장치도 출현하고 있지 않다.

<발명의 요약>

전자 메모리 탬퍼링 및 셀룰러 전화 메모리 탬퍼링을 방지하기 위해 제안된 종래 솔루션 및 방법의 이들 및 다른 문제와 제한은 통상 전자 메모리 내용을 허가안된 액세스 및 조작으로부터 보호하는 본 발명의 예시적인 실시예에 의해 극복된다.

본 발명의 하나의 국면에 따르면, 보안은 전자 장치내 전자 메모리 내용이 탬퍼링되지 않았던 것을 보장하기 위해 그것을 주기적으로 감사하는 것에 의해 달성된다. 감사는 전자 메모리의 선택된 내용에 해시 계산을 실행하여 그러한 내용의 감사 서명 또는 감사 해시값을 구하는 것을 수반한다. 감사 해시값은 인증된 메모리 내용에서 이전에 구한 유효 해시값과 비교된다. 유효 해시값은 전자 메모리내에 암호화된 형태로 저장되고 비교를 위해서만 해독되는 것이 바람직하다. 감사 해시값과 유효 해시값 사이의 불일치는 메모리 탬퍼링을 나타낼 수 있고, 그러한 이유로, 전자 메모리를 포함하는 전자 장치가 작동하지 않게 될 수 있거나 또는 경고 표시가 이루어질 수 있다.

본 발명의 다른 국면에 따르면, 셀룰러 전화 메모리에 포함된 것 등의 전자 메모리 내용(셀룰러 전화의 ESN을 포함함)은 메모리 내용에 대한 액세스가 허용되기 전에 인증된 데이터 전송 장치에 의해 갱신될 수 있다. 데이터 전송 장치 인증은 공개/개인 키(public/private key) 인증 방식의 사용을 수반한다. 데이터 전송 장치가 전자 장치와 인터페이스하여 액세스를 요구할 때, 전자 장치는 데이터 전송 장치를 인증하기 위한 처리를 개시한다. 이것은 전자 장치와 데이터 전송 장치 사이의 일련의 메시지 교환을 수반할 수 있다. 공개 키는 암호화된 메시지를 해독하기 위해 사용되는 전자 장치내에 유지되거나 또는 데이터 전송 장치내에 유지된 기밀 개인 키로 "서명(sign)"된다. 구체적으로, 데이터 전송 장치가 전자 장치를 프로그램할 것을 요구할 때, 인증 처리가 개시된다. 전자 장치는 데이터 전송 장치로 챌린지 메시지를 송출하는 것에 의해 응답한다. 챌린지 메시지는 데이터 전송 장치내에 유지된 개인 키를 사용하여 디지털 서명(digital signature)으로 서명된다. 서명된 챌린지 메시지는 공개 키를 사용하여 그것을 인증하는 전자 장치로 송출된다. 일단 인증되면, 데이터 전송 장치는 전자 장치내의 특권적 커맨드 및 능력을 액세스하는 것이 허용된다.

전자 메모리의 모든 리프로그래밍에 이어서, 전자 장치는 해시 계산을 실행하여 수정된 메모리 내용에 대한 새로운(유효) 해시값을 구한다. 새로운 해시값은 공개 키에 의한 디지털 서명을 위해 데이터 전송 장치로 복귀된다. 서명된 새로운 해시값은 저장을 위해 전자 장치로 복귀된다. 전자 장치가 그 후의 메모리 감사를 실행할 때, 최종 감사 해시값이 새로운 유효 해시값과 비교된다.

도면의 간단한 설명

본 발명의 상기 및 그밖의 목적, 특징 및 이점은 도면과 관련한 설명을 읽을 때 더욱 용이하게 이해될 것이다.

도 1은 셀룰러 통신 시스템의 이상적 레이아웃을 도시한 도면.

도 2는 셀룰러 콜을 설정하는 종래 셀룰러 인증 방법을 설명하는 흐름도.

도 3은 종래 셀룰러 전화 프로세서 및 메모리 구성을 도시한 도면.

도 4는 본 발명의 예시적인 실시예에 따른 셀룰러 전화 프로세서 및 메모리 구성을 도시한 도면.

도 5는 본 발명의 하나의 실시예에 따른 예시적인 셀룰러 전화 개시 처리를 설명하는 흐름도.

도 6은 본 발명에 따른 예시적인 주기적 메모리 확인 처리를 설명하는 도면.

도 7은 본 발명의 하나의 실시예에 따른 예시적인 데이터 전송 장치를 도시한 도면.

도 8은 본 발명의 하나의 실시예에 따라 데이터 전송 장치를 인증하는 예시적인 처리를 설명하는 흐름도.

도 9는 본 발명의 하나의 실시예에 따라 초기 ESN을 셀룰러 메모리에 넣는 예시적인 처리를 설명하는 흐름도.

도 10은 본 발명에 따라 확립된 ESN을 리프로그램하는 예시적인 처리를 설명하는 흐름도.

도 11은 본 발명의 예시적인 실시예에 따른 보호된 메모리 구성을 도시한 도면.

도 12는 본 발명의 하나의 실시예에 따른 예시적인 셀룰러 전화 프로그래머를 도시한 도면.

실시예

본 발명에 따른 장치 및 방법을 수반하는 예시적인 전자 메모리를 셀룰러 전화 애플리케이션의 문맥으로 이하에 설명한다. 다음에 설명하는 예들은 본 발명을 수용하는 이상적인 애플리케이션을 설명하기 위해 단지 제공될 뿐이다.

도 4를 참조하면, 컨트롤러(400)는 셀룰러 전화(예를 들면, 도 12의 (1204) 참조)의 동작을 제어한다. 컨트롤러(400)는 플래쉬 프로그램 메모리(420), EEPROM(electronically erasable programmable read only memory)(410), 및 랜덤 액세스 메모리(RAM)(408)과 관련하여 동작한다. 컨트롤러(400)는 마이크로프로세서(402) 및 내부 판독 전용 메모리(IROM)(403)를 구비한다. IROM(403)은 부트 코드(404), 해싱 코드(405), 인증 코드(409), 및 공개 암호화 키(406)를 포함한다. 또한, 컨트롤러(400)는 보호된 스테이틱 랜덤 액세스 메모리(PSRAM)(407), 인터럽트 컨트롤러(421) 및 선택된 메모리 내용에 대하여 마이크로프로세서(402)가 주기적으로 해시 계산을 개시하기 위한 하드웨어-기반 타이머(hardware-based timer)(401)도 포함한다. EEPROM(410)은 사용자 프로파일 데이터(412), ESN(414), MIN(416) 및 서명된/서명안된(signed/unsigned) 유효 해시값쌍(418)을 구비한다. 셀룰러 전화의 일반적 동작에 수반되는 명령어 코드는 플래쉬 프로그램 메모리(420)에 포함된다. RAM 메모리(408)는 정상 셀룰러 전화 콜 처리의 일부인 동작을 위한 스크

래치패드(scratchpad)로서 사용된다. 민감한 데이터를 수반하는 동작, 해시값 계산 및 인증 처리는 PSRAM(407)과 관련하여 실행되는 것이 바람직하다. 컨트롤러(400)는 플래쉬 프로그램 메모리(420), RAM(408) 및 EEPROM(410)과 메모리 버스(424)를 거쳐 통신한다.

본 발명의 예시적인 실시예에 따라 도 4에 도시한 시스템의 전화기 전원투입 및 메모리 확인을 위한 처리는 도 5에 도시한다. 셀룰러 전화가 켜진후, IROM(403)내의 부트 코드(404)는 컨트롤러를 기동하기 위해 마이크로프로세서(402)에 의해 실행된다(블록 500). 그 후, IROM(403)에 포함된 해시 코드(405)는 EEPROM(410)에 저장된 ESN값(414) 및 플래쉬 프로그램 메모리(420)의 선택된 내용에 대하여 감사 해시값 계산을 실행하기 위해 실행된다(블록 502). 그 후, 컨트롤러는 EEPROM(410)에 저장된 서명된 유효 해시값쌍(418)을 인증한다(블록 504). 이것은 공개 키(406)로 서명된 유효 해시값을 처리한후 그 결과를 서명안된 해시값과 비교하는 것에 의해 서명된 유효 해시값을 인증하는 것을 수반할 수 있다. 그 후, 인증된 해시값은 PSRAM(407)에 저장된다(블록 506). 블록(502)에서 구한 감사 해시값은 블록(504)에서 구한 인증된 해시값과 비교된다(블록 508). 두 개의 해시값이 일치하면, 마이크로프로세서 프로그램 카운터는 플래시 메모리(420)내의 적절한 위치에 설정되고, 주기적 해시값 계산 처리가 인에이블되고(블록 510), 그 후 셀룰러 전화는 정상 동작을 시작한다(블록 512). 블록(508)에서 해시값들이 일치하지 않으면, 시스템은 무한 루프로 들어가거나(블록 514) 또는 그렇지않으면 디스에이블된다. 상기 처리는 그렇게 하는 것이 해시값 불일치를 발생시켜 전화가 동작불능으로 되게 하므로, 클로너가 플래쉬 메모리내 수정된 프로그램 또는 EEPROM(410)내의 수정된 ESN를 교체하는 것을 방지한다.

셰도우 메모리(422)가 정상 동작 개시후 유효 플래쉬 메모리(420)를 대신하는 것을 방지하기 위해, 주기적 해시값 처리를 실행하는 것이 바람직하다. 정상 전화 동작중, 주기적 해시값 계산은 타이머의 만료에 응답하여 또는 다른 시스템 이벤트에 응답하여 발생할 수 있다. 도 4에 도시한 예시적인 실시예에 있어서, 주기적 해시 계산은 NMI(non-maskable interrupt)를 발생시키는 하드웨어-기반 타이머(401)의 만료에 응답하여 개시된다. NMI는 소프트웨어 처리에 의해 "마스크(mask)"될 수 없는 하드웨어지향(hardware-oriented) 인터럽트이다. 따라서, 클로너는 NMI를 무시하도록 설계되는 셰도우 코드를 구성할 수 없다. 정규 인터럽트도 마이크로프로세서 리소스에 대한 액세스를 얻기 위해 정상적인 셀룰러 전화 이벤트로부터의 다른 정규 인터럽트와 경합해야 하는 하드웨어 인터럽트이다. 정규 인터럽트는 서비스를 요구하는 가장 높은 우선 순위 인터럽트로 될 때 인정되어 처리된다.

완전한 해시값 계산은 정상 전화 동작에 의해 견딜 수 있는 것보다 시간이 더 걸릴 수 있으므로, 하나의 주기(예를 들면, 수초)에 걸쳐 펼쳐진 몇 개의 세그먼트로 조각내서 처리를 실행하는 능력을 제공하는 것이 바람직하다. 바람직한 실시예의 다른 국면에 따르면, 하드웨어-기반 타이머는 해시값 계산의 하나의 세그먼트를 실해하기 위해 2개의 스텝 처리를 호출한다. 먼저, 마스크불가능한 인터럽트(NMI)는 주기적 해시값 계산에 포함되도록 스케쥴된 다음 플래쉬 또는 EEPROM 메모리 위치의 내용을 마이크로프로세서가 즉시 검색하여 그것을 PSRAM에 저장하게 한다. NMI는 그것이 발생할 때 액티브로 되는 마이크로프로세서 태스크에 대하여 무시할만한 영향을 미치는 짧고 우선 순위가 가장 높은 종류의 인터럽트이다. 이것은 해시 계산에 의한 검출을 피하기 위해 클론 소프트웨어에 의해 취해질 수 있는 액션이 없다는 것을 보장한다. 두 번째로, NMI 루틴에 의해 이전에 포획된 메모리 바이트에 기초하여 해시값 계산의 현재 세그먼트를 완료하기 위한 서비스를 요구하는 낮은 우선 순위 표준 인터럽트도 하드웨어-기반 타이머(401)에 의해 발생된다. 이 태스크는 정상 콜 처리 태스크가 요구될 때, 하드웨어 타이머가 만료하여 전화를 디스에이블하기 전 미리정한 최대 시간(T)동안 연기될 수 있다. 최대 시간(T)은 모든 합법적인 콜 처리가 완료되고, 해시 계산 세그먼트가 끝나며, 하드웨어 타이머가 만료전 그의 카운트다운 사이클의 처음으로 리셋되기에 충분하도록 선택된다. 해시값 계산의 세그먼트를 주기적으로 완료하기 위해 두 종류의 인터럽트를 사용하는 전략은 셰도우 플래쉬 메모리에 존재하는 클론 소프트웨어에 의해 보안 검사가 바이패스될 수 없는 것을 보장하면서 시스템 응답에 있어서의 모든 저하를 피한다.

본 발명에 따른 예시적인 주기적 해시값 계산 처리를 설명하는 흐름도를 도 6에 도시한다. 이 도면을 참조하면, NMI 및 정규 인터럽트는 하드웨어 타이머(401)의 T1 카운터가 만료할 때(블록 602), 블록(604)에서 발생된다. 일단 NMI가 마이크로프로세서의 제어를 얻으면(블록 604), 해시 계산이 요구되는 플래쉬 또는 EEPROM의 다음 바이트가 PSRAM으로 복사되는동안, 시스템은 짧은 기간동안 정규 인터럽트를 디스에이블 또는 큐(queue)한다(블록 606). 그 후, 제어는 NMI가 발생하였을 때 실행중이었던 태스크로 복귀된다(블록 608). 정상 상태하에서, 짧은 기간내에, 하드웨어-기반 타이머(401)로부터의 정상 인터럽트도 서비스되고(블록 610), 해시 계산의 세그먼트는 PSRAM에 이전에 저장되어 있던 메모리 바이트에 따라 완료된다(블록 616). 해시값 계산이 아직 완료하지 않았으면, 하드웨어-기반 타이머(T1 & T2)(401)는 그들의 초기값으로 리셋되고(블록 624), 정상 전화 동작은 타이머 T1의 다음 만료까지 계속된다(블록 600). 정규 인터럽트가 서비스되기전(블록 610) 타이머 T2가 만료되면(블록 612), 전화는 디스에이블된다(블록 614). 타이머 T2의 디폴트 만료는 (만일 정규 인터럽트가 정확히 서비스되지 않으면) 클로너가 주기적 해시 계산을 디스에이블하는 것을 방지한다.

이러한 해시값의 주기적인 조각 계산은 감사 해시값 계산이 완료될때까지 계속된다(블록 618). 그 후, 이전에 인증된 해시값이 PSRAM에서 페치되고 감사 해시값과 비교된다(블록 620). 그들이 일치하면, 하드웨어-기반 타이머(401)는 리셋되고(블록 624), 전화는 정상적으로 계속 동작한다(블록 600). 그들이 일치하지 않으면, 시스템은 예를들면 마이크로프로세서(402)를 정지 상태(halt condition)로 하는 것에 의해 디스에이블된다(블록 622).

해시 계산이 실행되는 셀룰러 전화 메모리의 선택된 내용은 플래쉬 메모리(420)로부터의 내용 및 EEPROM(414)내의 ESN을 구비하는 것이 바람직하다. 이것은 클로너가 플래쉬 메모리 또는 EEPROM을 물리적으로 제거하거나 또는 수정하고, 셀룰러 캐리어를 속여 빼앗도록 설계된 수정 ESN 및/또는 프로그램 코드를 포함하는 리프로그램된 장치로 그들을 교체하는 것을 방지한다. 선택된 메모리 내용 및 사용된 해시값 계산은 해시값 계산에 포함된 메모리의 하나의 비트라도 수정되면 전화를 동작불능으로 하는 것이 바람직하다.

본 발명의 다른 국면에 따르면, 셀룰러 전화는 데이터 전송 장치를 사용하여 안전한 방식으로 프로그램될 수 있다. 본 발명에 따른 예시적인 데이터 전송 장치를 도 7에 도시한다. 컨트롤러(400)의 참조 숫자, 그의 내용 및 관련 메모리는 도 4의 도면 참조 기호와 동일하다. 예시적인 데이터 전송 장치(750)는 컨트롤러(400)의 IROM(403)내의 공개 암호화 키(406)에 대응하는 개인 암호화 키(754)를 포함하는 안전한 마이크로프로세서(752)를 구비한다. 안전한 마이크로프로세서(752)는 인터페이스(758)를 거쳐 셀룰러 전화 컨트롤러(400)와 통신한다. 인터페이스(758)는 RS-232 링크 등의 유선 시리얼 접속, 무선 적외선 인터페이스 또는 셀룰러 전화의 메인 안테나(도시하지 않음) 등의 RF 인터페이스 또는 셀룰러 전화내의 다른 안테나일 수 있다.

데이터 전송 장치(750)에 의한 셀룰러 전화 메모리 액세스는 엄격한 인증 처리가 완료된 후에만 허용된다. 구체적으로, 컨트롤러(400)(및 관련 메모리 구성 요소)는 데이터 전송 장치(750)가 그의 확실성을 보장하기 위한 챌린지-응답 처리를 받은후에만 데이터를 다운로드하기 위해 액세스될 수 있다. 도 8은 본 발명의 예시적인 실시예에 따라 데이터 전송 장치(750)를 인증하는 예시적인 처리를 설명하는 도면이다. 첫 번째 스텝(블록 800)에서, 전화는 도 5에 대하여 설명한 부정 행위 방지 처리를 사용하여 바람직하게 동작 상태로 된다. 인터페이스가 확립된 후, 안전한 프로세서(752)는 그에 의해 발생된 난수(Rand1)와 함께 컨트롤러(400)에게 프로그래밍 요구 메시지를 송출한다(블록 802). 그에 응답하여, 컨트롤러(400)는 안전한 마이크로프로세서(752)에게 난수 챌린지 코드(Rand2)를 보낸다(블록 804). 그 후, 안전한 마이크로프로세서(752)는 Rand1, Rand2 및 개인 키(754)에 따라 챌린지 응답을 발생한다(블록 806). 그 후, 챌린지 응답은 컨트롤러(400)로 복귀된다(블록 808). 이 챌린지 응답은 Rand1, Rand2 및 공개 키(406)을 사용하여 컨트롤러(400)에 의해 처리된다(블록 810). 그 후, 처리된 챌린지 응답은 그의 값과 Ran2가 비교되는 것에 의해 인증된다.(블록 812). 챌린지 응답이 적절히 해독되면(예를 들면, Rand2), 데이터 전송 장치의 확실성이 검증되고 전화는 프로그래밍 모드로 들어간다(블록 812). 그 후, 데이터 전송 장치(750)는 셀룰러 전화내의 여러 메모리를 액세스할 수 있고 및/또는 새로운 플래쉬 메모리(420) 내용을 다운로드할 수 있다.

챌린지 응답이 유효하지 않으면, 실패 계수가 증가된다(블록 816). 실패 계수는 미리결정된 수(maxcount)에 도달하였는가를 알아보기 위해 검사된다(블록 818). 실패 계수는 데이터 전송 장치(750)가 잡음이 있는 매체를 거쳐 컨트롤러(400)와 통신하고 있는가를 고려한 것이다. 최종 전송 에러는 인증 실패의 원인으로 될 수 있다. 따라서, 셀룰러 전화를 프로그래밍 모드로 하기 위해 데이터 전송 장치(750)에게 한번이상의 기회를 주는 것이 바람직하다. 본 발명의 예시적인 실시예에서는 적절하게 50의 maxcount가 결정되었다. 미리결정된 수에 도달하지 않았으면, 인증 실패가 발생한 것을 나타내는 메시지가 데이터 전송 장치(750)로 보내진다(블록 822). 그러한 지시를 수신할 때, 인증 처리는 블록(802)에서 다시 시작된다. 미리결정된 시도 회수에 도달하였으면, 전화는 동작불능 상태로 되고, 허가된 서비스를 위해 전화가 복귀해야하는 것을 사용자에게 나타내는 메시지가 표시될 수 있다.

데이터 전송 장치(750)가 모든 ESN 리프로그래밍 또는 플래쉬 메모리(420)로의 다운로드를 완료한 후, 전화내의 컨트롤러(400)는 예를 들면 플래쉬 메모리(420)의 수정된 내용 및 ESN(414)을 포함하는 새로운 해시 계산을 시작한다. 최종 해시값은 개인 키(754)를 사용하는 디지털 서명을 위해 데이터 전송 장치(750)로 보내진다. 그 후, 서명된 해시값은 그것과 동일한 해시값의 서명안된 버전과 함께 EEPROM(410)에 저장되도록 컨트롤러(400)로 복귀된다.

ESN은 본 발명에 따라 리프로그램될 수 있지만, 보안 이유로 인해, ESN 프로그래밍은 허가된 공장 대리인에 의해서 보다는 공장에서 실행되는 것이 바람직하다. ESN의 프로그래밍은 두가지 상황, 즉 제조중 초기 ESN 프로그래밍 및 기존의 ESN 리프로그래밍시 발생할 수 있다. 초기 ESN은 도 7에 도시한 것과 마찬가지 데이터 전송 장치를 사용하여 프로그램될 수 있다. 초기 ESN 프로그래밍 처리는 도 9를 참조하여 다음에 설명된다.

첫 번째 스텝(블록 900)으로서, 전화는 동작 상태로 된다(도 5 참조). 전화와의 인터페이스 확립에 이어서, 안전한 프로세서(752)는 ESN 프로그래밍 요구 메시지를 난수(Rand1)와 함께 컨트롤러(400)로 보낸다(블록 902). 컨트롤러(400)는 전화내의 ESN이 새로 제조된 전화인 경우에 항상 제로인 것처럼, 모두 제로인가를 결정하기 위해 검사를 실행한다(블록 904). ESN이 모두 제로가 아니면, ESN 프로그래밍 모드 요구는 거부된다(블록 906). ESN이 모두 제로이면, 도 8의 스텝(804) 내지 (820)에서 설명한 것과 실질적으로 마찬가지인 챌린지-응답 처리가 개시된다(블록(908) 참조). 데이터 전송 장치(750)의 성공적인 인증에 이어서, 새로운 ESN이 EEPROM(410)에 다운로드될 수 있다.

데이터 전송 장치(750)가 ESN을 EEPROM(410)에 다운로드하는 것을 완료한후, 컨트롤러(400)는 새로운 ESN(414)을 구비하는 새로운 해시 계산을 개시한다. 최종 해시값은 개인 키(754)를 사용하는 디지털 서명을 위해 데이터 전송 장치(750)로 보내진다. 그 후, 서명된 해시값(418)은 그것과 동일한 해시값의 서명안된 버전과 함께 EEPROM(410)에 저장되도록 컨트롤러(400)로 복귀된다.

기존의 ESN도 본 발명을 수용하는 시스템에서 리프로그램될 수 있다. ESN리프로그래밍 처리는 법적으로 허가된 공장 대리인이 아니고 공장에서만 실행되는 것이 바람직하다. 공장에서만 이용가능하고, 전화내의 이전에 프로그램된 ESN을 변경하기 위해 전화에 로드되는 한 세트의 마이크로프로세서 명령을 사용함으로써 보안이 추가된다. 이 처리는 도 7에 도시한 것과 마찬가지인 데이터 전송 장치를 사용하여 실행될 수 있고, 이하 도 10을 참조하여 설명된다.

첫 번째 스텝으로서(블록 1000), 전화는 도 8에 도시한 처리에 따라 정규 프로그래밍 모드로 된다. 공장 데이터 전송 장치(750)는 ESN 리프로그래밍을 용이하게 하기 위해 셀룰러 전화의 PSRAM 메모리(407)에 다운로드될 수 있는 ESN 리프로그래밍 코드(756)를 포함한다. 시스템이 프로그래밍 모드로 되었으면, ESN 리프로그래밍 코드(756)는 PSRAM(407)에 다운로드된다(블록 1002). ESN 리프로그래밍 코드(756) 실행시, 컨트롤러(400)는 기존 ESN을 제로로 하고(블록 1004), ESN 리프로그래밍 처리를 개시한다(블록 1006).

데이터 전송 장치(750)가 새로운 ESN을 EEPROM(410)에 입력하는 것을 완료한 후, 컨트롤러(400)는 새로운 ESN(414)을 구비하는 새로운 해시 계산을 개시한다(블록 1008). 최종 해시값은 개인 키(754)를 사용하는 디지털 서명을 위해 데이터 전송 장치(750)로 보내진다(블록 1010). 그 후, 서명된 해시값(418)은 그와 동일한 해시값의 서명안된 버전과 함께 EEPROM(410)에 저장되도록 컨트롤러(400)로 복귀된다(블록 1012).

본 발명의 예시적인 실시예에서 해시값 계산 및 디지털 서명은 단방향 해싱 함수 및 개인/공개 키 인증 방식을 사용하여 실행된다. 단방향 해시 함수는 셀룰러 전화내의 메모리 내용을 나타내는 해시값을 구하기 위해 사용된다. 공개/개인 키 시스템은 EEPROM에 저장된 유효 해시값에 보안을 제공하고 셀룰러 전화내의 메모리를 조작하려는 데이터 전송 장치 또는 프로그래머를 인증하기 위해 사용된다. 단방향 해싱은 당분야 공지이고, 예를 들면, Moore에게 허여된 미국 특허 5,343,527호에 기재되어 있다.

단방향 해시 함수는 순방향에서의 계산은 단순하지만 역방향에서의 계산은 곤란한 함수이다. 단방향 해시 함수 H(M)은 본 발명의 예시적인 실시예에서 선택된 전자 메모리 내용을 구성하는 임의의 길이 입력 M에 대하여 작용한다. M에 대하여 실행되는 해시 함수는 고정 길이 해시값 h를 리턴한다(수학식 1 참조).

수학식 1

$$h = H(M)$$

임의 길이 입력을 취하여 고정 길이의 출력을 발생할 수 있는 수많은 함수가 있지만, 단방향 해시 함수는 다음의 추가 특성을 갖는다. M이 주어질 때, h를 계산하는 것이 용이하고, h가 주어질 때 M을 계산하는 것이 어렵고, M이 주어질 때 H(M)=H(M') 등의 다른 메시지 M'를 찾는 것이 어렵다.

단방향 해시에 대한 기본적 공격은 메모리 입력(해시된 내용)의 해시값이 주어질 때, 클로너가 H(M)=H(M') 등의 다른 세트의 메모리 내용 M'를 만들려고 노력하는 것이다. 클로너가 이것에 성공하면, 단방향 해시 함수의 보안가 훼손된다. 단방향 해시의 목적은 M의 고유한 서명, 즉 지문을 제공하는 것이다. 본 발명에 있어서, 안전한 단방향 해시 함수는 감사 해시값이 발생하도록 셀룰러 전화 메모리의 선택된 내용에 대하여 실행된다. 감사 해시값은 인증된 것으로 알고 있는 메모리로부터의 선택된 메모리 내용에 대하여 단방향 해시 함수를 실행하는 것에 의해 미리 발생된 유효 해시값과 비교된다.

바람직한 실시예에서, MD5 등의 메시지 다이제스트 알고리즘은 안전한 단방향 해시 계산을 위해 사용된다. MD5 알고리즘은 입력 메시지(즉, 선택된 메모리 내용)의 메시지 다이제스트 또는 N비트 해시를 발생한다. MD5 알고리즘은 선택된 내용내의 하나의 비트 변경이 통계적으로 해시값 비트 변경의 절반으로 이어짐에 있어서 매우 민감하다. MD5 알고리즘은 그의 속도 및 단순성 때문에 알려져 있다. 속도는 셀룰러 전화의 마이크로프로세서에 대한 시간 요구가 통상의 시스템 처리와 용인할 수 없게 인터페이스할만큼 크게 될 수 없다는 점에 있어서 중요한 고려사항이다.

MD5 알고리즘은 증분 기준으로 실행되어 해시 처리의 인터럽트를 허용하는 것에 의해 정규 마이크로프로세서 태스크가 해싱이 재개되기 전에 어드레스될 수 있으므로 적당하다. 또한, MD5 알고리즘은 종래 마이크로프로세서 아키텍쳐에 사용하기에도 적합하다. 본 발명의 실시예에 따라 사용될 수 있는 다른 단방향 해시 알고리즘은 이것에 제한되는 것은 아니지만, Serfu, H-Hash, MD2, MD4, SHA(Secure Hash Algorithm) 및 HAVAL을 구비한다. 당분야의 통상의 기술자는 단방향 해시 처리를 실행하도록 마이크로프로세서를 용이하게 프로그램할 수 있을 것이다.

공개 키 알고리즘은 두 개의 키, 즉 메시지를 암호화하고 해독하는 등의 태스크, 메시지 인증 및 디지털 서명을 위해 개인적으로 유지되는 것(기밀)과 공개적으로 이용가능한 것을 사용한다. 이 키는 다른 목적을 달성하기 위해 다른 방식으로 사용될 수 있다. 예를 들면, 메시지 기밀을 유지하는 것이 목적이면, 수신자만이 메시지를 해독할 수 있도록 개인 키가 수신자에 의해 안전하게 유지되어야 한다. 그러한 경우, 암호화 키는 공개적으로 알려져야 하고 또한 특정의 잠재적 수신자와 관련되도록 알려져야 한다. 송신자가 이 처리에 있어서 정보 비밀을 보장할 수 있더라도, 수신자는 송신자 확실성을 보증할 수 없다. 한쌍의 키중 개인(기밀) 키가 암호화를 위해 송신자에 의해 기밀로 유지되면, 대응하는 공개 키를 갖는 수신자는 기밀의 보증이 없음에도 불구하고, 송신자의 확실성을 보증할 수 있다. 이것은 본 발명에 따른 데이터 전송 장치를 인증하기 위해 사용되는 후자의 방식이다.

공개 키 알고리즘은 공개 키로부터 개인 키를 추론하기 위해 연산 불가능으로 되는 수학적 트랩도어 함수에 따라 작용한다. 공지의 RSA(Rivest, Shamir, Adleman) 알고리즘의 경우에 있어서, 보안는 두 개의 큰 소수의 곱을 인수분해하는 것의 어려움에 의존한다. 키 선택은 함께 곱해져 큰수 n을 생성하는 두 개의 큰 소수 p 및 q의 선택부터 시작한다.

수학식 2

$$n = pq$$

그 후, 암호화 키 e는 e 및 (p-1)(q-1)이 상대적 소수가 되도록 랜덤하게 선택된다. 마지막으로, 유클리드의 알고리즘(Euclid's algorithm)을 사용하여,

수학식 3

$$F = (p-1)(q-1)$$

수학식 4

$$ed = 1 (\mathrm{mod}\ F)$$

로 되는 해독 키 d를 계산한다.

수 e 및 n은 공개 키이고, 수 d는 개인 키이다. 수학식 5는 RSA 암호화 처리를 제공하고, 수학식 6은 해독 처리를 제공한다.

수학식 5

$$C = M^{e} (\mathrm{mod}\ n)$$

수학식 6

$$M = C^{d} (\mathrm{mod}\ n)$$

n을 인수분해할 수 있는 상대자는 수학식 3을 사용하여 모듈러스 F를 결정한 후, 공개 키 e가 주어질 때 수학식 4에서 개인 키 d를 결정할 수 있다. 물론, 상술한 바와 같이, n은 통상 그러한 인수분해를 불가능하게 할 정도로 크다. RSA 알고리즘의 더욱 상세한 것은 Rivest 등에게 허여된 미국 특허4,405,829호에서 찾을 수 있다.

본 발명의 바람직한 실시예에서는 FS(Fiat-Shamir) 알고리즘 또는 그의 변형이 사용된다(그의 내용이 본 명세서에 참조로서 모두 포함된 미국 특허4,748,668호 참조). FS 알고리즘은 통상의 셀룰러 전화의 연산 능력을 제한하기에 잘 맞는 인증 및 디지털 서명 방식을 이행하도록 적응된다.

FS 알고리즘은 2차 나머지(quadratic residue)(v_i) 모듈로 n의 역수를 찾는 어려움에 따라 인수를 사용하는 점에 있어서 RSA 등의 이전 방식과 다르다. 구체적으로, FS 방식은 길이가 바람직하게는 512와 1064비트 사이에 있는 두 개의 큰 소수의 곱인 수 n을 선택하는 것을 수반한다. 공개 키(v):v_1, v_2, ...v_k 및 개인 키(s):s_1, s_2, ...s_k는 s_i = sqrt($1/v_i$) mod n으로 되도록 발생된다. 상기 식의 문맥내에서 역수 ($1/v_i$) mod n을 찾음에 있어서의 어려움은 소수 n의 인수를 찾는것의 어려움과 동일한 것으로 보여질 수 잇다. 보안를 희생하지 않고, 이 알고리즘은 다른 방식보다 더욱 더 신속하게 실행한다. 실제로, FS 방식은 FS 계산이 필요한 인증 연산을 완료하기 위해 통상 필요한 모듈 곱셈의 단지 1% 내지 4%만을 요구하는 점에 있어서 RSA 방식을 능가한다고 알려져 있다. 이것은 동일한 태스크를 실행하기 위해 RSA 방식을 사용하는 것보다 크기가 2자리수 향상한 속도에서의 서명된 해시값의 인증에 대응한다. 따라서, 데이터 전송 장치 인증 및 주기적 감사 해시값 비교는 RSA 방식을 사용하는 것보다 FS 방식을 사용하여 상당히 빠르게 실행될 수 있다. 셀룰러 전화 또는 다른 전자 메모리를 공장 단계에서 대량으로 프로그램할 때, FS 알고리즘을 사용하는 것은 저장을 위해 유효 해시값의 디지털 서명을 더욱 신속히 발생하는 것에 의한 생산 시간을 저감시킨다. 적용가능한 다른 알고리즘은 이것에 제한되는 것은 아니지만, ELGAMAL, DSA, Fiege-Fiat-Shamir를 포함한다.

본 발명의 다른 국면에 따르면, 셀룰러 전화내의 컨트롤러 하드웨어는 클로너가 안전한 메모리의 내용을 결정하거나 또는 그렇지않다면 상술한 보안 방식을 바이패스하는 것을 방지하는 보안 특징을 갖는다. 도 11은 컨트롤러 하드웨어, 외부 메모리 및 메모리/어드레스 버스 구성의 상세를 도시한 것이다. 칩 셀렉트 로직(1122) 및 보안 로직(1124)을 제외하고, 컨트롤러내 구성 요소의 기능 및 동작은 도 4에서 설명한 것과 동일하다. 칩 셀렉트 로직(1122)은 마이크로프로세서 어드레스 버스(1102)상의 어드레스를 디코드하여, 버스(1102)에 접속된 메모리 구성 요소 및 하드웨어 장치에게 하드웨어 선택 신호를 제공한다. 예를 들면, 어드레스가 IROM 메모리(403)에 할당된 어드레스 버스(1102)에 나타날 때, IROM 칩 셀렉트(CS)가 인에이블된다.

보안 로직(1124)은 IROM 메모리(403)이외의 메모리 장치에 저장된 마이크로프로세서 명령 코드를 사용하여 하드웨어-기반 타이머(401)를 리셋하거나 또는 RSRAM(407)의 내용을 액세스하려는 시도를 검출하도록 기능하다. 예를 들면, PSRAM(407)내 메모리 위치의 타겟 어드레스를 갖는 플래쉬 메모리(420)에 위치된 판독 또는 기록 명령이 불법 동작으로서 검출될 수 있다. 모든 불법적 액세스 시도는 마이크로프로세서가 정상 동작을 개재하기 위해 셀룰러 전화의 완전한 파워 리셋을 요구하는 정지 상태로 되게 한다.

보안 로직은 다음 논리식의 구현이다.

논리식 1 S = ↑Supvr·B

논리식 2 Halt = notS·(A+ C)

여기서, S = 보안 모드

↑Supvr = 마이크로프로세서의 감독 모드로의 천이

A = PSRAM 메모리의 칩 셀렉트 신호

B = IROM 메모리의 칩 셀렉트 신호

C = 하드웨어 타임의 칩 셀렉트 신호

Halt = 파워가 제거되고 전화에 재공급될 때까지 마이크로프로세서가 무한 루프로 되거나 또는 영구 대기 상태로 되게 하는 마이크로프로세서로의 하드웨어 제어 입력.

상기 논리식1은 IROM(403) 칩 셀렉트가 액티브임(·B)과 동시에 마이크로프로세서가 감시 모드로 천이할때마다(↑Supvr) 보안 모드(S)가 설정되는 것을 의미한다. 상기 논리식2는 컨트롤러(400)가 보안 모드가 아니고(not S) PSRAM(407) 또는 하드웨어 타이머 칩 셀렉트가 액티브(·(A+C))이면, 마이크로프로세서 정지 입력이 활성화되는 것을 의미한다. 이 로직은 PSRAM(407)에 대한 합법적 액세스 및 하드웨어 타이머(401)에 대한 리셋 커맨드가 IROM(403)에 저장된 코드로부터 나오는 것이 바람직하므로, 상술한 해시값 비교 및 인증 처리에 의해 제공되는 보안 측정(measures)의 바이패스를 효과적으로 방지한다.

IROM 메모리(403)내에 위치한 모든 합법적 코드(부트 코드, 해시 코드, 공개 키 코드, 인증 코드)는 보안 모드를 루틴의 처음에 설정하고 그 루틴을 종료할 때 클리어되게 하는 명령에 의해 일괄처리되는 것이 바람직하다. 본 발명의 바람직한 실시예에서, 소프트웨어 인터럽트 명령(최근 마이크로프로세서에서 공통적으로 이용가능함)은 마이크로프로세서(402)가 감시 모드로 전환되고 마이크로프로세서 하드웨어 신호 SPVR이 액티브로 되게 하도록 IROM(403)내 각 루틴의 처음에 있다. IROM(403) 칩 셀렉트 신호가 그때에 액티브로 되므로, 보안 모드 S가 설정된다. 소프트웨어 루틴의 끝에서 리턴 명령을 실행하는 것은 보안 모드를 취소시킨다.

본 발명의 다른 국면에 따르면, 데이터 전송 장치는 범용 컴퓨터와 조합하여 사용될 수 있는, 공장에서 제공한 보안 유닛(factory-supplied security unit)을 포함한다. 예시적인 구성을 도 12에 도시한다. 보안 유닛(1200)은 표준 커넥터(1206)를 거쳐 PC(1202)의 I/O 포트에 부착된다. PC(1202)의 제2포트는 셀룰러 전화(1204)와의 인터페이스를 위해 RS-232, 케이블 또는 적외선 링크 등의 제2표준 커넥터(1208)과 관련하여 사용된다. 도 8에 도시한 처리는 셀룰러 전화 리프로그래밍 처리를 실행하기 위해 도 12에 도시한 구성을 사용하여 실행될 수 있다. 표준 PC 및 보안 유닛(1200)을 갖는 허가된 공장 서비스 대리인은 전화를 리프로그램하기 위해 구비된다.

본 발명의 또 다른 국면에 따르면, 기존의 셀룰러 전화에는 내부 인쇄 회로 카드 어셈블리에 대한 액세스를 획득하는 것을 수반하지 않는 공격에 대하여 안전한 필드 프로그래밍 능력이 제공될 수 있다. 이러한 보호 수준은, 전화내 메모리 내용을 외부 전화 커넥터를 통하여 액세스가능한 테스트 커맨드를 사용하여 수정하는 클로닝 공격의 대부분의 일반적 방법에 대하여 매우 효과적이다. 이것은 필드 프로그래밍 커맨드에 대한 액세스 승인에 앞서 도 8에서 설명한 DTD(Data Transfer Device) 인증 프로시저를 사용하도록 현재 셀룰러 전화를 업그레이드하는 것에 실행될 수 있다. 인증 소프트웨어 코드 및 공개 키는 모두 기존의 플래쉬 메모리에 저장되므로, 기존의 종래 설계에 대한 모든 변경을 피할 수 있다.

본 발명의 예시적인 애플리케이션은 셀룰러 전화내 전자 메모리를 안전하게 하고 프로그래밍하는 것에 적용되는 단방향 해싱 및 키 암호화 시스템에 대하여 설명되었다. 그러나, 당 분야의 통상의 기술자는 메모리 내용의 서명을 구하는 모든 적절한 함수, 계산, 알고리즘, 방법 또는 시스템이 본 발명에 따라 적용될 수 있다는 것을 용이하게 이해하고 인식할 것이다. 또한, 본 발명은 특정 실시예를 참조하여 설명되었다. 그러나, 상술한 바람직한 실시예 이외의 특정 형태로 본 발명을 구현할 수 있는 것이 당업자에게 용이하고 명확하게 될 것이다. 예를 들면, 본 발명의 정신을 벗어나지 않고 전자 메모리 및/또는 전자 메모리 프로그래밍 또는 액세싱 장치에 있어서 본 발명을 구현할 수 있다. 또한, 본 발명은 디지털 신호 프로세서, 애플리케이션 지정 프로세서 또는 그밖의 프로세서 또는 전자 메모리 지향 시스템에 적용되어 실행될 수 있다. 따라서, 본 명세서에서 설명된 바람직한 실시예는 단지 예시이고 어떠한 방식으로든 제한되는 것으로 고려되어서는 아니된다. 본 발명의 범위는 이전 설명에 의하기 보다는 첨부 특허청구범위에 의해 주어진다.

(57) 청구의 범위

청구항 1.

메모리(410, 420); 및

인증된 메모리 내용에 대해 해시 계산을 실행하여 유효 해시값을 생성하는 수단, 하드웨어-기반 시간의 만기에 따라 상기 해시값을 주기적으로 도출하는 수단, 상기 메모리(410, 420)의 내용에 대해 해시 계산을 실행하여 감사 해시값(audit hash value)을 도출하는 수단, 및 상기 감사 해시값과 상기 유효 해시값을 비교하는 수단을 포함하는 마이크로프로세서(402)

를 포함하며,

상기 계산 및 비교는 탬퍼링(tampering)으로부터 안전한 전자 장치.

청구항 2.

제1항에 있어서,

상기 마이크로프로세서(402)는 상기 감사 해시값을 주기적으로 도출하고 상기 감사 해시값과 상기 유효 해시값을 비교하는 수단을 포함하는 전자 장치.

청구항 3.

삭제

청구항 4.

제1항에 있어서,

상기 메모리는 플래쉬 메모리(420) 및 EEPROM(410)을 포함하는 전자 장치.

청구항 5.

제1항에 있어서,

상기 마이크로프로세서(402)와 함께 상기 해시 계산을 실행하는 보호된 랜덤 액세스 메모리(407)를 더 포함하는 전자 장치.

청구항 6.

제4항에 있어서,

상기 마이크로프로세서는 상기 플래쉬 메모리(420) 및 상기 EEPROM(410)의 선택된 내용에 기초하여 상기 감사 해시값을 도출하는 수단을 포함하는 전자 장치.

청구항 7.

제6항에 있어서,

상기 선택된 내용은 전자 일련 번호를 포함하는 전자 장치.

청구항 8.

제6항에 있어서,

상기 선택된 내용은 마이프로프로세서 프로그램 코드를 포함하는 전자 장치.

청구항 9.

제1항에 있어서,

상기 마이크로프로세서(402)는 상기 메모리(410, 420)내에 저장된 공개 키를 사용하여 상기 유효 해시값을 인증하는 수단을 포함하는 전자 장치.

청구항 10.

제1항에 있어서,

상기 마이크로프로세서(402)는 개인 키를 사용하여 주어진 디지털 서명으로 상기 유효 해시값을 암호화하는 수단을 포함하는 전자 장치.

청구항 11.

제1항에 있어서,

상기 마이크로프로세서(402)는 Snerfu, H-Hash, MD2, MD4, MD5, SHA(Secure Hash Algorithm) 및 HAVAL를 포함하는 해시 함수군 중의 하나를 사용하여 상기 해시 계산을 실행하는 수단을 포함하는 전자 장치.

청구항 12.

제1항에 있어서,

상기 마이크로프로세서(402)는 ELGAMAL, RSA, DSA, Fiege-Fiat-Shamir 및 Fiat-Shamir를 포함하는 공개/개인 키 시스템 알고리즘군중의 하나를 사용하여 인증 및 암호화하는 수단을 포함하는 전자 장치.

청구항 13.

제5항에 있어서,

상기 보호된 랜덤 액세스 메모리에 대한 액세스를 감독하는 보안 로직을 더 포함하는 전자 장치.

청구항 14.

제1항에 있어서,

상기 전자 장치는 셀룰러 전화인 전자 장치.

청구항 15.

제6항에 있어서,

상기 플래쉬 메모리의 내용은 상기 전자 장치의 동작 명령어들을 포함하고, 상기 EEPROM의 내용은 유효 해시값을 포함하고, 상기 마이크로프로세서는 인증된 플래쉬 및 EEPROM 내용의 선택된 부분들에 단방향 해시 계산을 실행하여 유효 해시값을 발생하는 수단, 상기 선택된 부분들에 상기 해시 계산을 수행하는 것에 의해 감사 해시값을 주기적으로 발생하는 수단, 및 상기 플래쉬 및 상기 EEPROM 메모리중 적어도 하나가 변경되었는 가를 평가하기 위해 상기 감사 해시값과 상기 인증된 유효 해시값을 비교하는 수단을 포함하는 전자 장치.

청구항 16.

제15항에 있어서,

상기 마이크로프로세서(402)는 Snerfu, H-Hash, MD2, MD4, MD5, SHA(Secure Hash Algorithm) 및 HAVAL를 포함하는 해시 함수군 중의 하나를 사용하여 단방향 해시 계산을 실행하는 수단을 포함하는 전자 장치.

청구항 17.

제10항에 있어서,

상기 마이크로프로세서(402)는 상기 전자 장치 외부의 처리 수단을 사용하여 상기 개인 키에 의해 디지털 서명으로 상기 유효 해시값을 암호화하는 수단을 포함하는 전자 장치.

청구항 18.

전자 장치에서 메모리 탬퍼링을 검출하는 방법에 있어서,

선택된 메모리 내용이 인증된 메모리(410, 420)의 상기 선택된 내용에 대해 해시 계산을 실행하는 것에 의해 발생되는 서명된 유효 해시값을 저장하는 단계;

상기 메모리(410, 420)의 상기 선택된 내용에 대해 상기 해시 계산을 실행하는 것에 의해 감사 해시값을 발생하는 단계; 및

상기 감사 해시값과 상기 유효 해시값을 비교하여 상기 감사 해시값과 상기 유효 해시값 사이의 차가 상기 선택된 메모리 내용의 변경을 나타내도록 하는 단계

를 포함하며,

상기 저장 단계, 발생 단계, 및 비교 단계는 탬퍼링으로부터 안전한 방법.

청구항 19.

제18항에 있어서,

상기 감사 해시값을 발생하는 단계는 보호된 랜덤 액세스 메모리(protected random access memory)(407)와 함께 실행되는 방법.

청구항 20.

제18항에 있어서,

개인 키에 기초하여 디지털 서명으로 상기 유효 해시값을 서명하는 단계를 더 포함하는 방법.

청구항 21.

제18항에 있어서,

상기 감사 해시값을 발생하고 상기 감사 및 유효 해시값을 비교하는 단계들은 주기적으로 실행되는 방법.

청구항 22.

제14항에 있어서,

상기 감사 해시값을 발생하는 단계는 하드웨어-기반 타이머의 만료에 따라 실행되는 방법.

청구항 23.

제14항에 있어서,

상기 감사 해시값을 발생하는 단계는 감사 해시값 세그먼트들을 계산하는 것을 수반하는 방법.

청구항 24.

제23항에 있어서,

상기 감사 해시값 세그먼트의 계산은 상기 전자 장치내에서 발생하는 다른 처리가 완료되는 동안 필요에 따라 지연될 수 있는 방법.

청구항 25.

제18항에 있어서,

상기 유효 해시값에는 디지털 서명이 주어지고, 상기 감사 해시값과 상기 유효 해시값을 비교하는 단계는 상기 서명에 대하여 상기 유효 해시값을 인증하는 단계를 포함하는 방법.

청구항 26.

제18항에 있어서,

상기 전자 장치는 셀룰러 전화인 방법.

청구항 27.

메모리 프로그래밍 능력을 갖는 전자 장치에 대한 허가안된 액세스를 방지하는 시스템에 있어서,

데이터 전송 장치(750)로부터 수신된 액세스 요구 메시지에 응답하여 챌린지-응답(challenge-response) 인증 처리를 개시하는 마이크로프로세서(402)를 포함하며,

상기 데이터 전송 장치(750)는 개인 암호화 키를 사용하여 챌린지 메시지를 서명하는 수단, 및 상기 서명된 챌린지 메시지를 상기 전자 장치로 송신하는 수단을 포함하고,

상기 전자 장치는 상기 개인 암호화 키에 대응하는 공개 키를 사용하여 상기 서명된 챌린지 메시지를 인증하는 수단, 및 상기 챌린지 메시지가 상기 인증에 의해 복구되지 않으면, 상기 데이터 전송 장치(750)를 거부하는 수단을 더 포함하는 시스템.

청구항 28.

제27항에 있어서,

상기 전자 장치는 셀룰러 전화인 시스템.

청구항 29.

제28항에 있어서,

제1 및 제2 포트를 갖는 범용 컴퓨터를 더 포함하며,

상기 데이터 전송 장치(750)는 상기 제1 포트에 부착하기 위한 수단을 포함하고, 상기 셀룰러 전화는 상기 제2 포트에 부착하기 위한 수단을 포함하고, 상기 셀룰러 전화는 상기 데이터 전송 장치로부터 수신된 상기 셀룰러 전화를 프로그램하라는 요구에 응답하여 챌린지를 리턴하는 수단을 포함하고, 상기 챌린지는 상기 데이터 전송 장치에 의해 서명되고 인증을 위해 상기 셀룰러 전화로 리턴되어, 상기 서명된 챌린지의 인증을 통한 상기 챌린지의 복구가 데이터 전송 장치 인증을 나타내어 상기 셀룰러 전화가 프로그래밍 모드로 진입하게 되는 시스템.

청구항 30.

메모리 프로그래밍 능력을 갖는 전자 장치에 대한 허가안된 액세스를 방지하는 방법에 있어서,

데이터 전송 장치로부터의 액세스 요구 메시지에 응답하여 챌린지 메시지를 송신하는 단계;

개인 암호화 키를 사용하여 상기 데이터 전송 장치(750)에서 상기 챌린지 메시지를 서명하는 단계;

상기 전자 장치로 상기 서명된 챌린지 메시지를 송신하는 단계;

상기 개인 암호화 키에 대응하는 공개 키를 사용하여 상기 전자 장치(750)내에서 상기 서명된 챌린지 메시지를 인증하는 단계; 및

상기 챌린지 메시지가 상기 인증 단계에 의해 복구되지 않으면, 상기 데이터 전송 장치(750)를 거부하는 단계

를 포함하는 방법.

청구항 31.

제30항에 있어서,

상기 전자 장치는 셀룰러 전화인 방법.

청구항 32.

제30항에 있어서,

상기 서명된 챌린지 메시지는 상기 챌린지 메시지의 부분들에 의존하는 챌린지 응답 메시지이고, 상기 방법은 상기 서명된 챌린지 응답 메시지가 상기 데이터 전송 장치의 인증을 확인하면 인증의 프로그래밍 모드로 진입하는 단계를 더 포함하는 방법.

청구항 33.

프로그래밍 능력을 갖는 전자 장치에 있어서,

상기 전자 장치에 대한 허가안된 액세스를 방지하는 마이크로프로세서(402)를 포함하며,

상기 전자 장치는 데이터 전송 장치(750)로부터의, 상기 전자 장치를 액세스하려는 요구에 응답하여 상기 데이터 전송 장치에게 챌린지 메시지를 발생하는 수단을 포함하고,

상기 데이터 전송 장치는 개인 암호화 키를 사용하여 상기 챌린지 메시지를 서명하는 수단, 및 상기 전자 장치로 상기 서명된 챌린지 메시지를 송신하는 수단을 포함하고,

상기 전자 장치는 상기 개인 암호화 키에 대응하는 공개 키를 사용하여 상기 서명된 챌린지 메시지를 인증하는 수단, 및 상기 챌린지 메시지가 상기 인증에 의해 복구되지 않으면 상기 데이터 전송 장치(750)를 거부하는 수단을 더 포함하는 전자 장치.

청구항 34.

제33항에 있어서,

상기 전자 장치는 셀룰러 전화이고, 상기 데이터 전송 장치는 프로그래머인 전자 장치.

청구항 35.

메모리 액세스를 방지하는 시스템에 있어서,

마이크로프로세서(402);

명령어 코드를 포함하는 판독 전용 메모리(403);

보호된 랜덤 액세스 메모리(407); 및

상기 보호된 랜덤 액세스 메모리(407)에 대한 액세스 시도들을 검출하고, 상기 판독 전용 메모리(403)에 의한 액세스를 허용하고, 그렇지 않으면 상기 마이크로프로세서(402)를 정지 상태로 하고 그러한 액세스를 방지하는 보안 로직(1124)

을 포함하는 시스템.

청구항 36.

제35항에 있어서,

하드웨어-기반 타이머(401)를 더 포함하며,

상기 보안 로직(1124)은 상기 판독 전용 메모리(403)에 의한 액세스를 허용하고, 그렇지 않으면 상기 하드웨어-기반 타이머(401)에 대한 액세스를 금지하는 수단을 포함하는 시스템.

청구항 37.

제35항에 있어서,

상기 판독 전용 메모리(403)내의 명령어 코드에 따른 상기 보호된 랜덤 액세스 메모리(407)에 대한 액세스는 상기 시스템이 감독 모드(supervisory mode)일 때만 발생할 수 있는 시스템.

청구항 38.

제35항에 있어서,

상기 시스템은 셀룰러 전화에서 메모리 액세스를 금지하는 시스템.

청구항 39.
삭제

청구항 40.
삭제

청구항 41.
삭제

청구항 42.
삭제

청구항 43.
삭제

청구항 44.
삭제

청구항 45.
삭제

청구항 46.
삭제

청구항 47.
삭제

청구항 48.
삭제

청구항 49.
삭제

청구항 50.
삭제

청구항 51.
삭제

청구항 52.
삭제

청구항 53.
삭제

청구항 54.
삭제

도면

도면1

도면2

200
MIN m 및 ESN m 을 수신
202
MIN m에 기초하여
ESN sys 를 검색
204
ESNsys = ESN m ?
예
206
액세스 허용
아니오
208
액세스 거부

도면3

330
RAM
320
322
ROM 또는 플래쉬
프로그램 메모리
EEPROM
310
사용자 프로파일
312
ESN
314
MIN
316
308
300
컨트롤러
301
마이크로프로세서
306
318
LED
302
IROM
부트 코드
304

도면4

RAM
408
420
422
플래쉬 프로그램 메모리
EEPROM
410
사용자 프로파일
412
ESN
414
MIN
416
서명된/서명 안된 해시값 쌍
418
402
424
400
컨트롤러
마이크로프로세서
PSRAM
407
Int
NMI
HALT
IROM
403
421
인터럽트 컨트롤러
부트 코드
404
해시 코드
405
401
하드웨어-기반 타이머 T1 & T2
공개키
인증 코드
406
409

도면5

마이크로프로세서 IROM 코드로부터 전화를 부트
500
IROM 코드는 메모리 내용에 따라 감사 해시값을 계산
502
IROM 코드는 EEPROM에 저장된 해시값 쌍을 인증
504
IROM 코드는 인증된 해시값을 보호된 SRAM에 저장
506
514
508
감사 해시값이 PSRAM 내의 인증된 해시값과 일치하는가?
아니오
전화를 무한 루프로 놓는다
예
512
510
주기적 해시 계산 처리를 개시, 프로그램 카운터를 설정
플래쉬 코드를 사용하여 정상 이동 전화 동작을 시작

도면6

정상 동작을 계속
600
하드웨어 타이머 T1가 만료?
602
아니오
예
NMI 및 정규 인터럽트를 발생
604
해시값 계산에서 후속 바이트를 포획
606
정상 동작을 계속
608
아니오
정규 인터럽트 서비스
610
아니오
하드웨어 타이머 T2가 만료?
612
예
전화를 디스에이블
614
예
624
하드웨어 타이머를 리셋
해시값 계산의 후속 세그먼트를 계산
616
해시 계산을 완료?
618
아니오
예
해시값이 일치?
620
예
아니오
전화를 디스에이블
622

도면7

400
401
421
402
420
408
플래쉬 프로그램 메모리
RAM
하드웨어-기반 타이머 T1 & T2
인터럽트 컨트롤러
마이크로프로세서
INT
NMI
HALT
컨트롤러
IROM
부트 코드
해시 코드
공개키
인증 코드
PSRAM
EEPROM
사용자 프로파일
ESN
MIN
서명된/서명 안된 해시값 쌍
409
406
405
404
403
407
410
412
414
416
418
758
데이터 전송 장치
안전한 프로세서
인증/디지털 서명 코드
개인키
ESN 리프로그래밍 코드
750
752
753
754
756

도면8

800
전화를 동작 상태로
802
TD는 Rand 1과 함께 프로그래밍 요구 메시지를 송출
804
챌린지 코드 (Rand 2)를 복귀
806
Rand 1, Rand 2 및 개인키에 따라 챌린지 응답을 발생
808
챌린지 응답을 복귀
810
Rand 1, Rand 2 및 공개키를 사용하여 챌린지 응답을 처리
812
챌린지 응답이 유효?
아니오
예
814
전화를 프로그래밍 모드로 둔다
816
실패 계수를 증가
818
실패 계수= MaxCount?
아니오
예
820
전화를 로크
822
인증 실패 메시지를 발생, 프로그래밍 요구의 재송출을 요구

도면9

900
전화를 동작 상태로
902
TD는 Rand 1과 함께 ESN 프로그래밍 요구 메시지를 송출
904
ESN의 모두 제로?
아니오
906
요구를 거부
예
908
챌린지 응답 처리를 개시하여 전화를 ESN 프로그래밍 모드로 둔다

도면12

셀룰러 전화
1204
1202
1210
시큐어리티 유닛
1200
안전한 프로세서
개인키
1254
1208
1206

도면10

1000
전화를 프로그래밍 모드로
1002
DTD는 ESN 리프로그래밍 코드를 PSRAM에 다운로드
1004
컨트롤러는 PSRAM 코드를 사용하여 ESN을 제로로 함
1006
ESN 리프로그래밍 처리를 개시
1008
해시값을 재계산
1010
새로운 해시값을 디지털 서명을 위해 DTD로 다시 보냄
1012
EEPROM에 저장하도록 서명된 해시값을 복귀

도면11

컨트롤러
어드레스
데이터
1102
402
마이크로
프로세서
HALT
NMI
SPVR
INT
420
플래쉬
메모리
CS R/W
410 408
EEPROM
CS R/W
RAM
CS R/W
420
인터럽트
컨트롤러
R/W
CS
1122
칩 셀렉트
로직
1124
SPVR MODE
A
B
C
보안 로직
정지
어드레스
데이터
401
하드웨어
-기반
타이머
T1
T2
R/W
CS
400
403
IROM
R/W
CS
407
PSRAM
CS
R/W