(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.^{7}
H04L 9/00

(45) 공고일자 **2003년11월14일**
(11) 등록번호 **10-0405574**
(24) 등록일자 **2003년11월03일**

(21) 출원번호	10-2000-7002387	(65) 공개번호	특2001-0023733
(22) 출원일자	2000년03월06일	(43) 공개일자	2001년03월26일
번역문 제출일자	2000년03월06일		
(86) 국제출원번호	PCT/US1998/14858	(87) 국제공개번호	WO 1999/13613
(86) 국제출원출원일자	1998년07월17일	(87) 국제공개일자	1999년03월18일

(81) 지정국

국내특허 : 알바니아, 아르메니아, 오스트리아, 오스트레일리아, 아제르바이잔, 보스니아-헤르체고비나, 바베이도스, 불가리아, 브라질, 벨라루스, 캐나다, 스위스, 중국, 쿠바, 체코, 독일, 덴마크, 에스토니아, 스페인, 핀랜드, 리히텐슈타인, 영국, 그루지야, 가나, 감비아, 크로아티아, 헝가리, 인도네시아, 이스라엘, 아이슬란드, 일본, 케냐, 키르기즈, 북한, 대한민국, 카자흐스탄, 세인트루시아, 스리랑카, 라이베리아, 레소토, 리투아니아, 룩셈부르크, 라트비아, 몰도바, 마다가스카르, 마케도니아, 몽고, 말라위, 멕시코, 노르웨이, 뉴질랜드, 폴란드, 포르투칼, 루마니아, 러시아, 수단, 스웨덴, 싱가포르, 슬로베니아, 슬로바키아, 시에라리온, 타지키스탄, 투르크메니스탄, 터어키, 트리니다드토바고, 우크라이나, 우간다, 미국, 우즈베키스탄, 베트남, 유고슬라비아, 짐바브웨,

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

EA 유라시아특허 : 아르메니아, 아제르바이잔, 벨라루스, 키르기즈, 카자흐스탄, 몰도바, 러시아, 타지키스탄, 투르크메니스탄,

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

OA OAPI특허 : 부르키나파소, 베넹, 중앙아프리카, 콩고, 코트디브와르, 카메룬, 가봉, 기네, 기네비쏘, 말리, 모리타니, 니제르, 세네갈, 차드, 토고,

(30) 우선권주장	08/924,740	1997년09월05일	미국(US)

(73) 특허권자

인텔 코오퍼레이션
미합중국 캘리포니아 산타클라라 미션 칼리지 블러바드 2200

(72) 발명자

나돈조셉엠
미국오레곤97201포틀랜드컬리지스트리트사우스웨스트1438

맨골드리차드피
미국오레곤97116포레스트그로브캔사스시티로드노스웨스트7155

프포텐하우어조디엘
미국아리조나85284템프워너에스테이트108호이스트1101

시피키이스엘
미국아리조나85226챈들러더블린웨스트3741

오크스미스데이비드더블유
미국오레곤97225포틀랜드레이버로드사우스웨스트6995

말리쥬스키리차드엘

미국오레곤97116포레스트그로브12th에비뉴2218

그라운크게리엘
미국오레곤97008비버튼트레일플레이스사우스웨스트12120

(74) 대리인 최종식
배순자
특허법인 신성
박해천
원석희
정지원

심사관 : 정재헌

(54) 위조방지 방법 및 장치

요약

한 장치에서, 다수의 혼동(obfuscated) 프로그래밍 명령어들은 상기 혼동 프로그래밍 명령어들의 실행이 감시되고 있는지 자체-검증하도록 구비된다. 다른 장치에서, 다수의 혼동 프로그래밍 명령어들은 장치가 상기 혼동 프로그래밍 명령어들의 단일 단계 실행을 지원하는 모드로 동작하고 있는지 판단하도록 구비된다. 또다른 장치에서, 다수의 혼동 프로그래밍 명령어들은 경과된 실행시간의 양이 임계치를 초과했는지 검증하도록 구비된다(단계 154). 또다른 장치에서, 제1 및 제2 위조방지 기법을 각각 구현하기 위해 혼동 프로그래밍 명령어들의 제1 및 제2 그룹이 제공되며, 상기 프로그래밍 명령어들의 제1 및 제2 그룹은 제1 및 제2 위조방지 기법에 대응하는 제1 및 제2 키값을 위해 하나의 저장 위치를 공유한다.

대표도

도 6

색인어

혼동 프로그래밍 명령어, 무결성 검증, 시스템 보안, 위조방지

명세서

기술분야

본 발명은 시스템 보안(system security) 분야에 관한 것이다. 특히, 본 발명은 위조방지(tamper resistant) 방법 및 장치에 관한 것이다.

배경기술

예를 들어, 금융 거래, 부재 권한부여(unattended authorization) 및 콘텐츠 관리와 같은 많은 애플리케이션은 그들의 동작의 기본적인 무결성(basic integrity)이 인정되거나 또는 적어도 검증될 필요가 있다. 비록 이 기술분야에 암호화 및 해독 기술과 같은 다양한 보안 방법이 알려져 있지만, 이러한 보안 방법은 쉽게 손상될 수 있으며, 그 이유는 이들 애플리케이션 및 보안 방법이 개방형의 억세스가능한 아키텍처를 가진 시스템 상에 구현되어, 보안 방법을 포함하는 소프트웨어 및 하드웨어가 모두 부당한 사용자 또는 부당한 프로그램에 의해 감시되고 변경될 수 있기 때문이다.
개방형의 억세스가능한 아키텍처에 기반한 시스템은 보안 방법을 사용함에도 불구하고 근본적으로 안전하지 못한 플랫폼이다. 그러나, 개방성 및 억세스가능성은 다양한 장점을 제공하여, 이러한 시스템의 성공에 기여한다. 그러므로, 이러한 개방성 및 억세스가능성에도 불구하고 이들 근본적으로 안전하지 못한 플랫폼 상에서도 소프트웨어 실행이 실질적으로 감시불가능하거나 변경불가능하게 만드는 기술이 요구된다.

발명의 상세한 설명

발명의 요약
한 장치에서, 다수의 혼동(obfuscated) 프로그래밍 명령어들은 상기 혼동 프로그래밍 명령어들의 실행이 감시되고 있는지 자체-검증하도록 구비된다.
다른 장치에서, 다수의 혼동 프로그래밍 명령어들은 장치가 상기 혼동 프로그래밍 명령어들의 단일 단계 실행을 지원하는 모드로 동작하고 있는지 판단하도록 구비된다.
또다른 장치에서, 다수의 혼동 프로그래밍 명령어들은 경과된 실행시간의 양이 임계치를 초과했는지 검증하도록 구비된다.
또다른 장치에서, 제1 및 제2 위조방지 기법을 각각 구현하기 위해 혼동 프로그래밍 명령어들의 제1 및 제2 그룹이 제공되며, 상기 프로그래밍 명령어들의 제1 및 제2 그룹은 제1 및 제2 위조방지 기법에 대응하는 제1 및 제2 키값을 위해 하나의 저장 위치를 공유한다.

도면의 간단한 설명

본 발명은 첨부도면에 도시된 실시예를 이용하여 설명되며, 도면에서 유사한 참조번호는 유사한 구성요소를 나타낸다.
도1은 본 발명의 다양한 기술사상과 병합된 예시적인 위조방지 모듈의 개요를 도시한 블록도.
도2 및 도3은 본 발명의 무결성 검증 방법의 스타트-업 및 실행시간 동안의 연산 흐름의 일실시예를 도시한 흐름도.
도4는 본 발명의 침입자 검출 방법의 연산 흐름의 일실시예를 도시한 흐름도.
도5 및 도6은 본 발명의 2가지 감시 검출 방법의 연산 흐름의 일실시예를 도시한 흐름도.
도7은 다양한 위조방지 방법을 상호결합하기 위한 본 발명의 결합 기법의 일실시예를 도시한 블록도.
도8은 본 발명의 기술사상을 병합한 스크램블된 콘텐츠를 위한 위조방지 플레이어의 일실시예를 도시한 블록도.
도9는 본 발명을 실시하기에 적합한 컴퓨터 시스템의 일실시예를 도시한 블록도.

실시예

다음의 설명에서는 본 발명의 다양한 관점이 설명된다. 그러나, 이 기술분야 에 통상의 지식을 가진 자는 본 발명의 관점의 전부 또는 단지 일부만 가지고도 본 발명이 실시될 수 있다는 것을 이해할 것이다. 설명목적상, 본 발명의 완전한 이해를 제공하기 위해 특정 번호, 재료 및 구성이 기재되어 있다. 그러나, 이 기술분야에 통상의 지식을 가진 자는 이러한 특정 세부사항 없이도 본 발명이 실시될 수 있다는 것을 이해할 것이다. 다른 예로서, 본 발명을 불명확하게 만들지 않기 위해 공지된 특징들은 생략되거나 간략화된다.
설명의 일부분은 이 기술분야에 통상의 지식을 가진 자에 의해 그 작업의 본질을 다른 통상의 지식을 가진 자에게 전달하기 위해 일반적으로 사용되는 방식에 일치하는, 데이터, 플래그, 비트, 값, 문자, 스트링, 번호 등과 같은 컴퓨터 시스템에 의해 수행되는 연산에 관해 제시된다. 이 기술분야에 통상의 지식을 가진 자에게 잘 이해될 수 있는 바와 같이, 이러한 수량들은 컴퓨터 시스템의 기계적 전기적 구성요소들을 통해 저장, 전송, 조합 또는 조작될 수 있는 전기적, 자기적 또는 광학적 신호의 형태를 가질 수 있으며, 컴퓨터 시스템이란 용어는 독립형, 부속형 또는 내장형이 될 수 있는 범용 및 특수목적 데이터 처리기 또는 시스템을 포함하는 것을 말한다.
본 발명의 이해에 가장 도움이 되는 방식으로 여러 분리된 단계들로서 다양한 연산들이 설명되게 되지만, 그 설명하는 순서가 이들 연산들이 반드시 순서, 특히 제시되는 순서에 의존하는 것을 의미하는 것으로 이해되어서는 안된다.
이제 도1을 참조하면, 본 발명의 다양한 기술사상과 병합된 예시적인 위조방지 모듈의 일실시예의 블록도가 도시되어 있다. 도시된 바와 같이, 예시적인 위조방지 모듈(100)은 비-위조방지부(102)와 위조방지부(104)를 포함하고 있다. 도시된 실시예에 있어서, 이들 2개의 부분은 함께 링크되어 단일의 실행가능한 모듈을 형성한다. 본 출원의 목적을 위해, 용어 "모듈"은 이들 부분 사이의 배타적(exclusive) 통신을 용이하게 하는 다양한 부분들 사이의 구조적 관계를 의미하는 일반적인 의미로 사용된 것이다.
미국 특허 출원 제08/662,679호에 기재된 바와 같이, 비-위조방지부(102)는 예시적인 위조방지 모듈(100)의 민감하지 않은(non-sensitive) 다양한 서비스를 구현하는 다수의 플레인 텍스트 프로그래밍 명령어를 포함하고, 반면에, 위조방지부(104)는 예시적인 위조방지 모듈(100)의 다양한 민감한 서비스를 구현하는 프로그래밍 명령어들의 플레인 텍스트 및 혼동 셀(106)들의 다양한 그룹을 포함한다. 하나의 민감한 서비스 또는 민감한 서비스들의 집합을 구현하는 각각의 셀 그룹은 적어도 하나의 플레인 텍스트 셀(106)을 포함한다. 간단하게 말하면, 서비스와 관련된 비밀(secretes)들이 시간과 공간적으로 분산되어 있으며, 따라서 혼동을 준다. 서비스를 혼동시키기 위해 사용되는 혼동 셀들의 수는 서비스 또는 민감성(sensitivity)에 의존한다. 일반적으로, 더 많은 수의 혼동 셀들이 사용될수록, 그러한 혼동이 해독되기가 더욱 어렵게 된다. 보다 상세한 설명은 미국 특허 출원 제08/662,679호를 참조하자.
부가적으로, 본 발명에 따르면, 플레인 텍스트 및 혼동 셀(106)의 선택된 그룹은 예시적인 위조방지 모듈(100)이 침입받거나 감시되고 있지 않다는 것을 동작중에 검증하기 위해 다수의 위조방지 메저(measures)를 포함한다. 이들 위조방지 메저를 사용하는 그룹의 수와 사용되는 위조방지 메저의 수 및 빈도는 서비스 또는 민감성에 의존한다. 보다 상세하게 후술되는 바와 같이, 이들 위조방지 메저는 다수의 무결성 검증 메저와 다수의 감시방지(anti-observation) 메저를 포함한다. 무결성 검증 메저는 스타트-업 및 실행시간 동안에 비-위조방지부(102)의 무결성을 검증하는 제1 무결성 검증 메저와 플레인 텍스트 및 혼동 셀들의 그룹의 호출이 침입자에 의해 발생된 것이 아니라는 것을 검증하

는 제2 무결성 검증 메저를 포함한다. 감시방지 메저는 모듈(100)을 실행하는 프로세서가 단일 단계 실행을 지원하는 모드로 동작하고 있지 않다는 것을 검증하는 제1 감시방지 메저와 경과된 실행시간이 정상적인 비-감시(unobserved) 실행과 일치한다는 것을 검증하는 제2 감시방지 메저를 포함한다.

도2 및 도3은 제1 무결성 검증 메저의 연산 흐름의 일실시예를 도시하고 있다. 도2는 스타트-업 시간의 연산 흐름을 도시하고, 도3은 실행시간 동안의 연산 흐름을 도시하고 있다. 도2에 도시된 바와 같이, 도시된 실시예에서 스타트-업 시간에 제1 무결성 검증 메저가 포함된 셀 그룹(GOC)은 블록(108)에서 비-위조방지부(102)를 스캐닝하고, 비-위조방지부(102)에 대한 서명(signature)를 계산한다. 다음에, GOC는 블록(110)에서 비-위조방지부(102)에 대해 미리 저장된 서명을 검색한다. 다음에, GOC는 블록(112-114)에서, 생성된 서명을 검증하기 위해 2개의 서명을 비교한다. 만일 생성된 서명이 성공적으로 검증되면, 그것은 비-위조방지부(102)가 변경되지 않았다는 것을 의미하며, GOC는 블록(116)에서 어떠한 검증 의존 연산도 스킵하지 않고 스타트-업 프로세스가 계속되도록 허용하고, 만일 성공적으로 검증되지 않으면, GOC는 블록(118)에서 검증 의존 연산을 스킵하고 스타트-업 프로세스가 계속되도록 한다. 검증 의존 연산의 예로는, 소정의 민감한 서비스를 배달하는데 필요한 비밀을 셋업하는 것과 관련된 연산이 있다.

도3에 도시된 바와 같이, 도시된 실시예에서, 실행시간 동안의 검증 체크 시간에 블록(120)에서 제1 무결성 검증 메저가 병합된 GOC는 비-위조방지부(102)의 다음 부분을 스캐닝하고, 비-위조방지부(102)에 대한 서명을 점증식으로(incrementally) 계산한다. 다음에, GOC는 블록(122)에서 점증식으로 계산된 서명을 갱신한다. 다음에, GOC는 블록(124)에서 비-위조방지부(102)의 끝에 도달했는지 검사한다. 만일 끝에 도달하지 못했으면, 프로세스는 종료되고, 만일 그렇지 않으면, 프로세스는 블록(126)에서 계속된다.

블록(126)에서, GOC는 비-위조방지부(102)에 대해 미리 저장된 서명을 검색한다. 다음에, GOC는 블록(128-130)에서 생성된 서명을 검증하기 위해 2개의 서명을 비교한다. 만일 생성된 서명이 성공적으로 검증되면, 그것은 비-위조방지부(102)가 변경되지 않았다는 것을 의미하며, GOC는 모듈(100)의 실행이 계속될 수 있도록 허용하고, 만일 성공적으로 검증되지 못하면, GOC는 블록(132)에서 모듈(100)의 실행이 종료되도록 한다. 모듈이 종료되도록 하는 것은 이 기술분야에 잘 알려진 방식으로 수행될 수 있다. 애플리케이션에 따라, 비-위조방지부의 무결성 검증 실패 시점으로부터 모듈이 더 이상의 다운스트림을 이행하지 않도록 하는 것이 바람직할 수 있다.

다시 말하면, 실행시간 무결성 체크는 실행중에 여러번의 검증 체크를 통해 점증식으로 수행된다. 이 기술분야에 통상의 지식을 가진 자는 이러한 점증식 방법이 성능에 민감한 서비스에 특히 유용하다는 것을 이해할 것이다. 실행중에 사용되는 검증 체크 횟수는 서비스 또는 민감성에 의존한다.

도4는 제2 무결성 검증 메저의 연산 흐름의 일실시예를 도시하고 있다. 도시된 실시예에서, 호출시에 제2 무결성 검증 메저가 병합된 GOC는 블록(134)에서 그 호출에 대한 리턴 어드레스를 검색한다. 도시된 실시예에서, GOC는 블록(136)에서 그 리턴 어드레스가 모듈(100)의 어드레스 공간내에 있는지 판단한다. 만일 리턴 어드레스가 모듈(100)의 어드레스 공간내에 있으면, 그것은 그 호출이 침입자로부터 발생한 것이 아니라는 것을 의미하며, GOC는 블록(138)에서 모듈(100)의 실행이 계속될 수 있도록 허용하고, 만일 리턴 어드레스가 모듈의 어드레스 공간내에 있지 않으면, GOC는 블록(140)에서 모듈(100)의 실행이 종료되도록 한다. 마찬가지로, 모듈이 종료되도록 하는 것은 이 기술분야에 잘 알려진 여러 가지 방식으로 수행될 수 있다. 애플리케이션에 따라, 침입이 검출되는 시점으로부터 모듈이 더 이상의 다운스트림을 이행하지 못하도록 하는 것이 바람직할 수 있다.

도5는 제1 감시방지 메저의 연산 흐름의 일실시예를 도시하고 있다. 도시된 실시예에서는, 실행 시간 동안의 미리 선택된 시점에서, 제1 감시방지 메저가 병합된 GOC는 블록(142)에서 프로세서 실행 모드 상태 변수를 검색한다. 도시된 실시예에서, GOC는 블록(144)에서 상태 변수가 예를 들어, 디버그 모드(debug mode)와 같이 단일 단계 실행을 지원하는 실행 모드를 나타내는지 판단한다. 만일 상태 변수가 단일 단계 실행을 지원하지 않는 실행 모드를 나타내면, 그것은 모듈(100)의 실 행이 감시되고 있지 않다는 것을 의미하며, GOC는 블록(146)에서 모듈(100)의 실행이 계속될 수 있도록 허용하고, 만일 그렇지 않으면, GOC는 블록(148)에서 모듈(100)의 실행이 종료되도록 한다. 마찬가지로, 모듈의 실행이 종료되도록 하는 것은 이 기술분야에 잘 알려진 여러 가지 방식으로 수행될 수 있다. 애플리케이션에 따라, 감시가 검출되는 시점으로부터 모듈이 더 이상의 다운스트림을 이행하지 못하도록 하는 것이 바람직할 수 있다. 프로세서의 실행 모드가 체크되는 횟수 및 실행 시간 동안의 정확한 시점은 서비스 또는 민감성에 의존한다.

도6은 제2 감시방지 메저의 연산 흐름의 일실시예를 도시하고 있다. 도시된 실시예에 있어서는, 실행시간 동안에 미리 선택된 시점에서, 제2 감시방지 메저가 병합된 GOC는 블록(150)에서 모듈(100)을 실행하는 프로세서로부터 타이머 값을 검색하고, 그 검색된 타이머 값(타임스탬프)을 기록한다. 다음에, GOC는 블록(152)에서 그것이 제공하기 위해 지정된 정상적인 서비스의 수행을 계속한다. 미리 선택된 나중의 시점에서, GOC는 블록(154-156)에서 경과된 실행시간의 양이 소정의 임계치를 초과했는지 판단하기 위해 최종 타임스탬프 이후에 경과된 실행 시간의 양을 체크한다. 만일 경과된 실행시간이 소정의 임계치를 초과하지 않았으면, 그것은 (예를 들어, 브레이크포인트를 설정함으로써) 모듈(100)의 실행이 감시되고 있지 않다는 것을 의미하며, GOC는 블록(158)에서 모듈(100)의 실행이 계속될 수 있도록 허용하고, 만일 그렇지 않으면, GOC는 블록(160)에서 모듈(100)의 실행이 종료되도록 한다. 마찬가지로, 모듈이 종료되도록 하는 것은 이 기술분야에 잘 알려진 여러 가지 방식으로 수행될 수 있다. 애플리케이션에 따라, 감시가 검출되는 시점으로부터 모듈이 더 이상 다운스트림을 이행하지 못하도록 하는 것이 바람직할 수 있다. 최종 타임스탬프 이래로 경과된 실행시간의 양이 체크되는 횟수 및 실행시간 동안의 정확한 시점은 서비스 또는 민감성에 의존한다.

도7은 위조방지 메저를 상호결합시키기 위한 결합 기법의 일실시예를 도시하고 있다. 도시된 바와 같이, 다양한 위조방지 메저와 관련된 키값(key values)에 대해 메저들이 예를 들어 메모리내의 공통 저장 위치를 공유하도록 함으로써 상이한 위조방지 메저들이 상호결합된다. 도시된 실시예에 있어서, GOC는 저장위치(168)의 일부분(162)에 비밀을 검색하기 위한 키를 저장하고, 모듈(100)의 실행이 감시되고 있는지 판단하기 위한 타임스탬프를 저장위치(168)의

더 적은 부분(162)에 저장한다. 경과된 실행시간을 판단하는데 있어서는, GOC는 단지 상기 부분(162) 보다 더 높은 비트만을 사용한다. 부가적으로, GOC는 인증 프로세스에 사용되는 의사난수(pseudo random numbers)를 생성하기 위한 시드(seed)로서 하위 비트(164)를 이용한다. 그러므로, 만일 침입자가 경과된 실행시간 체크 메저를 무력화시키기 위해 타임스탬프를 변경하려고 시도하면, 이것은 인증 프로세스 뿐만 아니라 비밀을 검색하려는 어떠한 시도도 실패하도록 한다. 마찬가지로, 만일 침입자가 인증 프로세스를 무력화시키키기 위해 의사난수를 생성하기 위한 시드를 변경하려고 시도하면, 이것은 경과된 실행시간 체크 뿐만 아니라 비밀을 검색하기 위한 어떠한 시도도 실패하도록 한다.

도8은 본 발명의 위조방지 기술을 적용한 스크램블된 콘텐츠를 위한 위조방지 플레이어의 일실시예를 도시하고 있다.

도시된 일실시예에 있어서, 위조방지 플레이어(172)는 비-위조방지 구성요소(171)와 위조방지 디코더(172)를 포함한다. 위조방지 구성요소(171)는 최종 사용자 인터페이스와 같은 일반적인 서비스 구성요소의 넓은 범주를 나타내도록 의도된 것이다. 이러한 일반적인 서비스 구성요소는 이 기술분야에 잘 알려진 다양한 기술중 하나를 이용하여 구현되는 다양한 서비스중 하나를 제공할 수 있다. 위조방지 디코더(172)는 스크램블된 압축 콘텐츠를 수신하고, 그에 응답하여, 예를 들어 YUV 비디오 및 AC3 오디오와 같은 콘텐츠를 렌더링하기 위한 적절한 신호를 출력하기 위해 콘텐츠를 디스크램블 및 압축해제한다.

위조방지 디코더(172)는 비-위조방지부(175)와 위조방지부(174,176,178,180) 및 비-위조방지부(175)를 위한 서명(173)을 포함한다. 비-위조방지부(175)는 플레인 텍스트 프로그래밍 명령어로 구성되고, 반면에, 위조방지부(174,176,178,180)는 프로그래밍 명령어들의 플레인 텍스트 및 혼동 셀들의 복수의 그룹으로 구성된다. 서명(173)을 포함하여, 비-위조방지부(175)와 위조방지부(174,176,178,180)는 이들 부분들 사이의 배타적 통신을 용이하게 하도록 구조적으로 관련되어 있다. 도시된 실시예에서는, 2개의 부분이 단일 실행가능 모듈로서 함께 링크되어 있다.

비-위조방지부(175)는 플레이어(170) 및 스크램블된 콘텐츠 공급자 장치가 서로에 대해 상호 인증되도록 하는 것을 포함하여, 스크램블된 콘텐츠의 디스크램블링을 달성하기 위해 통합된 위조방지부(174,176,178,180)의 서비스를 호출한다. 비-위조방지부(175)는 전술한 출력신호를 생성하기 위해 스크램블되지 않은 압축 콘텐츠를 압축해제한다.

서명(173)은 전술한 바와 같이 스타트-업 시간 및 실행시간 무결성 검증을 용이하게 하기 위해 소정의 위치에 미리 저장된다.

도시된 실시예에서, 위조방지부(172)의 위조방지 서비스는 스크램블된 콘텐츠를 수신하고 그에 응답하여 디코더(172)의 비-위조방지부를 위한 디스크램블된 콘텐츠를 생성하기 위해 상기 스크램블된 콘텐츠를 디스크램블하기 위한 위조방지 디스크램블러(174)를 포함한다. 일실시예에서, 위조방지 디스크램블러(174)는 스크램블된 콘텐츠를 디스크램블하기 위해 위조방지 비밀 홀더(180)로부터 검색되는 비밀키를 사용한다. 사용되는 비밀키의 수와 이들 키의 특성은 애플리케이션에 따라 다르며, 이것들은 본 발명을 이해하는데 있어 필수적인 것은 아니다. 위조방지 디스크램블러(174)는 프로그램 명령어들의 플레인 텍스트 및 혼동 셀로된 하나의 그룹으로 구성된다. 일실시예에서, 코어 디스크램블링 서비스는 향상된 성능을 제공하기 위해 플레인 텍스트 셀에 배치된다. 일실시예에서, GOC는 전술한 침입자 검출 무결성 검증 메저와 단일 단계 실행 모드 검출 감시방지 메저를 갖추고 있다. 일실시예에서, GOC는 또한, 경과 실행시간 검출 감시방지 메저를 갖추고 있다. 일실시예에서, GOC는 복수의 경과 실행시간 검출 감시방지 메저를 갖추고 있다. 일실시예에서, 경과 실행시간 검출 감시방지 메저는 스크램블된 콘텐츠를 디스크램블하는 것과 관련된 비밀키를 검색하기 위한 프로세스와, 플레이어(170)와 스크램블된 콘텐츠 공급자 장치를 상호 인증하기 위한 인증 프로세스와 상호결합된다.

도시된 실시예에서, 위조방지 디코더(172)의 위조방지 서비스는 스크램블된 콘텐츠 공급자 장치에 대해 위조방지 플레이어(170)를 인증시키고, 위조방지 플레이어(170)에 대해 스크램블된 콘텐츠 공급자 장치를 인증시키기 위한 위조방지 인증기(176)를 포함한다. 일실시예에서, 위조방지 인증기(176)는 인증 프로세스를 행하기 위해 위조방지 비밀 홀더(180)로부터 검색되는 비밀키를 사용한다. 사용되는 비밀키의 수와 이들 키의 특성은 애플리케이션에 따라 다르며, 이것들이 본 발명을 이해하는데 있어 필수적인 것은 아니다. 일실시예에서, 위조방지 인증기(176)는 프로그래밍 명령어들의 플레인 텍스트 및 혼동 셀들로된 하나의 그룹으로 구성된다. 일실시예에서, GOC는 전술한 침입자 검출 무결성 검증 메저와 단일 단계 실행 모드 검출 감시방지 메저를 갖추고 있다. 일실시예에서, GOC는 또한, 경과 실행시간 검출 감시방지 메저를 갖추고 있다. 일실시예에서, GOC는 복수의 경과 실행시간 검출 감시방지 메저를 갖추고 있다. 일실시예에서, 경과 실행시간 검출 감시방지 메저는 스크램블된 콘텐츠를 디스크램블하는 것과 관련된 비밀키를 검색하기 위한 프로세스와, 플레이어(170)와 스크램블된 콘텐츠 공급자 장치를 상호 인증하기 위한 인증 프로세스와 상호결합된다.

도시된 실시예에서, 위조방지 디코더(172)의 위조방지 서비스는 스타트-업 시간 및 실행시간 동안에 디코더(172)의 비-위조방지부를 무결성 검증하기 위한 위조방지 무결성 검증기(178)를 포함한다. 일실시예에서, 위조방지 무결성 검증기(178)는 비밀 홀더(180)에 대해 플레이어(170)와 스크램블된 콘텐츠 공급자 장치를 상호 인증시키기 위해 사용될 비밀키를 제공한다. 사용되는 비밀키의 수와 이들 키의 특성은 애플리케이션에 따라 다르며, 이것들이 본 발명을 이해하는데 있어 필수적인 것은 아니다. 일실시예에서, 위조방지 무결성 검증기(178)는 프로그래밍 명령어들의 플레인 텍스트 및 혼동 셀들로된 하나의 그룹으로 구성된다. 일실시예에서, GOC는 단일 단계 실행 모드 검출 감시방지 메저를 갖추고 있다. 일실시예에서, GOC는 또한, 경과 실행시간 검출 감시방지 메저를 갖추고 있다. 일실시예에서, GOC는 복수의 경과 실행시간 검출 감시방지 메저를 갖추고 있다. 일실시예에서, 경과 실행시간 검출 감시방지 메저는 스크램블된 콘텐츠를 디스크램블하는 것과 관련된 비밀키를 검색하기 위한 프로세스와, 플레이어(170)와 스크램블된 콘텐츠 공급자 장치를 상호 인증하기 위한 인증 프로세스와 상호결합된다.

마지막으로, 도시된 실시예에 있어서, 위조방지 디코더(172)의 위조방지 서비스는 스크램블된 콘텐츠를 디스크램블하는 것과 관련된 비밀을 저장하기 위한 위조방지 비밀 홀더(180)를 포함한다. 이 비밀 홀더(180)는 스크램블된 콘텐츠 공급자 장치에 대해 위조방지 플레이어(170)를 인증시키고 위조방지 플레이어(170)에 대해 스크램블된 콘텐츠 공

급자 장치를 인증시키기 위한 인증 프로세스와 관련된 비밀을 저장한다. 일실시예에서, 위조방지 비밀 홀더(180)는 셀 어레이 형태로 프로그래밍 명령어들의 플레인 텍스트 및 혼동 셀들로된 하나의 그룹으로 구성된다. 일실시예에서, GOC는 전술한 침입자 검출 무결성 검증 메저와 단일 단계 실행 모드 검출 감시방지 메저를 갖추고 있다. 일실시예에서, GOC는 또한, 경과 실행시간 검출 감시방지 메저를 갖추고 있다. 일실시예에서, GOC는 복수의 경과 실행시간 검출 감시방지 메저를 갖추고 있다.

그러므로, 플레이어(170)가 "개방형" 버스를 통해 그 콘텐츠 입력을 수신하는 경우 조차도, 그 콘텐츠가 보호되며, 그 이유는 콘텐츠가 스크램블된 형태로 "개방형" 버스를 통해 플레이어(170)로 제공되기 때문이다. 또한, 스크램블된 콘텐츠를 디스크램블하는 것과 관련된 비밀과 이러한 디스크램블을 수행하는 프로그래밍 명령어도 침입과 감시로부터 보호된다. 아직까지 코어 디스크램블링 서비스와 같은 성능에 민감한 연산들에는 부담이 주어지지 않았다. 마지막으로, 위조방지 서비스, 예를 들어, 디스크램블러(174), 인증기(176) 등은 고도로 이식가능하며, 다수의 디코더 구현예와 링크될 수 있다.

도9는 본 발명을 실시하는데 적합한 컴퓨터 시스템의 일실시예를 도시하고 있다. 도시된 실시예에서, 컴퓨터 시스템(200)은 프로세서(202), 프로세서 버스(206), 고성능 I/O 버스(210) 및 표준 I/O 버스(220)를 포함하고 있다. 프로세서 버스(206)와 고성능 I/O 버스(210)는 호스트 브릿지(208)에 의해 브릿지되어 있으며, 반면에, I/O 버스들(210,220)은 I/O 버스 브릿지(212)에 의해 브릿지되어 있다. 프로세서 버스(206)에는 캐시(204)가 연결되어 있다. 고성능 I/O 버스(210)에는 시스템 메모리(214)와 비디오 메모리(216)가 연결되어 있고, 비디오 메모리(216)에는 비디오 디스플레이(218)가 연결되어 있다. 표준 I/O 버스(220)에는 디스크 드라이브(222), 키보드 및 포인팅 장치(224) 및 DVD_ROM(226)이 연결되어 있다.

이들 구성요소는 이 기술분야에 알려진 그들의 통상적인 기능을 수행한다. 특히, 디스크 드라이브(222)와 시스템 메모리(214)는 프로세서(202)에 의해 실행될 때 본 발명의 위조방지 애플리케이션의 영구적인 카피 및 작업용 카피를 저장하기 위해 사용된다. 영구적인 카피는 공장에서 디스크 드라이브(222)로 사전에 로딩되거나, 분배 매체(도시 안됨)로부터 로딩되거나, 또는 온라인/네트워크 분배 소스(도시 안됨)로부터 다운로드될 수 있다. 이들 구성요소의 구성은 알려져 있다. 이 기술분야에 알려진 이들 구성요소의 다수의 구현예중 어느 것이라도 컴퓨터 시스템(200)을 구성하기 위해 사용될 수 있다.

물론, 본 발명을 실시하기 위해 대안의 아키텍처의 컴퓨터 시스템을 포함하여 대안의 구성을 가진 컴퓨터 시스템도 역시 사용될 수 있다.

일반적으로, 본 발명이 전술한 실시예에 관해 설명되었지만, 이 기술분야에 통상의 지식을 가진 자는 본 발명이 설명된 실시예들에 제한되지 않는 다는 것을 이해할 것이다. 본 발명은 첨부된 청구범위의 사상 및 범위내에서 수정 및 변경이 이루어질 수 있다. 그러므로, 전술한 설명은 본 발명을 제한하고자 하는 것이 아니라 예시적인 것으로 간주되어야 한다. 지금까지 다양한 위조방지 방법 및 장치에 관해 설명되었다.

(57) 청구의 범위

청구항 1.

위조를 감시(monitor tampering)하기 위한 장치에 있어서,
다수의 혼동(obfuscated) 프로그래밍 명령어들의 실행이 감시되고 있는지 자체-검증하도록 설계된 다수의 혼동 프로그래밍 명령어 셀들을 저장하고 있는 저장 매체; 및
상기 저장 매체에 연결되어 상기 프로그래밍 명령어들을 실행하기 위한 실행 유닛
을 포함하고,
상기 혼동 셀은 셀간 종속 변환 프로세스(inter-cell dependent mutation process)를 통해 변환되고,
상기 다수의 혼동 프로그램 명령어 셀들은 경과된 실행시간의 양이 임계치를 초과했는지 검증하도록 설계된 혼동 프로그래밍 명령어 셀들을 포함하는
위조 감시 장치.

청구항 2.

제 1 항에 있어서,
상기 다수의 혼동 프로그램 명령어 셀들은 상기 장치가 상기 혼동 프로그래밍 명령어 셀들의 단일 단계 실행을 지원하는 모드로 동작되고 있는지 판단하도록 설계된 혼동 프로그래밍 명령어 셀들을 포함하는
위조 감시 장치.

청구항 3.

제 2 항에 있어서,
상기 다수의 혼동 프로그램 명령어 셀들은 상기 단일 단계 실행 지원 판단을 수행하기 위해 상기 장치의 상태 변수에 억세스하도록 설계된 혼동 프로그래밍 명령어 셀들을 포함하는
위조 감시 장치.

청구항 4.

삭제

청구항 5.

제 1 항에 있어서,
상기 다수의 혼동 프로그램 명령어 셀들은 기록된 타임스탬프에 기반하여 상기 경과된 실행시간의 양을 계산하도록

설계된 혼동 프로그래밍 명령어 셀들을 더 포함하는
위조 감시 장치.

청구항 6.

제 5 항에 있어서,
상기 다수의 혼동 프로그램 명령어 셀들은 상기 장치의 타이머의 현재값을 검색하고 상기 타이머의 검색된 현재값을 기록된 타임스탬프로서 저장하도록 설계된 혼동 프로그래밍 명령어 셀들을 더 포함하는
위조 감시 장치.

청구항 7.

제 6 항에 있어서,
상기 타이머의 검색된 현재값을 기록된 타임스탬프로서 저장하도록 설계된 상기 혼동 프로그래밍 명령어 셀들은 적어도 하나의 다른 위조방지 기법에 의해 공유되는 저장 위치에 상기 검색된 현재값을 저장하는
위조 감시 장치.

청구항 8.

위조를 감시(monitor tampering)하기 위한 방법에 있어서,
(a) 다수의 혼동 프로그래밍 명령어 셀들을 실행하는 단계 - 여기서, 상기 혼동 셀들은 셀간 종속 변환 프로세스를 통해 변환됨 - ;
(b) 상기 실행이 감시되고 있지 않다는 것을 상기 다수의 혼동 프로그래밍 명령어 셀들에 의해 자체-검증하는 단계; 및
(c) 상기 단계 (b)에서 상기 실행이 감시되고 있는 것으로 검증되면 상기 단계 (a)의 실행을 종료시키는 단계
를 포함하고,
상기 단계 (b)는 경과된 실행시간의 양이 임계치를 초과했는지 검증하는 단계를 포함하는
위조 감시 방법.

청구항 9.

제 8 항에 있어서,
상기 단계 (b)는 상기 다수의 혼동 프로그래밍 명령어 셀들이 단일 단계 실행을 지원하는 모드로 실행되고 있는지 판단하는 단계를 포함하는
위조 감시 방법.

청구항 10.

제 9 항에 있어서,
상기 단계 (b)는 상기 다수의 혼동 프로그래밍 명령어 셀들이 상기 단일 단계 실행 지원 판단을 수행하기 위해 상태 변수에 억세스하는 단계를 포함하는
위조 감시 방법.

청구항 11.

삭제

청구항 12.

제 8 항에 있어서,
상기 단계 (b)는 기록된 타임스탬프에 기반하여 상기 경과된 실행시간의 양을 계산하는 단계를 포함하는
위조 감시 방법.

청구항 13.

제 12 항에 있어서,
상기 단계 (b)는 타이머의 현재값을 검색하고, 상기 타이머의 검색된 현재값을 기록된 타임스탬프로서 저장하는 단계를 더 포함하는
위조 감시 방법.

청구항 14.

제 13 항에 있어서,
상기 단계 (b)는 다른 위조방지 기법에 의해 공유되는 저장 위치에 상기 검색된 현재값을 저장하는 단계를 포함하는
위조 감시 방법.

청구항 15.

삭제

청구항 16.

삭제

청구항 17.

삭제

청구항 18.

삭제

청구항 19.

위조를 감시(monitor tampering)하기 위한 장치에 있어서,

경과된 실행시간의 양이 임계치를 초과했는지 검증하도록 설계된 다수의 혼동(obfuscated) 프로그래밍 명령어 셀들을 저장하고 있는 저장 매체; 및
상기 저장 매체에 연결되어 상기 프로그래밍 명령어들을 실행하기 위한 실행 유닛
을 포함하고,
상기 혼동 셀은 셀간 종속 변환 프로세스를 통해 변환되고,
상기 다수의 혼동 프로그램 명령어 셀들은 기록된 타임스탬프에 기반하여 상기 경과된 실행시간의 양을 계산하도록 설계된 혼동 프로그래밍 명령어 셀들을 포함하는
위조 감시 장치.

청구항 20.

삭제

청구항 21.

제 19 항에 있어서,
상기 다수의 혼동 프로그램 명령어 셀들은 상기 장치의 타이머의 현재값을 검색하고 상기 타이머의 검색된 현재값을 기록된 타임스탬프로서 저장하도록 설계된 혼동 프로그래밍 명령어 셀들을 더 포함하는
위조 감시 장치.

청구항 22.

제 21 항에 있어서,
상기 타이머의 검색된 현재값을 기록된 타임스탬프로서 저장하도록 설계된 혼동 프로그래밍 명령어 셀들은 적어도 하나의 다른 위조방지 기법에 의해 공유되는 저장 위치에 상기 검색된 현재값을 저장하는
위조 감시 장치.

청구항 23.

위조를 감시(monitor tampering)하기 위한 방법에 있어서,
(a) 다수의 혼동 프로그래밍 명령어 셀들을 실행하는 단계;
(b) 경과된 실행시간의 양이 임계치를 초과했는지 검증하는 단계; 및
(c) 상기 단계 (b)에서 상기 실행이 감시되고 있는 것으로 검증되면 상기 단계 (a)의 실행을 종료시키는 단계
를 포함하고,
상기 혼동 셀은 셀간 종속 변환 프로세스를 통해 변환되고,
상기 단계 (b)는 기록된 타임스탬프에 기반하여 상기 경과된 실행시간의 양을 계산하는 단계를 포함하는
위조 감시 방법.

청구항 24.

삭제

청구항 25.

제 23 항에 있어서,
상기 단계 (b)는 타이머의 현재값을 검색하고 상기 타이머의 검색된 현재값을 기록된 타임스탬프로서 저장하는 단계를 더 포함하는
위조 감시 방법.

청구항 26.

제 25 항에 있어서,
상기 단계 (b)는 다른 위조방지 기법에 의해 공유되는 저장 위치에 상기 검색된 현재값을 저장하는 단계를 포함하는
위조 감시 방법.

청구항 27.

제1 감시방지(anti-observation) 위조방지 기법과 감시검출 위조방지 기법을 각각 구현하도록 설계된 제1 및 제2 다수의 혼동(obfuscated) 프로그래밍 명령어 셀들을 저장하고 있는 저장 매체; 및
상기 저장 매체에 연결되어 상기 프로그래밍 명령어들을 실행하기 위한 실행 유닛
을 포함하고,
상기 제1 및 제2 다수의 혼동 프로그래밍 명령어 셀들은 상기 제1 감시방지 및 감시검출 위조방지 기법들에 대응하는 제1 및 제2 키값을 위해 하나의 저장 위치를 공유하고,
상기 혼동 셀은 셀간 종속 변환 프로세스를 통해 변환되며,
상기 제1 다수의 혼동 프로그램 명령어 셀들은 키-기반 비밀 검색 기법을 구현하도록 설계되고, 상기 제2 다수의 혼동 프로그래밍 명령어 셀들은 경과된 실행시간의 양이 임계치를 초과하지 않았다는 것을 검증하도록 설계된
장치.

청구항 28.

삭제

청구항 29.

제 27 항에 있어서,
상기 저장 매체는 제2 감시방지(anti-observation) 위조방지 기법을 구현하도록 설계된 제3 다수의 혼동 프로그래밍 명령어 셀들 - 여기서, 상기 제3 다수의 혼동 프로그래밍 명령어 셀들은 상기 제2 감시방지(anti-observation) 위조방지 기법에 대응하는 제3 키값을 위해 동일한 저장 위치를 공유함 - 을 더 저장하고 있는

장치.

청구항 30.

제 29 항에 있어서,

상기 제1 다수의 혼동 프로그램 명령어 셀들은 키-기반 비밀 검색 기법을 구현하도록 설계되고, 상기 제2 다수의 혼동 프로그래밍 명령어 셀들은 경과된 실행시간의 양이 임계치를 초과하지 않았다는 것을 검증하도록 설계되고, 상기 제3 다수의 혼동 프로그래밍 명령어 셀들은 인증 프로세스를 구현하도록 설계된

장치.

청구항 31.

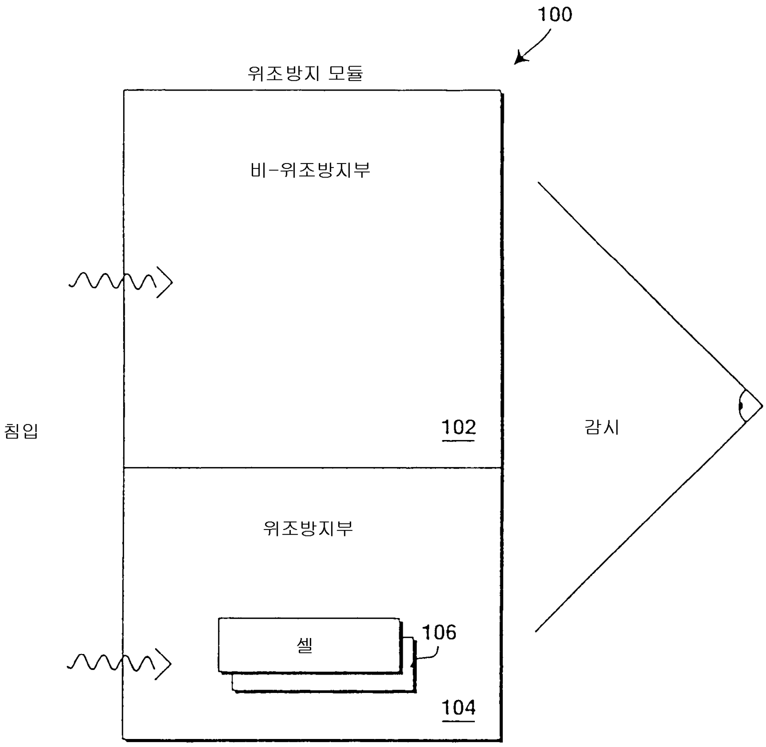
삭제

청구항 32.

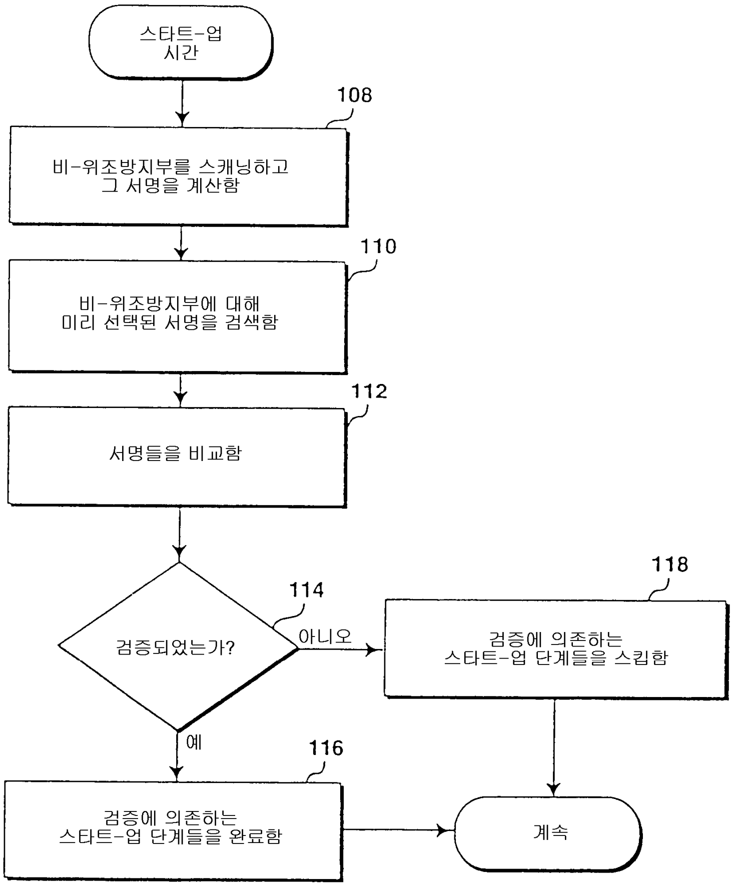
삭제

도면

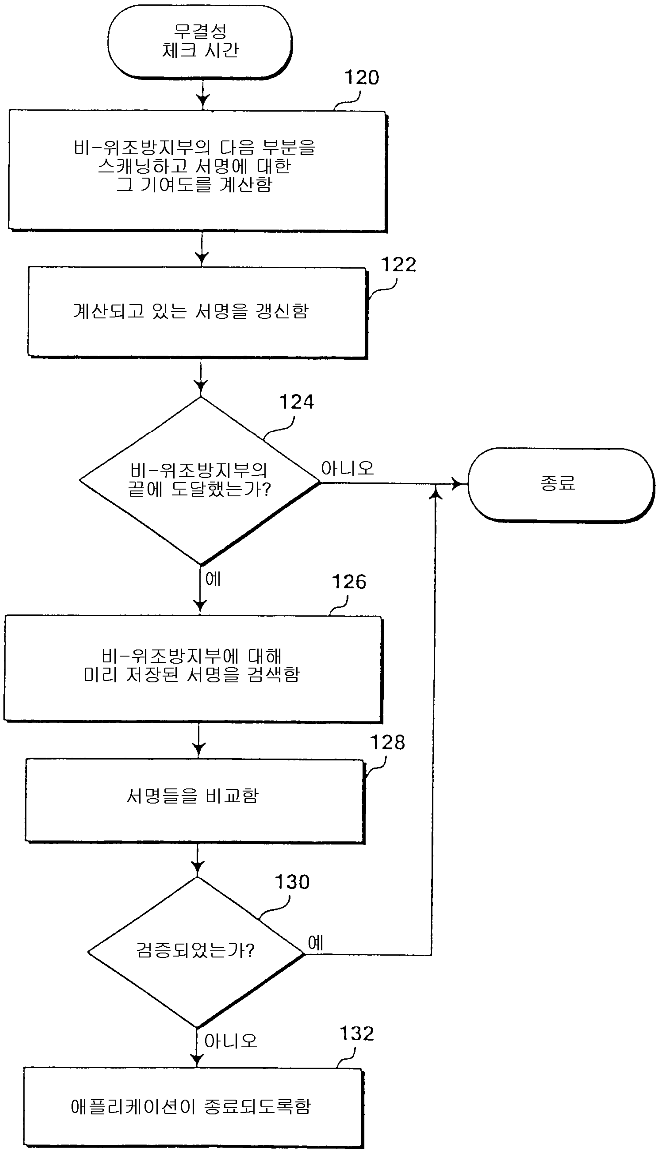
도면1


100
위조방지 모듈
비-위조방지부
102
침입
감시
위조방지부
셀
106
104

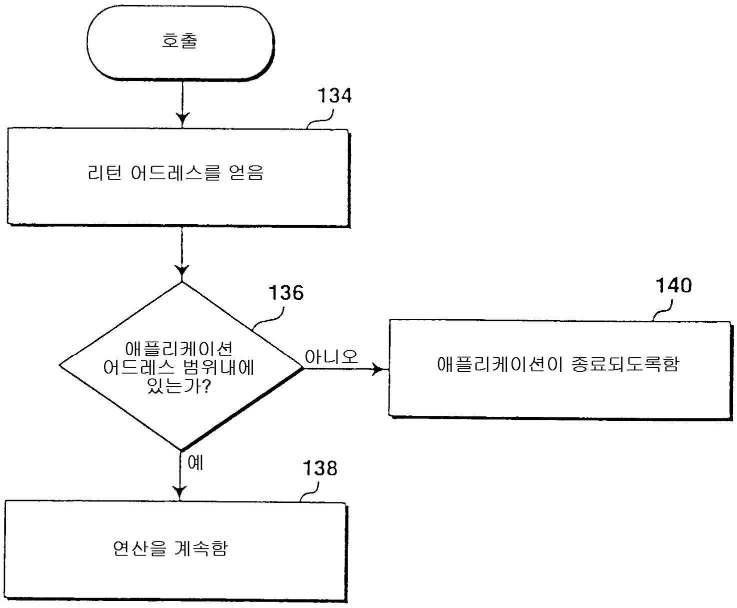
도면2


스타트-업 시간
108
비-위조방지부를 스캐닝하고 그 서명을 계산함
110
비-위조방지부에 대해 미리 선택된 서명을 검색함
112
서명들을 비교함
114
검증되었는가?
아니오
118
검증에 의존하는 스타트-업 단계들을 스킵함
예
116
검증에 의존하는 스타트-업 단계들을 완료함
계속

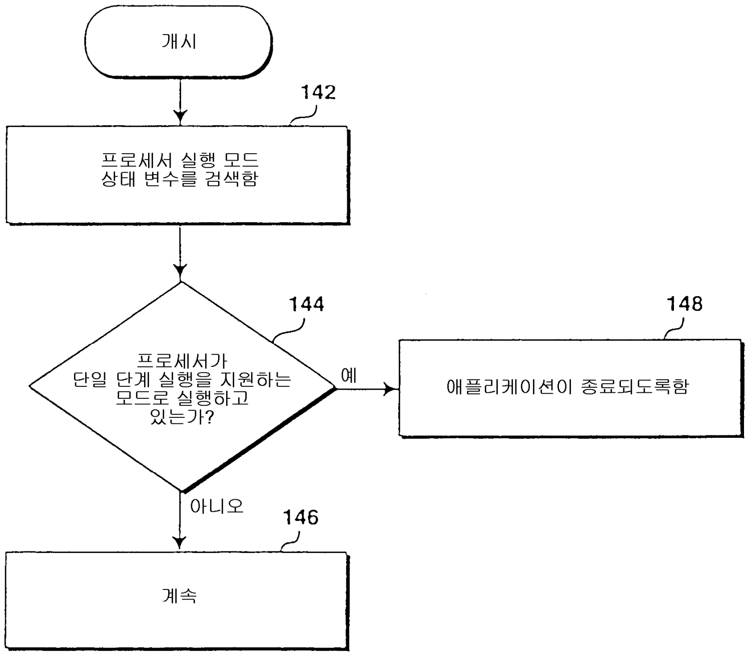
도면3


무결성
체크 시간
120
비-위조방지부의 다음 부분을
스캐닝하고 서명에 대한
그 기여도를 계산함
122
계산되고 있는 서명을 갱신함
124
비-위조방지부의
끝에 도달했는가?
아니오
종료
예
126
비-위조방지부에 대해
미리 저장된 서명을 검색함
128
서명들을 비교함
130
검증되었는가?
예
아니오
132
애플리케이션이 종료되도록함

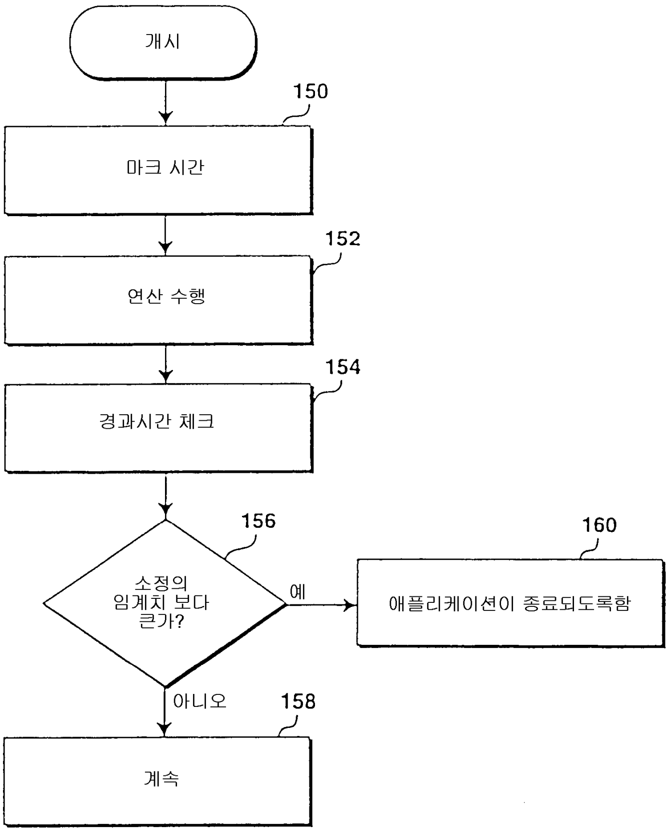
도면4


호출
134
리턴 어드레스를 얻음
136
애플리케이션
어드레스 범위내에
있는가?
아니오
140
애플리케이션이 종료되도록함
예
138
연산을 계속함

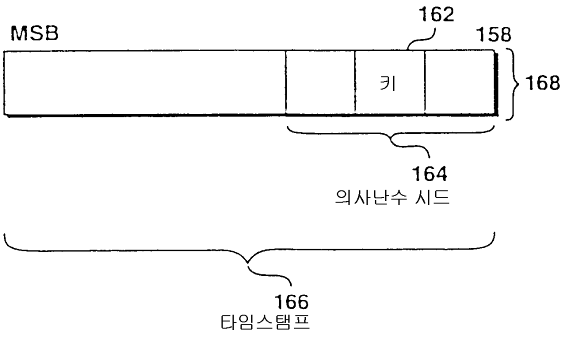
도면5


개시
142
프로세서 실행 모드 상태 변수를 검색함
144
프로세서가 단일 단계 실행을 지원하는 모드로 실행하고 있는가?
예
148
애플리케이션이 종료되도록함
아니오
146
계속

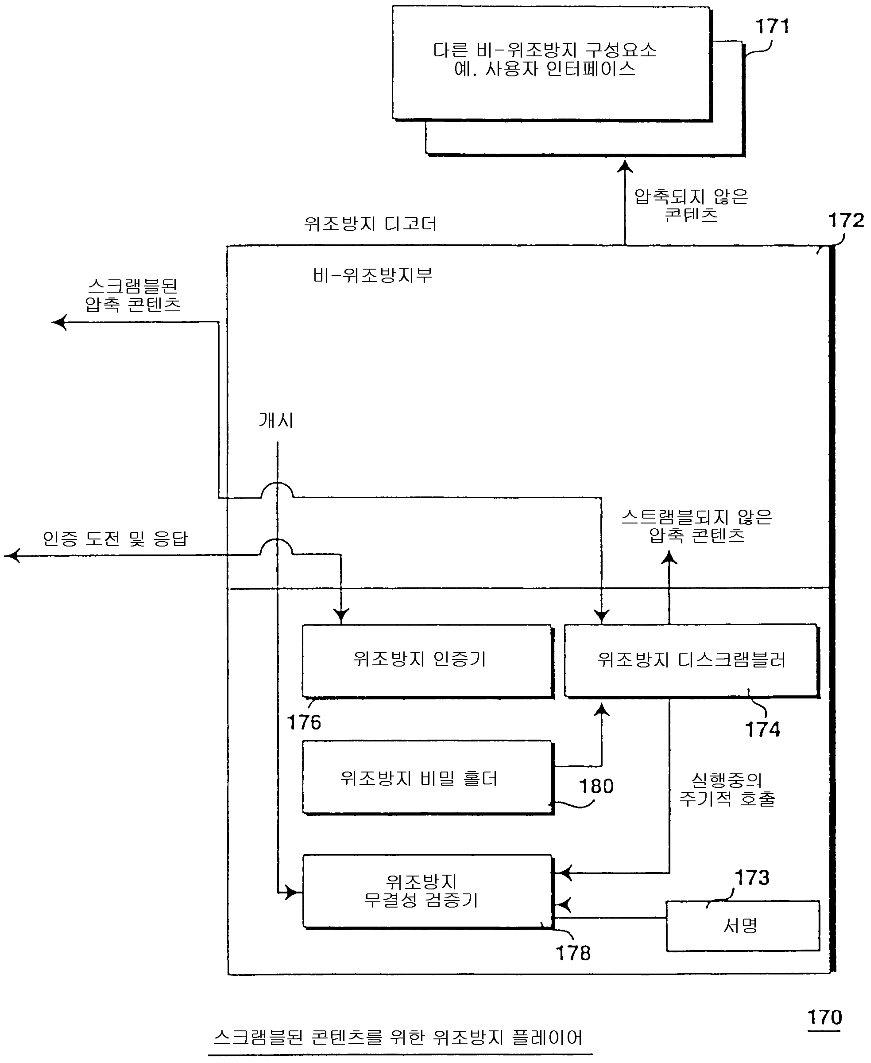
도면6


개시
150
마크 시간
152
연산 수행
154
경과시간 체크
156
소정의 임계치 보다 큰가?
예
160
애플리케이션이 종료되도록함
아니오
158
계속

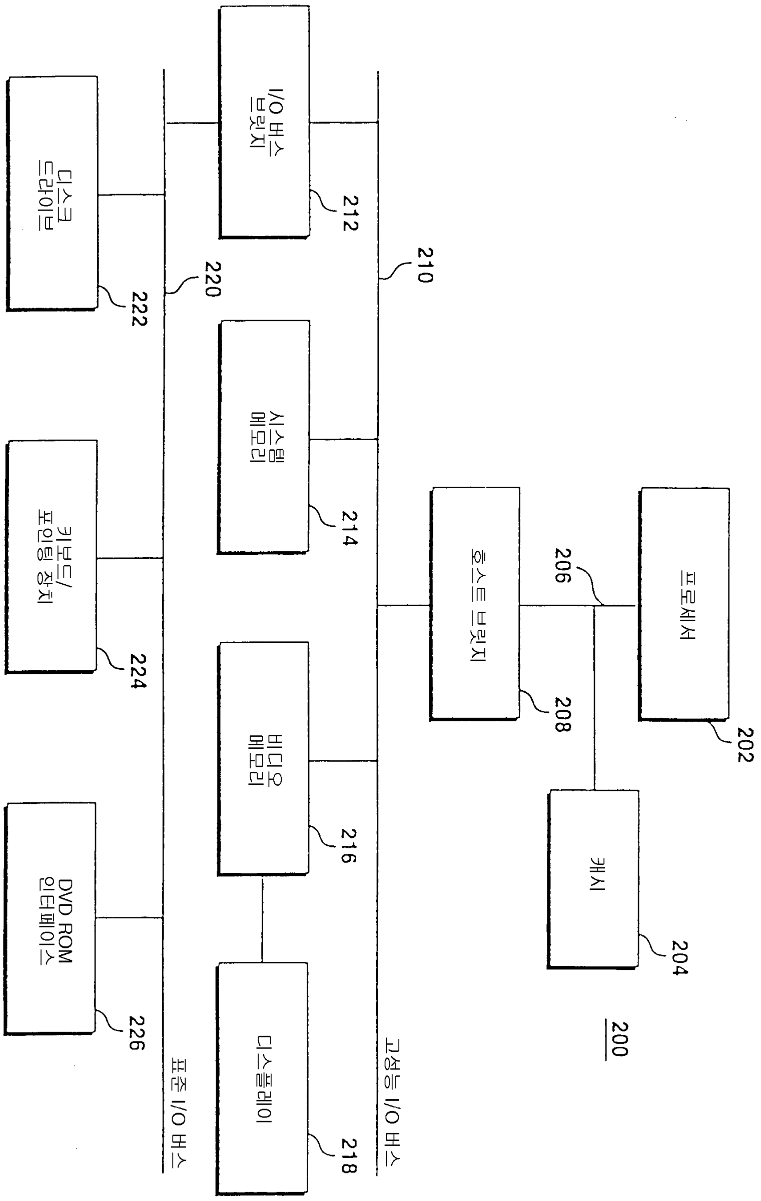
도면7


MSB
162
158
키
168
164
의사난수 시드
166
타임스탬프

도면8


다른 비-위조방지 구성요소
예. 사용자 인터페이스
171
압축되지 않은
콘텐츠
위조방지 디코더
172
비-위조방지부
스크램블된
압축 콘텐츠
개시
인증 도전 및 응답
스트램블되지 않은
압축 콘텐츠
위조방지 인증기
위조방지 디스크램블러
176
174
위조방지 비밀 홀더
180
실행중의
주기적 호출
위조방지
무결성 검증기
173
서명
178
170
스크램블된 콘텐츠를 위한 위조방지 플레이어

도면9


I/O 버스 브릿지
212
210
시스템 메모리
214
호스트 브릿지
206
208
프로세서
202
비디오 메모리
216
캐시
204
디스플레이
218
고성능 I/O 버스
200
디스크 드라이브
222
220
키보드/ 포인팅 장치
224
DVD ROM 인터페이스
226
표준 I/O 버스