(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년06월01일
(11) 등록번호 10-1626439
(24) 등록일자 2016년05월26일

(51) 국제특허분류(Int. Cl.)
G06F 21/50 (2013.01) *G06F 11/30* (2006.01)
(21) 출원번호 10-2013-7016393
(22) 출원일자(국제) 2011년12월13일
심사청구일자 2013년06월24일
(85) 번역문제출일자 2013년06월24일
(65) 공개번호 10-2013-0096311
(43) 공개일자 2013년08월29일
(86) 국제출원번호 PCT/US2011/064729
(87) 국제공개번호 WO 2012/087685
국제공개일자 2012년06월28일
(30) 우선권주장
12/978,043 2010년12월23일 미국(US)
(56) 선행기술조사문헌
KR1020060033980 A*
US20100011029 A1*
US20100313270 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인텔 코포레이션
미합중국 캘리포니아 95054 산타클라라 미션 칼리지 블러바드 2200
(72) 발명자
푸르나찬드란, 라제쉬
미국 97006 오레곤주 비버톤 에이피티 넘버 210 노쓰웨스트 슈미트 웨이 2408
아이씨, 셀림
미국 97007 오레곤주 비버톤 사우쓰웨스트 168번 플레이스 6870
(74) 대리인
양영준, 백만기

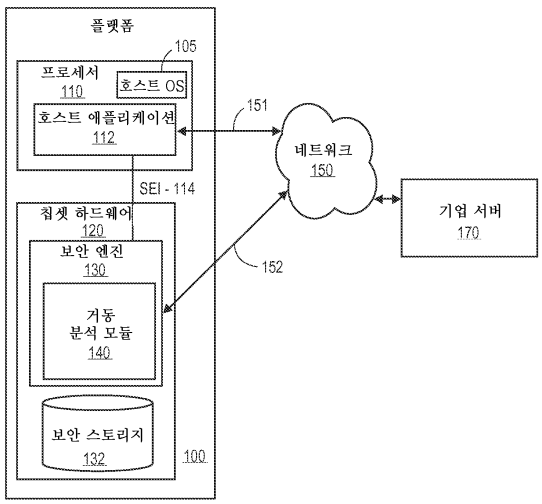
전체 청구항 수 : 총 18 항 심사관 : 서광훈

(54) 발명의 명칭 **서명-독립적 시스템 거동 기반 멀웨어 검출**

(57) 요 약

시스템 거동에 기초하여 멀웨어를 검출하기 위한 방법, 시스템, 및 컴퓨터 프로그램 제품이 기술된다. 활성일 것으로 예상된 적어도 하나의 프로세스가 하나의 또는 그 이상의 리소스들을 포함하는 프로세싱 시스템의 현재 동작 모드에서 식별된다. 현재 동작 모드 및 활성일 것으로 예상된 적어도 하나의 프로세스에 기초하여, 프로세싱 시스템의 하나의 또는 그 이상의 리소스들의 예상 활동 레벨이 계산된다. 복수의 리소스의 실제 활동 레벨이 결정된다. 예상 활동 레벨 및 실제 활동 레벨 간에 편차가 검출되면, 편차의 잠정적인 원인으로서 예상치 못한 활동의 소스가 식별된다. 예상치 못한 활동이 적법한지를 결정하기 위해 정책 가이드라인들이 사용된다. 예상치 못한 활동이 적법하지 않으면, 예상치 못한 활동의 소스가 멀웨어로서 분류된다.

대 표 도 - 도1



명 세 서

청구범위

청구항 1

컴퓨터 구현 방법으로서,

보안 엔진에 의해, 메인 프로세서 및 배터리를 포함하는 하나의 또는 그 이상의 리소스들을 포함하는 프로세싱 시스템의 현재 플랫폼 동작 모드에서 상기 프로세싱 시스템의 호스트 운영 체제의 명령에 의해 활성일 것으로 예상된 적어도 하나의 프로세스를 식별하는 단계 - 상기 보안 엔진은 상기 프로세싱 시스템의 상기 메인 프로세서와는 독립하여 동작함 -;

상기 보안 엔진에 의해, 상기 현재 플랫폼 동작 모드 및 상기 활성일 것으로 예상된 적어도 하나의 프로세스에 기초하여 상기 메인 프로세서의 예상 프로세서 주파수 및 상기 배터리의 예상 배터리 소모 레벨을 포함하는 상기 프로세싱 시스템의 상기 하나의 또는 그 이상의 리소스들의 예상 활동 레벨을 계산하는 단계;

상기 보안 엔진에 의해, 상기 프로세싱 시스템의 상기 메인 프로세서의 프로세서 주파수 및 상기 배터리의 배터리 소모 레벨을 포함하는 상기 하나의 또는 그 이상의 리소스들의 실제 활동 레벨을 결정하는 단계;

상기 예상 활동 레벨과 상기 실제 활동 레벨 간에 편차가 검출되면, 상기 보안 엔진에 의해, 상기 편차의 잠정적인 원인인 예상치 못한 활동의 소스로서 예상치 못한 활성인 프로세스 및 상기 예상치 못한 활성인 프로세스에 대응하는 애플리케이션을 식별하는 단계;

상기 보안 엔진에 의해, 정책 가이드라인들을 사용해서 상기 예상치 못한 활동이 적법한지를 결정하는 단계;

상기 예상치 못한 활동이 적법하지 않으면, 상기 보안 엔진에 의해, 상기 예상치 못한 활동의 상기 소스를 멀웨어로서 분류하는 단계;

상기 보안 엔진에 의해, 상기 프로세싱 시스템의 상기 현재 플랫폼 동작 모드의 새로운 플랫폼 동작 모드로의 변경을 식별하는 단계;

상기 보안 엔진에 의해, 상기 새로운 플랫폼 동작 모드에서 상기 프로세싱 시스템의 상기 호스트 운영 체제의 명령에 의해 활성일 것으로 예상된 제2의 적어도 하나의 프로세스를 식별하는 단계; 및

상기 보안 엔진에 의해, 상기 새로운 플랫폼 동작 모드 및 상기 활성일 것으로 예상된 제2의 적어도 하나의 프로세스에 기초하여 상기 예상 활동 레벨을 조정하는 단계

를 포함하는 방법.

청구항 2

제1항에 있어서,

상기 보안 엔진에 의해, 상기 프로세싱 시스템의 스냅샷을 대역 외 통신 채널을 통해 원격 서버에 송신하는 단계를 더 포함하고, 상기 원격 서버는 상기 스냅샷의 유효성 검사를 실행하는 방법.

청구항 3

제1항에 있어서,

상기 보안 엔진에 의해, 상기 프로세싱 시스템의 스냅샷을 대역 외 통신 채널을 통해 원격 서버에 송신하는 단계를 더 포함하고, 상기 원격 서버는 바이러스 서명들에 대해 상기 스냅샷을 분석하는 방법.

청구항 4

제1항에 있어서,

상기 호스트 운영 체제에 의해, 상기 예상치 못한 활동의 소스를 종료하는 단계를 더 포함하는 방법.

청구항 5

삭제

청구항 6

제1항에 있어서,

상기 정책 가이드라인들을 사용해서 상기 예상치 못한 활동이 적법한지를 결정하는 단계는

상기 소스가 서명된 것인지를 결정하는 단계를 포함하는 방법.

청구항 7

제1항에 있어서,

상기 정책 가이드라인들을 사용해서 상기 예상치 못한 활동이 적법한지를 결정하는 단계는

상기 예상치 못한 활동을 사용자에게 경고하는 단계; 및

상기 예상치 못한 활동에 대한 피드백을 상기 사용자로부터 획득하는 단계를 포함하는 방법.

청구항 8

프로세싱 시스템으로서,

호스트 운영 체제를 실행하도록 구성된 메인 프로세서;

상기 메인 프로세서와 독립하여 동작하도록 구성된 보안 엔진; 및

상기 보안 엔진에 연결된 메모리

를 포함하고,

상기 메모리는, 실행될 때, 상기 보안 엔진이

상기 메인 프로세서 및 배터리를 포함하는 하나의 또는 그 이상의 리소스들을 포함하는 상기 프로세싱 시스템의 현재 플랫폼 동작 모드에서 상기 호스트 운영 체제의 명령에 의해 활성일 것으로 예상된 적어도 하나의 프로세스를 식별하는 동작;

상기 현재 플랫폼 동작 모드 및 상기 활성일 것으로 예상된 적어도 하나의 프로세스에 기초하여 상기 메인 프로세서의 예상 프로세서 주파수 및 상기 배터리의 예상 배터리 소모 레벨을 포함하는 상기 프로세싱 시스템의 상기 하나의 또는 그 이상의 리소스들의 예상 활동 레벨을 계산하는 동작;

상기 프로세싱 시스템의 상기 메인 프로세서의 프로세서 주파수 및 상기 배터리의 배터리 소모 레벨을 포함하는 상기 하나의 또는 그 이상의 리소스들의 실제 활동 레벨을 결정하는 동작;

상기 예상 활동 레벨과 상기 실제 활동 레벨 간에 편차가 검출되면, 상기 편차의 잠정적인 원인인 예상치 못한 활동의 소스로서 예상치 못한 활성인 프로세스 및 상기 예상치 못한 활성인 프로세스에 대응하는 애플리케이션을 식별하는 동작;

정책 가이드라인들을 사용해서 상기 예상치 못한 활동이 적법한지를 결정하는 동작;

상기 예상치 못한 활동이 적법하지 않으면 상기 예상치 못한 활동의 상기 소스를 멀웨어로서 분류하는 동작;

상기 프로세싱 시스템의 상기 현재 플랫폼 동작 모드의 새로운 플랫폼 동작 모드로의 변경을 식별하는 동작;

상기 새로운 플랫폼 동작 모드에서 상기 프로세싱 시스템의 상기 호스트 운영 체제의 명령에 의해 활성일 것으로 예상된 제2의 적어도 하나의 프로세스를 식별하는 동작; 및

상기 새로운 플랫폼 동작 모드 및 상기 활성일 것으로 예상된 제2의 적어도 하나의 프로세스에 기초하여 상기 예상 활동 레벨을 조정하는 동작

을 실행하게 하는 명령어들을 포함하는 프로세싱 시스템.

청구항 9

제8항에 있어서,

상기 명령어들은, 실행될 때, 상기 보안 엔진이

상기 프로세싱 시스템의 스냅샷을 대역 외 통신 채널을 통해 원격 서버에 송신하는 동작을 포함하는 동작들을 더 실행하게 하고,

상기 원격 서버는 상기 스냅샷의 유효성 검사를 실행하는 프로세싱 시스템.

청구항 10

제8항에 있어서,

상기 명령어들은, 실행될 때, 상기 보안 엔진이

상기 프로세싱 시스템의 스냅샷을 대역 외 통신 채널을 통해 원격 서버에 송신하는 동작을 포함하는 동작들을 더 실행하게 하고,

상기 원격 서버는 바이러스 서명들에 대해 상기 스냅샷을 분석하는 프로세싱 시스템.

청구항 11

제8항에 있어서,

상기 명령어들은, 실행될 때, 상기 호스트 운영 체제가

상기 예상치 못한 활동의 소스를 종료하는 동작을 포함하는 동작들을 더 실행하게 하는 프로세싱 시스템.

청구항 12

삭제

청구항 13

제8항에 있어서,

상기 정책 가이드라인들을 사용해서 상기 예상치 못한 활동이 적법한지를 결정하는 동작은

상기 소스가 서명된 것인지를 결정하는 동작을 포함하는 프로세싱 시스템.

청구항 14

제8항에 있어서,

상기 정책 가이드라인들을 사용해서 상기 예상치 못한 활동이 적법한지를 결정하는 동작은

상기 예상치 못한 활동을 사용자에게 경고하는 동작; 및

상기 예상치 못한 활동에 대한 피드백을 상기 사용자로부터 획득하는 동작을 포함하는 프로세싱 시스템.

청구항 15

컴퓨터 판독 가능 기억 매체로서,

프로세싱 시스템에서 실행될 때, 상기 프로세싱 시스템의 메인 프로세서와 독립하여 동작하는 보안 엔진이,

상기 메인 프로세서 및 배터리를 포함하는 하나의 또는 그 이상의 리소스들을 포함하는 상기 프로세싱 시스템의 현재 플랫폼 동작 모드에서 상기 프로세싱 시스템의 호스트 운영 체제의 명령에 의해 활성일 것으로 예상된 적어도 하나의 프로세스를 식별하는 동작;

상기 현재 플랫폼 동작 모드 및 상기 활성일 것으로 예상된 적어도 하나의 프로세스에 기초하여 상기 메인 프로세서의 예상 프로세서 주파수 및 상기 배터리의 예상 배터리 소모 레벨을 포함하는 상기 프로세싱 시

스템의 상기 하나의 또는 그 이상의 리소스들의 예상 활동 레벨을 계산하는 동작;

상기 프로세싱 시스템의 상기 메인 프로세서의 프로세서 주파수 및 상기 배터리의 배터리 소모 레벨을 포함하는 상기 하나의 또는 그 이상의 리소스들의 실제 활동 레벨을 결정하는 동작;

상기 예상 활동 레벨과 상기 실제 활동 레벨 간에 편차가 검출되면, 상기 편차의 잠정적인 원인인 예상치 못한 활동의 소스로서 예상치 못한 활성인 프로세스 및 상기 예상치 못한 활성인 프로세스에 대응하는 애플리케이션을 식별하는 동작;

정책 가이드라인들을 사용해서 상기 예상치 못한 활동이 적법한지를 결정하는 동작;

상기 예상치 못한 활동이 적법하지 않으면 상기 예상치 못한 활동의 상기 소스를 멀웨어로서 분류하는 동작;

상기 프로세싱 시스템의 상기 현재 플랫폼 동작 모드의 새로운 플랫폼 동작 모드로의 변경을 식별하는 동작;

상기 새로운 플랫폼 동작 모드에서 상기 프로세싱 시스템의 상기 호스트 운영 체제의 명령에 의해 활성일 것으로 예상된 제2의 적어도 하나의 프로세스를 식별하는 동작; 및

상기 새로운 플랫폼 동작 모드 및 상기 활성일 것으로 예상된 제2의 적어도 하나의 프로세스에 기초하여 상기 예상 활동 레벨을 조정하는 동작

을 포함하는 동작들을 실행하게 하는 명령어들을 저장한 컴퓨터 판독 가능 기억 매체.

청구항 16

제15항에 있어서,

상기 명령어들은, 실행될 때, 상기 보안 엔진이

상기 프로세싱 시스템의 스냅샷을 대역 외 통신 채널을 통해 원격 서버에 송신하는 동작을 포함하는 동작들을 더 실행하게 하고,

상기 원격 서버는 상기 스냅샷의 유효성 검사를 실행하는 컴퓨터 판독 가능 기억 매체.

청구항 17

제15항에 있어서,

상기 명령어들은, 실행될 때, 상기 보안 엔진이

상기 프로세싱 시스템의 스냅샷을 대역 외 통신 채널을 통해 원격 서버에 송신하는 동작을 포함하는 동작들을 더 실행하게 하고,

상기 원격 서버는 바이러스 서명들에 대해 상기 스냅샷을 분석하는 컴퓨터 판독 가능 기억 매체.

청구항 18

제15항에 있어서,

상기 명령어들은, 실행될 때, 상기 프로세싱 시스템이

상기 예상치 못한 활동의 소스를 종료하는 동작을 포함하는 동작들을 더 실행하게 하는 컴퓨터 판독 가능 기억 매체.

청구항 19

삭제

청구항 20

제15항에 있어서,

상기 정책 가이드라인들을 사용해서 상기 예상치 못한 활동이 적법한지를 결정하는 동작은

상기 소스가 서명된 것인지를 결정하는 동작을 포함하는 컴퓨터 판독 가능 기억 매체.

청구항 21

제15항에 있어서,

상기 정책 가이드라인들을 사용해서 상기 예상치 못한 활동이 적법한지를 결정하는 동작은

상기 예상치 못한 활동을 사용자에게 경고하는 동작; 및

상기 예상치 못한 활동에 대한 피드백을 상기 사용자로부터 획득하는 동작을 포함하는 컴퓨터 판독 가능 기억 매체.

발명의 설명

기 술 분 야

[0001] <저작권 공고>

[0002] 저작권 보호의 대상인 자료가 본 명세서에 포함된다. 저작권 소유자는 특허청 특허 파일들 또는 기록들에 나타나는 대로 임의의 사람에 의한 특허 문서의 복사에 이의가 없지만, 어떤 식으로든 저작권에 대한 모든 권리들을 보유한다.

[0003] 본 발명은 일반적으로 데이터 프로세싱 시스템들의 멀웨어 검출에 관한 것이다.

배 경 기 술

[0004] 현대 사회의 모바일 디바이스들이 급증함에 따라, 모바일 컴퓨팅 환경들에서 실행되는 애플리케이션들의 수와 정교함이 증가하고 있다. 모바일 디바이스들은 이제 금융/은행 거래들, 건강(health and wellness) 모니터, 지불 처리, 및 소셜 네트워킹 등의 매우 민감한 거래들을 처리하는데 사용되고 있다. 매우 민감한 거래들은 모바일 디바이스들이 해커들 및 멀웨어의 매력적인 목표가 되게 한다. 모바일 디바이스에 유용한 컴퓨팅 리소스들, 스토리지, 및 배터리 수명을 제한하는 소형 인수(small form factor) 때문에, 전형적인 항 바이러스 기술들은 모바일 디바이스에서 유용성이 제한적이다.

도면의 간단한 설명

[0005] 도 1은 본 발명의 일 실시예에 따라 서명-독립적이고 시스템 거동 기반인 멀웨어 검출을 가능하게 하도록 구성된 시스템의 블록도이다.

도 2는 본 발명의 일 실시예에 따른 도 1의 시스템의 상세한 블록도이다.

도 3은 본 발명의 일 실시예에 따라 서명-독립적 시스템 거동 기반 멀웨어 검출을 실행하기 위한 한 방법의 흐름도이다.

도 4는 본 발명의 일 실시예에 따라 시스템이 동작하는 동안 사용자에 의해 야기된 새로운 애플리케이션들을 모니터하기 위한 한 방법의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0006] 본 발명의 실시예들은 서명-독립적이고 시스템 거동 기반인 멀웨어 검출을 실행하기 위한 방법, 시스템, 및 컴퓨터 프로그램 제품을 제공할 수 있다. 일 실시예에서, 본 방법은 하나의 또는 그 이상의 리소스들을 포함하는 프로세싱 시스템의 현재 동작 모드에서 활성일 것으로 예상된 적어도 하나의 프로세스를 식별하는 단계; 현재 동작 모드 및 활성일 것으로 예상된 적어도 하나의 프로세스에 기초하여 프로세싱 시스템의 하나의 또는 그 이상의 리소스들의 예상 활동 레벨을 계산하는 단계; 복수의 리소스들의 실제 활동 레벨을 결정하는 단계; 예상 활동 레벨과 실제 활동 레벨 간에 편차가 검출되면, 편차의 잠정적인 원인으로서 예상치 못한 활동의 소스를 식별하는 단계; 정책 가이드라인을 사용해서 예상치 못한 활동이 적법한지를 결정하는 단계; 및 예상치 못한 활동이 적법하지 않으면 예상치 못한 활동의 소스를 멀웨어로서 분류하는 단계를 포함한다.

[0007] 본 방법은 프로세싱 시스템의 스냅샷을 원격 서버에 송신하는 단계를 더 포함할 수 있으며, 원격 서버는 스냅샷의 유효성 검사를 실행하고/하거나 바이러스 서명들에 대해 스냅샷을 분석한다. 본 방법은 예상치 못한 활동의

소스를 종료하는 단계를 더 포함할 수 있다. 일 실시예에서, 본 방법은 프로세싱 시스템의 현재 동작 모드의 새로운 동작 모드로의 변경을 식별하는 단계; 활성일 것으로 예상된 제2의 적어도 하나의 프로세스를 식별하는 단계; 및 새로운 동작 모드 및 활성일 것으로 예상된 제2의 적어도 하나의 프로세스에 기초하여 예상 활동 레벨을 조정하는 단계를 더 포함한다. 일 실시예에서, 정책 가이드라인을 사용해서 예상치 못한 활동이 적법한지를 결정하는 단계는 소스가 서명된 것인지를 결정하는 단계를 포함한다. 정책 가이드라인을 사용해서 예상치 못한 활동이 적법한지를 결정하는 단계는 예상치 못한 활동을 사용자에게 경고하는 단계 및 예상치 못한 활동에 대한 피드백을 사용자로부터 획득하는 단계를 더 포함할 수 있다.

[0008] 본 명세서에서 본 발명의 "하나의 실시예" 또는 "일 실시예"에 대한 언급은, 실시예와 관련해서 기술된 특정 특징, 구조, 또는 특성이 본 발명의 적어도 하나의 실시예에 포함됨을 의미한다. 따라서, 본 명세서에서 각종 장소들에 나타나는 구절들 "일 실시예에서", "일 실시예에 따라" 등의 출현들은 반드시 모두 동일한 실시예와 관련되는 것은 아니다.

[0009] 설명을 위해, 특정 구성들 및 세부 사항들이 본 발명의 철저한 이해를 제공하기 위해 기재된다. 그러나, 본 명세서에서 제시된 특정 세부 사항들 없이 본 발명의 실시예들이 실시될 수 있음이 당업자에게 명백해질 것이다. 또한, 널리 공지된 특징들은 본 발명을 모호하게 하지 않기 위해 생략 또는 간소화될 수 있다. 각종 일례들은 본 설명의 도처에 제공될 수 있다. 이는 단지 본 발명의 특정 실시예들의 설명들이다. 본 발명의 범위는 제공된 일례들로 제한되지 않는다.

[0010] 전형적인 데스크탑 시스템들에서, 다수의 사용자들은 컴퓨터가 실행 가능 파일들(executables)을 다운로드 또는 실행한 후에 인식된 바이러스들을 검출 및 제거할 수 있는 항바이러스 소프트웨어를 설치할 수 있다. 항바이러스 소프트웨어 애플리케이션이 바이러스들을 검출하기 위해 사용하는 2가지 일반적인 방법들이 있다. 제1의 가장 일반적인 바이러스 검출 방법은 바이러스 서명 정의들의 리스트를 사용하는 것이다. 이 기술은 컴퓨터의 메모리(RAM, 및 부트 섹터들)의 콘텐츠 및 고정 또는 이동 드라이브들(하드 드라이브들, 플로피 드라이브들)에 저장된 파일들을 검사하고, 인식된 바이러스 "서명들"의 데이터베이스와 파일들을 비교함으로써 작업한다. 이 검출 방법의 한가지 단점은, 최종 바이러스 정의 업데이트보다 먼저 앞서 온 바이러스들로부터만 사용자들이 보호된다는 점이다. 다른 단점은, 상당한 리소스들이, 수백만 엔트리들을 가질 수 있는, 바이러스 서명들의 데이터베이스를 저장하는데 필요해서, 모바일 디바이스에서 유효한 스토리지의 양을 초과한다는 점이다.

[0011] 바이러스 검출의 제2 방법은, 바이러스 소프트웨어에 의해 보여지는 일반적인 거동들에 기초하여 바이러스들을 찾기 위해 휴리스틱 알고리즘(a heuristic algorithm)을 사용하는 것이다. 본 방법은 서명이 아직 생성되지 않은 신규의 바이러스들을 검출하는 기능을 갖지만, 바이러스 소프트웨어에 의해 보여지는 일반적인 거동들이 미리 식별될 것을 요구한다. 또한, 이 기술은, 광대한 컴퓨팅 리소스들이 일반적인 거동들을 식별 및 추적하는데 요구되며, 이 광대한 컴퓨팅 리소스들이 모바일 디바이스에서 유효하지 않을 수 있다는 단점을 가진다.

[0012] 도 1은 본 발명의 일 실시예에 따라 서명-독립적이고 시스템 거동 기반인 멀웨어 검출을 실행하도록 구성된 시스템의 블록도이다. 모바일 컴퓨터 시스템 및/또는 모바일 전화에 대응하는 플랫폼(100)은 칩셋(120)에 접속된 프로세서(110)를 포함한다. 프로세서(110)는 플랫폼(100)에 프로세싱 파워를 제공하고, 싱글-코어 또는 멀티-코어 프로세서일 수 있으며, 하나 보다 더 많은 프로세서가 플랫폼(100)에 포함될 수 있다. 프로세서(110)는 하나의 또는 그 이상의 시스템 버스들, 통신 경로들 또는 매체들(도시되지 않음)을 통해 플랫폼(100)의 다른 컴포넌트들에 접속될 수 있다. 프로세서(110)는 기업 서버(170)로의 네트워크(150)를 통해 인터커넥션(151)을 통해 통신하는 호스트 애플리케이션(112) 등의 호스트 애플리케이션들을 실행한다. 호스트 애플리케이션(112)은 호스트 운영 체제(105)의 제어 하에서 실행된다.

[0013] 칩셋(120)은, 플랫폼(100)의 보안을 관리하기 위해, 프로세서(110)와 무관하게 동작하는 내장된 마이크로프로세서로서 구현될 수 있는 보안 엔진(130)을 포함한다. 보안 엔진(130)은 암호 동작들 및 다른 사용자 인증 기능을 제공한다. 일 실시예에서, 프로세서(110)는 호스트 운영 체제(105)의 지휘 하에서 동작하는 반면, 보안 엔진(130)은 호스트 운영 체제(105)에 의해 액세스될 수 없는 안전한 격리된 환경을 제공한다. 이 안전한 환경은 본 명세서에서는 보안 파티션이라고 한다. 안전한 환경은 보안 스토리지(132)를 또한 포함한다.

[0014] 일 실시예에서, 보안 엔진(130)에서 실행중인 거동 분석 모듈(140)은 서명-독립적이고 시스템 거동 기반인 멀웨어 검출을 제공하기 위해 호스트 애플리케이션(112)에 의해 사용된다. 호스트 애플리케이션(112)은, 보안 엔진 인터페이스(SEI)(114)를 통해, 서명-독립적이고 시스템 거동 기반인 멀웨어 검출을 포함하는, 보안 엔진(130)의 서비스들을 요청한다. 거동 분석 모듈(140)은 보안 엔진(130)에 의해 실행되는 펌웨어로서 구현될 수 있다.

[0015] 보안 엔진(130)과 기업 서버(170) 간의 통신은 대역 외 통신 채널(152)을 통해 발생한다. 일 실시예에서, 대역 외 통신 채널(152)은 호스트 시스템의 보안 엔진(130)과 기업 서버(170) 간의 안전한 통신 채널이다. 대역 외 통신 채널(152)은, 보안 엔진(130)이 플랫폼(100)의 호스트 운영 체제(105)와 무관하게 외부 서버들과 통신할 수 있게 한다.

[0016] 도 2는 도 1의 시스템의 컴포넌트들의 더 상세한 뷰를 도시한다. 도 2에 도시된 실시예에서, 거동 분석 사용자 인터페이스(212)는 모바일 운영 체제(OS)(205)에 의해 제공된 환경에서 실행중인 호스트 애플리케이션이다. 거동 분석 모듈 사용자 인터페이스(212)는 서명-독립적이고 시스템 거동 기반인 멀웨어 검출을 제공하기 위해 거동 분석 모듈(240)을 호출한다. 거동 분석 모듈 사용자 인터페이스(212)와 거동 분석 모듈(240) 간의 상호 작용은 구현 특정적이며, 직접 또는 모바일 OS(205)를 통해 발생할 수 있다. 일 실시예에서, 거동 분석 모듈 사용자 인터페이스(212)는 거동 분석 모듈(240)의 동적 세팅들을 무시하는 옵션을 제공한다.

[0017] 모바일 OS(205)는, 유휴 기간들 중에 플랫폼(200) 서브시스템들을 중단하고, 프로세서(210)가 저전력 상태에서 동작하는 시간의 양을 증가시키는 전원 관리자(207)를 포함한다. 전원 관리자(207)는 모바일 디바이스(200)를 위한 전력 절약을 증가시키기 위해 가능한 최저 전력 상태로 프로세서(210)를 유지한다.

[0018] 거동 분석 모듈(240)이 보안 엔진(230) 내에서 실행되기 때문에, 거동 분석 모듈(240)은 보안 엔진 인터페이스(SEI)(214)를 통해 액세스된다. 거동 분석 모듈(240)은 프로세서 모니터(241), 배터리 모니터(242), 웨이크 이벤트 모니터(243), 및 통신/로깅 에이전트(244)를 포함하는 수개의 서브-모듈들을 포함한다.

[0019] 프로세서 모니터(241)는 거동 분석 모듈(240)에 프로세서 사용 정보를 제공한다. 프로세서 모니터(241)는 커널 관리자/메뉴(도시되지 않음)와 인터페이스함으로써 프로세서 사용을 모니터한다. 프로세서 모니터(241)는 또한 프로세스들이 제한된 특권들 및/또는 주파수들로 실행될 수 있게 한다.

[0020] 배터리 모니터(242)는 거동 분석 모듈(240)에 배터리 사용 정보를 제공한다. 배터리 사용은 과도한 논-프로세서 리소스 사용을 검출하기 위해 모니터된다. 예를 들어, 배터리 모니터(242)는 그래픽 엔진 리소스 또는 오디오 서브시스템의 과도한 사용을 검출할 수 있다. 배터리 모니터(242)는 배터리(250)용의 드라이버(도시되지 않음)와 인터페이스함으로써 배터리 사용을 모니터한다.

[0021] 웨이크 이벤트 모니터(243)는 시스템 컨트롤러 유닛(SCU)(208)과 함께 작업하며, 웨이크 이벤트들을 모니터한다. 웨이크 이벤트 모니터(243)는 소정의 동작 모드에 대해 예상치 못한 웨이크 이벤트들을 필터링하도록 SCU(208) 레지스터들을 구성한다. 시스템 컨트롤러 유닛(SCU)(208)은 미세한 플랫폼 전원 관리 지원을 제공한다. 플랫폼(200) 웨이크 이벤트들은 SCU(208)를 통해 웨이크 이벤트 모니터(243)에 라우팅된다.

[0022] 거동 분석 모듈(240)이 야기될 때, 보안 스토리지(232)로부터 정책 세팅들을 로드한다. 거동 분석 모듈(240)은 모바일 OS(205) 전원 관리자(207)로부터 현재 플랫폼 동작 모드를 획득한다. 플랫폼 동작 모드의 일례들은 브라우징, 비디오/오디오 재생, 카메라, 전화 등을 포함한다. 현재 동작 모드에 기초하여, 거동 분석 모듈(240)은 활성일 것으로 예상된 적어도 하나의 프로세스를 식별한다. 예를 들어, 오디오 재생 모드 중에, 오디오 서브시스템 프로세스는 활성일 것으로 예상되며, 예상된 프로세서는 오직 버퍼들을 셋업 및 클리닝하는 데에만 관여될 것이다.

[0023] 거동 분석 모듈(240)은 플랫폼(200)의 리소스들의 활동 레벨들을 모니터하고 실제 활동 레벨들을 예상 활동 레벨들과 비교한다. 예상 활동 레벨들은 시스템의 동작 모드 및 그 동작 모드에서 활성일 것으로 예상된 프로세스에 기초하여 결정된다. 예를 들어, 프로세서 모니터(241)는 현재 동작 모드에서 프로세서(210) 및 배터리(250)의 예상 활동 레벨을 결정하기 위해 커널 프로세서 메뉴/관리자(도시되지 않음)와 인터페이스한다. 시스템 컨트롤러 유닛(SCU)(208)에 의해 처리되는 웨이크 이벤트들의 수 및 타입뿐만 아니라, 프로세서(210) 및 배터리(250)의 실제 활동 레벨이 그 후 모니터된다. 실제 활동 레벨과 예상 활동 레벨 간에 편차가 발견되면, 예상치 못한 활동의 소스가 편차의 잠정적인 원인으로서 식별된다.

[0024] 예상치 못한 활동의 소스는 시스템에서 현재 활성인 프로세스들을 식별하기 위해 커널 스케줄러(도시되지 않음)와 함께 작업함으로써 거동 분석 모듈(240)에 의해 식별된다. 이 현재 활성인 프로세스들은 플랫폼의 현재 동작 모드에서 실행중일 것으로 현재 예상되는 애플리케이션들에 매핑된다. 활성인 프로세스가 현재 동작 모드에서 예상된 애플리케이션에 매핑될 수 없으면, 그 활성인 프로세스 및 연관된 애플리케이션은 예상치 못한 활동의 소스로서 식별된다.

[0025] 예상치 못한 활동의 소스가 식별되면, 거동 분석 모듈(240)은 정책 가이드라인을 사용해서 예상치 못한 활동이

적법한지를 결정한다. 예를 들어, 정책 가이드라인은, 애플리케이션이 적법하다고 생각되게 하기 위해 서명되어야만 하도록 구성될 수 있다. 정책 가이드라인은, 예상치 못한 활동에 대해 사용자에게 경고하고, 애플리케이션이 적법한지를 결정하기 위해 사용자 피드백이 획득되도록 구성될 수 있다.

[0026] 예상치 못한 활동이 적법하지 않다고 결정되면, 예상치 못한 활동의 소스는 멀웨어로서 분류될 수 있다. 정책 가이드라인은 멀웨어를 어떻게 처리할지를 결정하는데 사용될 수 있다; 예를 들어, 예상치 못한 활동의 소스는 종료될 수 있고/있으며, 스냅샷이 다른 분석을 위해 시스템에서 취해질 수 있다. 예를 들어, 시스템의 스냅샷은 분석을 위해 원격 서버에 송신될 수 있다. 원격 서버는 스냅샷의 유효성 검사를 실행하고/하거나 바이러스 서명들에 대해 스냅샷을 분석할 수 있다.

[0027] 거동 분석 모듈(240)은, 플랫폼(200) 동작 모드의 변경이 있을 때 모바일 OS(205) 전원 관리자(207)에 의해 통지받을 수 있다. 예를 들어, 플랫폼(200)이 초기에 오디오 재생 모드이고 사용자가 브라우저를 야기하면, 시스템은 "브라우저 + 오디오 재생" 동작 모드로 변경한다. 모바일 OS(205) 전원 관리자(207)로부터의 통지에 기초하여, 거동 분석 모듈(240)은 거짓 경고들을 트리거링하는 것을 방지하도록 세팅들 및 예상 활동 레벨을 조정한다.

[0028] 통신/로깅 에이전트(244)는 시스템의 상태의 스냅샷들을 정기적으로 로그하고, 검증 및/또는 분석을 위해 도 1의 기업 서버(170) 등의 원격 서버에 이 정보를 송신할 수 있다. 로그된 정보를 송신할 때, 통신/로깅 에이전트(244)는 기업 서버(170)와의 안전한 통신 채널을 설정한다. 스냅샷들에서 포착된 정보는 구현 특정적이며, 검출된 비정상 활동의 통계들, 실행중인 비서명 애플리케이션들의 식별 및/또는 코드, 사용자의 디바이스 사용 패턴, 특권 세팅들을 무시하고자 시도하는 로그들, 및 이상한 거동 패턴들의 로그들을 포함할 수 있다.

[0029] 플랫폼(200)은 메모리(204) 및 보안 스토리지(232) 등의 메모리 디바이스들을 더 포함한다. 이 메모리 디바이스들은 랜덤 액세스 메모리(RAM) 및 판독 전용 메모리(ROM)를 포함할 수 있다. 이 설명을 위해, 용어 "ROM"은 소거 가능 프로그래밍 가능 ROM(EPROM), 전기적 소거 가능 프로그래밍 가능 ROM(EEPROM), 플래시 ROM, 플래시 메모리 등의 비휘발성 메모리 디바이스들을 일반적으로 지칭하는데 사용될 수 있다. 보안 스토리지(232)는 통합 드라이브 일렉트로닉스(IDE) 하드 드라이브들 등의 대용량 스토리지 디바이스들, 및/또는 플로피 디스크들, 광 스토리지, 테이프들, 플래시 메모리, 메모리 스틱들, 디지털 비디오 디스크들, 생물학적 스토리지 등의 다른 디바이스들 또는 매체들을 포함할 수 있다. 일 실시예에서, 보안 스토리지(232)는, 모바일 OS(205)로부터 격리된, 칩셋(220) 내에 내장된 eMMC NAND 플래시 메모리이다.

[0030] 프로세서(210)는, 또한, 디스플레이 컨트롤러(202), 소형 컴퓨터 시스템 인터페이스(SCSI) 컨트롤러들, 통신 컨트롤러(206) 등의 네트워크 컨트롤러들, USB(universal serial bus) 컨트롤러들, 키보드 및 마우스 등의 입력 디바이스들 등의 추가 컴포넌트들에 통신 연결될 수 있다. 플랫폼(200)은 각종 시스템 컴포넌트들을 통신 연결하기 위해, 메모리 컨트롤러 허브, 입력/출력(I/O) 컨트롤러 허브, PCI 루트 브리지 등의 하나의 또는 그 이상의 브리지들 또는 허브들을 더 포함할 수 있다. 본 명세서에서 사용된 용어 "버스"는 지점간 경로들뿐만 아니라 공유 통신 경로들을 지칭하는데 사용될 수 있다.

[0031] 예를 들어, 통신 컨트롤러(206) 등의 일부 컴포넌트들은 버스와 통신하기 위한 인터페이스들(예를 들어, PCI 커넥터)을 가진 어댑터 카드들로서 구현될 수 있다. 일 실시예에서, 하나의 또는 그 이상의 디바이스들은 프로그래밍 가능 또는 프로그래밍 불가능 로직 디바이스들 또는 어레이들, 주문형 반도체들(ASICs), 내장형 컴퓨터들, 스마트 카드들 등의 컴포넌트들을 사용해서, 내장된 컨트롤러들로서 구현될 수 있다.

[0032] 본 명세서에서 사용된 용어들 "프로세싱 시스템" 및 "데이터 프로세싱 시스템"은 단일 기계, 또는 함께 동작하는 통신 연결된 기계들 또는 디바이스들의 시스템을 광범위하게 아우르도록 의도된 것이다. 일례의 프로세싱 시스템들은, 제한 없이, 분산 컴퓨팅 시스템들, 슈퍼컴퓨터들, 고성능 컴퓨팅 시스템들, 컴퓨팅 클러스터들, 메인프레임 컴퓨터들, 미니-컴퓨터들, 클라이언트-서버 시스템들, 퍼스널 컴퓨터들, 워크스테이션들, 서버들, 휴대형 컴퓨터들, 랩탑 컴퓨터들, 태블릿들, 전화들, 퍼스널 디지털 어시스턴트들(PDAs), 핸드헬드 디바이스들, 오디오 및/또는 비디오 디바이스들 등의 엔터테인먼트 디바이스들, 및 정보를 처리 또는 송신하기 위한 다른 디바이스들을 포함한다.

[0033] 플랫폼(200)은, 적어도 부분적으로, 키보드, 마우스, 터치 스크린, 음성-활성화 디바이스, 제스처-활성화 디바이스 등의 종래의 입력 디바이스들로부터의 입력에 의해, 및/또는 다른 기계, 생물 측정 피드백, 또는 다른 입력 소스들 또는 신호들로부터 수신된 커맨드들에 의해, 제어될 수 있다. 플랫폼(200)은, 예를 들어, 통신 컨트롤러(206), 모뎀, 또는 다른 통신 포트들 또는 연결들을 통해, 도 1의 기업 서버(170) 등의 하나의 또는 그 이

상의 원격 데이터 프로세싱 시스템들로의 하나의 또는 그 이상의 커넥션들을 사용할 수 있다.

[0034] 플랫폼(200)은 근거리 통신망(LAN), 광역 통신망(WAN), 인트라넷, 인터넷 등의 물리적 및/또는 논리적 네트워크에 의해 다른 프로세싱 시스템들(도시되지 않음)에 상호 접속될 수 있다. 네트워크를 수반하는 통신들은, 무선 주파수(RF), 위성, 마이크로웨이브, IEEE(Institute of Electrical and Electronics Engineers) 802.11, 블루투스, 광, 적외선, 케이블, 레이저 등을 포함하는, 각종 유선 및/또는 무선 단거리 또는 장거리 반송파들 및 프로토콜들을 사용할 수 있다.

[0035] 도 3은 본 발명의 일 실시예에 따라 서명-독립적이고 시스템 거동 기반인 멀웨어 검출을 실행하기 위한 한 방법의 흐름도이다. 도 3의 방법 단계들은 도 1 및 도 2의 시스템의 컴포넌트들에 의해 실행되는 것으로 기술될 것이다. 본 방법은 "플랫폼에서 거동 분석 모듈이 인에이블되는가?"라는 결정 단계(302)에서 시작한다. 거동 분석 모듈(240)이 플랫폼(200)에서 인에이블되지 않으면, 프로세스는 종료한다. 거동 분석 모듈(240)이 인에이블되면, 제어는 "보안 스토리지로부터 정책 세팅들을 로드"하는 단계(304)로 진행한다. 프로세서(210) 및 배터리(250) 등의 상이한 리소스들에 대한 예상 활동 레벨들의 정책 세팅들은 상이한 동작 모드들에 대해 설정되어 보안 스토리지(232)의 정책 데이터베이스에 저장된다. 이 정책 세팅들은 메모리로 로드되고, 거동 분석 모듈(240)은 "전원 관리자로부터 플랫폼의 현재 동작 모드를 획득"하는 단계(306)로 진행한다. 거동 분석 모듈(240)은 모바일 OS(205) 전원 관리자(207)로부터 현재 동작 모드를 획득한다. 진행 중에, "플랫폼 동작 모드의 변경시 전원 관리자가 거동 분석 모듈에 통지"하는 단계(308)에 도시된 바와 같이, 모바일 OS(205) 전원 관리자(207)는 플랫폼 동작 모드의 변경이 있는 경우 거동 분석 모듈(240)에 통지한다.

[0036] "전원 관리자로부터 플랫폼의 현재 동작 모드를 획득"하는 단계(306)로부터, 제어는 "동작 모드에 기초하여, 대응 모드에 대해 활성일 것으로 예상된 프로세스들을 결정"하는 단계(310)로 진행하여, 거동 분석 모듈(240)은 플랫폼(200)의 현재 동작 모드에 기초하여 활성일 것으로 예상된 적어도 하나의 프로세스를 식별한다. 제어는 "현재 동작 모드에 대해 예상 활동 레벨(근사한 프로세서 주파수 및 배터리 소모)을 계산"하는 단계(312)로 진행하여, 거동 분석 모듈(240)은 현재 동작 모드를 고려해서 플랫폼(200)의 리소스들의 예상 활동 레벨을 계산한다. 예를 들어, 근사한 프로세서 주파수 및 배터리 소모 레벨이 계산될 수 있다. 그 후, 제어는 "예상 활동 레벨로부터 실제 활동 레벨의 편차들을 모니터"하는 단계(314)로 진행한다. 단계(314)에서, 거동 분석 모듈(240)은 예상 활동 레벨로부터의 편차들에 대해 실제 활동 레벨을 모니터한다. 예를 들어, 프로세서 모니터(241)는 예상 활동 레벨들로부터의 프로세서 주파수, 특권 지속 기간, 및 사용 지속 기간의 편차들에 대해 모니터한다. 배터리 모니터(242)는 예상된 배터리 소모로부터의 배터리 사용의 편차들에 대해 모니터한다. 웨이크 이벤트 모니터(243)는 시스템 컨트롤러 유닛(SCU)(208)을 사용해서 현재 동작 모드가 주어지면 예상치 못한 수의 웨이크 이벤트들을 모니터한다.

[0037] 제어는 "예상 활동 레벨로부터 실제 활동 레벨의 편차들을 모니터"하는 단계(314)로부터 "임의의 편차가 검출되었는가?"라는 결정 단계(316)로 진행한다. 검출된 편차가 없으면, 제어는 "시스템의 스냅샷을 취하고 스냅샷을 로그"하는 단계(322)로 진행하여, 시스템의 스냅샷이 취해지고 통신/로깅 에이전트(244)에 의해 로그에 기록된다. 스냅샷에 대해 수집된 데이터의 양 및 스냅샷들이 취해진 회수는 구현 특정적이며 원래의 장비 제조자/원래의 디바이스 제조자(OEM/ODM)에 의해 결정될 수 있다. 일 실시예에서, 시스템의 스냅샷은 원격 서버에 의해 분석될 수 있으며, 바이러스 서명 매칭이 원격 서버에서 실행될 수 있어서, 클라이언트 프로세싱 시스템에서의 서명 프로세싱을 위해 더 적은 수의 리소스들을 필요로 한다.

[0038] "임의의 편차가 검출되었는가?"라는 결정 단계(316)에서 편차가 검출되면, 제어는 "예상치 못한 활동 레벨의 소스를 식별"하는 단계(318)로 진행한다. 단계(318)에서, 예상치 못한 프로세서 주파수의 소스 등의 예상치 못한 활동 레벨의 소스는 편차의 잠정적인 소스로서 식별된다. 그 후, 제어는 "정책 가이드라인을 사용해서 예상치 못한 활동이 적법한지를 결정"하는 단계(320)로 진행한다. 상술된 바와 같이, 예상치 못한 활동의 소스가 식별되면, 거동 분석 모듈(240)은 정책 가이드라인을 사용해서 예상치 못한 활동이 적법한지를 결정한다. 예를 들어, 정책 가이드라인은, 애플리케이션이 적법하다고 생각되게 하기 위해 서명되어야만 하도록 구성될 수 있다. 정책 가이드라인은, 예상치 못한 활동에 대해 사용자에게 경고하고, 애플리케이션이 적법한지를 결정하기 위해 사용자 피드백이 획득되도록 구성될 수 있다. 제어는 "적법한 활동인가?"라는 결정 단계(322)로 진행한다. 예상치 못한 활동이 적법하다고 결정되면, 제어는 "정책 세팅들에 따라 액션을 취한다"라는 단계(326)로 진행한다. 예를 들어, 추가 모니터 루틴들이 예상치 못한 활동의 소스인 애플리케이션을 모니터하기 위해 야기될 수 있다.

[0039] "적법한 활동인가?"라는 결정 단계(322)에서, 예상치 못한 활동이 적법하지 않다고 결정되면, 제어는 "예상치

못한 활동의 소스를 멀웨어로서 분류"하는 단계(324)로 진행하여, 예상치 못한 활동의 소스는 멀웨어로서 분류된다. 그 후, 제어는 "정책 세팅들에 따라 액션을 취한다"라는 단계(326)로 진행하여, 예상치 못한 활동 레벨의 소스를 종료하고/하거나, 시스템 스냅샷을 원격 서버에 통지하는 등, 멀웨어를 처리하기 위한 적합한 액션이 취해진다. 그 후, 제어는 "시스템의 스냅샷을 취하고 스냅샷을 로그"하는 단계(328)로 진행하여, 시스템의 스냅샷이 취해지고 통신/로깅 에이전트(244)에 의해 로그에 기록된다.

[0040] 도 4는 본 발명의 일 실시예에 따라 시스템이 동작하는 동안 사용자에 의해 야기된 새로운 애플리케이션들을 모니터하기 위한 한 방법의 흐름도이다. "사용자에 의해 새로운 애플리케이션/서비스가 개시되었는가?"라는 결정 단계(402)에서, 거동 분석 모듈(240)은 플랫폼(200)의 사용자에 의해 새로운 애플리케이션 또는 서비스가 론치되었는지를 결정한다. 새로운 애플리케이션 또는 서비스가 론치되지 않았으면, 프로세스는 종료한다. 새로운 애플리케이션 또는 서비스가 론치되었으면, 제어는 "애플리케이션/서비스가 서명되었는가?"라는 결정 단계(404)로 진행한다. 애플리케이션 또는 서비스가 서명되었으면, 제어는 "애플리케이션/서비스가 그에 따라 동작 모드를 실행 및 업데이트하는 것을 허용/거부"하는 단계(408)로 진행한다. 거동 분석 모듈(240)은 애플리케이션 또는 서비스가 그에 따라 동작 모드를 실행 및 업데이트할 기회를 허용 또는 거부한다.

[0041] "애플리케이션/서비스가 서명되었는가?"라는 결정 단계(404)에서, 애플리케이션 또는 서비스가 서명되지 않았으면, 제어는 "사용자에게 경고하고 사용자 피드백에 기초하여 적응"하는 단계(406)로 진행한다. 사용자는 거동 분석 모듈 사용자 인터페이스(212)를 통해 경고를 받고, 거동 분석 모듈(240)은 사용자 피드백에 따라 자신의 거동을 적응시킨다. 예를 들어, 사용자는 모든 애플리케이션들 및 서비스들이 서명되는 요구 사항을 무시하고, 서명되지 않더라도 애플리케이션이 실행될 수 있게 하는 명령어를 제공할 수 있다. 대안으로, 거동 분석 모듈(240)은 비서명 애플리케이션들이 허용되지 않음을 사용자에게 통지할 수 있다. "사용자에게 경고하고 사용자 피드백에 기초하여 적응"하는 단계(406)로부터, 제어는 "애플리케이션/서비스가 그에 따라 동작 모드를 실행 및 업데이트하는 것을 허용/거부"하는 단계(408)로 진행한다. 거동 분석 모듈(240)은 애플리케이션 또는 서비스가 그에 따라 동작 모드를 실행 및 업데이트할 기회를 허용 또는 거부한다.

[0042] 도 4를 참조해서 기술된 프로세스는 새로운 애플리케이션이 론치될 때 또는 예상 활동 레벨로부터의 실제 활동 레벨의 편차가 발생했다고 결정될 때마다 실행될 수 있다. 도 4를 참조해서 기술된 프로세스는 예상치 못한 활동이 적법한지를 결정하는데 사용될 수 있다.

[0043] 본 명세서에서 서명-독립적이고 시스템 거동 기반인 멀웨어 검출을 위해 기술된 기술들은 전형적인 멀웨어 검출 방법들에 비해 수개의 장점들을 제공한다. 수백만의 멀웨어 서명들에 대해 소프트웨어 프로그램들을 검사하지 않고 멀웨어 검출이 실행되기 때문에, 상당한 스토리지 및 컴퓨팅 리소스들이 절약된다. 본 명세서에 기술된 거동 분석 모듈은 멀웨어를 앞서서 식별하기 위해 프로세서(들) 및 배터리 등의 리소스들의 활동 레벨뿐만 아니라 프로세싱 시스템의 동작 모드를 이용한다. 동작 모드가 변경될 때 거동 분석 모듈이 동적으로 적응하기 때문에, 거짓 경고들이 방지된다. 거동 분석 모듈은 또한 동작을 분석할 때 애플리케이션 또는 서비스가 서명되어 있는지를 고려한다.

[0044] 본 명세서에 기술된 거동 분석 모듈은 구성 가능하며 정책에 기초한다. 거동 분석 모듈은 시스템의 스냅샷들을 취하고 검증을 위해 원격 기업 서버에 스냅샷들을 제공하는 기능을 가진다.

[0045] 또한, 본 명세서에 기술된 거동 분석 모듈은 프로세싱 시스템의 운영 체제로부터 격리된 안전한 환경에서 동작한다. 이는, 거동 분석 데이터가, 사용자, 운영 체제, 호스트 애플리케이션들, 및 멀웨어를 포함하는, 신뢰할 수 없는 당사자들에 액세스될 수 없음을 보장한다. 정책 세팅들 및 거래 로그들이 쉽게 조작할 수 없는 보안 스토리지에 또한 저장된다. 정책들 및 경고들은 원격 기업 서버로부터 안전하게 통신될 수 있어서, 거동 분석 모듈이 변화무쌍한 멀웨어 환경에 적응할 수 있게 한다.

[0046] 본 명세서에 기술된 메커니즘들의 실시예들은 하드웨어, 소프트웨어, 펌웨어, 또는 이 구현 방식들의 조합으로 구현될 수 있다. 본 발명의 실시예들은, 적어도 하나의 프로세서, 데이터 기억 시스템(휘발성 및 비휘발성 메모리 및/또는 기억 소자들을 포함), 적어도 하나의 입력 디바이스, 및 적어도 하나의 출력 디바이스를 포함하는 프로그래밍 가능 시스템들에서 실행중인 컴퓨터 프로그램들로서 구현될 수 있다.

[0047] 프로그램 코드는 본 명세서에 기술된 기능들을 실행하고 출력 정보를 생성하도록 입력 데이터에 적용될 수 있다. 또한, 본 발명의 실시예들은 본 발명의 동작들을 실행하기 위한 명령어들을 포함하거나 또는 본 명세서에 기술된 구조들, 회로들, 장치들, 프로세서들 및/또는 시스템 특징들을 정의하는, HDL 등의 설계 데이터를 포함하는 기계 액세스 가능 매체를 포함한다. 이러한 실시예들은 또한 프로그램 제품들이라고 할 수 있다.

[0048] 이러한 기계 액세스 가능 기억 매체는, 하드 디스크들 등의 기억 매체, 플로피 디스크들, 광 디스크들, 콤팩트 디스크 판독 전용 메모리들(CD-ROMs), 콤팩트 디스크 리라이터블(CD-RWs), 및 광자기 디스크들을 포함하는 임의의 다른 타입의 디스크, 판독 전용 메모리(ROM), 동적 랜덤 액세스 메모리(DRAM), 정적 랜덤 액세스 메모리(SRAM) 등의 랜덤 액세스 메모리(RAM), 소거 가능 프로그래밍 가능 판독 전용 메모리(EPROM), 플래시 프로그래밍 가능 메모리(FLASH), 전기적 소거 가능 프로그래밍 가능 판독 전용 메모리(EEPROM) 등의 반도체 디바이스들, 자기 또는 광 카드들, 또는 전자 명령어들을 저장하기에 적합한 임의의 다른 타입의 매체를 포함하는, 기계 또는 디바이스에 의해 제조 또는 형성된 입자들의 유형의 구성들을, 제한 없이, 포함할 수 있다.

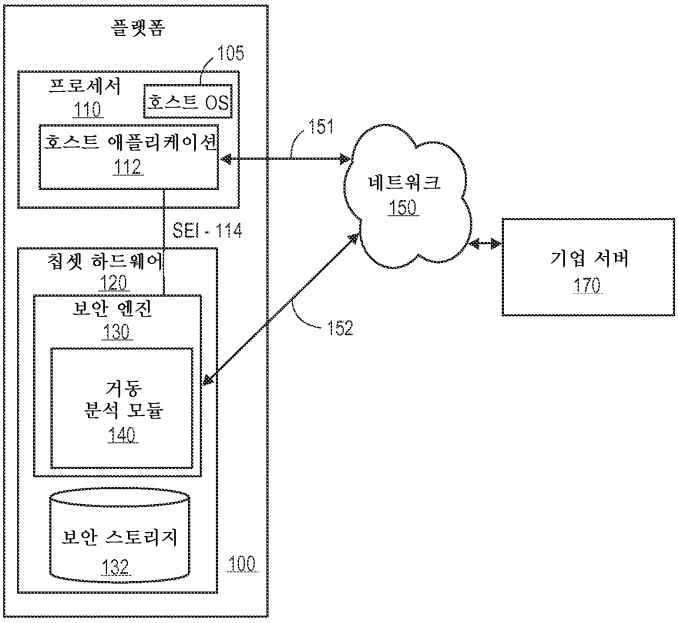
[0049] 출력 정보는, 공지된 방식으로, 하나의 또는 그 이상의 출력 디바이스들에 적용될 수 있다. 이 적용을 위해, 프로세싱 시스템은, 예를 들어, 디지털 신호 프로세서(DSP), 마이크로컨트롤러, 주문형 반도체(ASIC), 또는 마이크로프로세서 등의 프로세서를 가진 임의의 시스템을 포함한다.

[0050] 프로그램들은 프로세싱 시스템과의 통신을 위해 고급 절차적 또는 객체 지향적 프로그래밍 언어로 구현될 수 있다. 또한, 프로그램들은, 원하는 경우, 어셈블리 또는 기계어로 구현될 수 있다. 사실상, 본 명세서에 기술된 메커니즘들은 임의의 특정 프로그래밍 언어로 범위가 제한되지 않는다. 임의의 경우에, 언어는 컴파일링된 또는 해석된 언어일 수 있다.

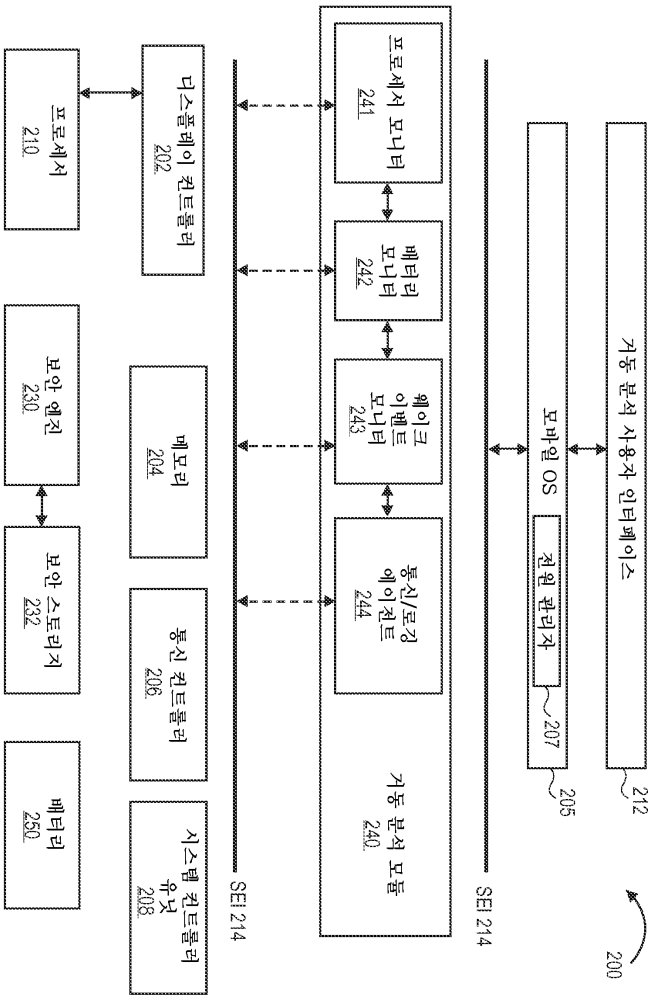
[0051] 서명-독립적이고 시스템 거동 기반인 멀웨어를 검출을 실행하기 위한 방법들 및 시스템들의 실시예들이 본 명세서에 제시된다. 본 발명의 특정 실시예들이 도시 및 기술되었지만, 첨부된 청구항들의 범위로부터 벗어나지 않은 채로 다수의 변경들, 변형들 및 수정들이 이루어질 수 있음이 당업자에게 명백할 것이다. 따라서, 변경들 및 수정들이 더 넓은 양상들로 본 발명으로부터 벗어나지 않은 채로 이루어질 수 있음을 당업자는 알 것이다. 첨부된 청구항들은 본 발명의 범위 및 원리 내에 속한 이러한 모든 변경들, 변형들 및 수정들을 그 범위 내에서 포함할 것이다.

도면

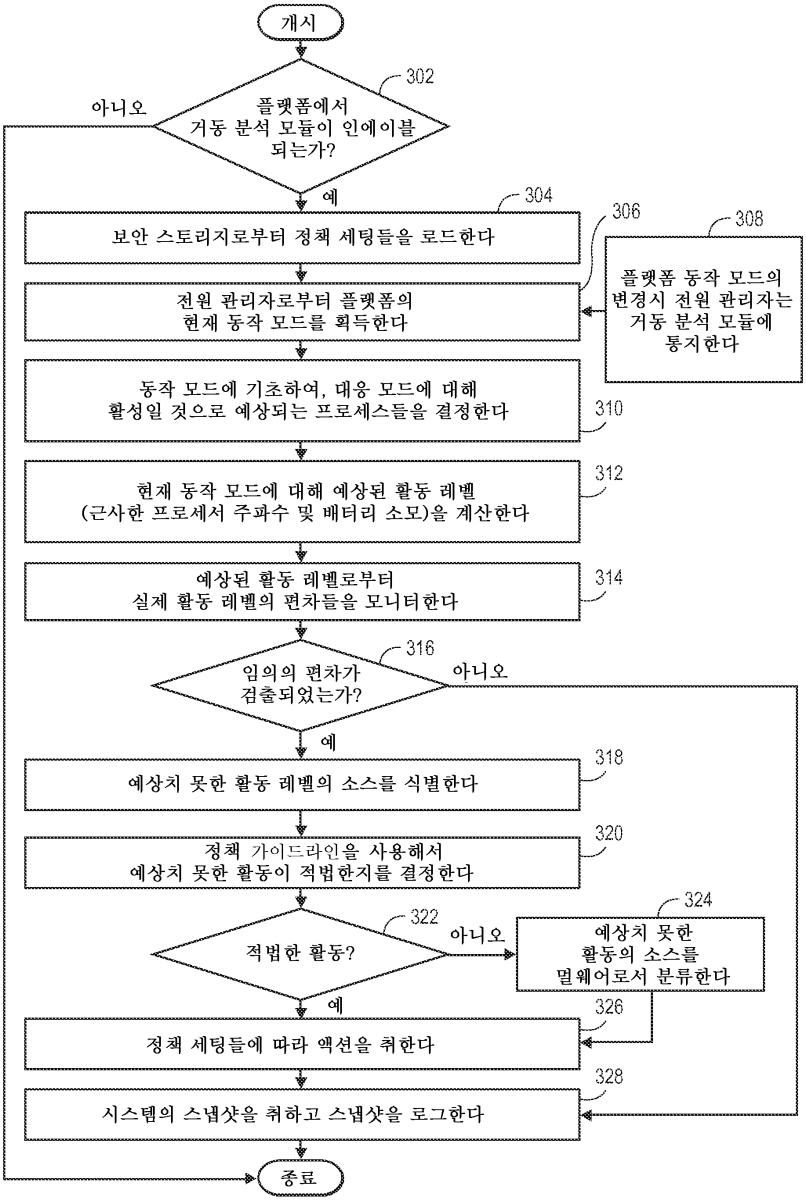
도면1



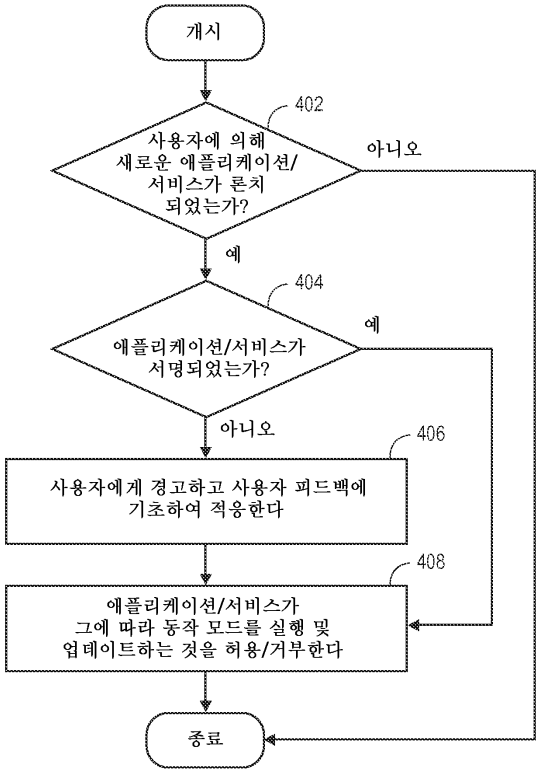
도면2


200
212
거동 분석 사용자 인터페이스
205
모바일 OS
전원 관리자
207
SEI 214
거동 분석 모듈
240
프로세서 모니터
241
배터리 모니터
242
웨이크 이벤트 모니터
243
통신/로깅 에이전트
244
SEI 214
디스플레이 컨트롤러
202
메모리
204
통신 컨트롤러
206
시스템 컨트롤 유닛
208
프로세서
210
보안 엔진
230
보안 스토리지
232
배터리
250

도면3


개시
302
플랫폼에서 거동 분석 모듈이 인에이블 되는가?
아니오
예
304
보안 스토리지로부터 정책 세팅들을 로드한다
306
308
플랫폼 동작 모드의 변경시 전원 관리자는 거동 분석 모듈에 통지한다
전원 관리자로부터 플랫폼의 현재 동작 모드를 획득한다
동작 모드에 기초하여, 대응 모드에 대해 활성일 것으로 예상되는 프로세스들을 결정한다
310
현재 동작 모드에 대해 예상된 활동 레벨 (근사한 프로세서 주파수 및 배터리 소모)을 계산한다
312
예상된 활동 레벨로부터 실제 활동 레벨의 편차들을 모니터한다
314
316
임의의 편차가 검출되었는가?
아니오
예
318
예상치 못한 활동 레벨의 소스를 식별한다
정책 가이드라인을 사용해서 예상치 못한 활동이 적법한지를 결정한다
320
322
적법한 활동?
아니오
324
예상치 못한 활동의 소스를 멀웨어로서 분류한다
예
326
정책 세팅들에 따라 액션을 취한다
328
시스템의 스냅샷을 취하고 스냅샷을 로그한다
종료

도면4


개시
402
사용자에 의해
새로운 애플리케이션/
서비스가 론치
되었는가?
아니오
예
404
애플리케이션/서비스가
서명되었는가?
예
아니오
406
사용자에게 경고하고 사용자 피드백에
기초하여 적응한다
408
애플리케이션/서비스가
그에 따라 동작 모드를 실행 및
업데이트하는 것을 허용/거부한다
종료