(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년09월28일
(11) 등록번호 10-1186737
(24) 등록일자 2012년09월21일

(51) 국제특허분류(Int. Cl.)
G06F 21/00 (2006.01) *G06K 9/00* (2006.01)
G06F 21/20 (2006.01)
(21) 출원번호 10-2010-7007166
(22) 출원일자(국제) 2008년09월08일
심사청구일자 2010년04월01일
(85) 번역문제출일자 2010년04월01일
(65) 공개번호 10-2010-0049685
(43) 공개일자 2010년05월12일
(86) 국제출원번호 PCT/US2008/075562
(87) 국제공개번호 WO 2009/033139
국제공개일자 2009년03월12일
(30) 우선권주장
11/851,856 2007년09월07일 미국(US)
(56) 선행기술조사문헌
US20050081040 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
오센테크, 인코포레이티드
미국 플로리다 32901 멜번 스위트 100 리알토 로드 100
(72) 발명자
보쉬라, 마이클
미국 플로리다 32903 인디아랜틱 아파트먼트 에프 브리타니 드라이브 1899
리, 제프리 씨.
미국 플로리다 32935 멜버른 인디안 리버 드라이브 857
(뒷면에 계속)
(74) 대리인
김문종, 손은진

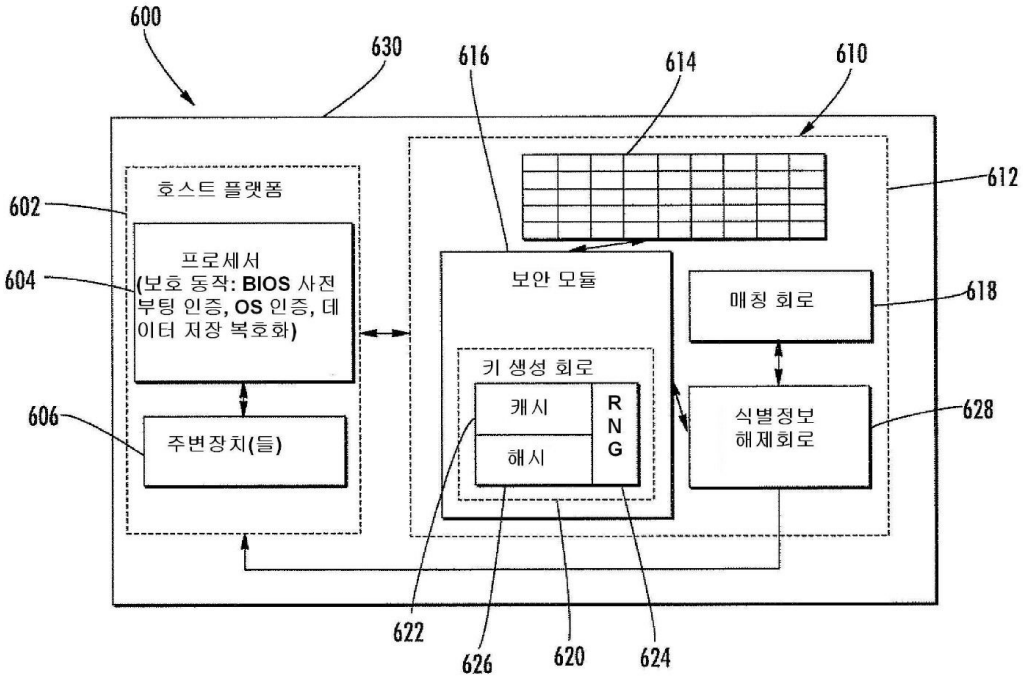
전체 청구항 수 : 총 19 항 심사관 : 박진아

(54) 발명의 명칭 **식별정보 해제를 가지는 손가락 감지 장치, 전자장치 및 관련 방법**

(57) 요 약

집적회로(IC) 기판, IC 기판 상의 손가락 감지 요소들의 배열, 손가락 매칭을 수행하기 위한 상기 IC 기판 상의 매칭 회로, 및 상기 IC 기판 상의 식별정보 해제 회로를 포함한 손가락 감지 장치가 제공된다. 상기 식별정보 해제 회로는 또 다른 장치가 적어도 하나의 보호 동작을 수행할 수 있게 손가락 매칭에 기반하여 적어도 하나의 사용자 식별정보를 해제하도록 매칭 회로와 같이 동작할 수 있다. 이에 따라, 보안이 강화되며, 사용자는 하나 이상의 보호 동작이 확실하게 수행되도록 단일 손가락 매치를 사용할 수 있다. 상기 적어도 하나의 사용자 식별정보는 예를 들어, 사용자 패스워드, 패스프레이즈(passphrase), 사용자 명칭, 인증, 키 데이터 중의 적어도 하나를 포함할 수 있다.

대 표 도



(72) 발명자

민티어, 그레고리 토마스

미국 플로리다 32937 인디안 하버 비치 마르테시아 웨이 108

포터, 게리 에스.

미국 플로리다 32950 말라바 1600 유에스 하이웨이 1 #240 베이 써클 카멜롯 알브이 파크

반다미아, 앤드류 제이.

미국 플로리다 32955 록리지 #1303 헌팅턴 레인 1410

왈드론, 제임스, 알.

미국 플로리다 32765 오비에도 알렌데일 드라이브 1180

특허청구의 범위

청구항 1

집적회로(IC) 기판과,

IC 기판 상의 손가락 감지 요소들의 배열과,

손가락 매칭을 수행하기 위한 상기 IC 기판 상의 매칭 회로와,

또 다른 장치가 적어도 하나의 보호 동작을 수행할 수 있게 손가락 매칭에 기반하여 적어도 하나의 사용자 식별정보를 해제하도록 상기 매칭 회로와 같이 동작하는 상기 IC 기판 상의 식별정보 해제 회로를 포함하며;

상기 또 다른 장치는 상기 IC 기판 외부의 호스트 플랫폼을 포함하며;

상기 호스트 플랫폼은 적어도 하나의 사용자 식별정보에 기반하여 BIOS 사전부팅 인증, 동작시스템 인증, 및 호스트 플랫폼 저장 복호화(storage decryption) 가운데 적어도 하나를 수행하는 것을 특징으로 하는 손가락 감지 장치.

청구항 2

제 1항에 있어서,

상기 매칭 회로에 의해 사용되는 적어도 하나의 키를 내부에 저장하는 IC 기판 상의 적어도 하나의 키 캐시(key cache)를 더 포함하는 것을 특징으로 하는 손가락 감지 장치.

청구항 3

제 1항에 있어서,

상기 적어도 하나의 사용자 식별정보는 사용자 패스워드, 패스프레이즈(passphrase), 사용자 명칭, 인증, 키 데이터 중의 적어도 하나를 포함하는 것을 특징으로 하는 손가락 감지 장치.

청구항 4

삭제

청구항 5

제 1항에 있어서,

상기 호스트 플랫폼은 적어도 하나의 사용자 식별정보에 기반하여 BIOS 사전부팅 인증과 동작시스템 인증 모두를 수행하는 것을 특징으로 하는 손가락 감지 장치.

청구항 6

삭제

청구항 7

제 1항에 있어서,

상기 호스트 플랫폼은 적어도 하나의 프리매치 기능을 수행하는 것을 특징으로 하는 손가락 감지 장치.

청구항 8

제 7항에 있어서,

상기 적어도 하나의 프리매치 기능은 상기 매칭 회로에 의한 사용을 위해 적어도 하나의 매치 스코어를 포함하는 것을 특징으로 하는 손가락 감지 장치.

청구항 9

제 1항에 있어서,

상기 IC 기판과 상기 호스트 플랫폼을 유지하는 공통 하우징을 더 포함하는 것을 특징으로 하는 손가락 감지 장치.

청구항 10

하우징과,

집적회로(IC) 기판과,

IC 기판 상의 손가락 감지 요소들의 배열과,

손가락 매칭을 수행하기 위한 상기 IC 기판 상의 매칭 회로와,

상기 하우징에 의해 유지되는 호스트 플랫폼과,

상기 호스트 플랫폼이 적어도 하나의 보호 동작을 수행할 수 있게 손가락 매칭에 기반하여 적어도 하나의 사용자 식별정보를 해제하도록 상기 매칭 회로와 같이 동작하는 IC 기판 상의 식별정보 해제 회로를 포함하며;

상기 호스트 플랫폼은 적어도 하나의 사용자 식별정보에 기반하여 BIOS 사전부팅 인증, 동작시스템 인증, 및 호스트 플랫폼 저장 복호화(storage decryption) 가운데 적어도 하나를 수행하는 것을 특징으로 하는 전자 장치.

청구항 11

제 10항에 있어서,

상기 매칭 회로에 의해 사용되는 적어도 하나의 키를 내부에 저장하는 IC 기판 상의 적어도 하나의 키 캐시를 더 포함하는 것을 특징으로 하는 전자 장치.

청구항 12

제 10항에 있어서,

상기 적어도 하나의 사용자 식별정보는 사용자 패스워드, 패스프레이즈(passphrase), 사용자 명칭, 인증, 키 데이터 중의 적어도 하나를 포함하는 것을 특징으로 하는 전자 장치.

청구항 13

제 10항에 있어서,

상기 호스트 플랫폼은 적어도 하나의 사용자 식별정보에 기반하여 BIOS 사전부팅 인증과 동작시스템 인증 모두를 수행하는 것을 특징으로 하는 전자 장치.

청구항 14

삭제

청구항 15

제 10항에 있어서,

상기 호스트 플랫폼은 적어도 하나의 프리매치 기능을 수행하는 것을 특징으로 하는 전자 장치.

청구항 16

또 다른 장치가 적어도 하나의 보호 동작을 수행하게 하는 방법으로서,

집적회로(IC) 기판, IC 기판 상의 복수의 손가락 감지 요소들, 및 상기 IC 기판 상의 매칭 회로를 포함하는 손가락 센서를 이용하여 매칭 여부를 판별하는 단계와,

또 다른 장치로 하여금 매칭 여부에 기반하여 적어도 하나의 사용자 식별정보를 해제하고, 마찬가지로 IC 기판 상에 있으며, 상기 매칭 회로와 같이 동작하는 식별정보 해제 회로의 이용에 기반하여 적어도 하나의 보호 동작을 수행할 수 있게 하는 단계를 포함하며;

또 다른 장치는 상기 IC 기판 외부의 호스트 플랫폼을 포함하며, 상기 호스트 플랫폼은 적어도 하나의 사용자 식별정보에 기반하여 BIOS 사전부팅 인증, 동작시스템 인증, 및 호스트 플랫폼 저장 복호화(storage decryption) 가운데 적어도 하나를 수행하는 것을 특징으로 하는 또 다른 장치가 적어도 하나의 보호 동작을 수행하게 하는 방법.

청구항 17

제 16항에 있어서,

상기 매칭 회로에 의해 사용되는 IC 기판 상에 있는 키 캐시에 적어도 하나의 키를 더 저장하는 것을 포함하는 것을 특징으로 하는 또 다른 장치가 적어도 하나의 보호 동작을 수행하게 하는 방법.

청구항 18

제 16항에 있어서,

상기 적어도 하나의 사용자 식별정보는 사용자 패스워드, 패스프레이즈(passphrase), 사용자 명칭, 인증, 키 데이터 중의 적어도 하나를 포함하는 것을 특징으로 하는 또 다른 장치가 적어도 하나의 보호 동작을 수행하게 하는 방법.

청구항 19

삭제

청구항 20

제 16항에 있어서,

상기 호스트 플랫폼은 적어도 하나의 사용자 식별정보에 기반하여 BIOS 사전부팅 인증과 동작시스템 인증 모두를 수행하는 것을 특징으로 하는 또 다른 장치가 적어도 하나의 보호 동작을 수행하게 하는 방법.

청구항 21

삭제

청구항 22

제 16항에 있어서,

상기 호스트 플랫폼은 적어도 하나의 프리매치 기능을 수행하는 것을 특징으로 하는 또 다른 장치가 적어도 하나의 보호 동작을 수행하게 하는 방법.

청구항 23

제 22항에 있어서,

상기 적어도 하나의 프리매치 기능은 상기 매칭 회로에 의한 사용을 위한 적어도 하나의 매치 스코어를 포함하는 것을 특징으로 하는 또 다른 장치가 적어도 하나의 보호 동작을 수행하게 하는 방법.

청구항 24

제 16항에 있어서,

상기 IC 기판과 상기 호스트 플랫폼을 유지하는 공통 하우징을 더 포함하는 것을 특징으로 하는 또 다른 장치가 적어도 하나의 보호 동작을 수행하게 하는 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 생체인식 감지에 관한 것이며, 더 상세하게는 집적회로 손가락 센서를 이용한 손가락 감지 장치, 전자장치 및 관련 방법에 관한 것이다.

배 경 기 술

[0002] 지문 감지 및 매칭(matching)은 개인 식별 또는 개인 검증을 위한 확실하고, 광범위하게 사용되는 기술이다. 특히, 지문 식별에 대한 일반적인 접근은 샘플 지문 또는 그의 이미지를 스캐닝하고, 상기 이미지 및/또는 상기 지문 이미지의 고유 특성을 저장하는 것을 수반한다. 샘플 지문의 특성은 이를 테면, 검증 목적을 위한 적절한 개인 식별을 하기 위해 데이터베이스에 이미 있는 기준 지문용 정보에 비교될 수 있다.

[0003] 지문 감지의 특히 이로운 접근법은 본 발명의 양수인에게 양수된 미국특허출원 제5,953,679호에 개시된다. 상기 지문 감지기는 전계(electric field) 신호로 사용자 손가락을 작동시키며, 집적 회로 기판상의 전계 감지 화소의 배열로 전계를 감지하는 집적 회로 센서이다. 상기 센서는 컴퓨터, 휴대폰, PDA(personal digital assistants) 등과 같은 다수의 상이한 형태의 전자 장치들에 대한 접근을 제어하는데 사용된다. 특히, 지문 센서는 그가 소형의 풋프린트(footprint)를 가질 수 있으며, 사용자가 사용하기에 상대적으로 용이하며, 합리적인 인증 능력을 제공하기 때문에 사용된다.

[0004] 마찬가지로 본 발명의 양수인에게 양도된 세트락(Setlak)에 의한 미국공개특허출원 제2005/0089203호는 사용자의 다중 생체인식을 감지할 수 있으며, 고정 배치 센서 또는 슬라이드형 손가락 센서에 적응되기도 하는 집적회로 생체인식 센서를 개시한다. 슬라이드형 손가락 센서는 사용자의 손가락이 미끄러지는 작은 감지면을 구비한다. 슬라이딩 과정 동안에 집합된 이미지는 이를 테면 인증과 같은 매칭을 위해 집합될 수 있으며, 예를 들면 내비게이션을 위해 사용될 수도 있다.

[0005] 우치다(Uchida)의 미국공개특허출원 제2001/0025342호는 생체인식 입력 장치 및 개별로 제공된 생체인식 검증기를 가지는 생체인식 식별 시스템 및 방법에 관한 것이다. 상기 생체인식 데이터 입력 장치는 생체인식 데이터 센서와, 상기 생체인식 데이터 입력 장치를 식별하는 비밀 정보를 사용하여 디지털 생체인식 데이터를 인코딩하고, 상기 데이터를 생체인식 검증기로 전송하는 인코더를 구비한다. 상기 생체인식 검증기는 디지털 생체인식 데이터를 재생하기 위해 상기 비밀 정보를 사용하여 상기 인코딩된 데이터를 디코딩한다. 상기 시스템 및 방법은 복호화 및 디코딩을 위해 검증기로 전송되는 데이터의 디지털 워터마킹 및/또는 암호화의 사용을 포함한다.

발명의 내용

해결하려는 과제

[0006] 몇몇의 종래 지문보안시스템은 라이브 샘플(live sample)에 매칭되는 템플릿을 표시하는 인덱스를 간단히 반환한다. 호스트 컴퓨터상에서 운용되는 애플리케이션은 그때 이러한 응답에 기반하여 그 자신의 저장소로부터 보안자료를 검색할 것이다. 이러한 접근법의 단점은 해커(hacker)가 소프트웨어 및 하드웨어 스택을, 예를 들면, 존재하는 손가락에 상관없이 유효 지수를 항상 반환하는 간단한 동적 링크 라이브러리(Dynamic-link library : DLL)로 교체할 수 있다는 것이다. 실제로, 손가락의 존재를 필요로 하는 것은 아니다. 이에 따라, 애플리케이션 및 소프트웨어가 교차 인증하는 경우, 악성 소프트웨어가 상기 반환된 응답을 소망하는 임의의 것으로 변경할 수 있는 단일의 배치가능한 공격점이 존재한다.

[0007] 캘리포니아주 에머빌의 오펙 인크(UPEK, Inc.)는 그의 TCS3 센서 및 TCD42 디지털 식별 엔진에 기반한 완성 생체인식 서브시스템인 TouchStrip®

지문인증모듈(TCED)을 공급한다. 시장으로의 통합을 간소화하고 신속한 시간 진행을 위해 USB-준비된 플렉스 케이블 커넥터를 구비한 소형 PCB상에 모든 것이 장착된다. 안타깝게도, 이러한 이른바 두 개-칩의 손가락 감지 접근법이 다른 접근법들에 비해 상대적으로 고비용일 수 있다.

[0008] 이용될 수 있는 보안문제를 가진 손가락 감지의 접근법들이 있다. 또한, 두 개의 전용 칩들을 필요로 하는 것과 같은 현존하는 일부 손가락 감지 접근법들은 실행하기에 상대적으로 고비용일 수 있다.

[0009] 전술한 배경들의 측면에서, 따라서 본 발명의 목적은 강화된 보안을 가지는 손가락 감지 장치, 전자장치 및 관련 방법을 제공하는 것이다.

과제의 해결 수단

[0010] 본 발명에 따른 상기 및 기타 목적, 특징, 이점들은, 집적회로(IC) 기판, 상기 IC 기판 상의 손가락 감지 요소들의 배열, 손가락 매칭을 수행하기 위한 상기 IC 기판 상의 매칭 회로, 및 상기 IC 기판 상의 식별정보 해

제 회로를 포함한 손가락 감지 장치에 의해 제공된다. 상기 식별정보 해제 회로는 또 다른 장치가 적어도 하나의 보호 동작을 수행할 수 있게 손가락 매칭에 기반하여 적어도 하나의 사용자 식별정보를 해제하도록 매칭 회로와 같이 동작할 수 있다. 이에 따라, 보안이 강화되며, 사용자는 하나 이상의 보호 동작이 확실하게 수행되도록 단일 손가락 매치를 사용할 수 있다. 상기 IC 기판 상에 있는 호스트 플랫폼을 다른 장치가 포함할 수 있으며, 상기 호스트 플랫폼은 적어도 하나의 사용자 식별정보에 기반하여 BIOS 사전부팅 인증, 동작시스템 인증, 및 호스트 플랫폼 저장 복호화 가운데 적어도 하나를 수행할 수 있다.

[0011] 상기 손가락 감지 장치는 매칭 회로에 의해 사용될 적어도 하나의 키를 내부에 저장하는 IC 기판 상의 적어도 하나의 키 캐시를 더 포함할 것이다. 상기 적어도 하나의 사용자 식별정보는 예를 들어, 사용자 패스워드, 패스 프레이즈(passphrase), 사용자 명칭, 인증, 키 데이터 중의 적어도 하나를 포함할 수 있다.

[0012] 일부 변형예에 있어서, 상기 호스트 플랫폼은 적어도 하나의 사용자 식별정보의 해제에 기반하여 BIOS 사전부팅 인증(BIOS preboot authentication) 및 동작시스템인증 모두를 수행할 수 있다.

[0013] 또한, 상기 호스트 플랫폼은 적어도 하나의 프리매치 기능을 수행할 수 있다. 또한, 상기 적어도 하나의 프리매치 기능은 매칭 회로에 의한 사용을 위해 적어도 하나의 매치 스코어를 생성하는 것을 포함할 수 있다. 일부 변형에 있어서, 상기 손가락 감지 장치는 IC 기판 및 호스트 플랫폼을 유지하는 공통 하우징을 더 포함하는, 이를 테면, 랩탑, 휴대폰 또는 PDA와 같은 전자 장치 형태일 수 있다.

[0014] 일 방법 측면은 또 다른 장치가 적어도 하나의 보호 동작을 수행할 수 있게 하는 것이다. 상기 방법은 집적회로(IC) 기판, 상기 IC 기판 상의 복수의 손가락 감지 요소들, 및 상기 IC 기판 상의 매칭 회로, 상기 하우징에 의해 유지되는 호스트 플랫폼을 포함한 손가락 센서를 이용하여 매치를 판별하는 것을 포함한다. 상기 방법은 또한, 다른 장치가, 상기 매치에 기반하여 적어도 하나의 사용자 식별정보를 해제하고, 마찬가지로 상기 IC 기판 상에 있으며, 상기 매칭 회로와 협력하는 식별정보 해제 회로의 이용에 기반하여 적어도 하나의 보호 동작을 수행할 수 있게 하는 것을 포함할 수 있다.

발명의 효과

[0015] 다음은 본 발명의 다양한 실시형태들에 의해 개별적으로 또는 결합으로 제공될 수 있는 다양한 보안 특성들의 기재이다. 하드웨어 보안 사용자 식별정보(예. 사용자 ID 및 암호): 상기 사용자 식별정보는 센서에 의해 랩핑되며, 보안 4-단계 하드웨어 기반 최종 매치에 따라서만 센서에 의해 랩핑되지 않거나 해제된다. 온-센서 4-단계 매치(On-Sensor 4-step Match): 1- 매치 임계값(match threshold)보다 크게 처리하는 이미지 처리 데이터 요소; 2- 검증되는 디지털 워터마킹(watermarked) 데이터; 3- 등록 SMR_{val}에 동일한 SMR_{mv}; 및 4- 만료되지 않은 감시 타이머를 포함하는 센서로부터 식별정보를 해제하는데 필요한 센서 상의 4-단계 최종-매치. 하드웨어 암호화 템플릿: 템플릿들이 상기 센서를 절대 떠나지 않는 키들을 사용하여 상기 센서와 함께 암호화된다. USB 인터페이스상의 암호화 이미지 및 데이터(이미지 데이터를 포함한, 상기 센서와 소프트웨어 사이에 전달된 모든 데이터)는 각기 보안 세션 상에 세션 암호화 키를 사용하여 암호화된다. 측정 시스템 특정 암호화 템플릿: 인증 동안에 측정된 시스템은 템플릿 서브스테이션의 저지를 보장한다. 템플릿들은 그들이 생성되었던 시스템상에서만 암호화 및 복호화될 수 있으며, AES128 암호화가 모든 템플릿들 상에서 사용될 수 있다. 하드웨어 생성 및 저장 키(모든 키)들이 상기 센서 내에 무작위로 생성된다. 키들은 상기 센서를 결코 떠나지 않는다.

[0016] 디지털 워터마킹 이미지 및 템플릿, 즉, 각 이미지 및 템플릿을 "워터마킹"함에 의한 호스트측 이미지 처리의 간섭방지(tamper-proof)를 보장한다. 측정된 구성요소들, 사전 부팅, 옵트(opt). FDE 및 OS 보안 구성요소들이 센서 측정 레지스터(SMR)에 측정되어 센서 동작 이전에 플랫폼 구성의 신뢰를 보장한다. 신뢰 소프트웨어 구성요소들(Trusted Software Components)인 디지털 서명 및 챌린지(challenge)/응답 메커니즘이 상기 애플리케이션을 포함한, 모든 소프트웨어 구성요소들 간의 신뢰를 보장한다. 디피 헬만 기반 보안 세션들은 센서와 드라이버 간의 신뢰를 보장한다. 소프트웨어 구성요소들 간의 보안 데이터 전송(상기 애플리케이션으로부터 상기 애플리케이션에 이르는 것을 포함한) 소프트웨어 구성요소들 사이에 전송된 모든 데이터는 SSL을 이용하여 암호화된다. TPM 강화 동작, 즉 TPM 옵트인(opt-in)은 센서와 장치 드라이버 간의 소프트웨어 보안 세션을 강화한다.

[0017] 본 발명의 장치에 의하면, 글로벌 공격을 방지할 수 있다. 사용자 식별정보 보안, 즉, 센서 내부에서만 복호화될 수 있고, 단지 유효 지문 인증을 뒤따라 센서로부터 해제될 수 있는 보안 페이로드(SP) 내에 암호화된 애플리케이션 정의 페이로드(AP). 개인 데이터 비공개 보장. TPM을 필요로 하지 않는다. 플렉시블(flexible)

애플리케이션 페이로드, 즉 네트워크 로그인 식별정보 - 사용자 명칭, 패스워드, 암호, 도메인 등. 사용자 정의 암호화 키, 웹 사이트 로그인 데이터 정정 - 즉, 피싱 차단(Anti-phishing), 서브-AP가 병합될 수 있다 - 상이한 시스템 구성요소들(PBA, FVE, OS)이 단일의 전체 AP로 그들 자신의 식별정보를 가지도록 허용한다.

도면의 간단한 설명

[0018] 도 1은 본 발명에 따른 손가락 센서와 강화 보안을 가지는 랩탑 컴퓨터 형태의 전자 장치의 사시도이다.

도 2는 본 발명에 따른 이미지 워터마킹을 이용한 손가락 감지 장치의 제1 실시형태의 개략적인 블록도이다.

도 3은 본 발명에 따른 템플릿 워터마킹을 이용한 손가락 감지 장치의 제2 실시형태의 개략적인 블록도이다.

도 4는 본 발명에 따른 암호화/복호화를 이용한 손가락 감지 장치의 제3 실시형태의 개략적인 블록도이다.

도 5는 본 발명에 따른 하이브리드 매칭을 이용한 손가락 감지 장치의 제4 실시형태의 개략적인 블록도이다.

도 6은 본 발명에 따른 고유의 세션 키를 이용한 손가락 감지 장치의 제5 실시형태의 개략적인 블록도이다.

도 7은 본 발명에 따른 센서로부터 보안 식별정보 해제(secure credential release)를 이용한 손가락 감지 장치의 제6 실시형태의 개략적인 블록도이다.

도 8은 본 발명에 따른 보안 소프트웨어 업데이트를 구현하는 손가락 감지 장치의 제7 실시형태의 개략적인 블록도이다.

도 9는 본 발명의 다양한 특징들에 따른 센서, 호스트 및 옵션 메모리의 구성요소들을 포함한 보안 감지 장치의 일 실시예를 도시한 고차적인 개략적 블록도이다.

도 10은 본 발명의 다양한 특징들에 따른 애플리케이션 페이로드(application payload) 및 암호화 보안 페이로드(encrypted secure payload)를 포함한 암호화된 사용자 템플릿의 생성을 도시하는 개략적인 블록도이다.

도 11은 본 발명의 다양한 특징들에 따른 보안 소프트웨어 업데이트 프로세스의 생성 국면에 있어서의 다양한 단계들의 일 실시예를 도시한 흐름도이다.

도 12는 본 발명의 다양한 특징들에 따른 보안 소프트웨어 업데이트 과정의 실행 국면에 있어서의 다양한 단계들의 일 실시예를 도시하는 흐름도이다.

도 13은 본 발명에 따른 BIOS PBA, FVE 및 OS 인증 특징을 구비한 센서 및 호스트를 포함한 보안 감지 장치의 일 실시예에 대한 고차적인 개략적 블록도이다.

도 14는 본 발명의 다양한 특징들에 따른 센서, 호스트 및 옵션 메모리의 구성요소들을 포함한 보안 감지 장치의 다른 실시예에 대한 개략적인 블록도이다.

도 15는 본 발명의 특징들에 따라 내부에 다양한 구성요소들을 포함한 센서의 일 실시예에 대한 개략적인 블록도이다.

도 16은 본 발명의 특징들에 따라 내부에 다양한 구성요소들을 포함한 센서의 하드웨어 보안 모듈에 있어서의 일 실시예에 대한 개략적인 블록도이다.

도 17은 본 발명의 특징들에 따른 센서 및 옵션 메모리의 일 실시예에 있어서의 하드웨어 보안 요소들을 도시한 개략적인 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0019] 본 발명은, 본 발명의 바람직한 실시형태들이 도시되는 첨부 도면과 관련하여 이하의 상세한 설명에 의해 더욱 잘 이해될 것이다. 이 발명은 그러나, 다수의 상이한 형태로 구현될 수 있으며, 여기 전술한 실시형태들에 제한되는 것으로 해석되어서는 아니 된다. 그보다는, 이들 실시형태는 이러한 개시가 철저하고 완전하며, 본 기술분야의 당업자에게 본 발명의 범위를 충분히 전달할 수 있도록 제공된다.

[0020] 도 1을 지금 참조하면, 본 발명의 하나 이상의 측면들에 따라 강화된 보안특징을 가지는 컴퓨터(10)가 먼저 기술된다. 상기 컴퓨터(10)는 예시적으로 랩 탑 컴퓨터로 도시되지만, 본 발명은 다른 컴퓨터(예, 데스크탑 컴퓨터)에도 마찬가지로 적용가능하다. 또한, 본 발명의 특징은 무선통신장치, PDA(Personal Digital Assistant) 장치와 같은 다른 전자 장치, 또는 생체인식 접근 제어에서 유익할 수 있는 임의의 다른 전자 장

치들에 응용가능하다.

[0021] 컴퓨터(10)는 베이스(12) 또는 하우징에 연결되는 디스플레이(11)를 구비한다. 키보드(13)와 생체인식 보안 센서(14)가 예를 들어, 상기 베이스(12)의 상부측 상에 구비될 수 있다. 물론, 상기 생체인식 보안 센서(13)는 상기 컴퓨터(10) 상의 다른 적절한 위치들에 장착될 수 있다. 상기 생체인식 보안 센서(13)는 손가락 센서일 수 있다.

[0022] **A. 제1 실시형태**

[0023] 도 2를 지금 더 참조하면, 도 1의 컴퓨터(10)와 같은, 보안 전자 장치(100)의 제1 실시형태의 추가 세부사항이 기술될 것이다. 상기 컴퓨터(10)는 예시적으로 본 기술분야의 당업자에게 인정될 수 있는 것으로서, 프로세서(106)와, 메모리, 디스크 드라이브 등과 같은 다른 관련 주변장치(106)를 구비한 호스트 플랫폼을 포함한다. 예를 들어, 적절한 메모리는 내부에 저장된 기본 입력/출력 시스템(BIOS) 명령어를 가질 수 있거나, 자기 디스크(예, 하드디스크)가 내부에 저장되는 작동 시스템(OS)을 가질 수도 있다. 상기 작동 시스템은 예를 들어 윈도우일 수 있지만, 본 발명은 다른 동작 시스템과도 마찬가지로 사용될 수 있다.

[0024] 상기 손가락 감지 장치(110)는 집적회로(IC) 기판(112), 상기 (IC) 기판상의 손가락 감지 요소들(114)의 배열, 상기 IC 기판상에 있으며, 이미지 워터마크가 내부에 삽입된 손가락 이미지 데이터를 생성하기 위해 손가락 감지 요소들의 배열과 협력하는 이미지 워터마크 회로(116)를 포함한다. 상기 손가락 이미지 데이터는 예를 들어, 피부 내에 또는 표면에서의 융선(ridge), 골(valley), 기공 및/또는 모세관에 기반한 데이터를 포함할 수 있다. 상기 손가락 감지 장치(110)는 예시적으로 적어도 상기 이미지 워터마크에 기반하여 손가락 매칭을 수행하기 위해 IC 기판(112) 상에 매칭 회로(118)를 포함한다. 손가락 매칭은 본 발명의 양수인에게 양도된 Boshra의 미국공개특허출원 제2005/0129291호에 더 개시된다.

[0025] 상기 손가락 감지 요소들(114)의 배열은 손가락 감지 화소들의 배열을 포함할 수 있다. 상기 이미지 워터마크 회로(116)는 이미지 워터마크가 내부에 삽입된 손가락 이미지 데이터를 생성하기 위해 상기 손가락 감지 화소(114)의 배열로부터의 값을 왜곡할 수 있다. 더 상세하게는, 상기 워터마크 회로(116)는 손가락 감지 화소(114)의 배열로부터의 위치 값을 왜곡할 수 있다.

[0026] 상기 이미지 워터마크 회로(116)는 예시적으로, 이미지 워터마크가 내부에 삽입된 손가락 이미지 데이터를 생성하기 위해 이미지 워터마크 키를 생성하는 이미지 워터마크 키 생성 회로(120)를 더 포함할 수 있다. 예를 들어, 상기 이미지 워터마크 회로(120)는 그 내부에 이미지 워터마크를 저장하는 키 캐시(key cache)(122)를 더 포함할 수 있다. 또한, 일부 유익한 변화들에 있어서, 상기 키 캐시(122)는 IC 기판으로부터 이미지 워터마크를 해제(release)하지 않는다. 상기 키 생성 회로(120)는 무작위 번호 생성기(RNG)(124), 및 이미지 워터마크 키를 생성하기 위해 그와 협력하는 관련 해시 엔진(126)을 더 포함한다. 이에 따라, 보안이 더욱 강화된다.

[0027] 다른 이점들에 의하여, 상기 손가락 감지 장치(110)는 손가락 매칭에 기반하여 적어도 하나의 사용자 식별정보를 해제하기 위해 매칭 회로(118)와 협력하는 IC 기판(112) 상의 식별정보 해제 회로(128)를 더 포함할 수 있다. 이는 호스트 플랫폼(102)과 같은 또 다른 장치가 적어도 하나의 보호 동작을 수행할 수 있게 한다. 상기 이미지 워터마크 회로(116)는 예를 들면 등록(enroll)이 아닌, 매칭 동안에 이미지 워터마크가 내부에 삽입된 손가락 이미지 데이터를 생성할 수 있다.

[0028] 상기 감지 장치(110)는 또한, 예시적으로 IC 기판(112) 외부에 있으며, 적어도 하나의 프리매치 기능을 수행하는 호스트 플랫폼(102)을 포함한다. 상기 적어도 하나의 프리매치 기능은 예를 들어, 매칭 회로(118)에 의한 사용을 위해 적어도 하나의 매치 스코어를 생성하는 것을 포함할 수 있다. 상기 장치(110)는 상기 IC 기판(112)과 호스트 플랫폼(102)을 유지(carry)하는 공통 하우징(130)을 더 포함할 수 있다. 환언하자면, 상기 손가락 감지 장치(110)는 랩 탑, PDA, 휴대폰 등과 같은 전자 장치의 형태일 수 있다. 예를 들어, 상기 공통 하우징(130)은 랩탑 컴퓨터의 외부 하드케이스일 수 있거나, 상기 랩 탑에 연결되는 개별 포드(pod)일 수 있다.

[0029] 상기 제1 실시형태에 관련한 방법 측면은 손가락 감지를 위한 것이다. 상기 방법은 IC 기판(112)상의 손가락 감지 요소들(114)의 배열과 협력하는 상기 IC 기판(112) 상의 이미지 워터마크 회로(116)를 이용하여 이미지 워터마크가 내부에 삽입된 손가락 이미지 데이터를 생성하는 것과, 상기 IC 기판상의 매칭 회로(118)를 이용하여 적어도 상기 이미지 워터마크에 기반하여 손가락 매칭을 수행하는 것을 포함할 수 있다.

[0030] 상기 워터마크는 워터마크 검증 기술(예를 들어, A Survey of Watermarking Algorithms for image Authentication: C. Rey 및 J. Dugelay에 의해, EURASIP Journal on Applied Signal Processing, 613-621 페

이지, 2002년)을 이용하여 적어도 하나의 매치 스코어와의 상관성을 통해 검증될 수 있다.

[0031] **B. 제2 실시형태**

[0032] 도 3을 지금 더 참조하면, 도 1의 컴퓨터(10)와 같은, 보안 전자장치(200)의 다른 실시형태에 대한 추가 세부사항이 기술될 것이다. 상기 장치(200)는 프로세서(204)와 다른 관련 주변장치들(206)을 구비한 호스트 플랫폼(202)을 포함한다.

[0033] 상기 감지 장치(210)는 집적회로(IC) 기판(212)과, 상기 IC 기판상의 손가락 감지 요소들(214)의 배열, 상기 IC 기판상의 매칭 회로(218), 및 상기 IC 기판 외부에 있으며, 템플릿 워터마크가 내부에 삽입되는 손가락 템플릿 데이터를 생성하기 위해 상기 손가락 감지 요소들의 배열과 협력하는 호스트 플랫폼(202)을 구비한다. 또한, 상기 호스트 플랫폼(202)은 매칭 회로(212)에 의한 사용을 위해 내부에 템플릿 워터마크를 구비한 손가락 템플릿 데이터에 기반하여 매치 스코어를 생성할 수도 있다. 이에 따라, 손가락 감지 장치의 보안이 강화되며, 상대적으로 저비용의 센서(210)가 프로세서와 같은 호스트 플랫폼(202) 및 랩탑, PDA, 휴대폰 등에서 발견되는 관련 회로와의 사용을 위해 제공될 수 있다.

[0034] 상기 호스트 플랫폼(202)은 구별되는 손가락 특징들을 나타내는 수치(mathematical values)로서 손가락 템플릿을 생성할 수 있다. 이에 따라, 호스트 플랫폼(202)은 내부에 템플릿 워터마크가 삽입된 손가락 템플릿 데이터를 생성하기 위해 상기 수치를 왜곡할 수 있다. 상기 호스트 플랫폼은 템플릿 워터마크가 내부에 삽입된 손가락 템플릿 데이터를 생성하기 위해 손가락 융선(ridge) 흐름 데이터로서 템플릿 데이터를 생성하고, 상기 손가락 융선 흐름 데이터를 왜곡할 수 있다.

[0035] 상기 손가락 감지 장치(210)는 템플릿 워터마크가 삽입된 손가락 템플릿 데이터를 생성하기 위해 호스트 플랫폼(202)에 의한 사용을 위한 템플릿 워터마크 키를 생성하도록 IC 기판(212) 상에 키 생성 회로(220)를 가지는 워터마크 회로(216)를 더 포함할 수 있다. 상기 손가락 감지 장치(210)는 내부에 템플릿 워터마크 키를 저장하기 위해 IC 기판(212) 상에 템플릿 키 캐시(222)를 포함할 수도 있다. 상기 템플릿 키 생성 회로(222)는 무작위 번호 생성기(RNG)(224), 및 템플릿 워터마크 키를 생성하기 위해 그와 협력하는 관련 해시 엔진(226)을 더 포함할 수 있다.

[0036] 상기 손가락 감지 장치(210)는 손가락 매칭에 기반하여 적어도 하나의 사용자 식별정보를 해제하며, 이로써 상기 호스트 플랫폼(202)이 적어도 하나의 보호 동작을 수행하게 하기 위해 매칭 회로(218)와 협력하는 IC 기판(212) 상의 식별정보 해제 회로(228)를 더 포함할 수 있다. 또한, 상기 호스트 플랫폼(202)은 예를 들면, 매칭 동안이 아닌, 등록(enrollment) 동안에 템플릿 워터마크가 내부에 삽입된 손가락 템플릿 데이터를 생성할 수 있다. 물론, 여러 개의 유익한 변화들에 있어서, 공통 하우징(230)은 IC 기판(212)과 호스트 플랫폼(202)을 유지할 수 있으며, 즉, 상기 손가락 감지 장치(210)는 랩탑, PDA, 휴대폰 등과 같은 전자 장치의 형태로 있거나 또는 그에 포함될 수 있다.

[0037] 상기 제2 실시형태에 관련한 방법은 손가락 감지를 목적으로 한 것이다. 상기 방법은 템플릿 워터마크가 내부에 삽입되는 손가락 템플릿 데이터를 생성하는 것과, 집적회로(IC) 기판(212)의 외부에 있으며, 상기 IC 기판상의 손가락 감지 요소들(214)의 배열과 협력하는 호스트 플랫폼(202)을 이용하여, 템플릿 워터마크가 내부에 삽입되는 손가락 템플릿 데이터에 기반하여 매치 스코어를 생성하는 것을 포함할 수 있다. 상기 방법은 IC 기판(212) 상에 있는 매칭 회로(218)의 매치 스코어를 이용하여 매칭을 수행하는 것을 더 포함할 수 있다.

[0038] 상기 워터마크는 워터마크 검증 기술(예를 들어, A Survey of Watermarking Algorithms for image Authentication: C. Rey 및 J. Dugelay에 의해, EURASIP Journal on Applied Signal Processing, 613-621 페이지, 2002년)을 이용하여 적어도 하나의 매치 스코어와의 상관성을 통해 검증될 수 있다.

[0039] **C. 제3 실시형태**

[0040] 도 4를 지금 더 참조하면, 도 1의 컴퓨터(10)와 같은, 보안 전자장치(300)의 제3 실시형태에 대한 추가 세부사항이 기술될 것이다. 상기 장치(300)는 프로세서(304)와 다른 관련 주변장치들(306)을 구비한 호스트 플랫폼(302)을 포함한다.

[0041] 상기 손가락 감지 장치(310)는 예시적으로, 집적회로(IC) 기판(312)과, 상기 (IC) 기판상의 손가락 감지 요소들(314)의 배열, 및 손가락 템플릿 데이터를 포함한 사용자 템플릿과 적어도 하나의 사용자 식별정보를 암호화하기 위해 상기 손가락 감지 요소들(314)의 배열과 협력하는 상기 IC 기판(312) 상의 암호화 회로(316)를 포함한다. 예를 들어, 상기 적어도 하나의 사용자 식별정보는 호스트 플랫폼(302)과 같은, 또 다른 장치가 적

어도 하나의 보호 동작을 수행하여 보안을 강화할 수 있게 한다.

[0042] 상기 암호화 회로(316)는 템플릿 암호화 키에 기반하여 사용자 템플릿을 암호화할 수 있다. 상기 암호화 회로(316)는 더 나아가 페이로드 암호화 키에 기반하여 적어도 하나의 사용자 식별정보를 암호화할 수 있다. 키 생성 회로(320)가 템플릿 암호화 키와 페이로드 암호화 키를 생성하기 위해 IC 기판(312) 상에 제공될 수 있다.

[0043] 키 캐시(322)가 그 내부에 상기 템플릿 암호화 키와 페이로드 암호화 키를 저장하기 위해 상기 IC 기판(312) 상에 제공될 수 있다. 상기 키 생성 회로(320)는 예시적으로, 무작위 번호 생성기(324)와, 상기 템플릿 암호화 키 및 상기 페이로드 암호화 키를 생성하기 위해 그와 협력하는 관련 해시 엔진(326)을 더 포함한다.

[0044] 상기 손가락 감지 장치(310)의 암호화 회로(316)는 IC 기판(312) 상에 있으며, 상기 템플릿 암호화 키 및 상기 페이로드 암호화 키에 기반하여 사용자 템플릿을 복호화하기 위해 상기 키 캐시(322)와 협력하는 복호화 회로를 더 포함한다. 상기 손가락 감지 장치(310)는 적어도 상기 사용자 템플릿에 기반하여 손가락 매칭을 수행하기 위해 IC 기판(312) 상의 매칭 회로(318)와, 손가락 매칭에 기반하여 적어도 하나의 사용자 식별정보를 해제하기 위해 상기 매칭 회로(318)와 협력하는 상기 IC 기판(312) 상의 식별정보 해제 회로(328)를 포함할 수도 있다.

[0045] 상기 호스트 플랫폼(302)은 IC 기판(312)의 외부에 있으며, 적어도 하나의 프리매치 기능을 수행할 수 있다. 예를 들어, 상기 적어도 하나의 프리매치 기능은 매칭 회로(318)에 의한 사용을 위해 적어도 하나의 매치 스코어를 생성하는 것을 포함할 수 있다. 공통 하우징(330)이 상기 IC 기판(312)과 호스트 플랫폼(302)을 유지할 수 있다.

[0046] 이러한 제3 실시형태의 방법 측면은 마찬가지로, 손가락 감지를 위한 것이다. 상기 방법은 IC 기판(312)상의 손가락 감지 요소들(314)의 배열과 협력하며, 마찬가지로 IC 기판(312) 상에 있는 암호화 회로(316)를 사용하여 사용자 템플릿 데이터를 포함한 하나의 사용자 템플릿과 적어도 하나의 사용자 식별정보를 암호화하는 것을 포함할 수 있다.

[0047] **D. 제4 실시형태**

[0048] 도 5를 지금 더 참조하면, 도 1의 컴퓨터(10)와 같은, 보안 전자장치(400)의 제4 실시형태에 대한 추가 세부사항이 기술될 것이다. 상기 장치(400)는 프로세서(404)와 다른 관련 주변장치들(406)을 구비한 호스트 플랫폼(402)을 포함한다.

[0049] 상기 장치는 집적회로(IC) 기판(412)과, 상기 IC 기판상의 손가락 감지 요소들(414)의 배열과, 최종 손가락 매칭을 수행하기 위한 상기 IC 기판상의 매칭 회로(418)를 구비한 손가락 센서(410)를 포함한 손가락 감지 장치를 정의할 수 있다. 상기 호스트 플랫폼(402)은 적어도 하나의 손가락 프리매치 기능을 수행하기 위해 손가락 감지 요소들(414)의 배열과 협력할 수 있다. 또한, 상기 손가락 센서(410)와 호스트 플랫폼(402)은 그들 사이에 적어도 하나의 보안 기능(408)을 구현할 수 있다. 이에 따라, 상기 손가락 감지의 보안은 강화된다.

[0050] 예를 들어, 상기 적어도 하나의 보안 기능(408)은 적어도 하나의 워터마킹 기능을 포함할 수 있다. 상기 적어도 하나의 워터마킹 기능은, 차례로, 다른 실시형태들에 기재된 것으로서, 손가락 이미지 데이터 워터마킹과 손가락 템플릿 데이터 워터마킹 중에서 적어도 하나를 포함할 수 있다. 또한, 다른 방법으로, 상기 적어도 하나의 보안 기능은 마찬가지로 다른 실시형태들에 기재된 것으로서, 적어도 하나의 암호화/복호화 기능을 포함할 수 있다. 상기 적어도 하나의 암호화/복호화 기능은 예를 들어, 사용자 식별정보, 사용자 템플릿, 및 상기 손가락 센서와 상기 호스트 플랫폼 간의 통신 가운데 적어도 하나의 암호화를 포함할 수 있다.

[0051] 상기 손가락 센서(410)는 예시적으로, 상기 IC 기판(412) 상에 있으며, 무작위 번호 생성기(RNG)(424)와, 적어도 하나의 보안 키를 생성하기 위해 상기 RNG와 협력하는 해시 엔진(426)과, 상기 적어도 하나의 보안 키를 저장하기 위한 키 캐시(422)를 구비한 키 생성 회로(420)를 구비하는 보안 모듈(416)을 더 포함한다. 상기 손가락 센서(410)의 키 캐시(422)는 IC 기판상에 비휘발성 메모리의 적어도 일부에 의해 더 정의될 수 있다.

[0052] 상기 적어도 하나의 보안 기능은 적어도 하나의 타이밍 기능을 포함할 수 있다. 호스트 플랫폼(402)에 의해 수행되는 적어도 하나의 프리매치 기능은 손가락 센서(410)의 매칭 회로(418)에 의한 사용을 위해 적어도 하나의 매치 스코어를 생성하는 것을 포함할 수 있다. 공통 하우징(430)은 상기 손가락 센서(410)와 상기 호스트 플랫폼(402)을 유지할 것이다.

[0053] 이러한 제4 실시형태의 방법 측면은 마찬가지로 손가락 감지를 위한 것이다. 상기 방법은 집적회로(IC) 기판

(412) 상의 매칭 회로(418)와, 상기 IC 기판상의 손가락 감지 요소들(414)의 배열을 포함하는 손가락 센서(410)를 이용하여 최종 손가락 매칭을 실행하는 단계와, 상기 손가락 감지 요소들의 배열과 협력하는 호스트 플랫폼(402)을 이용하여 적어도 하나의 손가락 프리매치 기능을 실행하는 단계와, 상기 손가락 센서와 상기 호스트 플랫폼 간의 적어도 하나의 보안 기능(408)을 구현하는 단계를 포함할 수 있다.

[0054] **E. 제5 실시형태**

[0055] 도 6을 지금 더 참조하면, 도 1의 컴퓨터(10)와 같은, 보안 전자장치(500)의 다른 실시형태에 대한 추가 세부사항이 기술될 것이다. 상기 장치(500)는 프로세서(504)와 다른 관련 주변장치들(506)을 구비한 호스트 플랫폼(502)을 포함한다.

[0056] 상기 장치(500)는 집적회로(IC) 기판(512)과, 상기 IC 기판상의 손가락 감지 요소들(514)의 배열과, 상기 IC 기판상의 세션키 협상(session key negotiation) 회로(530)를 구비한 손가락 센서(510)를 포함하는 손가락 감지 장치를 정의할 수 있다. 상기 호스트 플랫폼(502)은 손가락 센서(510)의 외부에 있으며, 상기 세션키 협상 회로(530)와 협력하여 그것과 함께 각기의 통신 세션(communication session) 동안에 상기 손가락 센서와의 보안 통신(508)을 위한 고유의 세션키를 협상한다. 이에 따라, 상기 손가락 센서(510)와 호스트 플랫폼(502) 간의 통신 보안이 강화된다.

[0057] 상기 세션키 협상 회로(530)는 예를 들어 디피 헬만 키 협상(Diffie-Hellman key negotiation)을 구현할 수 있다. 또한, 상기 호스트 플랫폼(502)은 세션키 협상을 개시할 수 있다.

[0058] 상기 손가락 센서(510)는 예시적으로, 호스트 플랫폼(502)과의 통신과, 예를 들어 고유의 세션키를 사용하기 위해 그 위에 범용 직렬 버스 (Universal Serial Bus: USB) 통신 회로(532)를 더 포함한다. 상기 손가락 센서(510)와 호스트 플랫폼(502)은 복수의 등록 단계들 동안에 소정의 고유한 세션키를 사용할 수 있다. 또한, 상기 손가락 센서(510)와 호스트 플랫폼은 소정의 매칭 단계(match step) 동안에 소정의 고유한 세션키를 사용할 수 있다.

[0059] 상기 손가락 센서(510)는 IC 기판(512) 상에 있으며, 무작위 번호 생성기(RNG)(524), 적어도 하나의 보안키를 생성하기 위해 상기 RNG와 협력하는 해시 엔진(526), 및 상기 적어도 하나의 보안키를 저장하기 위한 키 캐시(522)를 구비하는 보안 모듈(516)을 더 포함할 수 있다.

[0060] 상기 손가락 센서(510)는 손가락 매칭을 수행하기 위해 IC 기판(512)상에 도시된 매칭 회로(518)와, 상기 손가락 매칭에 기반하여 적어도 하나의 사용자 식별정보를 해제하기 위해 상기 매칭 회로와 협력하는 상기 IC 기판상의 식별정보 해제 회로(528)를 더 포함할 수 있다.

[0061] 상기 호스트 플랫폼(502)은 적어도 하나의 프리매치 기능을 수행할 수 있다. 예를 들어, 상기 적어도 하나의 프리매치 기능은 손가락 센서(510)의 매칭 회로(518)에 의한 사용을 위해 적어도 하나의 매치 스코어를 생성하는 것을 포함할 수 있다. 랩탑, 휴대폰 또는 PDA와 같은 전자 장치의 형태에서, 상기 장치는 상기 손가락 센서(510)와 호스트 플랫폼(502)을 유지하기 위한 공통 하우징(530)을 더 포함할 수 있다.

[0062] 이러한 제5 실시형태의 방법 측면은 손가락 감지를 위한 것이다. 상기 방법은 그것과 함께 각기의 통신 세션 동안에 상기 손가락 센서(510)와 호스트 플랫폼(502) 간의 보안 통신(508)을 위해 고유의 세션키를 협상하는 것을 포함할 수 있다. 또한, 상기 손가락 센서(510)는 집적회로(IC) 기판(512), 상기 IC 기판상의 손가락 감지 요소들(514)의 배열, 및 호스트 플랫폼과 협력하는 상기 IC 기판상의 세션키 협상 회로(530)를 포함할 수 있다.

[0063] **F. 제6 실시형태**

[0064] 도 7을 지금 더 참조하면, 도 1의 컴퓨터(10)와 같은, 보안 전자장치(600)의 다른 실시형태에 대한 추가 세부사항이 기술될 것이다. 상기 장치(600)는 프로세서(604)와 다른 관련 주변장치들(606)을 구비한 호스트 플랫폼(602)을 포함한다.

[0065] 상기 손가락 감지 장치(610)는 예시적으로, 집적회로(IC) 기판(612)과, 상기 (IC) 기판상의 손가락 감지 요소들(614)의 배열, 손가락 매칭을 수행하기 위한 상기 IC 기판상의 매칭 회로(618), 및 상기 IC 기판상의 식별정보 해제 회로(628)를 포함한다. 상기 식별정보 해제 회로(628)는 호스트 플랫폼(602)과 같은 다른 장치가 적어도 하나의 보호 동작을 수행할 수 있도록 손가락 매칭에 기반하여 적어도 하나의 사용자 식별정보를 해제하기 위해 상기 매칭 회로(618)와 협력할 수 있다. 이에 따라, 사용자는 하나 이상의 보호 동작이 확실하게 수행되도록 단일 손가락 매치를 사용할 수 있다.

[0066] 상기 손가락 센서(610)는 IC 기판(612) 상에 있으며, 무작위 번호 생성기(RNG)(624), 적어도 하나의 보안키를 생성하기 위해 상기 RNG와 협력하는 해시 엔진(626), 및 상기 매칭 회로(618)에 의해 사용되는 적어도 하나의 키를 저장하기 위한 키 캐시(622)를 구비하는 보안 모듈(616)을 더 포함할 수 있다. 상기 적어도 하나의 사용자 식별정보는 예를 들어, 사용자 패스워드, 패스 프레이즈(passphrase), 사용자 명칭, 인증, 키 데이터 중의 적어도 하나를 포함할 수 있다.

[0067] 일부 변형에 있어서, 상기 IC 기판(612) 외부에 있는 호스트 플랫폼(602)을 다른 장치가 포함할 수 있다. 상기 호스트 플랫폼(602)은 적어도 하나의 사용자 식별정보의 해제에 기반하여 BIOS 사전부팅 인증(BIOS preboot authentication) 및 동작시스템인증 모두를 수행할 수 있다. 다른 실시형태들에서, 상기 호스트 플랫폼(602)은 적어도 하나의 사용자 식별정보에 기반하여 BIOS 사전부팅 인증, 동작시스템인증, 및 호스트 플랫폼 저장 복호화 가운데 적어도 하나를 수행할 수 있다.

[0068] 또한, 상기 호스트 플랫폼(602)은 적어도 하나의 프리매치 기능을 수행할 수 있다. 예를 들어, 상기 적어도 하나의 프리매치 기능은 매칭 회로(618)에 의한 사용을 위해 적어도 하나의 매치 스코어를 생성하는 것을 포함할 수 있다. 일부 변형에 있어서, 상기 손가락 감지 장치(610)는 IC 기판(612) 및 호스트 플랫폼(602)을 유지하는 공통 하우징(630)을 더 포함하는, 이를 테면, 랩탑, 휴대폰 또는 PDA와 같은 전자 장치 형태일 수 있거나 또는 상기와 같은 전자 장치 형태 내에 구비될 수 있다.

[0069] 상기 제6 실시형태의 방법 측면은 다른 장치가 적어도 하나의 보호 동작을 수행하도록 하기 위한 것이다. 상기 방법은 집적회로(IC) 기판(612), 상기 IC 기판상의 복수의 손가락 감지 요소들(614), 및 상기 IC 기판상의 매칭 회로(618)를 포함하는 손가락 센서(610)를 이용하여 매칭(match)를 결정하는 것을 포함한다. 상기 방법은 또한, 다른 장치가, 상기 매치에 기반하여 적어도 하나의 사용자 식별정보를 해제하는 것과, 마찬가지로 상기 IC 기판(612)에 있으며, 매칭 회로(618)와 협력하는 식별정보 해제 회로(628)를 이용하는 것에 기반하여 적어도 하나의 보호 동작을 수행가능하게 하는 것을 포함할 수 있다.

[0070] **G. 제7 실시형태**

[0071] 도 8을 지금 더 참조하면, 도 1의 컴퓨터(10)와 같은, 보안 전자장치(700)의 다른 실시형태에 대한 추가 세부사항이 기술될 것이다. 상기 장치(700)는 프로세서(704)와 다른 관련 주변장치들(706)을 구비한 호스트 플랫폼(702)을 포함한다.

[0072] 상기 장치(700)는 집적회로(IC) 기판(712)과, 상기 IC 기판상의 손가락 감지 요소들(714)의 배열, 및 상기 IC 기판상의 보안 소프트웨어 업데이트 회로(740)를 구비하는 손가락 센서(710)를 포함한 손가락 감지 장치를 정의한다. 또한, 상기 호스트 플랫폼(702)은 손가락 센서(710)의 외부에 있으며, 상기 손가락 센서와 관련한 호스트 소프트웨어를 가질 수 있다. 상기 호스트 플랫폼(702)은 시도된 소프트웨어 업데이트(708)를 인증하기 위해 보안 소프트웨어 업데이트 회로(740)와 협력할 수 있다. 업데이트가 인증되지 않으면, 보안 이유로 상기 업데이트 설치를 시도하는 사용자에게 업데이트 인증 표시가 제공되지 않을 수 있다. 이에 따라, 이롭게도 상기 센서(710)는 악성 소프트웨어의 설치 시도에 저항적이며, 전반적인 보안도 증진된다.

[0073] 예를 들어, 상기 보안 소프트웨어 업데이트 회로(740)는 시스템관리레지스터(SMR)와 같은, 적어도 하나의 레지스터(742)를 포함할 수 있다. 상기 손가락 센서(710)와 호스트 플랫폼(702)은 상기 적어도 하나의 레지스터(740)를 처리(clear)하기 위해 더 협력할 수 있다. 상기 손가락 센서(710)와 호스트 플랫폼(702)은 시도된 소프트웨어 업데이트(708)에 기반하여 상기 적어도 하나의 처리 레지스터(740) 내에서 소프트웨어 측정값을 확대하도록 더욱 협력할 수 있다. 이에 따라, 상기 보안 소프트웨어 업데이트 회로(740)는 상기 확대된 소프트웨어 측정값을 그의 소정값에 비교할 수 있다. 또한, 상기 소정값은 상기 시도된 소프트웨어 업데이트(708)에 있을 수 있다.

[0074] 상기 적어도 레지스터(742)는 적어도 하나의 비휘발성 레지스터를 포함할 수 있다. 또한, 상기 시도된 소프트웨어 업데이트는 적어도 하나의 손가락 센서 드라이브의 소프트웨어 업데이트를 포함할 수 있다. 일부 변형에 있어서, 상기 손가락 감지 장치(610)는 IC 기판(612) 및 호스트 플랫폼(602)을 유지하는 공통 하우징(630)을 더 포함하는, 이를 테면, 랩탑, 휴대폰 또는 PDA와 같은 전자 장치 형태일 수 있거나 또는 상기와 같은 전자 장치 형태 내에 구비될 수 있다.

[0075] 일 방법 측면은 손가락 센서(710)와 관련한 소프트웨어를 호스팅하는 호스트 플랫폼(702)의 소프트웨어를 업데이트하기 위한 것이다. 상기 방법은, 시도된 소프트웨어 업데이트를 인증하기 위해 상기 호스트 플랫폼(702)과 협력하여 IC 기판상의 손가락 감지 요소들(714)의 배열을 포함하는 손가락 센서(710)의 IC 기판(712)

상의 보안 업데이트 회로(742)를 이용하는 것을 포함한다. 상기 방법은 상기 시도된 소프트웨어 업데이트의 성공적인 인증에 기반하여 호스트 플랫폼(702)의 소프트웨어를 업데이트하는 것을 더 포함할 수 있다.

[0076] **H. 추가 실시예**

[0077] 본 발명의 특징들을 포함한 예시적인 실시형태들의 추가 세부사항이 도 9 내지 도 17과 관련하여 하기에 기술될 것이다. 초기에, 상기 기재에 사용된 일부 용어가 거론될 것이다. 글로벌 공격(Global Attack)은 하나의 기계에 완전할 수 있으며, 동일한 시스템을 사용하는 모든 기계에 사용될 수 있는 보안 시스템상의 임의의 공격을 의미한다. 이는 때때로, BORE 공격(Break Once Run Everywhere)으로서도 언급된다. 플래시 메모리는 전기적으로 삭제될 수 있으며, 재프로그램될 수 있는 비휘발성 컴퓨터 메모리이다. 비휘발성 메모리(NVM)는 장치의 전원이 꺼졌을 때에 생존하는 메모리이다. 센서 측정 레지스터(Sensor Measurement Registers)는 센서 하드웨어를 이용하여 여러 시스템 구성요소들을 측정하는 능력을 제공한다. 프리-매치 프로세서(PMP)는 호스트 상에서 운용되는 코드를 포함하며, 매칭 동작의 많은 CPU 집약부를 수행한다

[0078] "SSD(Single Swipe to Desktop)"은 작동 시스템 부팅(operating system boot)과 같은 부팅 순서(boot sequence)에서 사용자가 사전 부팅 동안에 그의 식별정보를 한번 인증하고, 다음 단계로 통과된 그의 식별정보를 가지게 허용하는 기능성이다. 키는 암호화 프로세스의 동작을 제어하는 한 조각의 정보(파라미터)이다. 암호화에서, 키는 평문에서 암호문으로의 특정 변환을 명시하며 또는 복호화 동안에 암호문을 평문으로 특정 변환하는 것을 명시한다. 키 암호화 키(KEK)가 AKEY로의 변경을 인증하기 위해 사용된다. 상기 KEK는 신뢰한 플랫폼 모듈(Trusted Platform Module: TPM)이 상기 KEK를 보호하는데 사용되지 않은 한, 일반적으로 부팅마다(every boot) 변경된다(이는 사용자 정책 결정이다). 상기 애플리케이션 키(AKEY)는 호스트와 센서 간에 교환된 모든 보안 데이터를 암호화 및 복호화하기 위해 상기 센서에 의해 사용될 수 있다. AKEY는 매 번의 보안 세션 동안에 변경된다.

[0079] 디피-헬만(DH)은 두 장치가 하나의 공유키를 협상(negotiate)하도록 허용하는 널리 공지된 보안키-교환 방법이다. 협상이 공공연하게 일어날 수 있지만, 모든 통신을 듣는 도청자(eavesdropper)가 상기 공유키를 판별할 수 없다는 점이 주요한 이점이다. 임시적인 쌍을 이룬 키들(Ephemeral Paired Keys: EPK)은 $K_{암호화}$ 및 $K_{변경}$으로서 나타내는 두 개의 키를 포함한다. $K_{암호화}$는 메시지 서명 또는 정보 암호화와 같은 암호화 동작에 사용된다. $K_{변경}$은 $K_{암호화}$를 변경하기 위해서만 사용된다. 예를 들어, SHA-1과 같은 보안 해시 알고리즘(Secure Hash Algorithm)은 미국연방정보처리기준으로서 미국 국립표준기술원(NIST)에 의해 공개되었으며, 미국 국가 안전국에 의해 지정되었다.

[0080] 몇몇의 고차원적 보안 특징들이 여기 기재된 다양한 실시형태들에 의해 구현될 수 있다. 이들 특징들은 하기에 기술된다. 일반 목적은 사용자가 그의 TPM을 옵트인(opt-in) 하지 않는 경우에 우수한 보안성을 제공하고, 상기 사용자가 그의 TPM을 옵트인 하는 경우에 최고 수준의 보안을 제공하는 것일 수도 있다. 이 문맥에서 우수한 보안은 적어도, 상기 시스템이 글로벌 공격에 강력하게 저항할 것이라는 것을 의미한다. 최고 수준의 보안은 상기 시스템이 매치-온-센서(match-on-sensor) 시나리오에 의해, 매칭기(matcher)와 상기 시나리오가 수반하는 사용자 제한 없이, 제공되는 보안과 동일해야만 한다는 것을 의미한다.

[0081] 일부 비-TPM 소망 특징들(non-TPM desired features)은 상기 매칭기가 저장 및 실행 동안에 템퍼링되는 것으로부터 보호해야만 하고; 상기 템플릿이 저장 동안에 템퍼링되는 것으로부터 보호되어야만 하며, 이러한 보호는 기존의 개별 템플릿을 변경하는 것과, 템플릿 저장소로 전체 템플릿을 대체 및 부가하는 것을 모두 포함하며; 상기 템플릿은 비공개(privacy)를 보호하고 눈속임(snoofing)을 숨기기 위해 스누핑(snooping)하는 것으로부터 보호되어야만 하며; 센서 모듈로부터 호스트로의 이미지 정보는 비공개를 보호하고, 전자 위조(electronic spoofing)를 방지하기 위해 암호화되어야만 하며; 성공적인 인증에 따라, 상기 시스템은 매칭되는 템플릿의 표시 대신에 보안 페이로드(security payload: 등록시에 제공된)를 반환해야만 하며, 이러한 페이로드는 클라이언트-서버 아키텍처를 위해 이미 사용되는 다중 기록 능력을 이용하여 상기 템플릿에 확실하게 병합될 수 있으며; 상기 아키텍처는 손상된 클라이언트 PC(서버측 상의 소정의 적절한 소프트웨어)로부터 보호되는 로컬 영역 네트워크를 제공해야만 하며; 윈도우 지문 서비스와 윈도우 애플리케이션 사이의 인터페이스는 보호되어야만 하며; 상기 거론한 보호들에 사용된 암호화, 키 관리 및 키 교환 방식은 글로벌 공격에 (가능한 한) 저항적이어야만 하는 것을 포함할 수 있다.

[0082] 상기 TPM이 적절한 상태로 이용가능할 때에, 높은 수준의 보안을 제공하는 것이 가능하다. 보안 능력의 증가로, 상기 아키텍처는 다음의 추가적인 보안 요건에 부응할 수 있다: 상기 보안 아키텍처는 원격의 소프트웨어

기반 공격에 대해 장기간 사용 키(long-term key)를 보호할 수 있으며; 상기 장기간 사용 키가 획득되는 경우(하드웨어 공격을 사용하여), 상기 키는 단일 기계 상에서만 유용할 것이다.

[0083] 도 9를 참조하면, 상기 거론한 소망하는 특징들에 부응하는데 사용될 수 있는 일부 기능성이 기술될 것이다. 이러한 기능성은 하드웨어 및 소프트웨어 구성요소들 모두에서 구현될 수 있다. 이는 다양한 보안 구성요소들 및 그들의 각 위치들에 대한 최상의 기재이다. 상기 센서 구성요소들은 센서 실리콘으로 직접적으로 건설될 수 있는 마이크로 하드웨어 보안 모듈(μHSM)을 포함할 수 있으며, 다음을 포함한 여러 가지 중요한 암호화 기능을 수행할 수 있다: 센서의 최종 테스트 동안에 상기 μHSM이 생성시키는 고유의 비공개 키(privacy key)를 통한 고유의 장치 독자성(이러한 키는 저장되어 상기 μHSM 모듈 외부에 절대 해제되지 않는다); 키(keys), 논스(nonces), 및 시드 값(seed values)을 생성하는데 사용하기 위한 무작위 번호 생성기; 디지털 서명 생성 및 코드 측정을 위한 SHA-1 엔진; 이미지, 템플릿 등을 암호화하기 위한 AES-CCM 엔진; 및 가속형 디피-헬만 및 DSA 동작을 위한 PKE 엔진. 센서의 모든 암호 동작은 센서 로직의 제어 하에 μHSM에 의해 수행될 수 있다.

[0084] 상기 보안 센서는 그가 매칭 동작의 최종 단계를 수행하도록 허용하는 로직을 포함할 수 있다. 상기 호스트 상의 프리-매치 프로세서(PMP) 소프트웨어는 최고로 복잡하고 CPU 집약적인 작업을 수행하며, 중간 결과를 센서로 제공한다. 상기 센서의 내부 매칭기는 그때 예를 들어 이미지 워터마킹 정보를 사용하여 호스트로부터 데이터를 검증하고, 최종 매칭 스코어를 산출한다.

[0085] 상기 센서는 4개의 센서 측정 레지스터를 포함할 수 있다. 상기 센서 로직은 이들 레지스터로 측정들을 연쇄시키기 위해 μHSM의 SHA1 엔진 및 그의 비공개 키를 사용한다. 이를 위한 프로세스는 일단 새로운 측정이 이들 레지스터 가운데 하나에 연쇄되면, SMR을 이전 상태에 일치하는 값으로 되돌릴 새로운 측정을 결정하는 것이 연산 불가능해지는 방식으로 이루어진다. 또한, 상기 연쇄(concatenation) 프로세스가 초기 상태에서 시작할 경우, 정확히 동일한 순서로 동일한 정밀 측정들을 연쇄하는 것은 소정의 센서 상의 SMR에 정확히 동일한 값을 항상 결과할 것을 보장한다.

[0086] 상기 호스트 소프트웨어는 상기 SMR에 연쇄될 수 있는 측정들을 제공하며, 초기화 및 등록 동작들 동안에 센서 로직이 비-휘발성 메모리에 일부 SMR 값을 저장하도록 지시한다. 뒤따른 동안에, 상기 센서 로직은 상기 저장 값들에 현재 SMR(current SMR) 값을 비교할 수 있다. 이들 값들이 동일한 경우, 그때 상기 센서 로직은 암호화 정보의 특정 항목 해제를 승인한다.

[0087] 상기 호스트가 한번 필요한 암호 정보를 획득하면, 그때 그는 SMR(들)을 위해 센서로 무작위 측정을 제공할 수 있다. 이는 임의의 미래 실체가 비밀 정보에 접근하는 것을 방지하는 효과를 가진다. 상기 보안 센서에는 각각이 상이한 목적을 가지는 4개의 SMR이 있을 수 있다. SMR_{OS}은 그 자체 측정을 위한 장치 드라이버, 플랫폼, 및 매칭기에 의해 사용된다. 이들 측정이 일단 센서에 의해 검증되면, 상기 호스트는 현재의 호스트 루트 키(Host Root Key: HRK) 카피(copy)를 요청하기 위해 승인될 수 있다. SMR_{PBA}는 그 자체 측정을 위해 BIOS 옵션 ROM, 플랫폼, 및 매칭기에 의해 사용된다. 이들 측정값들이 센서에 의해 일단 검증되면, 상기 호스트는 현재의 호스트 루트 키(HRK)의 카피를 요청하기 위해 승인될 수 있다. SMR_0이 제3의 매칭기와 같은 다른 실체에 의한 사용을 위해 보존될 수 있다. SMR_{MV}은 템플릿 내용을 보안하고, 그를 특정 센서, 기기 및 매칭기에 결합하기 위해 상기 매칭기와 센서에 의해 사용된다. 이 레지스터의 값은 다른 것들과 같이 NVM로 저장될 수 없으며, 대신에 센서의 페이로드 키를 사용하여 등록시에 각각의 템플릿으로 암호화될 수 있다. 상기 센서는 상기 템플릿 및 그의 보안 페이로드가 템퍼링되지 않았으며, 현재 기기(current machine) 상에서 현재 센서를 사용하여 생성되었음을 확실히 하기 위해 매칭 시간에 그것을 복호화하고, 점검할 수 있다.

[0088] 상기 보안 센서는 예를 들면, 128 바이트의 재기록가능한 플래시 메모리를 포함하는 비-휘발성 메모리(NVM)를 포함할 수 있다. 이러한 메모리는 센서와 호스트 모두를 위한 장기간 사용 키(long-term keys), 저장된 SMR 값, 및 상태 플래그를 저장하기 위해 사용될 수 있다. 이 메모리의 내용은 센서 로직에만 보일 수 있다. 상기 보안 센서는 호스트가 일부 동작을 수행하는데 소요되는 시간의 추적을 지속함에 의해 지문 보안 시스템상의 디버거(debugger) 또는 인-서킷 에뮬레이터(in-circuit emulator) 공격을 방지하기 위해 사용되는 감시 타이머(watchdog timer)를 포함할 수도 있다.

[0089] 지문 기반 보안에 관련한 여러 구성요소들이 호스트 상에 존재할 수 있으며, 도 9를 더 참조하여 기술될 것이다. 이들 구성요소들의 일부는 제1 OS 부팅 이벤트(boot event) 이전에 동작할 수 있으며, 다른 것들은 OS 환경 내에서만 운용될 것이다. 다음은 이들 구성요소의 고차적 기술이 제공된다.

[0090] 상기 BIOS 옵션 ROM은 BIOS 이미지에 링크되는 임의의 구성요소이며, 자산 보호와 데이터 보호 모두를 제공한다. 이는 사용자의 인식 없이 바이오스(bios)의 내용을 변경하기 어렵기 때문에 안전한 사전-부팅 인증 방법이다. 이는 강화된 루트(enhanced-root)의 측정 확실성을 제공한다. 이러한 구성요소는 OS가 부팅 과정을 시작하기 전에 사용자가 지문 인증을 수행하는 것을 필요로 하거나 이를 허용한다. 이는 그것을 도용할 수 누군가에게 예를 들어, 랩탑과 같은 컴퓨터가 무용지물이 되게 한다. 데이터 저장 접근법에 따라서, 하드 디스크는 이러한 인증이 수행되기 전에 비-잠금되는 것을 필요로 하지 않다. 이는 드라이브 상의 데이터에 추가적인 보호를 제공한다. 옵션 ROM이 SSD(single swipe to desktop)의 임의 능력을 제공한다. 이러한 특징은 소유자 정책 제어하에 있을 수 있다.

[0091] 통합 확장형 펌웨어 인터페이스(UEFI) 가능 시스템에서, 상기 UEFI 드라이버 및 애플리케이션은 종래의 BIOS 시스템에 사용되는 옵션 ROM을 대체한다. 제공되는 보안의 수준은 상기 UEFI 사양이 추가적인 보안 특징들로 업데이트되는 경우, 상기 옵션 ROM 접근에 의해 제공되는 것에 일치할 수 있다. 상기 UEFI 구성요소는 제1 하드 드라이브의 특정 부분 상에 저장될 수 있다. 상기 드라이버는 센서와의 USB 통신을 구축하기 위해 UEFI 프레임워크 기능들을 사용한다.

[0092] 전체 볼륨 암호화(Full Volume Encryption: FVE) 라이브러리는 전체 하드 드라이브 암호화를 제공하는 애플리케이션에 링크될 수 있는 ×86 라이브러리일 수 있다. 예를 들어, 이는 세이프부트(Safeboot)의 FDE 제품이거나 또는 마이크로소프트의 비트로커(Bitlocker)일 수 있다. 전형적으로, 이들 암호화 시스템은 PBA 이후이지만, OS 부팅 이전에 운영된다. 상기 라이브러리는 보안 센서와 적절하게 동작하게 동작하는데 필요한 모든 기능성을 제공할 수 있다.

[0093] OS 센서 장치 드라이버는 높은 보안환경에서 수행되어야만 하는 모든 기능들을 수행할 수 있다. 상기 드라이버가 오링(Ring 0)에서 운영되기 때문에, 그의 동작을 방해하기 어려우며, 때문에 이는 더욱 안전하게 동작할 수 있다. 상기 드라이버 기능성은: 호스트와 보안 센서 사이에 이동하는 데이터의 암호화 및 복호화; 식별 트랜잭션(identify transaction)의 일대다 부분(one-to-many portion) 동안에 전체 매칭기 동작과 함께 보안 매치를 하기 위한 프리-매치 처리; 상기 호스트와 보안 센서 간의 디피-헬만 키 협상; 및 상기 서비스와의 교차-인증을 포함할 수 있다.

[0094] 상기 OS 서비스는 애플리케이션과 지문 시스템 간에 보안 인터페이스를 제공한다. 예상되는 기능성은 신뢰 애플리케이션이 지문 시스템 동작을 요청하게끔 하는 API 기능의 제공; 상이한 수준의 인증 가능성을 포함하여 "신뢰" 애플리케이션을 결정하는 방법의 제공, 즉, 동작의 서브셋은 일부 애플리케이션에 의해서만 수행될 수 있으며, 다른 것에 의해서는 수행될 수 없다; 스택에서 보안 통신 채널 상하에 있는 소프트웨어 구성요소들 사이에 상기 보안 통신 채널을 구축하는 방법의 제공, 이는 애플리케이션과 서비스 간에 및 상기 서비스와 드라이버 간에 전송된 모든 데이터가 스누핑(snooping) 및 템퍼링에 저항 되어야만 한다는 것을 의미한다; 지문 시스템 초기화를 수행하기 위한 로직의 제공, 많은 지문 시스템 초기화는 상기 서비스의 제어하에 발생한다; 초기화가 완료될 때까지 모든 다른 지문 동작의 방지; 및 상기 장치 드라이버와 애플리케이션 간의 사용자 프롬프트(prompt)와 피드백을 위해 채널의 제공을 포함할 수 있다.

[0095] OS 로그인 애플리케이션(GINA/VCP) 소프트웨어 구성요소는 로그인 동안에 OS에 사용자 식별정보를 제공하는 책임이 있다. 이러한 본 접근은 로그인 애플리케이션이 로그인을 승인하기 위해 애플리케이션 페이로드(AP)에 저장된 정보 또는 상기 AP에 포함된 데이터로부터 획득된 정보를 사용하는 것을 가정할 수 있다. 이러한 태스크를 달성하기 위해, 상기 애플리케이션은 서비스로부터 AP를 요청할 수 있다. 이는 지문 시스템이 이전의 성공적인 지문 인증(사전 부팅 또는 전체 볼륨 암호화와 같은)에서, 또는 새로운 지문 인증 순서의 개시에서 해제되었던 AP를 반환하게 할 것이다.

[0096] 새로운 인증 순서가 요구되는 경우, 그때 로그인 애플리케이션은 지문 시스템으로부터 사용자 기반 메시지로 프롬프트 및 피드백을 제공해야만 한다.

[0097] 상기 OS 초기화 애플리케이션 소프트웨어 구성요소는 특정 사용자 소유권의 PC 동안에 일반적으로 한 번만 운영될 것이다. 이는 임의의 다른 지문 시스템 동작이 가용 되기 전에 운영되어야만 한다. 초기화의 과정에서, 애플리케이션은 사용자로부터의 정보 획득을 필요로 할 것이다. 이러한 정보는 소유권자 암호구(pass-phrase) 및 지문 시스템 정책 정보를 포함할 수 있다. 상기 초기화 구성요소는 모든 동작들을 완료하기 위해 시스템 재부팅을 걸쳐서 동작하는 것을 필요로 할 수 있다.

[0098] 다른 클라이언트 애플리케이션은 웹 페이지 및 대화 상자에서 패스워드 대체기능을 제공하고, 폴더 및 파일

암호화 및 복호화를 승인하며, 필요한 다른 지문기반의 승인 동작을 수행하는 것을 필요로 할 수 있다.

[0099] 본 지문 보안 아키텍처의 데이터 저장 시스템은 하나의 저장 매체에 제한되는 것은 아니지만, 센서 플래시 저장 접근이 보안의 견지에서 바람직할 수 있다. 상기 센서 플래시 데이터 저장 접근은 글로벌 서비스 거부 공격(global denial service attack)을 방지할 수 있는 유일한 접근일 수 있다. 이는 상기 센서가 사용자가 인증되는 경우를 제외하고, 플래시의 기록 및 삭제를 방제할 수 있기 때문에 가능하다. 상기 데이터 저장소는 템플릿, 프리-매치 프로세서, 호스트 키 블롭(blobs), 및 PBA 로드가능한 바이너리가 저장될 수 있으며, OS와 사전 부팅 소프트웨어 구성요소들에 접근할 수 있게 되는 위치(들)를 제공해야만 한다. 필요한 경우, 상기 OS 및 사전 부팅 데이터 저장소는 따로 분리되지만, 중복되는 저장소일 수 있다. 이는 센서 플래시의 경우에 필요하지 않으며, 다른 데이터 저장 접근들을 넘어서 이가 선호되는 또 다른 이유이다.

[0100] 지문 보안 시스템의 이전 버전들은 라이브 샘플에 매치되는 템플릿이 무엇인지를 표시하는 인덱스를 간단히 반환하였다. 상기 애플리케이션은 그때 이 응답에 기반하여 그 자신의 저장소로부터 보안자료를 검색할 것이다. 이러한 접근의 문제점은 해커가 우리의 전체 소프트웨어 및 하드웨어 스택을, 존재하는 손가락에 상관없이 유효 지수를 항상 반환하는 간단한 동적 링크 라이브러리(DLL)로 교체할 수 있다는 것이다. 실제로, 손가락의 존재를 필요로 하는 것은 아니다. 애플리케이션 및 소프트웨어가 교차 인증하는 경우에도, 악성 소프트웨어가 회귀 응답을 임의의 소망하는 것으로 변경할 수 있는 단일 배치가능한 공격점이 여전히 존재한다.

[0101] 다양한 실시형태들에서, 본 접근은 상기 애플리케이션과 지문 시스템의 상호작용 방식을 근본적으로 변경함에 의해 이러한 형태의 공격들을 제거하는 것을 탐색할 수 있다. 본 접근에서, 상기 애플리케이션은 등록 동안에 지문 시스템에 보안자료를 포함한 페이로드를 제공할 수 있다. 상기 지문 시스템은 매칭 손가락이 검증될 때까지; 페이로드를 애플리케이션에 반환하는 순간에 페이로드 보안을 유지할 수 있다. 이러한 접근으로, 상기 지문 시스템을 대체하거나 또는 그의 응답을 변경하는 것은 아무런 성과도 없는데, 이는 상기 애플리케이션이 상기 페이로드에 저장된 보안자료 없이 동작을 지속할 수 없기 때문이다.

[0102] 사용자가 손가락 치기를 사용하여 OS에 로그인하게 할 애플리케이션을 가정한다. 다음 표는 종래의 접근법 대 본 접근법에서 발생할 수 있는 이벤트를 도시한다.

표 1

[0103]

종래 접근법	본 접근법
애플리케이션이 지문 인증을 요청	애플리케이션이 지문 인증을 요청
지문 시스템이 라이브 샘플을 획득	지문 시스템이 라이브 샘플을 획득
템플릿이 라이브 샘플에 매칭	탬플릿이 라이브 샘플에 매칭
매칭 템플릿 결정(있는 경우)	매칭 템플릿 결정(있는 경우)
애플리케이션이 매칭 템플릿을 인지(있는 경우)(이는 단일 공격점)	보안 페이로드가 템플릿으로부터 검색되고 센서 내부에서 복호화
애플리케이션이 그 자신의 저장소로부터 사용자 식별번호를 탐색하기 위해 반환 정보를 사용	페이로드로부터 사용자 식별번호가 애플리케이션에 반환

[0104] 상기 예에 도시된 바와 같이, 해커가 본 접근으로부터 상기 반환 응답을 변경하는 것이 유리하지 않은데, 이는 상기 응답이 한 세트의 유효 사용자 식별정보이어야만 하기 때문이다. 해커가 상기 식별정보를 이미 아는 경우, 그때 상기 지문 시스템을 공격할 이유는 없다. 그들은 이미 OS에 로그인 하는데 필요한 모든 정보를 가지고 있다.

[0105] 다음은 상기 다양한 실시형태들에 존재할 수 있는 통신 보안의 다양한 특징들에 관한 거론이다. 센서-호스트(드라이버) 보안 세션이 제공될 수 있다. 상기 센서가 보안 페이로드의 복호화를 수행할 수 있기 때문에, 상기 센서와 호스트 간에 전송된 데이터는 스누핑(snooping)으로부터 보호될 수 있다. 이는 보안 세션의 구축을 통해 달성될 수 있다. 일단 보안 세션이 구축되면, 센서에 의해 보내진 모든 이미지 및 보안 자료는 예를 들어 AES128-CCM 암호화 방식을 사용하여 암호화될 수 있다. 상기 암호화는 보안 세션의 초기화 동안에 생성될 수 있는 공유키를 사용하여 입력될 수 있다. 상기 공유 암호키는 상기 키를 구축하는데 사용하는 방법에 상관없이, 동작의 현재 상태에 따라 여러 상이한 방식으로 획득될 수 있으며, 각각의 보안 세션 위한 새로운 키여야만 한다. 보안 세션은 일반적으로 단일 트랜잭션 동안 지속된다. 이는 각 이미지가 새로운 키로 암호화되는 건을 보장할 것이다. 보안 세션을 구축하는데 있어서 추가 세부사항이 하기 제공된다.

[0106] 클라이언트 애플리케이션-서비스 보안 통신이 제공될 수 있다. 상기 서비스와 임의의 클라이언트 애플리케이

션 간의 통신 채널은 두 개의 목적을 달성할 수 있다: 두 실체 간의 모든 데이터와 명령 흐름이 스누핑되고, 템퍼링되는 것을 보호; 및 둘째로, 상기 애플리케이션과 서비스 간에 신뢰를 확립. 이들 두 개의 목적은 두 개의 개별 보안 접근법을 사용하여 달성될 수 있다. 스누핑과 템퍼링은 클라이언트와 서비스 간의 보안망(Secure Socket Layer: SSL) 프로토콜을 사용하여 방지될 수 있다. 보안망(SSL) 프로토콜은 임의의 두 실체가 사전에 서로에 대해 어떠한 것도 아는 것 없이 보안 통신 채널을 협상하고 생성하는 것을 가능하게 하는 산업 표준 프로토콜이다. 이러한 프로토콜의 세부사항은 본 기술분야의 당업자에게 공지되었다.

[0107] 고유의 클라이언트 ID에 연결된, 쌍을 이룬 롤링 키들을 사용하여 상기 실체들 간에 신뢰가 구축될 수 있다. 이들 키는 상기 서비스와 클라이언트 간에 전송된 모든 메시지들에 서명하거나 또는 (추가) 암호화하는데 사용될 수 있다. 상기 쌍을 이룬 롤링 키들의 사용 및 관리는 SSL 세션 내부에서 발생할 수 있으며, 때문에 동작에 있어서 두 층(layer)의 보안이 있다는 것을 유의해야 한다. 쌍을 이룬 롤링 키들의 실행 세부사항은 하기에서 확인할 수 있다.

[0108] SSL과 회전 키(revolving keys)의 기능성은 정적 라이브러리에서 실행될 수 있다. 이러한 라이브러리는 애플리케이션 제공자에 의해 클라이언트 애플리케이션에 링크될 수 있으며, 보안 API를 제공할 수도 있다. 또한, 상기 쌍을 이룬 롤링 키들을 위한 초기값 및 클라이언트 ID가 이 라이브러리에 배치될 수도 있다. 상기 키 쌍의 현재값은 상기 클라이언트 애플리케이션과 서비스에 의해 안전하게 저장될 필요가 있을 수 있다. 상기 서비스는 관련한 클라이언트 ID와 함께 각 애플리케이션을 위한 한 쌍들을 저장할 수 있다.

[0109] 서비스-드라이버 보안 통신이 제공될 수 있다. 상기 서비스와 장치 드라이버 간의 통신 채널은 모든 데이터와 명령 트래픽(traffic)이 스누핑되고, 템퍼링되는 것 양쪽으로부터 보호할 수 있다. 또한, 상기 두 실체는 교차 인증할 수 있다. 이러한 태스크를 달성하기 위해, 서비스와 드라이버는 상기 서비스와 드라이버가 연결될 때마다 새로운 보안 인터페이스를 생성하기 위해 SSL의 요소들을 사용할 수 있다. 일단 연결되면, 상기 두 실체는 쌍을 이룬 롤링 키들을 사용하여 교차 인증할 수도 있다. 이들 키의 출발 값들은 하드 코딩될 수 있지만, 제1 연결 이후에 무작위로 변경될 수 있다.

[0110] 이벤트들의 일반 순서는 다음을 포함할 수 있다: 서비스가 드라이버를 탐색하고 연결 프로세스를 시작하며, 드라이버가 SSL 협상을 시작하며, 드라이버 및 서비스가 SSL 키 협상을 완료하며, 이들 키가 다음번에 상기 드라이버와 서비스가 연결될 때까지 실제로 유지될 것이며, 이는 플러그-엔(n)-플레이 이벤트 또는 재부팅일 수 있다; 이 기기 상에서 처음인 경우, 드라이버는 쌍을 이룬 롤링 키들을 사용하여 상기 서비스와 교차 인증을 시작한다; 드라이버와 서비스는 상기 드라이버에 의해 이루어진 각기 서비스 존재 확인에 대해 재인증한다.

[0111] 상기 방식을 따라 보안 이미지들을 복호화하는 것 없이 센서로부터 서버 기반 애플리케이션으로 직접적으로 보안 이미지들을 제공하는 옵션이 있을 수 있다. 일반적으로, 이는 임의의 다른 클라이언트와 같은 보안 통신 채널을 사용하여 달성될 수 있다. 상기 클라이언트가 그의 이미지 획득 동안에 상기 센서에 의한 사용을 위해 고유의 키를 제공할 수 있다는 것이 부가될 수도 있다. 이러한 키는 현재 AKEY로서 센서에 설치될 수 있으며, 이미지 슬라이스들이 드라이버에 전달됨에 따라 상기 이미지 슬라이스들을 암호화하는데 사용될 수 있다. 상기 드라이버와 서비스는 이들 슬라이스들을 체인 바로 위로 정적 링크된 클라이언트 라이브러리가 복호화 및 이미지 처리를 수행할 것인 서버 기반 애플리케이션에 간단히 전송할 수 있다.

[0112] 다음 기재는 상기 시스템이 수행할 수 있는 주요 기능들 각각에 대한 예시적인 단계별 과정의 기재를 제공한다.

[0113] 보안 센서 통신 세션의 생성: 새로운 데이터 암호화 키가 호스트 상에 생성되어 센서의 μHSM에 설치될 때에, 보안 세션이 존재한다. 세션은 종단의(terminate) 세션 명령을 사용하여 호스트에 의해 종결된다. 데이터 암호화에 사용되는 키는 애플리케이션 키(AKEY)로 일컬어진다. 이러한 키는 키 암호화 키(KEK)를 사용하여, 호스트에 의해 센서 μHSM로 설정된다. 따라서, 상기 KEK는 새로운 AKEY가 설치될 수 있기 전에 μHSM로 설정되어야만 한다.

[0114] 이러한 접근에서, KEK는 일반적으로 특정 부팅에 걸쳐 사용되며, AKEY는 매 번의 보안 세션 동안에 변경될 수 있다. KEK는 새로운 보안 세션을 구축하는데 필요한 시간을 줄이기 위해 길게 유지된다. 시스템의 현재 상태에 따라, 새로운 KEK의 구축은 0.5초에 이르는 시간이 걸릴 수 있다.

[0115] KEK의 구축을 위한 다수의 방법이 있다. 특정 경우에 사용되는 방법은 센서와 호스트의 현재 상태에 따라 달라진다. 다음 표는 상태들을 열거하며, 그들의 특징을 기술한다.

표 2

[0116]

KEK 없음	호스트가 재부팅되고, 키 암호화 키(KEK)의 TPM 실링 카피(sealing copy)가 존재하지 않을 때마다 이러한 상태가 발생한다. 보통의 부팅 순서 동안에, 이러한 상태는 사전 부팅에서와, 장치 드라이버가 로딩할 때에 다시금 발생할 수 있다.
KEK 실링(sealed)	이러한 상태는 소유권자가 KEK를 보호하기 위해 TPM의 사용을 결정한 것을 표시한다. 대신에, 상기 KEK와 랩핑된(Wrapped) KEK는 TPM에 실링되며, 초기화(또는 정책 변화 동안에) 동안에 데이터 저장소에 배치된다.
KEK 랩핑(wrapped)	이러한 상태에서, 상기 호스트는 상기 KEK 및 "랩핑된" KEK의 메모리 기반 카피(copy)를 가지며, 상기 KEK를 μHSM로 로딩한다. 이러한 상태는 상기 센서가 전원을 잃고, 호스트가 그렇지 않은 경우 발생할 수 있다.
KEK 로딩	이러한 상태에서, 상기 KEK는 상기 센서의 μHSM에 성공적으로 설치되었다. 이러한 상태는 보안 세션이 구축될 수 있기 전에 존재해야만 한다.

[0117] 상기 KEK가 TPM에 실링(seal)되지 않았으며(센서 플러그에 기반), 호스트가 PBA 또는 OS로 부팅하는 것을 가정하며(상태 == KEK 없음), 상기 호스트는 KEK 로딩 상태로 이동하기 위해 다음 동작들을 수행할 수 있다:

[0118] 1- DH 세션이 호스트와 센서 간에 시작할 수 있기 전에, 변경 승인 명령이 μHSM 상에서 운영되어야만 한다. 이러한 명령은 드라이브 내에서 혼동되는 비공개 키와 공개 키를 포함한 메시지를 사용한다. 상기 공개 키는 메시지는 제조자의 비공개 키(KM_{PRIV})로 서명(sign)된다. 상기 서명은 제조자의 공개 키(KM_{PUB})에 대한 그의 카피를 이용하여 상기 μHSM에 의해 확인된다. 이러한 접근은 키 서버의 사용을 회피한다.

[0119] 2- 일단 변경 승인이 성공적으로 완료되면, 디피-헬만(DH) 협상이 상기 μHSM과 호스트 간에 수행된다. 이러한 동작의 결과는 일시적인 세션 보호키(K_{SP})이다. 유의: DH 협상 준비의 일 부분으로서, 호스트는 일시적인 디지털 서명 알고리즘(DSA) 키를 생성해야만 한다.

[0120] 3- 상기 호스트는 KEK로서 사용될 새로운 랜덤 키를 생성한다.

[0121] 4- 상기 호스트는 KEK를 암호화하기 위해 K_{SP}를 사용하며, 이어서 μHSM KEK 로컬 레지스터로 새로운 KEK를 설치하기 위해 DM 메시지를 사용한다.

[0122] 5- 상기 호스트는 이어서 μHSM가 상기 KEK를 "랩핑(wrap)"하도록 명령한다. 상기 μHSM는 내부 비공개키를 사용하여 상기 KEK를 암호화하고 서명하며, 상기 호스트에 그것을 제공한다. 이러한 랩핑된 KEK는 이 특정 센서에 의해서만 복호화될 수 있다.

[0123] 6- 일단 호스트가 KEK를 랩핑하면, "KEK 로딩"으로 상태가 이행한다. 바로 AKEY를 설정하고 보안 세션을 구축하는 것이 바람직하다.

[0124] 상기 KEK가 TPM에 실링(seal)되었으며(센서 플러그에 기반), 호스트가 PBA 또는 OS로 부팅하는 것을 가정하며(상태 == "KEK 실링"), 상기 호스트는 KEK 로딩 상태로 이동하기 위해 다음 동작들을 수행할 수 있다:

[0125] 1. 호스트가 데이터 저장소로부터 KEK 블롭(blob)을 판독하고 TPM에 그것을 "실링하지 않도록" 명령한다. 환경이 상기 실링하지 않는 동작을 허용하게 하도록 정정되는 경우, 상기 TPM은 내부 키를 사용하여 KEK 블롭을 복호화할 것이다. 상기 KEK 블롭은 상기 KEK의 선명한 카피와 랩핑된 KEK 모두를 가진다.

[0126] 2. 호스트가 상기 랩핑된 KEK를 센서 μHSM로 통과시키며, 그것이 로컬 KEK 레지스터로 상기 KEK를 랩핑하지 않도록 명령한다.

[0127] 3. 일단 상기 μHSM이 KEK를 랩핑하지 않으면, "KEK 로딩"으로 상태가 이행한다. 바로 AKEY를 설정하고 보안 세션을 구축하는 것이 바람직하다.

[0128] 호스트가 KEK와 랩핑된 KEK 모두의 메모리 기반 카피를 가지며(상태 == "랩핑된 KEK"), 상기 호스트는 KEK 로딩 상태로 이동하기 위해 다음 동작들을 수행할 수 있다:

[0129] 1. 호스트가 랩핑된 KEK를 센서 μHSM로 통과시키며, 그것이 로컬 KEK 레지스터로 상기 KEK를 랩핑하지 않도록 명령한다.

[0130] 2. 일단 상기 μHSM이 KEK를 랩핑하지 않으면, "KEK 로딩"으로 상태가 이행한다. 지금 AKEY를 설정하고 보안 세션을 구축하는 것이 바람직하다.

[0131] 일단 시스템이 "KEK 로딩" 상태가 되면, 보안 세션이 마음대로 개방 및 폐쇄될 수 있다. 이는 다음 단계들을 사용하여 이루어진다.

[0132] 1. 호스트가 이 세션을 위한 AKEY로서 사용하기 위한 새로운 랜덤 키를 생성한다. 세션 동안에, 이 키를 사용하여 모든 민감한 정보가 암호화될 것이다.

[0133] 2. 호스트가 AKEY를 포함하며, KEK에 의해 보호되는 새로운 μHSM_DH_MSG를 생성한다. 상기 메시지는 이어서 센서 μHSM로 보내진다.

[0134] 3. 상기 센서는 상기 메시지를 복호화하고 확인한다. 메시지가 유효하면, 상기 μHSM는 그것의 내부 AKEY 레지스터를 메시지에서 AKEY로 설정한다.

[0135] 4. 센서 로직은 이러한 활동을 모니터하고, 상기 μHSM가 성공적인 AKEY 변경을 가리키면, 상기 센서 상태를 SecureModeOn으로 설정한다.

[0136] 5. 이 시점에서 상기 보안 세션은 센서와 호스트 상이에 구축되었다. 상기 세션은 "종단의 보안 세션" 센서 명령을 사용하여 호스트에 의해 종결될 때까지 개방되어 유지된다.

[0137] 쌍을 이룬 롤링 키들(PRK)이 보안 아키텍처 내에서 여러 구성요소들 간의 링크에 사용될 수 있다. 이러한 부분은 이들 키 및 그들이 사용되고, 생성되고, 관리되는 방법을 기술한다. 쌍을 이룬 롤링 키는 $K_{암호화}(K_E)$ 및 $K_{변경}(K_C)$으로 언급되는 두 개의 키를 포함한다. $K_{암호화}$는 메시지 서명이나 정보 암호화 같은 암호화 동작을 위해 사용된다. $K_{변경}$은 $K_{암호화}$를 변경하기 위해서만 사용된다. 이들 키의 초기값은 일반적으로 그들이 사용될 2진수(binary)의 디폴트값으로서 설정된다. 이는 상기 키들을 사용하여 임의의 다른 동작이 수행되기 전에 상기 키들이 변경될 것이므로 공지된 지식일 수 있다.

[0138] 키 관리는 다음 단계들을 수반할 수 있다:

[0139] 1. 개시 소프트웨어는 궁극적으로 $K_{암호화}$가 될 것인 새로운 랜덤 키($K_{E'}$)를 생성한다.

[0140] 2. 그것은 이어서 새로운 키($K_C[K_{E'}] => K_{EPC}$)를 암호화하기 위해 $K_{변화}$에 대한 그의 카피를 사용한다.

[0141] 3. 상기 암호화 키(K_{EPC})는 이어서 명령으로 수신 소프트 구성요소로 보내진다.(상기 명령은 실제 사용에 따른 현재 K_E를 사용하여 암호화되거나 서명될 것이다)

[0142] 4. 상기 수신 구성요소는 메시지를 확인하고, 이어서 현재 K_C를 사용하여 새로운 K_E를 복호화하고 저장한다.

[0143] 5. 일단 이러한 트랜잭션이 완료되면, 개시 소프트웨어는 새로운 K_E를 저장한다.

[0144] 6. 다음 명령이 새로운 $K_{변경}$키를 설정할 것이다. 이는 $K_{C'}$가 새롭게 구축된 $K_E(K_E[K_{C'}] => K_{CPE})$를 사용하여 암호화된다는 점을 제외하면 $K_{암호화}$의 변경과 동일한 방식으로 이루어진다.

[0145] 이러한 접근에서, 상기 개시 구성요소는 보안이 높은 실체일 수 있다. 이는 서비스와 클라이언트 간에, 상기 서비스가 키 업데이트를 개시할 것인 반면, 상기 서비스와 드라이버 간에는 상기 드라이버가 개시할 것이라는 것을 의미한다. 상기 키 업데이트는 무작위로 일어나는 것이 예상된다.

[0146] 상기 초기화는 애플리케이션의 제어하에 윈도우 서비스(서비스), 장치-드라이버(드라이버), 사전 부팅 코드, 및 센서와 협력하여 수행될 수 있다. 또한, 상기 사전 부팅 코드 및 드라이버는 초기화 이전에 일부 동작들을 수행할 수 있으며, 센서 측정 레지스터(SMR)가 상기 초기화 동작을 위한 적정 상태에 있게 된다. 다음은 시스템이 비-초기화 상태로 있는 경우, 다양한 지문 시스템 구성요소들에 수행될 수 있는 작용의 목록이다. 이들 작용들은 다음을 따른 초기화 단계들에 의해 의존할 수 있다.

[0147] 1. 옵션-ROM 또는 다른 PBA 소프트웨어가 센서 상의 SMR_{PBA}로 그 자체 측정을 하며, 상기 측정은 초기화에 가

용하다. 이러한 측정은 BIOS 제공자에 의해 실행되는 경우, 코어 BIOS에 의해 수행될 수 있다.

[0148] 2. 장치 드라이버가 로딩하여, 상기 센서 상의 SMR_{OS}로 그 자체의 일부를 측정한다.

[0149] 3. 드라이버는 초기화가 완료되었는지 여부를 판별하기 위해 센서로부터 상태 플래그를 검색한다.(이러한 경우 INIT_완료 플래그가 설정되지 않는다)

[0150] 4. 서비스가 상기 드라이버로부터 지문 시스템 상태를 로딩 및 요청한다(이러한 경우 상기 드라이버는 상기 시스템이 아직 초기화되지 않았음을 보고한다)

[0151] 5. 클라이언트 애플리케이션 소프트웨어가 운영되어 지문 보안 시스템이 초기화되지 않았음을 판별한다. 사용자는 상기 지문 시스템을 초기화하도록 상기될 수 있다.

[0152] 다음은 일단 사용자가 초기화를 활성화하면 지문 시스템에 의해 수행될 수 있는 작용의 목록이다.

[0153] 1. 초기화 애플리케이션이 개시 사용자로부터 소유권자 암호구(Pass-phrase)를 얻을 것이다.

[0154] 2. 애플리케이션은 서비스가 개시할 것을 요청하고, 소유권자 암호구를 서비스에 통과시킨다.

[0155] 3. 서비스가 주요 메모리로 팩토리 프리-매치 프로세서(factory Pre-Match Processor: PMP)를 압축해제한다.

[0156] 4. 사전-부팅 사용자 인터페이스(PBUI) 바이너리(binary)가 존재하는 경우, 상기 서비스는 메모리로 상기 바이너리를 카피할 수도 있다(이러한 바이너리는 씨드되지 않을 것이기 때문에 압축해제가 필요하지 않다).

[0157] 5. 서비스는 드라이버가 초기화를 수행하도록 요청하고, 파라미터로서 PMP 및 PBUI의 위치와 소유권자 암호구를 통과한다.

[0158] 6. 상기 드라이버는 시스템이 센서 플래그를 사용하여 이미 초기화되었음을 확인하기 위해 점검한다.

[0159] 7. 상기 드라이버는 센서와의 보안 통신 세션을 구축한다.

[0160] 8. 상기 드라이버는 OS SMR들이 적어도 한번 확장되었음을 확인한다.

[0161] a. SMR_{OS}에 TRUE를 보고해야 한다.

[0162] b. TRUE가 아닌 경우, 그때 측정한다.

[0163] 9. 상기 드라이버는 센서에게 내부 키를 생성하도록 명령한다.

[0164] 10. 상기 드라이버는 소유권자 키를 설정한다.

[0165] a. 드라이버가 소유권자 암호구(SHA-1 해시)로부터 소유권자 키를 컴퓨팅한다.

[0166] b. 드라이버가 파라미터로서 새로운 소유권자 키 및 팩토리 디폴트(factory default) 소유권자 키를 가지고 센서로 소유권자 키 설정 명령을 보낸다.

[0167] c. 센서가 저장된 소유권자 키에 대해 구(old) 소유권자 키를 점검한다.

[0168] d. 센서가 NVM에 새로운 소유권자 키를 저장한다(20B).

[0169] 11. 센서에서 템플릿 플래그 보존이 설정되지 않으면, 그때 상기 플래그는 완전히 삭제된다. 상기 플래그가 설정되면, 그때 플래그는 템플릿을 가진 페이지들을 제외하고 삭제된다.(일부 형태의 소프트웨어 업데이트가 진행 중인 경우 이러한 플래그가 설정될 것이다).

[0170] 12. 드라이버가 적절한 플래그들과 함께 SMR 보관 명령을 보냄으로써 센서가 SMR_OS_VAL(센서 NVM에)에 현재의 SMR_{OS} 내용을 보관하도록 명령한다.

[0171] a. 센서는 자동으로 SMR_OS_VAL_SET 플래그를 True로 설정하며;

[0172] b. 유의: 대응하는 VAL_SET 플래그가 보관 전에 TRUE이면, 명령이 간과되어야만 하며 오류 코드가 돌아온다.

[0173] c. 유의: 이들 플래그의 재설정은 소유권자의 암호구를 사용하여 전체 시스템을 팩토리 디폴트로 도로 재설정함에 의해서만 수행될 수 있다.

[0174] 13. SMR_{PBA}가 확장되었으면, 드라이버는 적절한 플래그들과 함께 SMR 보관 명령을 보냄으로써 센서가

SMR_PBA_VAL(센서 NVM에)에 현재의 SMR_{PBA}를 보관하도록 명령한다.

[0175] a. 센서는 자동으로 SMR_PBA_VAL_SET 플래그를 True로 설정한다.

[0176] b. 유의: 대응하는 VAL_SET 플래그가 보관 전에 TRUE이면, 명령이 간과되어야만 하며 오류 코드가 돌아온다.

[0177] c. 유의: 이들 플래그의 재설정은 소유권자의 암호구를 사용하여 전체 시스템을 팩토리 디폴트로 도로 재설정함에 의해서만 수행될 수 있다.

[0178] 14. 드라이버는 플래시에 PBA 바이너리를 저장한다.

[0179] a. 유의: SPI 플래시 기록 및 삭제는 가용 플래시 업데이트 명령 이후와 현재 보안 세션의 종료 이전에만 가능하다.

[0180] 15. 상기 SMR을 무효 상태로 끝마치기(cap) 위해 무작위 번호(Random Number로 모든 SMR들을 확장한다.

[0181] 16. 저장 완료에 따라, 상기 드라이버는 센서가 업데이트 정책 명령을 사용하여 InitComplete 플래그를 설정하도록 명령한다.

[0182] a. 유의: 상기 InitComplete 플래그의 설정은 소유권자_키를 필요로 한다.

[0183] 17. 드라이버는 소유권자_키 메모리 위치를 와이핑(wipe)한다.

[0184] 18. 드라이버가 스파이 플래시(spy flash)에 NVRAM 백업, 해시 값 및 랩핑된 키를 보관한다.

[0185] 19. 드라이버가 보안 세션을 무효화한다.

[0186] 20. 초기화 완료.

[0187] 21. 서비스가 애플리케이션에 대한 제어를 되돌린다.

[0188] a. 소유권자의 등록 및 정책 설정 동작을 바로 진행하는 것을 권고. 상기 정책 설정 동작은, 바로 완료되는 경우 소유권자 암호구를 필요로 하며, 애플리케이션은 상기 소유권자로부터 그것을 재획득하는 것을 필요로 하지 않을 것이다.

[0189] 상기 등록 과정의 일 실시형태는 도 10을 추가로 관련하여 하기 기술할 것이다. 상기 과정은 애플리케이션 페이로드 캡슐화를 포함하여 진행할 것이다. 상기 단계의 고차적 기술이 다음 목록에 제공된다:

[0190] 1. 애플리케이션은 애플리케이션 페이로드 AP를 생성한다. 이는 키 자료, 인증일 수 있으며, 또는 다른 어떤 정보라도 사용자 특별허가를 승인하기 위한 전체 보안 구조에 의해 요구된다.

[0191] a. 이 페이로드의 내용은 소프트웨어에 불투명하며 이 단계 전에 상기 애플리케이션에 의해 암호화되는 것이 권고 된다

[0192] b. 상기 애플리케이션 페이로드는 3-k바이트의 크기로 제한될 수 있다.

[0193] 2. 상기 애플리케이션은 이어서 파라미터로서 상기 애플리케이션 페이로드를 통과하는 윈도우 서비스 손가락-등록 기능을 호출한다.

[0194] a. 모든 동작들 이전에, 보안 통신 채널은 애플리케이션과 서비스 간에 및 상기 서비스와 드라이버 간에 존재해야만 한다.

[0195] 3. 상기 서비스는 상기 애플리케이션 페이로드 상에 통과하는 장치 드라이버의 손가락 등록 기능을 호출한다.

[0196] 4. 상기 드라이버는 상기 센서와 함께 보안 세션을 구축한다.

[0197] a. 상기 센서는 또한, 템플릿 측정을 위해 SMR_{MV} 레지스터를 준비시키기 위해 상기 SMR_{MV} 레지스터를 초기화한다.(이는 보안 세션이 시작될 때마다 일어난다)

[0198] 5. 상기 드라이버는 상기 센서로부터 워터마킹되지 않은 이미지를 획득하는데 필요한 기능들을 수행할 것이다.

[0199] a. 사용자 프롬프트 및 피드백이 디스플레이를 위해 상기 애플리케이션으로 체인 백업(chain back up)을 가로질러야만 한다.

[0200] 6. 상기 드라이버는 상기 이미지를 복호화하고, 부분 템플릿을 구축하기 위해 그것을 사용한다.

[0201] 7. 상기 템플릿 품질이 등록가능할 때까지 단계 5 및 6을 반복한다.

[0202] 8. 상기 드라이버는 지금, 템플릿 데이터 워터마크의 생성에 사용하기 위해 고르게 분포된 무작위 왜곡 패턴을 생성할 것이다.

[0203] a. 상기 왜곡 패턴은 20-바이트의 템플릿 워터마크 키로 암호화된다.

[0204] 9. 상기 드라이버는 상기 왜곡 패턴을 정정하기 위해 템플릿 융선-흐름 노드들을 변형한다. 이는 인증 동작 동안에 확인될 템플릿 워터마크를 생성한다.

[0205] a. 상기 템플릿 워터마크는 인증 동안에 매칭기를 무효화하며, 대체 공격을 방지하는 방식으로 이 특정 템플릿에 상기 SP를 결합한다.

[0206] 10. 템플릿 데이터의 SHA1-기반 측정은 이어서 SMR 센서 확장 명령을 사용하여 SMR_{MV}로 확장된다.

[0207] a. 유의: 임의의 템플릿 압축이 이러한 측정 전에 발생해야만 한다.

[0208] 11. 상기 드라이버는 상기 템플릿에서 AP 서명으로서 사용될, 애플리케이션 페이로드의 SHA-1 측정을 수행한다.

[0209] a. 유의: 상기 AP 서명은 식별정보 업데이팅 및 템플릿 백업과 같은 다른 동작들에서 같은 사용자로부터의 템플릿을 식별하기 위해 사용된다. 이러한 이유로, 이는 상기 템플릿의 암호화 부분 외부에 배치되어야만 한다.

[0210] 12. 상기 드라이버는 상기 AP로부터의 AP 스트림 및 템플릿 워터마크 키를 생성한다. 예시적인 포맷은 다음과 같다:

[0211] a. SMR_{MV}의 보존 공간-20-바이트

[0212] 템플릿 워터마크 키-20-바이트

[0213] AP 길이-유니트 16(2-바이트)

[0214] AP

[0215] 13. 상기 드라이버는 AP 블록 암호화 명령을 사용하여 992 바이트의 블록으로 상기 센서에 상기 AP 스트림을 보내기 시작한다. 마지막 블록 상에, 임의의 사용하지 않은 바이트는 0으로 채워질 것이다.

[0216] 14. 이것이 제1 블록이면, 상기 센서는 B0블록 및 SMR_{MV}의 현재 내용을 상기 블록을 프리픽스(prefix)할 것이며, μHSM 및 그의 내부 페이로드 키를 사용하여 그것을 암호화할 것이다. 이것이 제1 블록이 아닌 경우, 상기 센서는 SMR_{MV}의 일부에 의해 변형된 것으로서 B0로 구성된 논스(nonce)를 프리픽스할 것이며, 상기 μHSM을 사용하여 그것을 암호화할 것이다.

[0217] a. 보내진 각 블록에 대해, 센서는 보안 페이로드로 암호화된 1024 바이트의 데이터를 반환할 것이다.

[0218] 15. 상기 드라이버는 상기 반환된 암호화 블록은 전체 SP 블롭으로 연쇄한다.

[0219] 16. 상기 드라이버는 상기 템플릿으로 SP와 AP 서명을 배치하고, 상기 템플릿의 말단에 필 데이터(fill data)를 첨부함으로써 템플릿 암호화를 준비하며, 때문에 그것은 템플릿 블록 크기의 배수로 종료한다(1008 바이트).

[0220] 17. 상기 드라이버는 암호화된 템플릿 블록 생성 명령을 사용하여 상기 템플릿을 블록으로 센서에 보낸다.

[0221] 18. 상기 센서는 그의 내부 템플릿 암호화 키(TEK)를 사용하여 템플릿 블록을 암호화하며, 호스트로 각 블록을 되돌려 보낸다.

[0222] 19. 상기 드라이버는 상기 암호화된 템플릿 블록들을 연쇄시키고, 헤더를 프리픽스하며(상기 산출한 AP 서명을 포함), 데이터 저장소(예, SPI 플래시)에 최종 템플릿을 기록한다.

[0223] a. 유의: 상기 드라이버는 SPI 플래시 부분에 대한 삭제 및 기록 동작을 승인하기 위해 호스트 루트 키(HRK)

를 제공한다.

[0224] 20. 상기 드라이버는 보안 세션을 종결하며, 호출 스택(call stack)의 제어를 되돌린다.

[0225] 보안 지문 인증 프로세스의 일 실시예가 지금 기술될 것이며, 매칭기 또는 템플릿을 변형하기 극도로 어렵게 하여, 페이로드에서 보안 정보에 대한 접근을 획득하도록 고안되었다. 제공된 보안은 다층이며, 상기 센서에 의해 제공되는 보안 환경의 이점들을 가진다.

[0226] 제1 보호층은 마지막의 가능한 순간에 상기 프리-매치 프로세서(PMP)를 로딩하고 복호화하며, 드라이버 프로세스의 일부로서 그것을 운용하는 것을 포함한다. 이는 공격 윈도우를 0링에서 운영되는 프로세스들로 및 매칭 동작의 타임프레임(timeframe)으로 제한한다(사전 부팅 동안에, 상기 PMP는 옵션 ROM 코드에 의해 로딩되며 운영될 수 있다). 본 기술분야의 당업자에 의해 인정될 수 있는 바와 같이, 0링은 최고 특권을 가지는 컴퓨터 아키텍쳐 수준이며, CPU 및 메모리와 같은 물리적 하드웨어와 대부분 직접적으로 상호작용한다.

[0227] 상기 센서는 다음 보호층을 제공한다. 상기 페이로드를 복호화하는 능력을 가진 유일한 실체로서, 센서는 매칭 동작 동안에 그 자체 측정을 위한 매칭기, 템플릿, 및 기기에 압력을 가할 수 있다. 상기 센서는 다양한 통신 이벤트들 사이의 시간을 측정할 수도 있으며, 호스트가 디버거로 정체된 경우 동작을 취소할 수도 있다. 상기 센서는 템플릿 워터마크, 이미지 워터마크를 점검하기도 하며, 최종 매치 동작을 수행한다. 다음 목록은 인증에 수반될 수 있는 단계들의 고차적 기술을 제공한다.

[0228] 1. 애플리케이션이 서비스로부터 인증을 요청하며, 이는 이어서 드라이버가 인증 동작을 개시하도록 명령한다.

[0229] 2. 상기 드라이버는 센서와의 보안 통신 세션을 구축하며, 이는 상기 센서가 SCR_{MV}를 개시하게끔 한다.

[0230] 3. 상기 드라이버는 워터마킹된 이미지를 포착하기 위해 상기 센서를 운영한다(프롬프트 및 사용자 피드백이 디스플레이 및 애플리케이션 콜백(callback)을 위해 상기 서비스로 통과된다).

[0231] 4. 가용한 이미지가 일단 획득되면, 상기 드라이버는 관심 템플릿을 찾기 위해 일 대 몇몇의 비-보안 매치(one-to-few unsecured match)를 수행한다.

[0232] b. 유의: 상기 템플릿은 센서의 복호화된 템플릿 블록 획득 명령을 사용하여 복호화될 것이다.

[0233] 5. 임의의 템플릿이 매치되도록 결정되는 경우, 그때 보안 매치가 드라이버에 의해 개시된다.

[0234] 6. 보안 매치의 시작에서, 상기 드라이버는 메모리로 PMP를 로딩 및 복호화할 것이며, 보안 페이로드를 센서로 보낸다.

[0235] 7. 상기 센서는 내부 RAM에 상기 보안 페이로드를 복호화할 것이며, 상기 템플릿 워터마크 키를 추출할 것이다. 그것은 유효 데이터가 호스트로부터 수신될 때마다 재설정하는 통신 감시 타이머의 운영을 시작할 것이다. 다른 방법으로, 상기타이머는 전체 프리-매치 동작 동안에 운영할 것이며, 전체 활동이 길어지는 경우 타임아웃 할 것이다.

[0236] 8. 상기 드라이버는 매치를 수행하는 것 외에도 다음 동작들을 포함한 안전한 프리-매치 동작을 수행할 것이다: 등록 동안에 이루어지는 기기, 템플릿 데이터, 및 매칭기 코드의 측정이 반복(적절한 순서로)될 것이며, SCR_{MV} 레지스터로 확장을 위해 센서로 보내질 것이다. 상기 블록 수준에서의 매칭기 중간 결과는 확인 및 최종 매치 측정을 위해 센서로 스트림될 것이다.

[0237] 9. 두 형태의 블록 스코어가 산출되어야만 하며, 하나의 세트는 이미지 중심이며, 이미지 워터마크를 확인하는데 사용되며, 다른 세트는 노드 중심이며, 템플릿 워터마크를 확인하는데 사용된다.

[0238] 10. 상기 블록 스코어들이 각 노드에 도달함에 따라, 상기 센서는 두 작용을 수행할 것이다: 상기 블록 스코어들은 상기 노드에 대한 최종 매치 스코어를 얻는 정정 방식(correct fashion)으로 축적될 것이며, 상기 워터마크 키는 상기 블록 스코어에 대하여 평가될 수 있다. 상기 워터마크가 블록 스코어에서 검출되지 않는 경우, 그때 다음 중의 하나는 사실이다: 템플릿이 실시간 변경되었다, 매칭기가 실시간 변경되었다, 상기 이미지가 실시간으로 템퍼링되었거나 개별 블록 스코어들이 실시간 변경되었다. 이들 경우들 중에 어떤 경우에도, 상기 매칭은 실패할 것이다. 이는 여러 형태의 공격들을 방지한다.

[0239] 11. 상기 보안 동안의 어떤 시간에도, 상기 매치, 상기 통신 감시 타이머가 끝나면, 그때 그것은 호스트가 디버거에 의해 중단되었음을 가정한다. 이러한 상황에서, 상기 센서는 상기 매칭을 실패하며, 상기 보안 세션을

무효화하며, 비 보안 모드로 반전할 것이다. 이는 상기 보안 매치 동작이 시작부터 다시 시작하게 할 것이다.

[0240] 12. 호스트 매치 동작의 결과에서, 최종 데이터가 위치 상관관계 정보 및 최종 측정와 함께, 센서로 보내질 것이다.

[0241] 13. 상기 센서는 중간 결과물의 평가를 완료할 것이며, 이것이 매치를 초래하기 위해 충분히 높은 스코어를 결과하는지 여부를 판별할 것이다.

[0242] 14. 이 점에서, 상기 센서는 또한, 등록 동안에 보안 페이로드 블롭에 암호화된 측정 대 SCR_{MV}의 내용을 비교한다.

[0243] 15. 상기 측정이 동일하며, 매치 스코어가 매우 충분하며, 워터마크가 정확하다면, 그때 상기 센서는 추가 작용을 위해 호스트에 복호화된 애플리케이션 페이로드 및 최종 매치 스코어를 되돌려 보낼 것이다. 그렇지 않으면, 상기 페이로드는 반환되지 않는다.

[0244] 16. 상기 센서는 가능한 템플릿 업데이트 동작에 사용하기 위해 이미지 워터마크를 되돌려 보내기도 한다.

[0245] 17. 매치가 성공적이면, 드라이버는 호출 애플리케이션에 AP를 반환한다.

[0246] 18. 상기 드라이버가 보안 세션을 종료한다.

[0247] 19. 상기 매치 스코어가 템플릿 업데이트를 가능하게 하는데 매우 충분하며, 상기 PMP가 노드 대체가 권고할 만하다고 판단하는 경우, 그때 PMP는 상기 이미지로부터 워터마크를 제거하기 위해 이미지 워터마크 키를 사용할 것이며, 그때 다음의 등록 절차들의 나중 부분들에 의해 템플릿 업데이트를 수행할 것이다.

[0248] a. 템플릿 업데이트가 필요한 경우 새로운 보안 세션이 개방될 것이다(이는 상기 센서가 SMR_{MV}를 다시 개시하게끔 한다).

[0249] b. 성공적인 템플릿 업데이트는 애플리케이션에 대한 템플릿 업데이트가 발생했다는 콜백(callback) 또는 메시지를 결과할 수 있다. 적어도, 디버그 추적에서 이는 통지되어야만 한다.

[0250] 일 실시예에서, 사용자는 예를 들어, 초기화 및 사용자 등록 후에 바로 애플리케이션을 초기화함으로써 초기 정책 설정을 선택하도록 촉진될 수도 있다. 상기 정책 설정 변경이, 상기 개시 어플리케이션이 소유권자로부터 이미 가졌을 소유권자 암호구를 필요로 하기 때문에 편리한 접근이다. 다음 목록은 지문 보안 시스템의 정책 정보를 설정하기 위한 예시적인 실행을 제공한다.

[0251] 1. 애플리케이션은 소유권자로부터 정책 선택을 요청한다. 이들 선택은: 가용/불가용 PBA; 가용/불가용 SSD(Single Swipe to Desktop); 가용/불가용 전체 볼륨 암호화; 가용/불가용의 강화 보안을 위한 TPM의 사용을 포함할 수 있다.

[0252] a. 유의: 상기 애플리케이션은 사용자 프롬프트 전에 현재의 정책 설정을 검색(retrieve)하는 것을 소망할 수 있다. 상기 서비스는 이를 위해 API를 제공해야만 한다(센서 명령: 보안 플래그 획득은 이러한 정보를 검색하기 위해 드라이버에 의해 사용될 수 있다.)

[0253] 2. 상기 애플리케이션은 파라미터로서 소유권자 암호구 및 정책 선택을 통과하는 정책 업데이트를 수행하도록 상기 서비스를 호출한다. 상기 서비스는 상기 동작을 완료하기 위해 이러한 요청 및 상기 파라미터를 아래 드라이버로 통과시킨다.

[0254] 3. 그때 상기 드라이버는 SHA-1을 사용하여 소유권자 암호구로부터 소유권자 키를 생성하며, 이어서 새로운 정책 선택들을 적절한 보안 플래그들로 변환한다.

[0255] 4. 새로운 보안 세션이 드라이버와 센서 간에 구축되며, 그때 정책 업데이트 명령이 파라미터로서 상기 소유권자 키와 보안 플래그들과 함께 상기 센서로 발행된다.

[0256] 5. 상기 보안 세션은 그때 폐쇄되며, 상기 동작의 결과가 호출 스택 위로 회귀 된다.

[0257] 사용자가 PC 및 네트워크를 위한 식별정보를 변경하는 것이 종종 필요하다. 이들 식별정보가 애플리케이션 페이로드(AP)로 직접적으로 저장되는 경우, 그때 상기 애플리케이션은 사용자가 그의 모든 손가락을 재등록할 필요 없이, 소유권자 암호구이 필요 없이 이들 식별정보를 업데이트하는 방법을 가질 필요가 있을 것이다. 상기 동작 보안을 유지하기 위해, 사용자는 이러한 동작의 일부로서 지문 시스템으로 인증하는 것을 필요로 한다. 이 사용자의 모든 손가락들에 동일한 AP가 사용된 한, 단지 하나의 손가락이 스위프트(swipe)될 수 있다.

외부 시스템이 각 손가락을 위해 상이한 AP들을 사용한다면, 그때 상기 과정은 모든 손가락들에 반복되어야만 할 것이다.

[0258] 다음 단계들은 한 사용자를 위한 AP들의 변경에 사용되는 과정을 도시한다. 상기 과정은, 기재로서, 한 사용자의 모든 손가락들에 동일한 AP가 사용되는 것을 가정한다.

[0259] 1. 애플리케이션이 새로운 AP를 생성하며, 파라미터로서 새로운 AP를 통과하는 AP 변경을 요청하도록 상기 서비스를 호출한다.

[0260] 2. 상기 서비스는 작용을 위해 상기 드라이버로 이러한 요청을 통과시킨다.

[0261] 3. 상기 드라이버는 성공적인 경우, 다음 정보들과 함께 상기 드라이버를 떠나는, 보안 지문인증 동작을 수행한다:

[0262] a. 비 암호화 상태의 가공되지 않은 템플릿 노드 정보(raw template node information in the clear);

[0263] b. 등록 동안에 상기 템플릿에 생성 및 저장되었던 AP 서명;

[0264] c. 상기 템플릿 워터마크 키;

[0265] d. 상기 새로운 AP(구 AP도 마찬가지, 그러나 이는 필요 없다).

[0266] 4. 상기 드라이버는 PMP_{CE}를 메모리로 로딩, 복호화, 및 압축하기 위해 사용하는 PEK(페이로드 암호화 키)를 얻기 위해 HRK를 사용하여 호스트 키 블롭을 복호화한다.

[0267] 5. 이때에, 상기 드라이버는 새로운 AP 주위에 새로운 보안 템플릿을 생성하는데 필요한 모든 자료들을 가진다.

[0268] 6. 상기 AP 서명은 동일한 AP를 가지므로 업데이트할 필요가 있는 저장소의 다른 템플릿들을 식별하는데 현재 사용될 수 있다.

[0269] 일치하는 AP 서명들을 가진 템플릿들이 업데이트에 대비하여 데이터 저장소로부터 검색된다.

[0270] 7. 상기 PMP 및 플랫폼 특정 정보(PSI)는 나중에 필요한 SMR_{MV} 확장에서의 사용을 위해 측정된다. 새로운 AP 서명이 또한 산출된다.

[0271] 8. 업데이트를 필요로 하는 각 템플릿을 위해, 다음 고리형 단계들이 수행될 수 있다:

[0272] a. 상기 드라이버가 센서와 새로운 보안 세션을 구축한다(이는 SMR_{MV}가 개시되게 한다).

[0273] b. 상기 드라이버는 다음으로 상기 센서를 사용하여 템플릿을 복호화한다(이미 복호화된 제1 템플릿 제외).

[0274] c. 현존하는 보안 페이로드(SP)가 상기 템플릿으로부터 버려지며, 상기 PMP 및 PSI 측정들이 적절한 센서의 SMR 확장 명령을 사용하여 SMR_{MV}로 확장된다.

[0275] d. 가공되지 않은 템플릿 노드 정보가 그때 측정되어 SMR_{MV}로 확장된다.

[0276] e. 상기 새로운 AP가 센서로 보내지며, SP로 변환된다; 이 동작의 세부사항을 위해, 등록 과정 부분에 참조가 이루어진다.

[0277] f. 상기 드라이버는 그때 새로운 SP를 상기 템플릿에 삽입하며, 상기 등록 과정에 사용되는 동일한 단계들을 사용한 암호화를 위해 상기 센서를 통해 새로운 템플릿을 보낸다.

[0278] g. 일단 헤더(상기 새로운 AP 서명을 가진)가 암호화된 템플릿의 앞에 붙으면, 상기 템플릿은 저장될 수 있다.

[0279] h. 상기 보안 세션은 지금 종료되어야만 한다.

[0280] i. 상기 드라이버가 이 사용자를 위해 모든 템플릿들이 업데이트될 때까지 한층 위 단계로 회귀한다.

[0281] 사용자-레벨 백업의 일 실시예가 지금 기술될 것이며, 임의의 등록 사용자에 의해 수행되어 단지 상기 사용자의 템플릿 백업을 결과할 수 있다. 이러한 형태의 백업은 마찬가지로, 상기 템플릿이 상기 백업이 생성되었던

동일한 기기(동일한 센서를 가진)에만 복구될 수 있다는 것에 제한된다. 이러한 형태의 백업은 지문 시스템으로부터 우연한 하나 이상의 템플릿 검출 보호만을 제공한다. 상기 사용자 수준에서의 백업 및 복구 동작들은 지문 확인에 의해 승인된다. 다음 목록의 동작들은 예시적인 실행 순서를 제공한다.

[0282] 1. 애플리케이션이 서비스로부터 사용자-레벨 백업을 요청한다.

[0283] 2. 상기 서비스는 아래 드라이버로 상기 요청을 통과시킨다.

[0284] 3. 상기 드라이버는 사용자의 템플릿들 가운데 하나를 식별하기 위해 지문 인증을 수행한다.

[0285] 4. 상기 드라이버는 AP 서명을 컴퓨팅하기 위해 해제된 AP를 사용하며, 동일한 AP를 가지는 저장소의 다른 템플릿들을 식별하기 위한 값을 사용한다.

[0286] 5. 상기 드라이버는 적절한 템플릿을 백업 데이터베이스로 상기 서비스에 반환한다.

[0287] 6. 상기 서비스는 백업 매체 상의 저장을 위해 상기 애플리케이션으로 상기 템플릿 백업 데이터베이스를 반환한다.

[0288] 일 예시적인 사용자-레벨 복구가 기술될 것이며, 임의의 사용자에 의해 수행될 수 있지만, 상기 사용자의 템플릿들을 복구하기 위해서만 그리고 그들을 최초로 백업한 컴퓨터에만 사용될 수 있다. 사용자-레벨 복구 승인을 위해 지문 인증을 필요로 한다. 다음 목록의 단계들은 상기 템플릿들을 복구하기 위해 수행된다.

[0289] 1. 애플리케이션이 파라미터로서 백업 템플릿 블롭을 통과하는 서비스로부터 사용자-레벨 복구를 요청한다.

[0290] 2. 상기 서비스가 추가 작용을 위해 상기 요청 및 템플릿 백업 데이터베이스를 위로 드라이버에 통과시킨다.

[0291] 3. 상기 드라이버는 상기 통과된 백업 템플릿들을 사용하여 지문 인증을 수행한다.

[0292] a. 유의: 상기 템플릿들이 이 기계에 속하지 않는 경우, 그때 그들은 적절히 복호화하지 않을 것이다. 이는 템플릿 대체를 방지한다.

[0293] 4. 성공적인 매치는 이들 템플릿의 소유권자가 상기 기계에 존재한다는 것을 증명한다.

[0294] 5. 상기 드라이버는 상기 템플릿이 존재하지 않는 경우, 상기 백업으로부터의 각 템플릿을 데이터 저장소로 즉시 배치한다.(바이트단위(byte-by-byte) 비교가 중복 템플릿들을 방지하기 위해 이루어진다.)

[0295] 일 예시적인 시스템 레벨 백업이 기술될 것이며, 이러한 과정은 상기 시스템 소유권자가 모든 템플릿들을, 다른 시스템상에 또는 센서가 교체된 후에 이 기계 상에 상기 템플렛들을 복구하게끔 하는 방식으로, 백업하는 것을 가능하게 한다. 이를 가능하게 하기 위해, AP가 정확한 소유권자 키가 제공되는 한, 지문 매치 없이 복호화되게 하는 센서 명령이 제공된다. 이러한 능력은 보안 위험일 수도 있으나, OEM들은 보안 개념(security implication)과 무관하게, 한 기기로부터 다른 기기로 및 한 센서로부터 다른 센서로 템플릿들을 이동시키는 편리한 방법을 소망한다.

[0296] 본질적으로, 이러한 명령은 상기 모든 템플릿들을 복호화함에 의해 이식가능한 템플릿 데이터를 생성하며, 보안 페이로드들로부터 AP들을 제거하고, 상기 AP 및 가공되지 않은 템플릿 데이터를 새로운 블롭에서 재-암호화한다. 템플릿과 AP 간의 관계는 유지되며, 상기 새로운 블롭은 사용자에 의해 제공되는 키로 암호화된다. 다음 목록은 이러한 동작의 추가 세부사항을 제공한다.

[0297] 1. 애플리케이션은 사용자로부터 소유권자 암호구 및 백업 암호구를 얻어야만 하며, 파라미터로서 모든 암호구들을 통과하는 서비스를 호출한다.

[0298] 2. 상기 서비스는 상기 소유권자 키 및 백업 암호화 키(BEK)를 생성하기 위해 암호구들을 사용하는 드라이버로 위로 상기 파라미터들을 통과시킨다.

[0299] 3. 데이터 저장소의 각 템플릿을 위해, 상기 드라이버는 다음 동작들을 수행할 것이다:

[0300] a. 상기 드라이버는 상기 템플릿을 복호화하기 위해 상기 센서를 사용할 것이다;

[0301] b. 상기 드라이버는 이어서 상기 템플릿으로부터 SP를 추출하여, 암호화를 위해 그것을 상기 센서로 통과시킬 것이다; 이는 세 개의 센서 명령들: SP 블록 보냄. 소유권자 키 확인 및 AP 블록 획득을 수반한다;

[0302] c. 다음으로 상기 드라이버는 암호화되지 않은 적절한 템플릿 데이터 및 암호화되지 않은 AP를 상기 두 개 사이의 결합을 유지하는 방식으로 백업 데이터베이스로 재 암호화할 것이다.

[0303] 4. 모든 템플릿들이 일단 처리되면, 전체 데이터베이스는 상기 생성된 BEK를 사용하여 암호화될 것이다.

[0304] 5. 상기 결과한 암호화된 백업 데이터베이스는 이어서 백업 매체 상의 저장을 위해 상기 호출 스택을 백업 통과(pass back up)한다.

[0305] 시스템 레벨 복구(임의의 기기로부터 백업이 있을 수 있다)의 일 실시예가 기술될 것이다. 이 복구 레벨은 시스템 레벨 백업 데이터베이스로만 수행될 수 있다. 이러한 복구의 개별 수행은 이 컴퓨터상의 센서를 위해 이 백업이 이루어졌을 때 사용된 백업 암호구와 현재 소유권자 암호구를 알아야만 한다. 이러한 형태의 복구는 다음의 환경으로부터 회복하는데 특히 유용하다: 작동하지 않는 센서의 교체 후에; 모든 시스템 템플릿들의 우연한 검출 후에; 사용자 템플릿들 및 식별정보들을 새로운 PC로 이동하는 경우에; 또는 측정된 임의의 시스템 구성요소를 PSI로 교체한 후에. 이것에 유사한 기능성은 이중 보안센서 동작을 가능하게 하는 외부 센서에 상기 템플렛들 및 식별정보들을 클론(clone)하는데 사용될 수 있다.

[0306] 작동하지 않는 센서 교체, PSI 구성요소 교체, 또는 새로운 기기로의 이동의 경우, 지문 시스템 초기화는 상기 복구를 수행하기 전에 완료되어야만 한다.

[0307] 다음 단계들은 템플릿들 및 식별정보들의 시스템 레벨 복구를 달성할 것이다.

[0308] 1. 애플리케이션이 매체로부터 백업 블롭을 로딩한다.

[0309] 2. 애플리케이션이 사용자로부터 소유권자 암호구 및 백업 암호구를 요청한다.

[0310] 3. 애플리케이션이 소유권자 암호구, 백업 암호구 및 블롭에 대한 포인터(pointer to blob)를 서비스로 통과시킨다.

[0311] 4. 서비스가 모든 애플리케이션 공급 정보를 드라이버에 전송한다.

[0312] 5. 드라이버가 데이터 저장 영역으로부터 PMP들을 검색한다.

[0313] 6. 드라이버가 PMP를 복호화하고 압축한다.

[0314] 7. 드라이버가 PMP를 측정한다.

[0315] 8. 드라이버가 PSI를 측정한다.

[0316] 9. 드라이버가 백업 암호구로부터 BEK를 생성한다.

[0317] 10. 각 템플릿에 대하여:

[0318] a. 드라이버가 센서와 보안 세션을 구축한다;

[0319] b. BEK를 사용하여 템플릿 및 AP를 복호화한다;

[0320] c. PMP 측정을 SMR_MV로 확장한다;

[0321] d. PSI를 SMR_MV로 확장한다;

[0322] e. 템플릿 데이터를 측정한다;

[0323] f. 템플릿 데이터를 SMR_MV로 확장한다;

[0324] g. AP를 센서로 보내고, SP를 요청한다.

[0325] h. 드라이버가 템플릿에 SP를 삽입한다;

[0326] i. 드라이버가 암호화를 위해 센서로 템플릿을 보낸다;

[0327] j. 센서가 암호화된 템플릿을 반환한다;

[0328] k. 보안 세션을 무효화한다;

[0329] l. 데이터 저장 영역에 템플릿을 저장한다.

[0330] 11. 다음 템플릿.

[0331] 12. 데이터 저장 영역에 템플릿 저장.

[0332] 보안 소프트웨어 업그레이드 과정의 일 실시예가 기술될 것이다. 소프트웨어가 일부 작동을 승인하기 위해 센

서에서 측정되기 때문에, 소프트웨어 업데이트(AFSS가 개시되어 강화된 보안 모드로 배치된 후에)는 신규 보관된 측정들을 저장하고, 오래 보관된 측정들을 폐기하는 것을 요한다.

[0333] NVRAM에서의 측정들의 변화가 두 가지 방식으로 승인될 수 있다: 유효한 소유권자 키를 제공하거나 또는 특수한 인증 메시지를 제공한다. 소프트웨어 업그레이드가 자동화 동작들로서 종종 수행되기 때문에, 소프트웨어 설치 및 업그레이드를 수행할 때에 인증 메시지를 사용하는 것이 권고 된다.

[0334] 인증 메시지 기반 소프트웨어 업그레이드를 위해, 다음 실체들은 이러한 업그레이드 방법에 수반될 수 있다: SW 개발; 보안 키 저장; 컴퓨터 서명; 보안 업데이트 애플리케이션; 인스톨러(Installer) 또는 클라이언트 애플리케이션; OS 장치 드라이버; 보안 센서. 상기 측정 소프트웨어는 OS, PBA 및 FDA 타임에 운영된다. 상기 인증 메시지가 일부 환경들 하에 상기 서비스를 통과할 수 있지만, 상기 서비스는 어떠한 보안 역할도 담당하지 않으며, 따라서 다음의 거론들에 포함되지 않는다는 것을 유의해야 한다.

[0335] 도 11 및 도 12의 구획면 차트는 상기 목록의 다양한 실체들의 작용을 도시한다. 상기 차트에 도시된 작용들의 상세한 설명이 뒤따른다.

[0336] 생성 단계를 위해:

[0337] 1. 소프트웨어 개발(SW)은 새로운 소프트웨어를 생성, 시험, 및 해제한다.

[0338] 2. 일단 상기 소프트웨어가 완전히 준비되면, SW는 이 소프트웨어를 위해 상기 센서 SMR로 궁극적으로 확장될 수 있는 측정들 가운데 하나를 산출한다. 예를 들어, 상기 새로운 소프트웨어가 PBA 소프트웨어의 로딩 가능한 드라이버부인 경우, SW는 이 소프트웨어의 어떤 부위가 상기 PBA 로더(loader)에 의해 측정될 것인지 안다. 따라서, SW는 타깃 기기상에 궁극적인 측정이 무엇일지를 산출할 수 있다.

[0339] 3. 이러한 SMR 확장 값은 SMR_NV 암호화되지 않은 인증 메시지(SMR_NV clear authorization message) 내에 삽입된다. 상기 메시지는 세 개의 비휘발성 보관 SMR 레지스터들 가운데 하나가 제거되도록 승인하는 특정 센서 펌웨어 패치로 구성된다.

[0340] 4. 상기 전체 인증 메시지는 이어서 다른 패치들을 인증하는데 사용되는 동일한 공유키를 사용하여 암호화된다. 이러한 키는 센서에 삽입되며, 상기 메시지를 암호화하기 위해 사용될 수 있는 제한 접근 PC상에 저장되기도 한다.

[0341] 5. 일단 상기 메시지가 암호화되면, 하드웨어 보안 모듈은 제조업체의 키 쌍(key pair) 중의 비공개 부분을 사용하여 상기 메시지에 서명하는데 사용될 것이다. 이러한 키의 비공개 부분은 결코 HSM을 떠나지 않는다. 상기 OS 장치 드라이버는 상기 메시지가 제조업자에 의해 생성되었음을 증명하는데 사용할 수 있는 이 키의 공개 부분 카피를 가질 수 있다. 이러한 경우에, 전체 메시지가 아닌, 상기 메시지의 요약이 서명된다는 것을 유의해야 한다.

[0342] 6. 상기 암호화 및 서명된 메시지는 이어서 타깃 기기상의 인스톨러(installer) 또는 다른 업데이트 애플리케이션에 의해 호출될 것인 보안 업데이트 애플리케이션에 삽입된다.

[0343] 7. 상기 보안 업데이트 애플리케이션은 이어서 인스톨러 패키지에 부가되거나 그렇지 않은 경우 상기 소프트웨어를 업그레이드할 실체에 제공된다.

[0344] 실행 단계를 위해:

[0345] 1. 상기 인스톨러 또는 애플리케이션이 적절한 위치에 업데이트된 소프트웨어를 배치하며, 파일 복사본들을 확인한다(이는 모든 설치 실체들에 일반적인 작용).

[0346] 2. 이것이 인스톨러-기반 업데이트인 경우, 상기 인스톨러는 보안 업데이트 애플리케이션을 운영하는 것을 필요로 한다는 것을 이미 알 것이다. BIOS 플래시 유틸리티와 같은 독립형 애플리케이션은 상기 정보를 가지지 않을 것이며, 때문에 그것은 그것이 운영되는 동일한 디렉터리에서 상기 애플리케이션의 카피를 확인해야만 하며, 보안 업데이트 애플리케이션이 확인되는 경우, 그것은 보안 업데이트 애플리케이션을 운영해야만 한다.

[0347] 3. 상기 보안 업데이트 애플리케이션은 제조업자 측에서 그것에 삽입된 인증 메시지로 통과한, OS 드라이버로부터의 보안 소프트웨어 업데이트를 요청한다. 상기 메시지는 센서가 특정한 비휘발성 보관 SMR 값을 제거하도록 권한을 부여한다.

[0348] 4. 상기 OS 드라이버는 상기 메시지를 입증하기 위해 상기 제조업자의 공개 키에 대한 그의 사본을 사용한다. 상기 입증이 실패하면, 상기 드라이버는 상기 보안 업데이트 애플리케이션으로 오류를 반환하며, 센서를 향하

여 인증 메시지를 통과시키는 것을 거부할 것이다.

[0349] 5. 상기 메시지가 유효하면, 상기 드라이버는 상기 센서를 향하여 상기 메시지를 보낸다.

[0350] 6. 상기 센서는 상기 센서 내부의 비공개 키를 사용하여 상기 메시지를 복호화할 것이다. 이러한 복호화가 실패하면, 가능한 공격을 가리키며, 상기 센서는 상기 드라이버로 실패 표시를 되돌리며, 보관된 SMR들 중의 어떤 것의 제거도 거절할 것이다.

[0351] 7. 상기 센서는 제거해야할 상기 보관 SMR 값을 결정하기 위해 상기 메시지의 정보를 사용한다. 상기 센서는 상기 정보를 포함한 NVRAM의 저 부분을 제거하며, 하나의 값이 보관되었음을 표시하는 플래그를 재설정한다. 이는 상기 업데이트된 소프트웨어가 궁극적으로 운영될 때에 새로운 측정이 이루어져 보관되는 것을 허용한다.

[0352] 8. 제거될 보관 SMR 값에 대한 정보 외에도, 상기 메시지는 새로운 소프트웨어가 운영될 때에 궁극적으로 상기 SMR로 확장될 측정들 가운데 하나의 예측을 포함할 수 있다. 이러한 예측은 미래의 확인을 위해 NVRAM에 저장된다.

[0353] 9. 상기 업데이트된 소프트웨어가 처음으로 로딩하고 운영될 때에 상기 과정의 다음 단계가 발생한다.

[0354] 10. 삽입된 모든 측정 코드를 위한 일반적인 동작의 부분으로서, 상기 소프트웨어의 임계부(critical portions)에 대한 측정이 적절한 센서 측정 레지스터(SMR)로 이루어져 확장된다.

[0355] 11. 각각의 측정이 SMR로 확장됨에 따라, 상기 센서 로직은 상기 예측에 대하여 상기 확장 값을 비교할 것이다(예측이 있는 경우). 상기 확장값들 중의 하나가 상기 예측에 일치하면, 휘발성 플래그가 상기 센서에 설정될 것이다.

[0356] 12. 상기 측정 과정의 끝에, 상기 측정 소프트웨어는 보관값이 존재하지 않는다는 것을 탐지할 것이며, 상기 SMR 보관 동작을 요청할 것이다.

[0357] 13. 예측 값이 존재하면, 예측 일치를 표시하는 플래그가 설정되지 않으며, 그때 상기 SMR 보관은 거부될 것이다.

[0358] 14. 상기 예측 값의 확인은 특정 소프트웨어 업데이트 애플리케이션이 AuthenTec에서 입력된(key) 소프트웨어하고만 작업할 것이며, 악성 소프트웨어의 설치에 사용될 수 없다는 것을 보장한다.

[0359] 다음은 시스템 부팅과 같은 이벤트 순서의 일 실시예를 기술한다. 사전 부팅, 전체 볼륨 암호화 및 OS 로딩(OS loading)이 도 13을 추가 관련하여 모두 포함된다. 이 부분에서, 모든 사전 부팅 동작들은 마치 그들이 옵션 ROM 및 사용자 인터페이스 바이너리 결합에 의해 수행되는 것처럼 언급된다. 일부 시스템들에 있어서, 이들 동작은 UEFI 드라이버들에 의해 수행될 것이다. 옵션 ROM은 센서와의 보안 세션을 구축한다. 옵션 ROM은 SMR_PBA로 자가 측정된다(또는 상기 BIOS는 강화 보안을 위한 측정을 수행할 수 있다). 옵션 ROM은 센서로부터 상태 플래그들을 판독한다: Init 확인_완료 = 사실; PBA 확인_구현(Enabled) = 사실. 플래그들이 일치하지 않으면, 부팅으로 계속하기 위해 소유권자 암호구를 요청한다: 암호구로부터 제시된 소유권자_키를 생성한다; 센서가 소유권자_키를 제시된 소유권자_키에 매치하는 것을 결정한다(유의: 안티 해머링(anti-hammering)이 소유권자 키 확인을 필요로 하는 모든 기능들을 위해 구현될 수 있다). PBA 옵션 ROM을 종료.

[0360] 옵션 ROM은 PSI 데이터를 측정하며 SMR_{PBA}로 확장된다. 옵션 ROM은 PMPce를 로딩하고 측정하며 SMR_{PBA}를 확장한다. 옵션 ROM은 PBUIe를 로딩 및 측정하며(존재하는 경우), SMR_{PBA}를 확장한다. 옵션 ROM은 센서로부터 HRK를 요청한다: 센서는 NVM의 SMR_PBA_VAL에 SMR_PBA의 값을 비교하며; 만일 동일하다면 HRK가 옵션 ROM에 보내진다. 옵션 ROM은 PEK를 메모리로 추출하는 HRK를 사용하여 호스트_키_블롭을 로딩 및 복호화한다. HRK 메모리 위치를 와이핑한다(wipe). 옵션 ROM은 PEK를 사용하여 메모리로 PMPce를 복호화하고 압축해제한다. PBUI가 존재하는 경우, 그때 옵션 ROM이 PEK를 사용하여 메모리로 PBUI를 로딩, 복호화 및 압축해제한다. 옵션 ROM이 PEK 메모리 위치를 와이핑한다. 옵션 ROM은 보안 지문 인증을 수행한다.

[0361] 인증이 성공적인 경우 그때: FDE_활성 또는 SSD_구현 = TRUE라면, 센서는 FDE 및/또는 OS 장치 드라이버로의 전달을 위해 센서 RAM으로 AP를 저장하며; FDE_활성 = FALSE면, 옵션 ROM은 SMR_{PBA} w/랜덤 데이터(캡(cap))를 확장하며; 보안 세션을 무효화하며; 사전 부팅 인증이 완료되며; 옵션 ROM이 BIOS로 제어를 되돌린다. 달리 그렇지 않으면, 매치가 성공적이지 않거나, 또는 부팅이나 정책에 따른 다른 인증 방법(암호구 등)으로 진행되는 경우(최대한도로), 재시도한다.

[0362] 전체 볼륨 암호화 또는 전체 디스크 암호화(FDE) 소프트웨어는 드라이브를 복호화할 수 있기 전에 식별정보를 필요로 한다. 이들 식별정보는 AP의 식별정보들의 일부일 수 있거나 저들 식별정보들로부터 생성될 수 있다. 상기 FDE 소프트웨어는 PBA로부터 가용한 경우 지문 인증을 수행하지 않고 센서로부터 상기 AP를 얻는다. 그렇지 않은 경우, 그것은 그 자신의 지문 인증을 수행해야만 한다. 상기 시스템이 전체 볼륨 암호화 구성요소를 가지는 것을 가정하면, 부팅 순서는 계속된다. FDE가 AP를 제공하기 위해 라이브러리를 요청 및 운영한다(유의: FDE 애플리케이션 내에 정적 링크된 라이브러리(ATLib)). ATLib가 센서로부터 상태 플러그를 요청한다. Init_완료 == FALSE이면, FDE로 실패 코드가 돌아온다(유의: FDE가 일부 다른 인증 방법을 수행해야만 할 수 있다)(소프트웨어 업데이트 동안에만 발생해야 한다). ATLib가 센서와 보안 세션을 구축한다. ATLib가 센서로부터 저장된 AP를 요청한다. AP가 존재하지 않는 경우, 그때 센서가 ATLib로 오류 코드를 돌려보내며, 이는 암호구가 사용되거나 옵션 ROM이 존재하지 않는 때에 발생한다.

[0363] AP가 존재하는 경우, 센서는 ATLib로 AP를 전달하며, (FDE_활성 및 SMR_{PBA} 유효)인 경우에만(유의: (FDE_활성 및 SMR_{PBA} 유효) 또는 (SSD_가용 및 SMR_{OS} 유효)인 경우, 센서가 사실상 AP를 반환할 것이다 - 왜냐하면 어떤 유형의 소프트웨어가 요청을 이루는지 센서가 알지 못하기 때문이다), 그 밖에 오류 코드가 ATLib로 반환 된다. ATLib가 센서로부터 AP를 수신한 경우(PBA가 AP를 보관함), 그때 ATLIB는 FDE에 AP를 제공하며 복귀한다. 그 밖에 옵션 ROM이 운영되지 않으면, ATLIB는 보안 지문 인증을 수행한다(유의:SMR_{PBA}가 사용되지 않았으며, 대신에 FDE에 의해 사용될 수 있기 때문에 작동한다). 그밖에 옵션 ROM이 시스템상에 있지만, 사용자가 암호구를 암호구를 입력한 경우: ATLib는 FDE로 오류 코드를 반환하며(사용자는 반드시 대체 인증을 제공해야 한다); ATLIB는 무효화를 위해 SMR_PBA로 랜덤 데이터를 확장해야만 한다(유의: 이는 BIOS에서 이전에 캡(cap)되었는지 여부와 무관하게 수행된다). 보안 세션을 무효화한다. FDE 인증이 완료된다. ATLIB FDE로 제어를 되돌린다.

[0364] SSD(single swipe to desktop) 구현 시스템에서, 드라이버는 새로운 보안 지문 인증을 수행하지 않고 센서로부터 애플리케이션 페이로드(AP)를 검색할 수 있을 수 있다. 상기 시스템이 소망하는 이러한 능력을 가지는 경우, 또는 PBA가 암호구를 회피하는 경우, 그때 상기 시스템은 로그인을 위해 반드시 스와이프(swipe)를 얻어야만 한다.

[0365] 각각의 경우, 상기 부팅 순서는 계속된다. 장치 드라이버는 로딩한다. 드라이버는 센서와 보안 세션을 구축한다. 드라이버는 PSI 데이터를 측정하며, SMR_{OS}로 확장한다. 드라이버가 로딩하여 PMPce를 측정하고 SMR_{OS}를 확장한다. 드라이버가 센서로부터 호스트 루트 키(HRK)를 요청한다: 센서가 NVM의 SMR_OS_VAL에 SMR_{OS}의 값을 비교하며; 동일한 경우 그때 HRK가 드라이버로 보내진다. 드라이버가 HRK를 사용하여 호스트 키 블롭을 복호화한다. 드라이버가 센서 μHSM를 사용하여 새로운 HRK를 생성한다. 드라이버가 센서에게 구 HRK와 새로운 HRK를 보내는 HRK의 재설정을 명령한다: 센서가 HRK의 재설정 전에 유효 SMR_{OS}를 확인해야만 한다(유의: 이는 부팅당 한번으로 HRK의 변경을 제한하며, 이는 누군가 로그인하기 전에 발생한다).

[0366] 드라이버가 센서로부터 저장된 AP를 요청한다. 센서가 드라이버에 AP를 전달한다: (SSD_구현 및 SMR_{OS} 유효); 그밖에(암호구가 사용되거나 대체 또는 SSD가 이용가능하지 않는) 경우에만, 오류 코드가 복귀된다. 드라이버가 SMR 무효화를 위해 SMR_{OS}로 랜덤 데이터를 확장한다. 드라이버가 새로운 HRK를 사용하여 호스트 키 블롭을 재 암호화하며, 데이터 저장소에 기록한다(유의: HRK_재설정이 실패되는 경우, 상기 드라이버는 구 HRK를 반환하고, 키 데이터를 와이핑해야만 하며, 이는 플러그 앤 플레이(PNP) 이벤트가 OS 부팅 외에 발생하는 경우 일어날 것이다.) 센서 서비스가 로딩하며; 센서 상태를 점검한다. INIT_완료 플래그가 설정되었는가?(응답이 yes임). 애플리케이션(GINA/VCP)이 서비스로부터 AP를 요청한다. 서비스가 드라이버로부터 AP를 요청한다. AP가 가용하지 않으면, 그때 드라이버는 보안 지문 인증을 수행한다. 보안 세션을 무효화한다. OS 인증이 완료된다. 드라이버가 서비스로 제어 및 AP를 반환한다. 서비스가 애플리케이션에 제어와 AP를 반환한다. 일반적인 부팅 순서가 종료된다.

[0367] 로밍 템플릿의 일 실시예가 기술될 것이다. 로밍 템플릿은 정책이 이를 승인하는 시스템상에서만 허용될 수 있다. 상기 센서는 이러한 정책이 효력이 있는지 여부를 식별하는 NVRAM의 플래그를 가질 수 있다. 로밍 템플릿은 템플릿 헤더의 비암호화된 부분의 정보에 기반하여 식별가능할 것이다. 로밍 템플릿과 비-로밍 템플렛의 주요 차이는 워크그룹 내의 로밍 템플릿들이 모두 동일한 키를 사용하여 암호화될 수 있다는 것이다. 이러한 키는 HRK 저장 위치를 사용하여 센서 NVRAM에 저장될 것이다. 상기 HRK 값은 워크그룹 또는 도메인 서버상의 애플리케이션으로부터 브로드캐스트에 의해 설정될 것이다. 센서의 플래그를 허용하는 플래그 로밍 템플릿이

사실로 설정되면, 일반적으로 될 수 있는 것처럼, HRK가 유효 SMR 환경상에 기반하여 드라이버에 해제되지 않을 것이다. 이러한 아키텍처는 특정 기계 상에서 로밍 템플릿과 고정-클라이언트 템플릿의 혼합물을 방지하지 않을 것이라는 유의해야 한다.

[0368] 단일 컴퓨터상에서 동작하는 다중 보안 센서들을 허용하기 위해(다중 등록을 요하지 않는), 한 센서로부터 다른 센서로 NVRAM 내용을 클론하는 것이 바람직할 수 있다. 이러한 동작은 사용자가 카피 될 센서를 위한 소유권자 암호구를 제공하는 것을 요할 것이다. 이는 마찬가지로 상기 수신 센서가 비-초기화 상태에 있는 것을 필요로 할 것이다. 초기화된 센서는 NVRAM 클론 데이터를 허용하지 않을 것이다. 의사코드(pseudo code)가 한 보안 센서로부터 다른 보안 센서를 복제하기 위한 이벤트 순서의 일 실시예를 기재한다.

[0369] 초기화되었는지 여부를 판별하기 위해 새로운 센서를 점검한다. 초기화되지 않은 경우: 사용자가 센서를 복제하도록 허용한다; 사용자로부터 현존 센서를 위한 소유권자 암호구를 획득하며 소유권자 키로 변환한다; 센서가 NVRAM 클론을 이출하여, 소유권자 키로 통과하도록 명령한다; 상기 센서는 NVRAM의 카피에 대한 소유권자 키를 확인할 것이며; 상기 키가 매치하면, 센서는 소유권자 키로부터 대칭 암호화 키를 획득하고, 센서는 획득된 키를 이용하여 NVRAM의 내용을 암호화 및 전송하며; 새로운 센서가 소유권자 키 및 클론 블록에 통과하는 NVRAM을 이입하도록 명령하며; 상기 센서가 초기화된 것인지를 확인하며; 아닌 경우, 센서는 소유권자 키로부터 복호화 키를 획득하며, 센서는 클론 블롭을 복호화하며, 센서는 복호화된 클론 블록의 소유권자 키에 대해 통과 소유권자 키(passed in owner key)를 점검한다. 소유권자 키가 매치하면, 복호화된 클론 블롭이 NVRAM으로 카피되며, 그렇지 않으면 FAIL 명령 된다. 그 밖에 작용이 필요하지 않다.

[0370] 도 14 내지 도 16을 참조하면, 호스트 플랫폼, 하드웨어 보안 모듈을 구비한 센서, 및 SPI-플래시 또는 하드 드라이브와 같은 임의의 외부 메모리를 포함한 시스템의 일 실시예에 대한 추가 세부사항이 기술될 것이다. 상기 보안 센서는 예를 들어, 30cm/초보다 큰 슬라이드 속도를 가지는 슬라이드 센서일 수 있다. 상기 센서는 도 16과 관련하여 하기 기술될 온-칩(On-Chip) 하드웨어 보안 모듈(μHSM)을 구비할 수 있다. NVRAM은 모든 암호화 키들을 안전하게 저장하며, 키들은 상기 센서를 절대로 떠나지 않는다. 온-칩 매치 엔진이 포함되며, 128-비트의 AES 암호화/복호화가 상기 보안 애플리케이션 페이로드뿐만 아니라, 모든 지문 이미지들 및 템플릿들과 관련될 수 있다. 암호화된 USB 2.0 전속 시스템 I/F가 제공될 수 있으며, 안전 코드 및 템플릿 저장소를 구비한 비공개 직렬 플래시 I/F가 제공될 수 있다. 상기 센서는 3.3V USB I/O를 가지는 1.8V 코어를 포함할 수 있다. 또한, 상기 센서는 45BGA 패키징:13.8 X 5 X 1.68mm, 개량형 내구성 표면 코팅, 및 통합형 손가락 드라이브. 정전 방전 능력(+/- 15KV)이 위조 손가락 거부를 위해 안티-스푸핑 (anti-spoofing)과 마찬가지로, 포함될 수 있다.

[0371] 하드웨어 보안 모듈이 마이크로프로세서-제어 보안 엔진을 정의할 수 있다. 입력된(keyed) SHA-1 해시 엔진은 SMR 측정을 위해 사용되며, 128 비트의 AES 엔진이 템플릿 등을 암호화한다. DH를 위한 공개키 엔진이 안전한 USB 통신을 가능하게 한다. 비휘발성 메모리가 포함되며 다른 탬퍼 보장 특징들(Tamper Assurance Features)이 도 16에 도시된다.

[0372] 도 17을 참조하면, 센서와 임의의 외부 메모리를 포함한 시스템의 일 실시예에 있어서의 하드웨어 보안 요소들이 도시된다. 거론한 바와 같이, 상기 센서 또는 시스템 측정 레지스터(SMR)들은 코드 측정들을 보유한다. 상기 센서의 NVM은 소프트웨어 상태 해쉬(hash), 영구적 키 저장소 및 센서 상태 플래그를 포함한다. 예를 들어, 512KB SPI-플래시와 같은 임의의 외부 메모리가 이미지 처리 코드, 센서-암호화된 사용자 템플릿들, 및 외부 랩핑된 SW 키들을 포함할 수 있다.

[0373] 본 발명의 다수의 변형 및 다른 실시형태들이 전술한 기재 및 관련 도면에 나타난 개시의 이점을 가지며 본 기술분야의 당업자에게 떠오를 것이다. 따라서, 본 발명은 개시된 특정 실시형태들에 제한되는 것이 아니며, 상기 변형 및 실시형태들은 첨부 청구항의 범위 내에 포함되는 것으로 의도한다는 것을 이해한다.

부호의 설명

[0374] 10: 컴퓨터

14: 보안 센서

100: 보안 전자 장치

110: 손가락 감지 장치

112: 집적회로(IC) 기판

114: 손가락 감지 요소들

116: 이미지 워터마크 회로

120: 키 생성 회로

122: 키 캐시(key cache)

124: 무작위 번호 생성기(RNG)

126: 해시 엔진

118: 매칭 회로

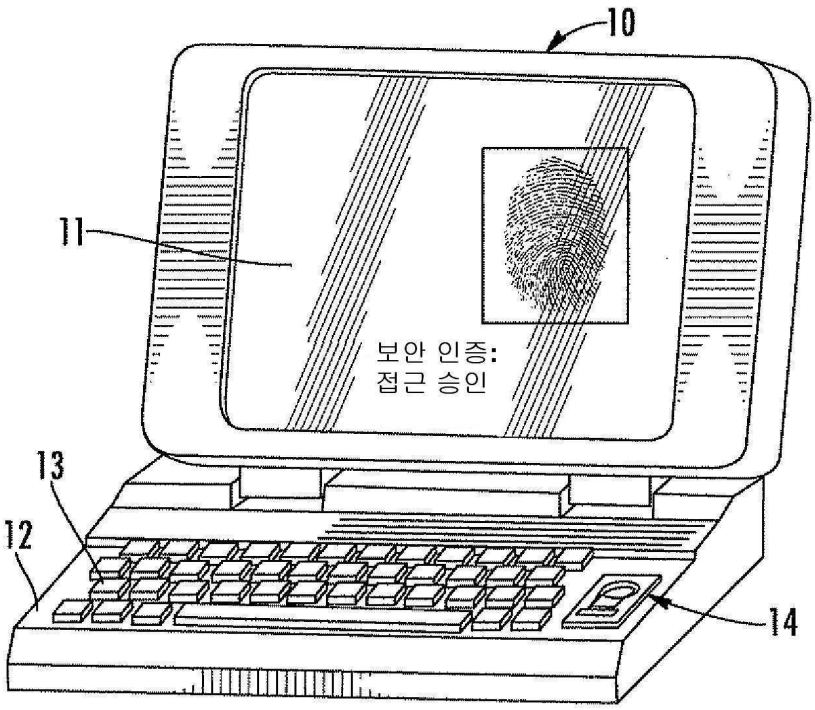
128: 식별정보 해제 회로

130: 하우징

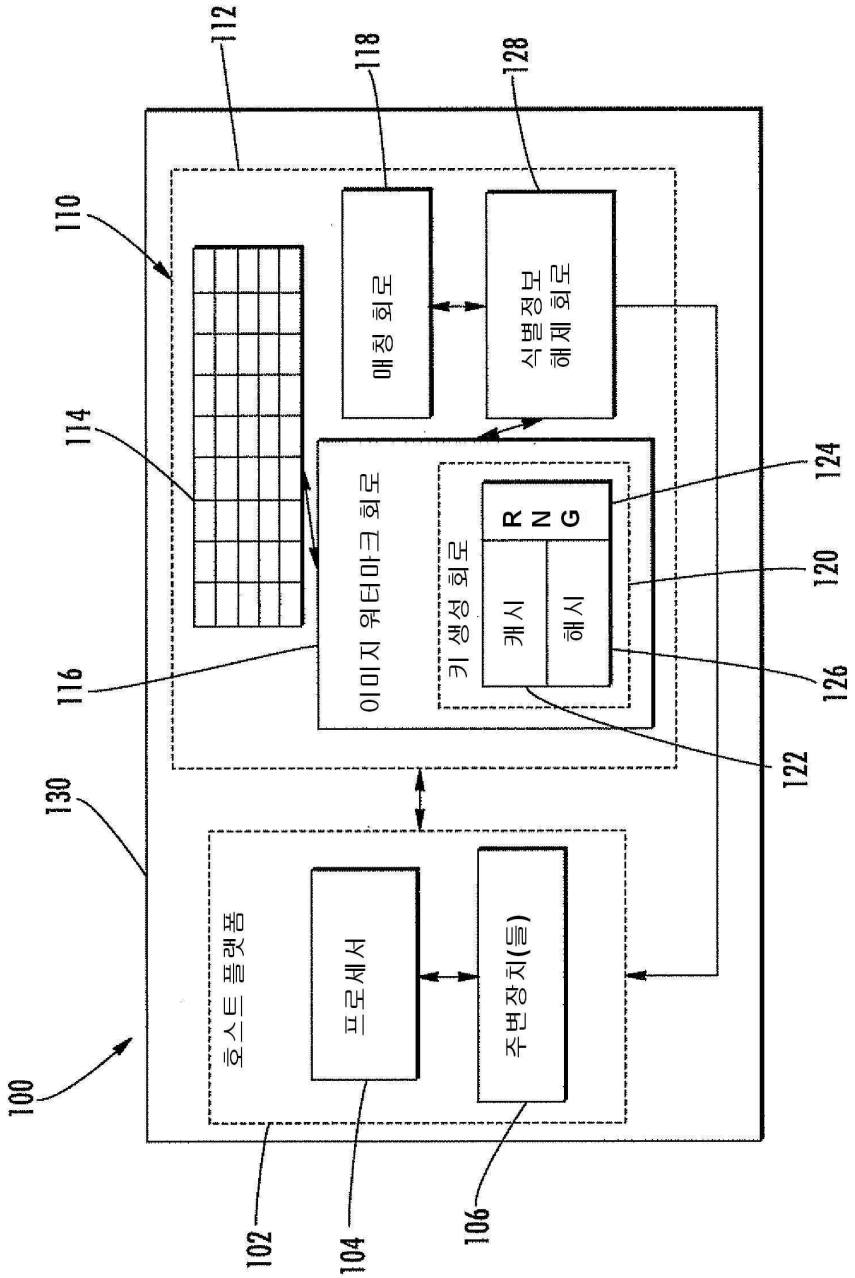
202: 호스트 플랫폼

도면

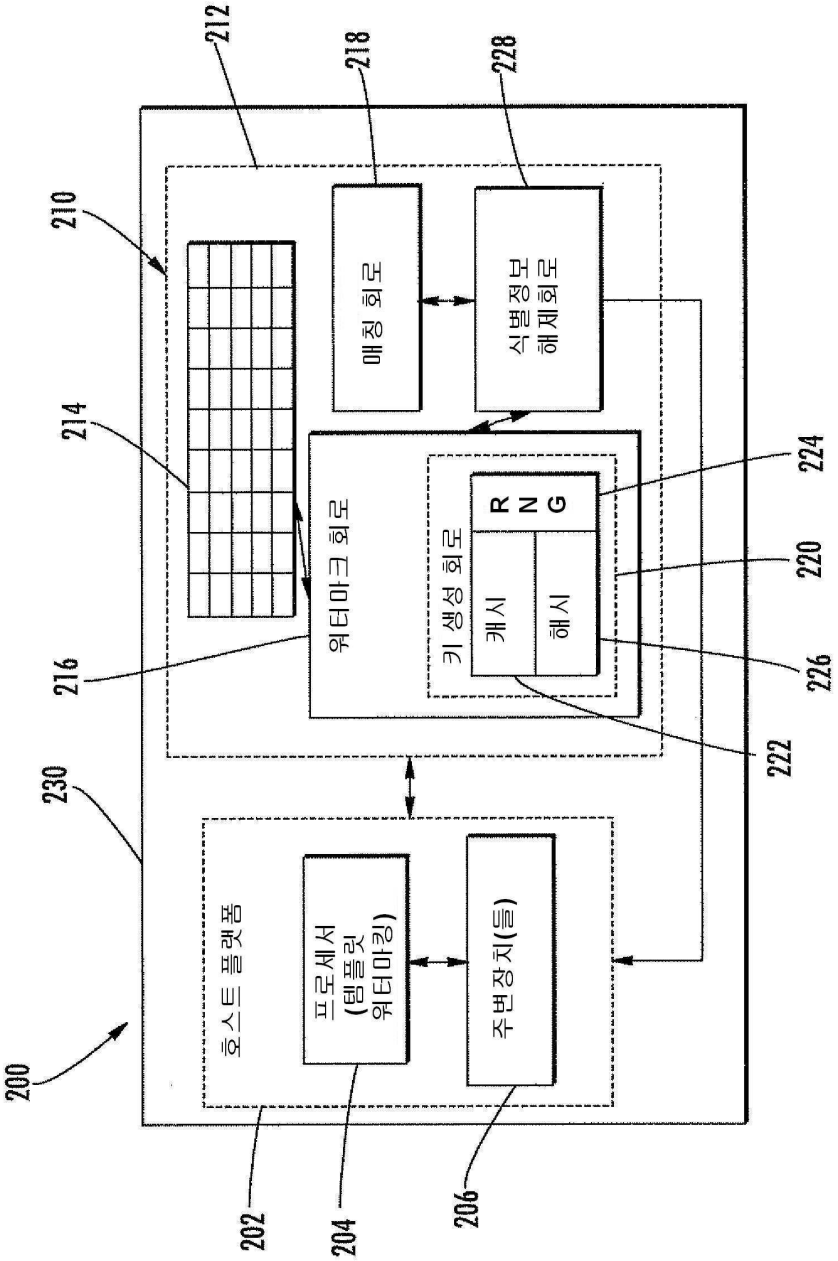
도면1



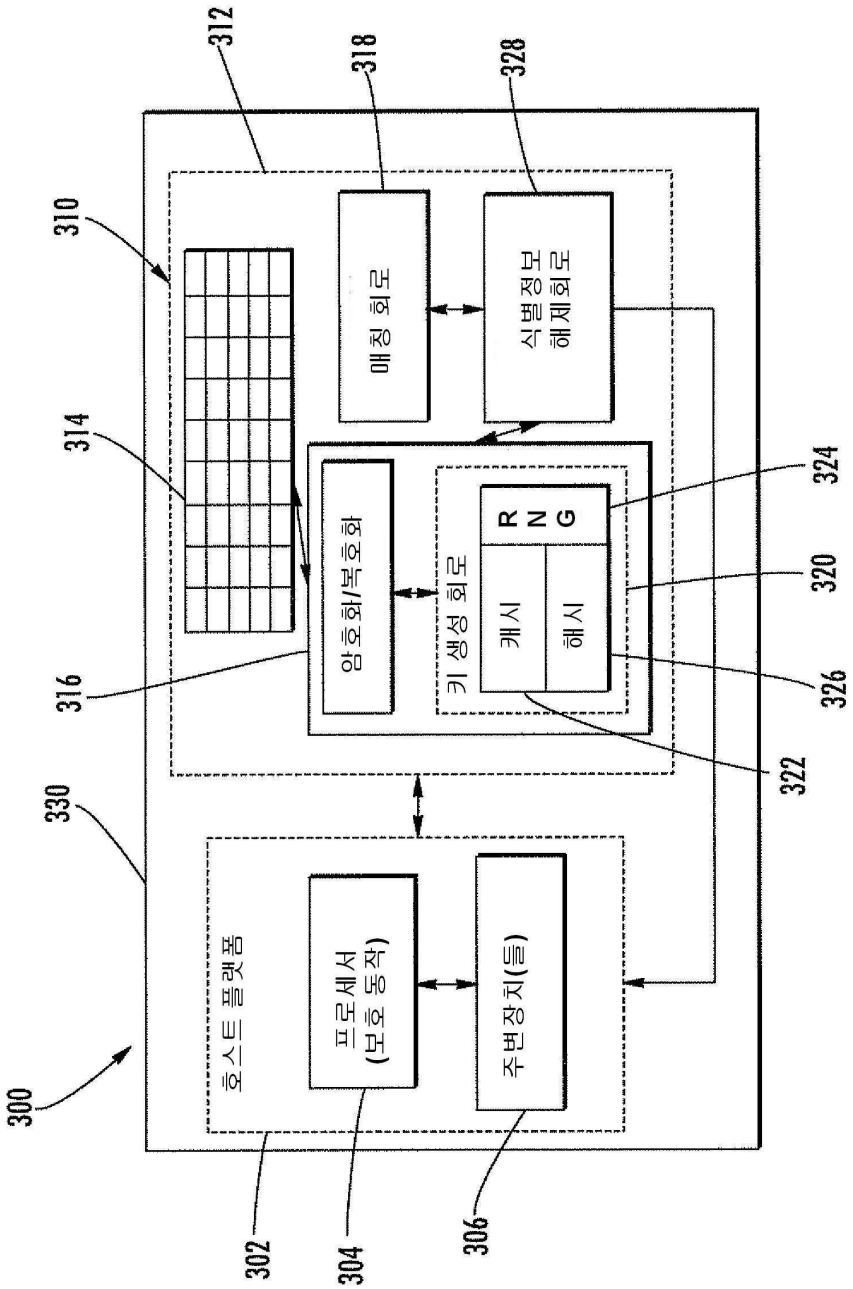
도면2


112
118
128
110
114
116
130
100
102
104
106
122
124
120
126
매칭 회로
식별정보 해제 회로
이미지 워터마크 회로
키 생성 회로
캐시
해시
R
N
G
호스트 플랫폼
프로세서
주변장치(들)

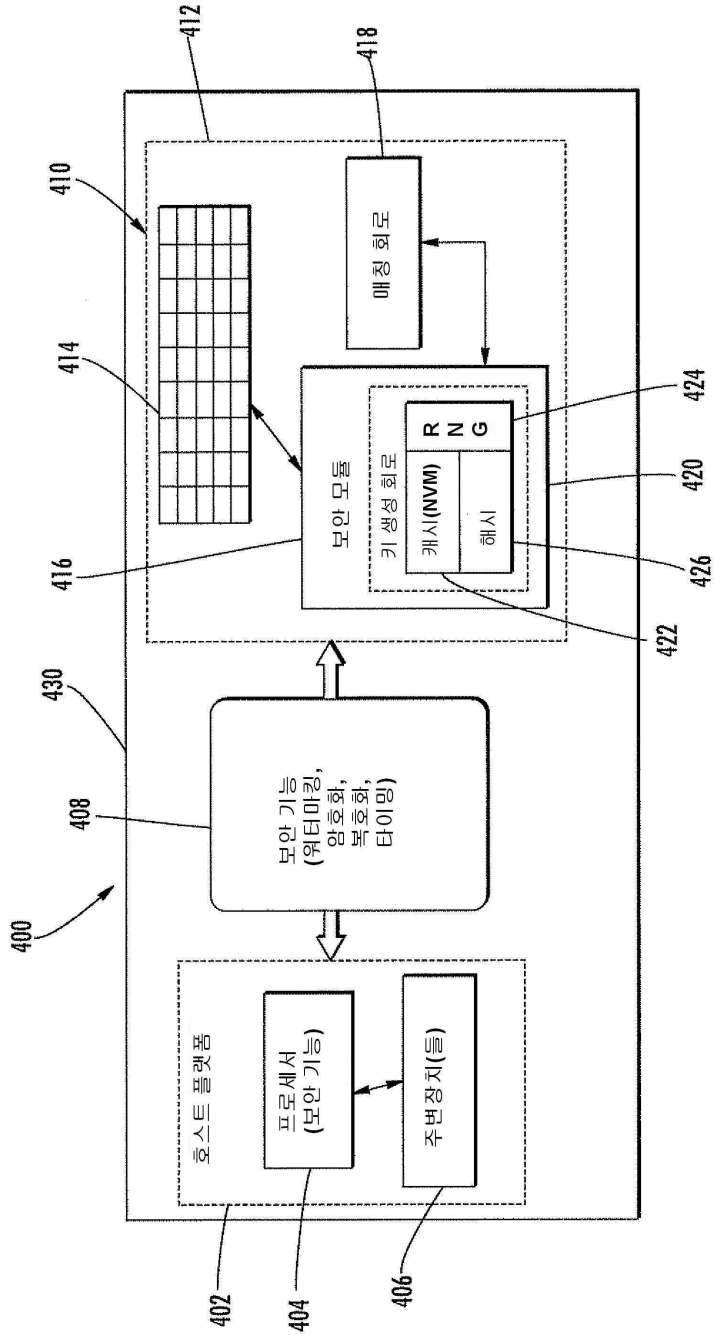
도면3


212
218
228
210
214
216
230
200
202
204
206
224
220
226
222
매칭 회로
식별정보
해제회로
워터마크 회로
키 생성 회로
R
N
G
캐시
해시
호스트 플랫폼
프로세서
(템플릿
워터마킹)
주변장치(들)

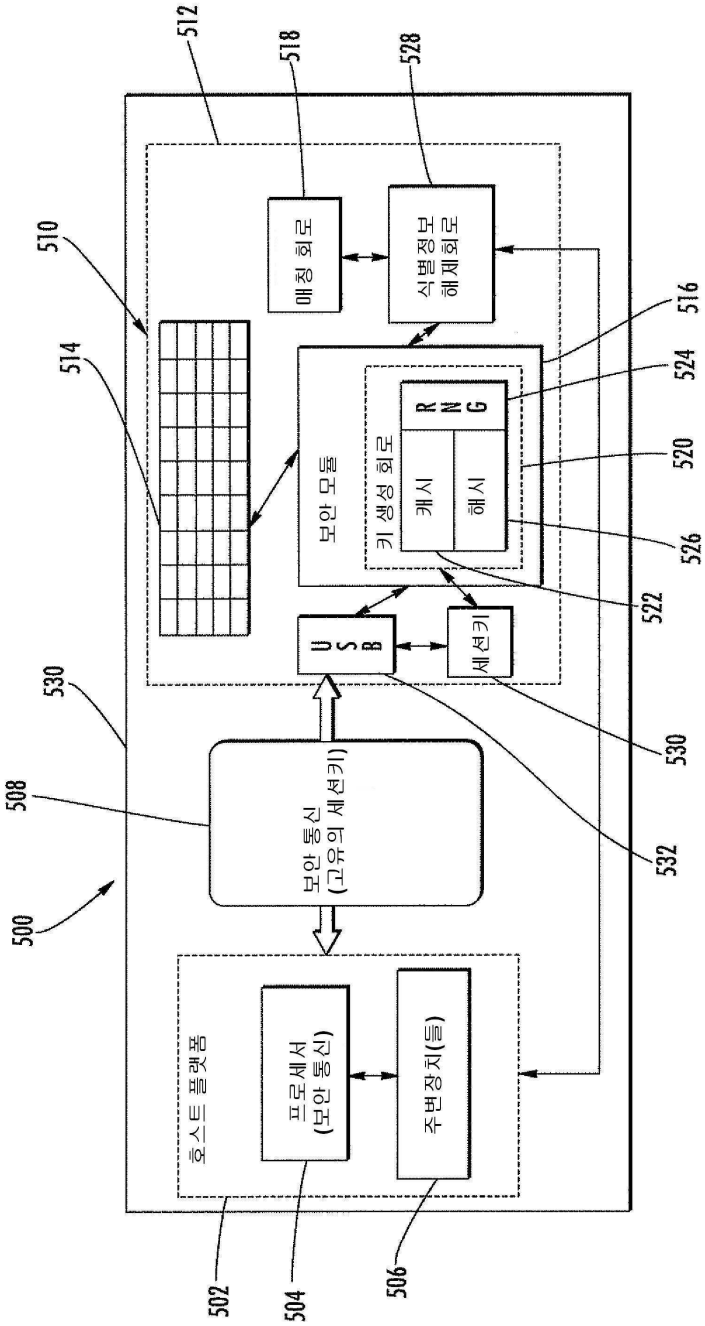
도면4


312
318
328
310
매칭 회로
식별정보
해제회로
314
324
암호화/복호화
키 생성 회로
R
N
G
320
캐시
해시
316
326
322
330
호스트 플랫폼
프로세서
(보호 동작)
주변장치(들)
300
302
304
306

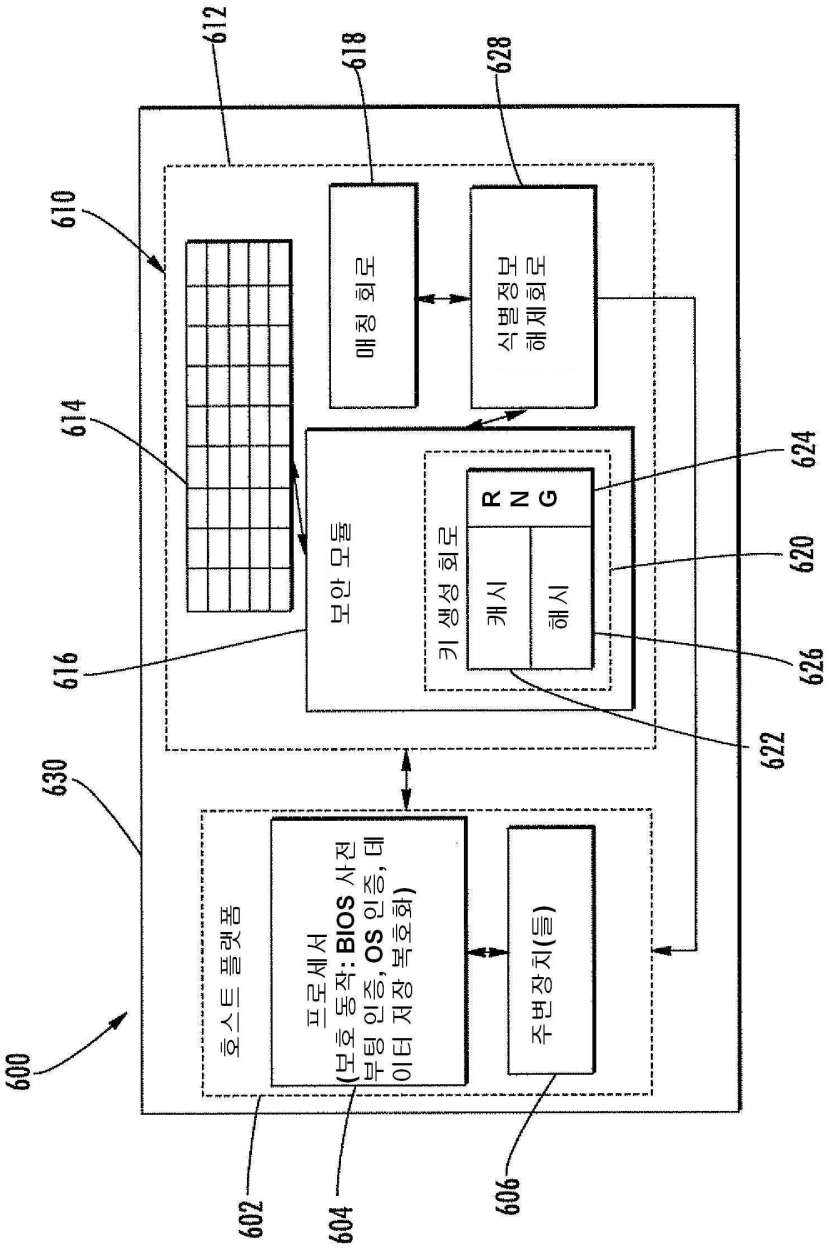
도면5


412
418
410
414
416
424
420
426
422
430
408
400
402
404
406
매칭 회로
보안 모듈
키 생성 회로
캐시(NVM)
해시
RNG
보안 기능
(워터마킹,
암호화,
복호화,
타이밍)
호스트 플랫폼
프로세서
(보안 기능)
주변장치(들)

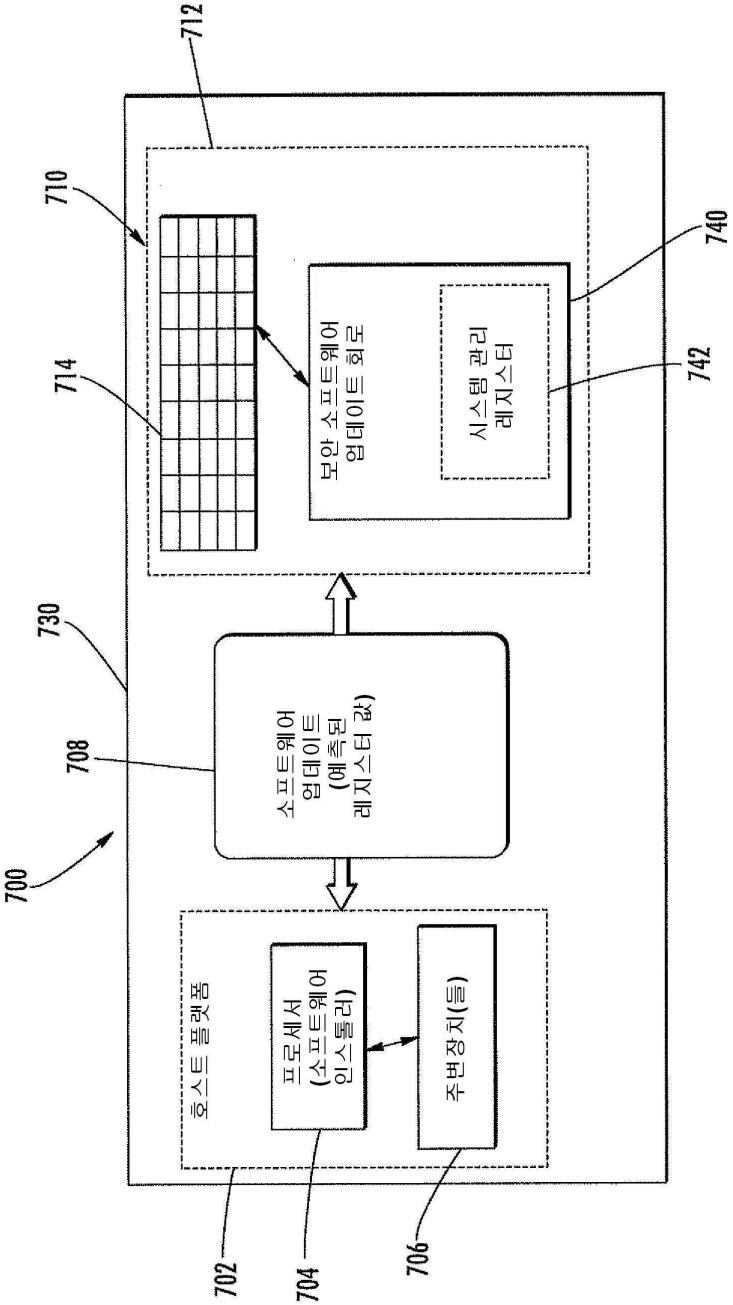
도면6


512
518
528
510
514
516
524
520
526
522
530
508
500
532
502
504
506
매칭 회로
식별정보 해제회로
보안 모듈
키 생성 회로
캐시
해시
RNG
USB
세션키
보안 통신 (고유의 세션키)
호스트 플랫폼
프로세서 (보안 통신)
주변장치(들)

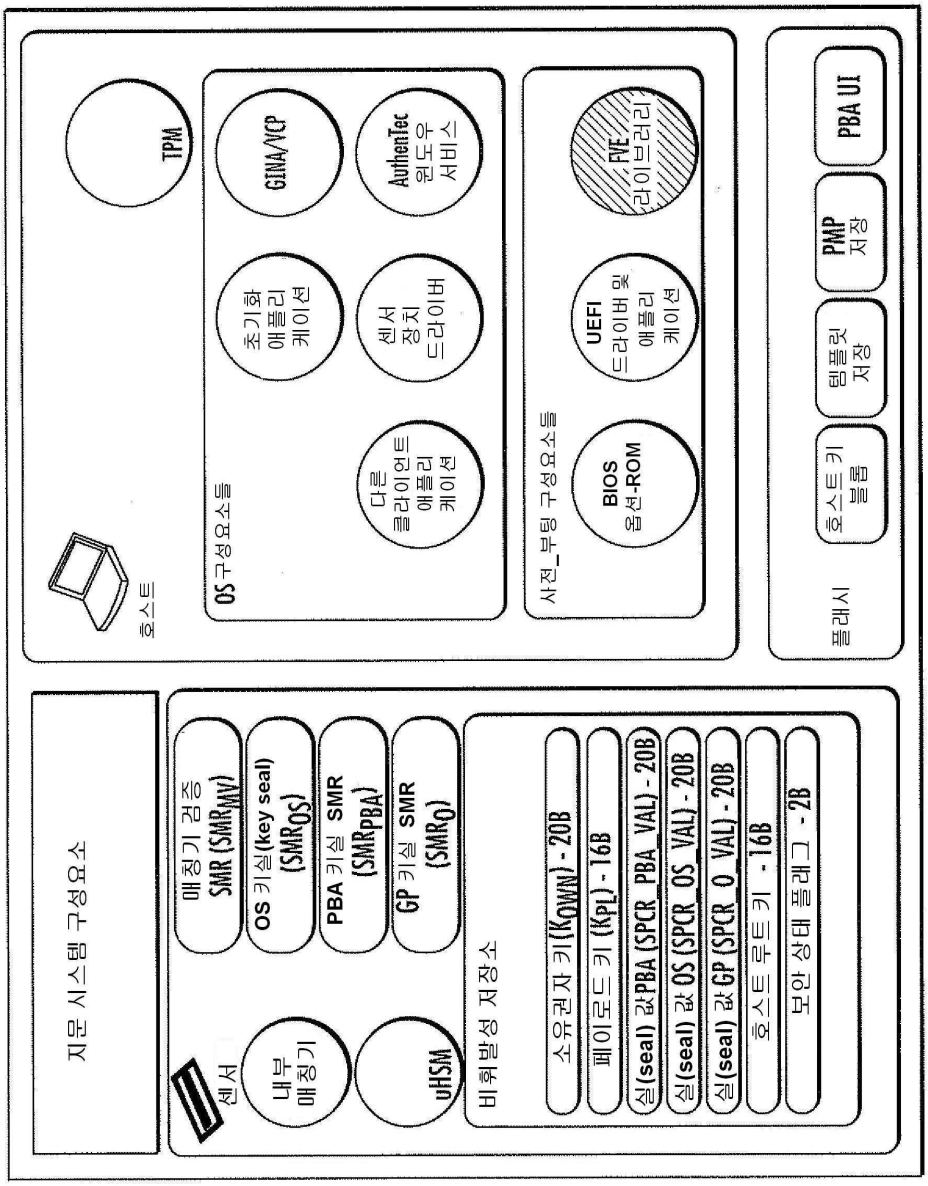
도면7


612
618
628
610
614
624
620
616
626
622
630
600
602
604
606
메칭 회로
식별정보 해제회로
보안 모듈
키 생성 회로
RNG
캐시
해시
호스트 플랫폼
프로세서
(보호 동작: BIOS 사전 부팅 인증, OS 인증, 데이터 저장 복호화)
주변장치(들)

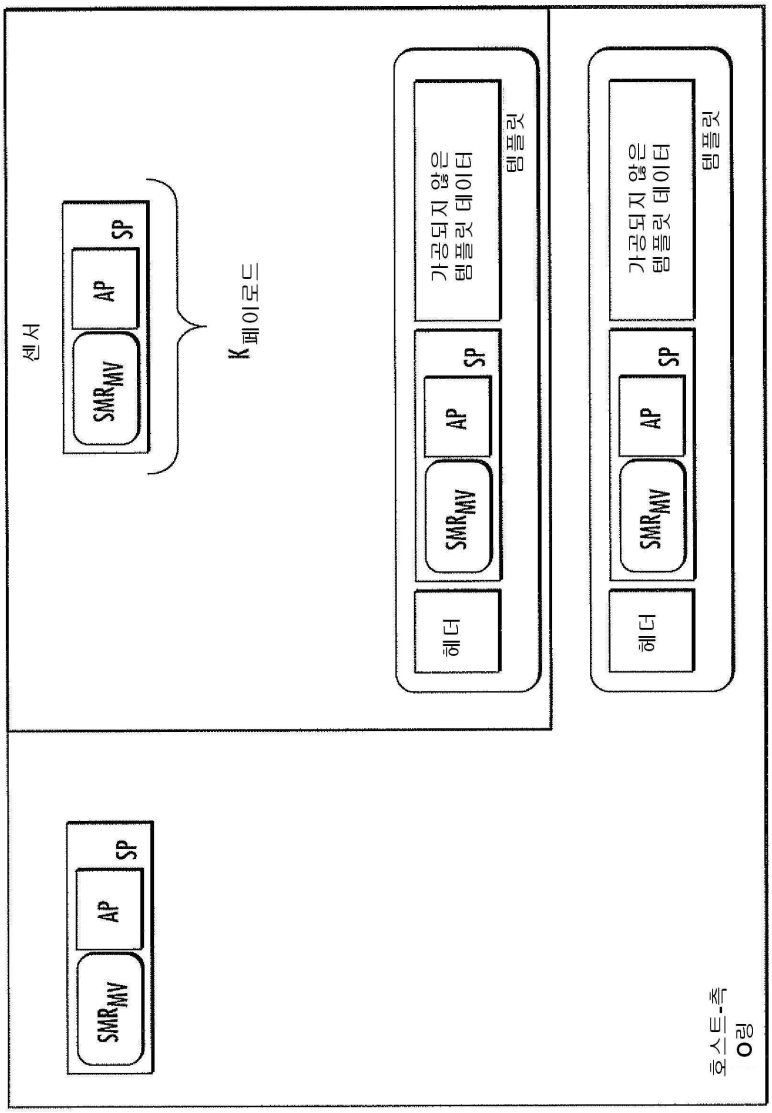
도면8


712
710
714
740
742
보안 소프트웨어 업데이트 회로
시스템 관리 레지스터
730
708
700
소프트웨어 업데이트 (예측된 레지스터 값)
호스트 플랫폼
프로세서 (소프트웨어 인스톨러)
주변장치(들)
702
704
706

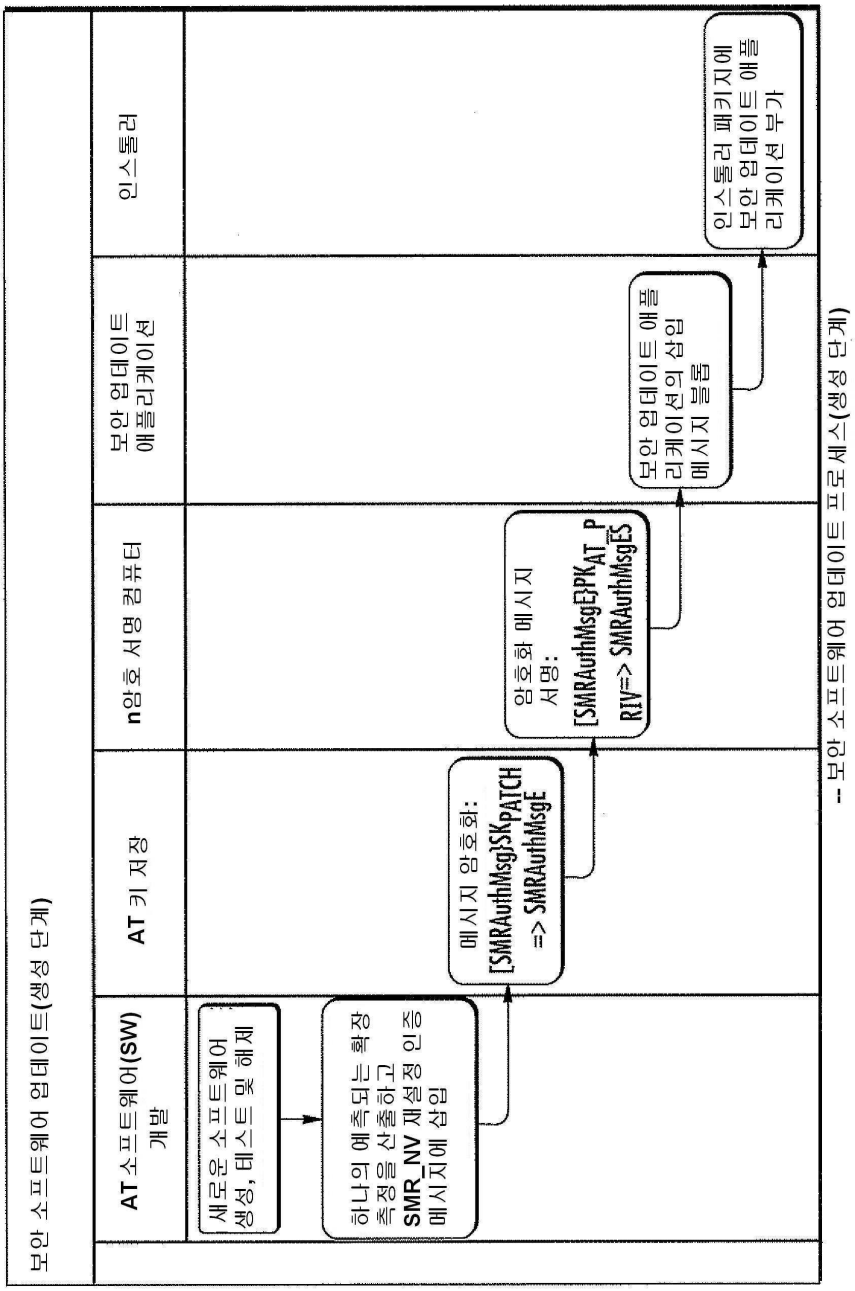
도면9


지문 시스템 구성요소
센서
내부 매칭기
uHSM
매칭기 검증 SMR (SMR_MV)
OS 키쉴(key seal) (SMR_OS)
PBA 키쉴 SMR (SMR_PBA)
GP 키쉴 SMR (SMR_O)
비휘발성 저장소
소유권자 키(K_OWN) - 20B
페이로드 키 (K_PL) - 16B
쉴(seal) 값PBA (SPCR_PBA_VAL) - 20B
쉴(seal) 값 OS (SPCR_OS_VAL) - 20B
쉴(seal) 값 GP (SPCR_O_VAL) - 20B
호스트 루트키 - 16B
보안 상태 플래그 - 2B
호스트
TPM
OS구성요소들
초기화 애플리케이션
GINA/VCP
다른 클라이언트 애플리케이션
센서 장치 드라이버
AuthenTec 윈도우 서비스
사전_부팅 구성요소들
BIOS 옵션-ROM
UEFI 드라이버 및 애플리케이션
FVE 라이브러리
플래시
호스트 키 블록
템플릿 저장
PMP 저장
PBA UI

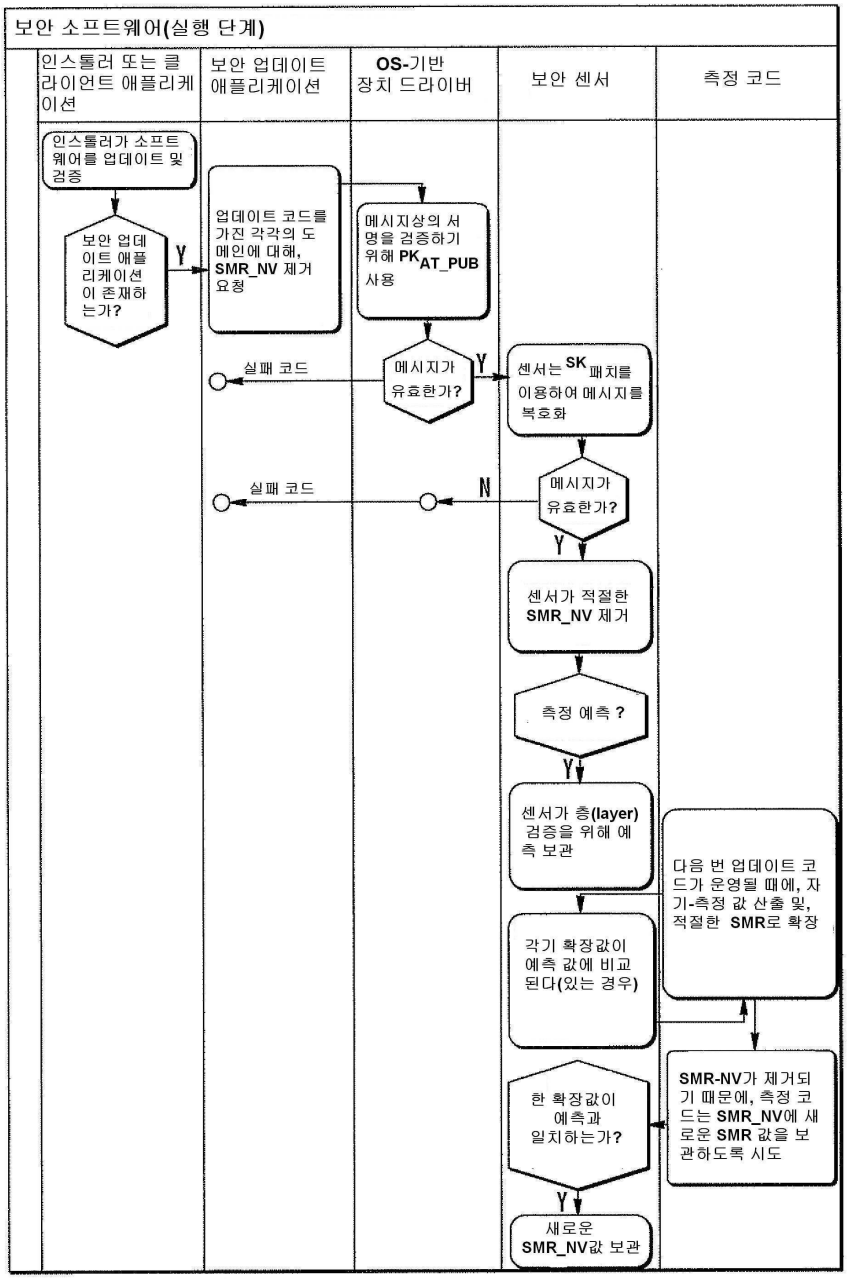
도면10


호스트-측
이링
SMR_MV
AP
SP
센서
K페이로드
헤더
SMR_MV
AP
SP
가공되지 않은
템플릿 데이터
템플릿
헤더
SMR_MV
AP
SP
가공되지 않은
템플릿 데이터
템플릿

도면11

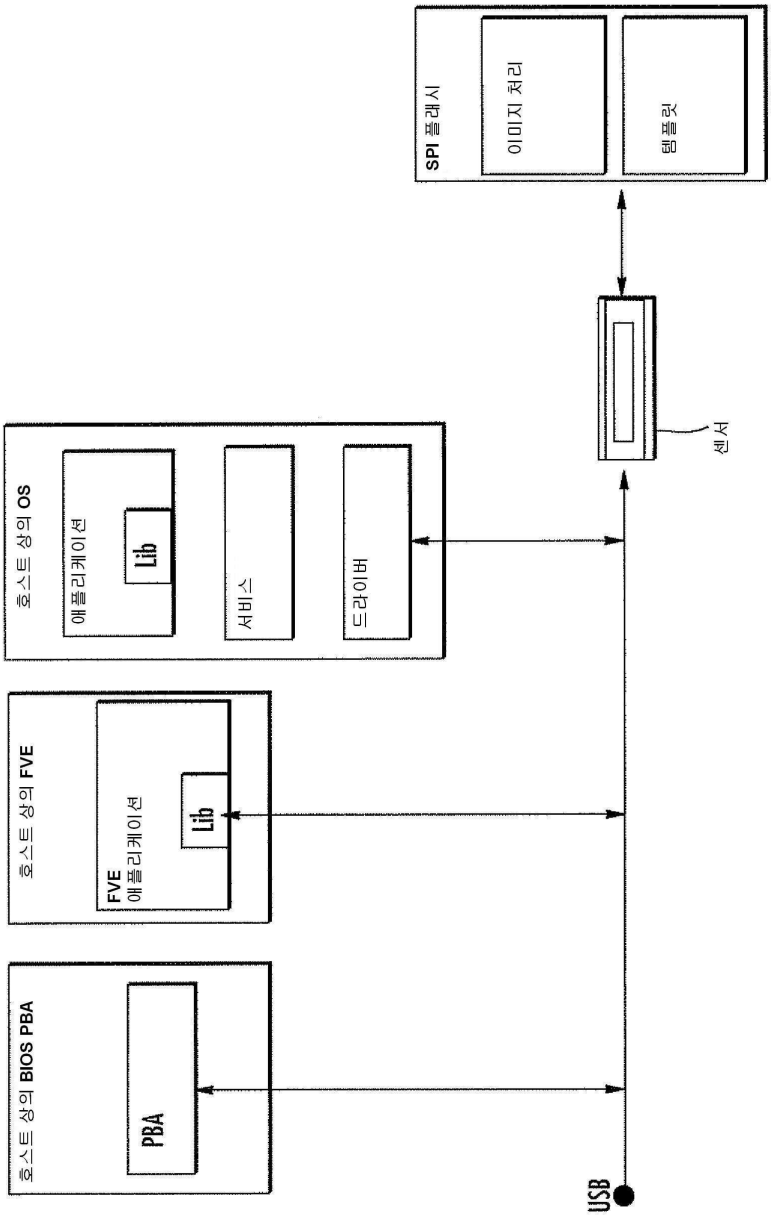

보안 소프트웨어 업데이트(생성 단계)
AT소프트웨어(SW) 개발
AT 키 저장
n암호 서명 컴퓨터
보안 업데이트 애플리케이션
인스톨러
새로운 소프트웨어 생성, 테스트 및 해제
하나의 예측되는 확장 측정을 산출하고 SMR_NV 재설정 인증 메시지에 삽입
메시지 암호화: [SMRAuthMsg]SK_PATCH => SMRAuthMsgE
암호화 메시지 서명: [SMRAuthMsgE]PK_AT_P RTV=> SMRAuthMsgES
보안 업데이트 애플 리케이션의 삽입 메시지 블롭
인스톨러 패키지에 보안 업데이트 애플 리케이션 부가
-- 보안 소프트웨어 업데이트 프로세스(생성 단계)

도면12

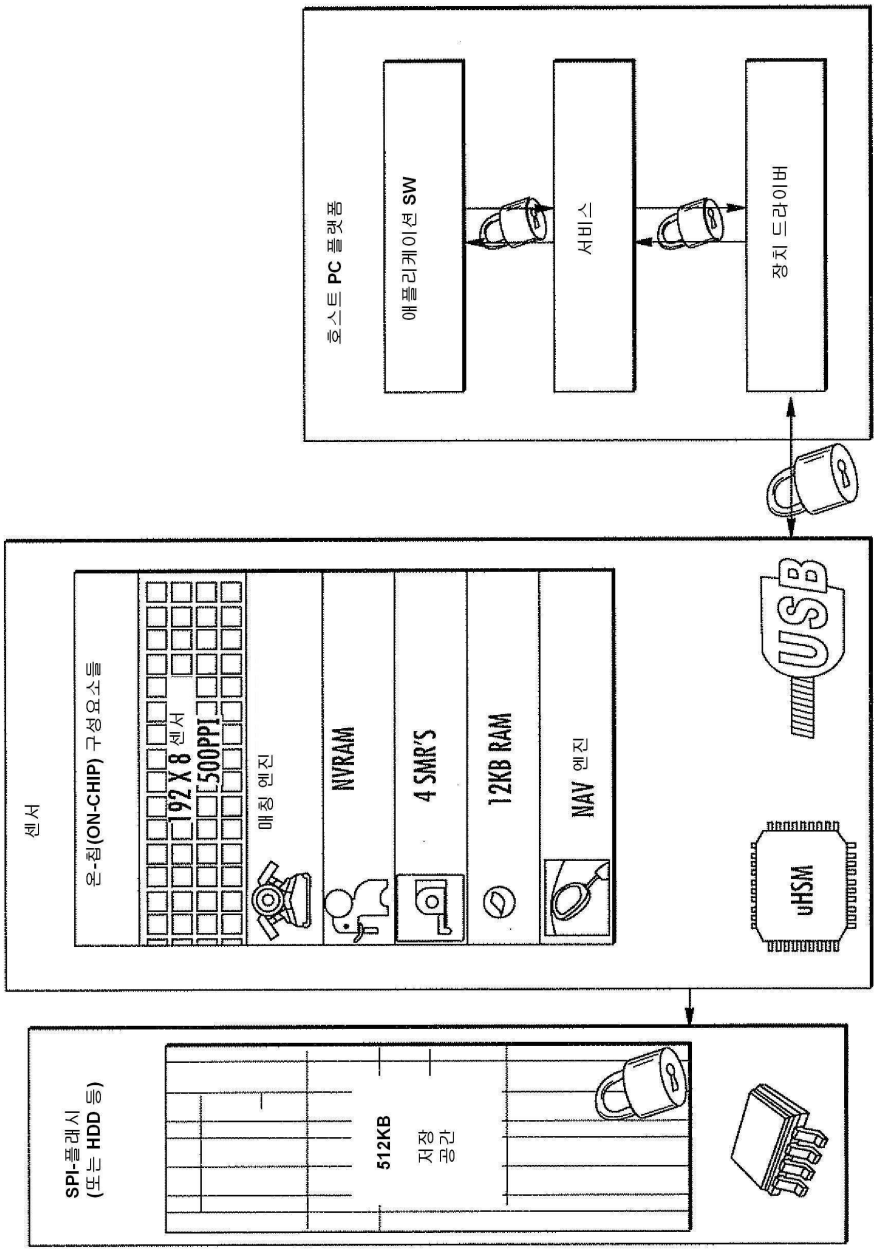


-- 보안 소프트웨어 업데이트 프로세스 (실행 단계)

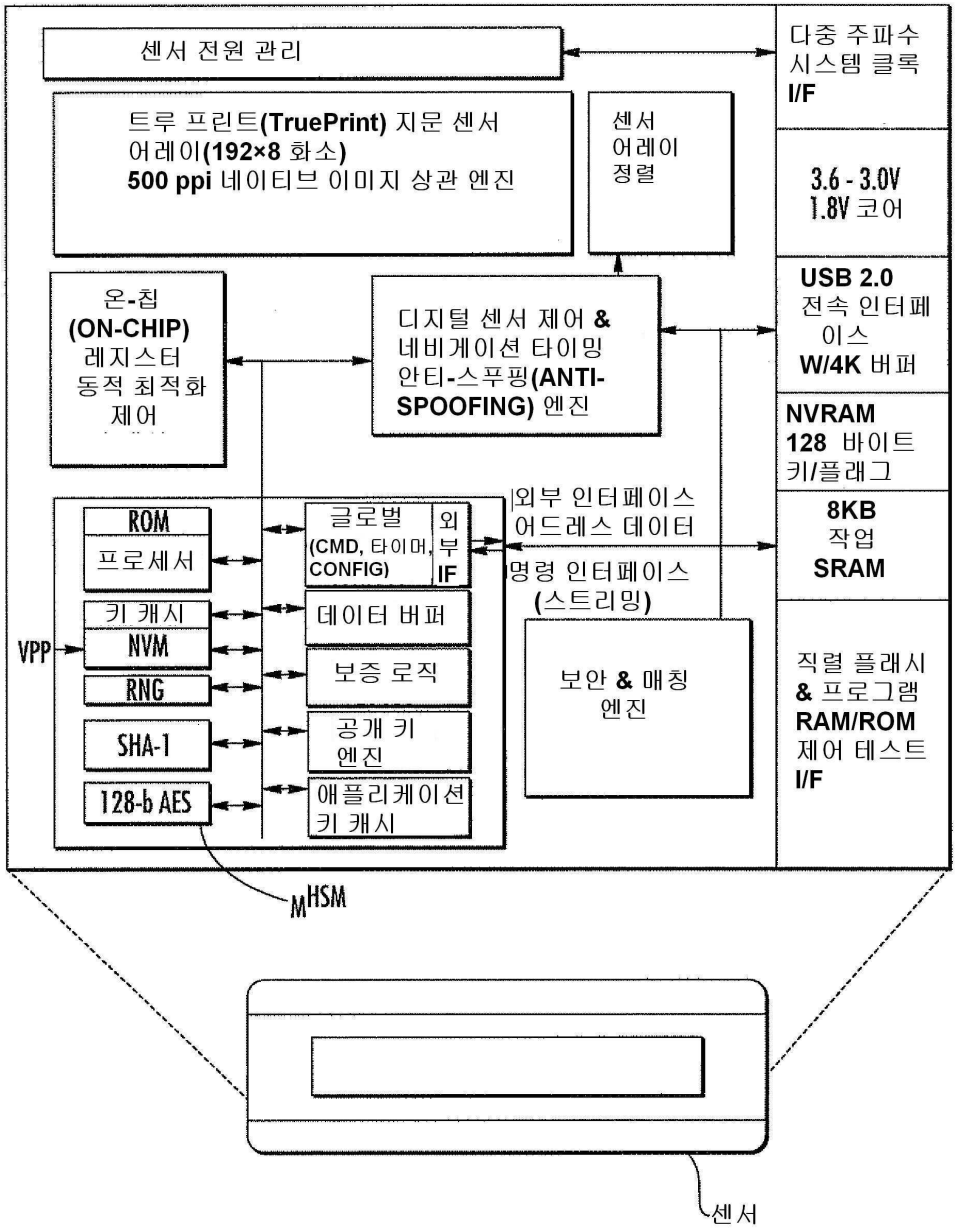
도면13


호스트 상의 BIOS PBA
PBA
호스트 상의 FVE
FVE
애플리케이션
Lib
호스트 상의 OS
애플리케이션
Lib
서비스
드라이버
USB
센서
SPI 플래시
이미지 처리
템플릿

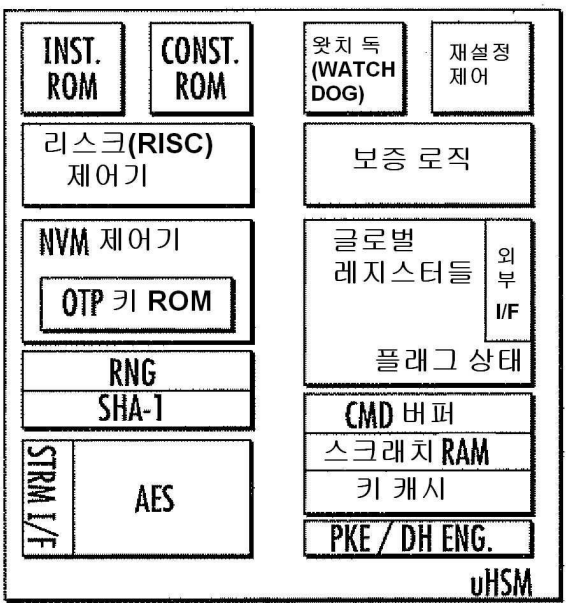
도면14


호스트 PC 플랫폼
애플리케이션 SW
서비스
장치 드라이버
센서
온-칩(ON-CHIP) 구성요소들
192 X 8 센서
500PPI
매칭 엔진
NVRAM
4 SMR'S
12KB RAM
MAV 엔진
USB
uHSM
SPI-플래시
(또는 HDD 등)
512KB
저장
공간

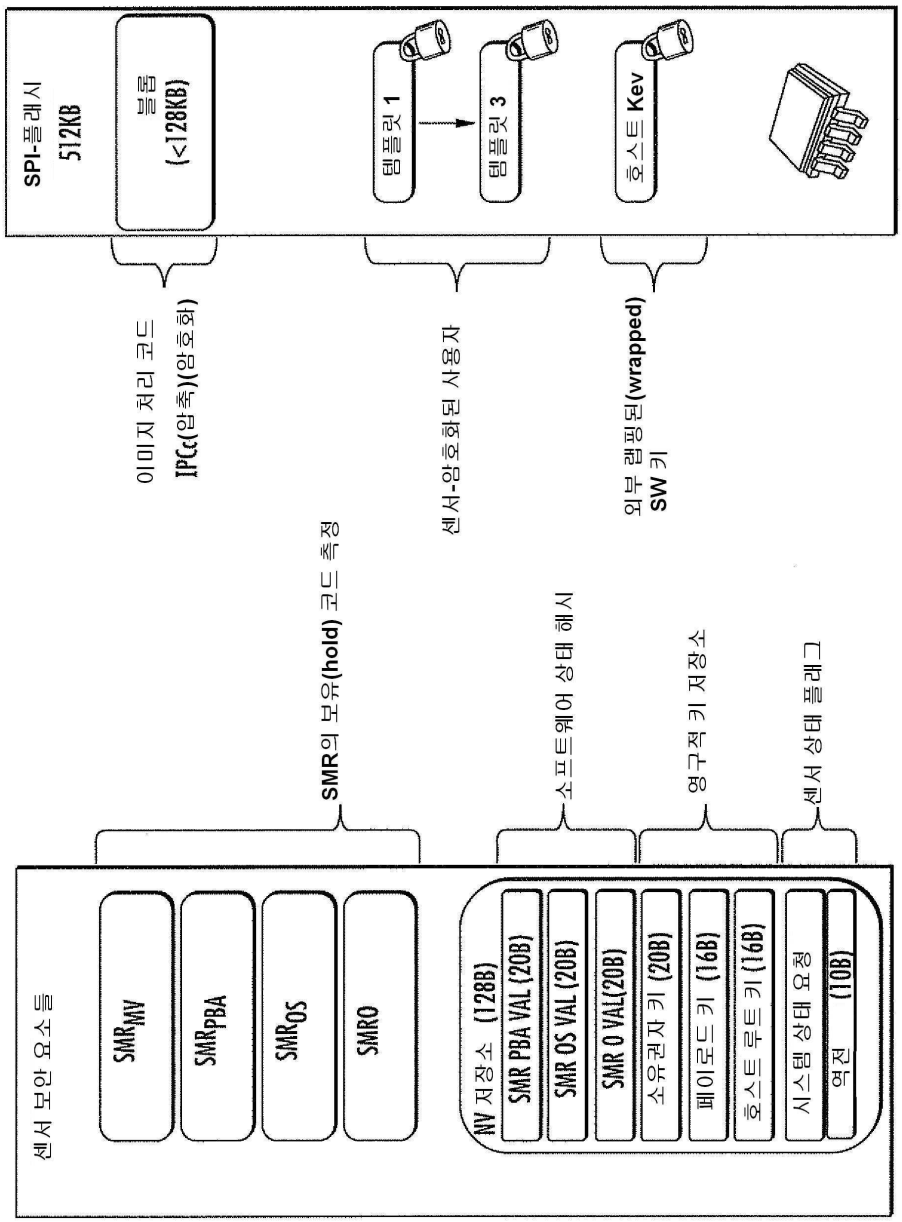
도면15


센서 전원 관리
다중 주파수 시스템 클록 I/F
트루 프린트(TruePrint) 지문 센서 어레이(192×8 화소) 500 ppi 네이티브 이미지 상관 엔진
센서 어레이 정렬
3.6 - 3.0V 1.8V 코어
온-칩 (ON-CHIP) 레지스터 동적 최적화 제어
디지털 센서 제어 & 네비게이션 타이밍 안티-스푸핑(ANTI-SPOOFING) 엔진
USB 2.0 전속 인터페이스 W/4K 버퍼
NVRAM 128 바이트 키/플래그
외부 인터페이스 어드레스 데이터
명령 인터페이스 (스트리밍)
8KB 작업 SRAM
ROM 프로세서
글로벌 (CMD, 타이머, CONFIG)
외부 IF
키 캐시
NVM
VPP
RNG
SHA-1
128-b AES
데이터 버퍼
보증 로직
공개 키 엔진
애플리케이션 키 캐시
보안 & 매칭 엔진
직렬 플래시 & 프로그램 RAM/ROM 제어 테스트 I/F
MHSM
센서

도면16


INST. ROM
CONST. ROM
왓치 독 (WATCH DOG)
재설정 제어
리스크(RISC) 제어기
보증 로직
NVM 제어기
OTP 키 ROM
글로벌 레지스터들
외부 I/F
플래그 상태
RNG
SHA-1
CMD 버퍼
스크래치 RAM
키 캐시
STRM I/F
AES
PKE / DH ENG.
uHSM

도면17


SPI-플래시
512KB
블롭
(<128KB)
템플릿 1
템플릿 3
호스트 Kev
이미지 처리 코드
IPC(압축)(암호화)
센서-암호화된 사용자
외부 랩핑된(wrapped)
SW 키
SMR의 보유(hold) 코드 측정
소프트웨어 상태 해시
영구적 키 저장소
센서 상태 플래그
센서 보안 요소들
SMR_MV
SMR_PBA
SMR_OS
SMRO
NV 저장소 (128B)
SMR PBA VAL (20B)
SMR OS VAL (20B)
SMR O VAL(20B)
소유권자 키 (20B)
페이로드 키 (16B)
호스트 루트 키 (16B)
시스템 상태 요청
역전 (10B)