(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2025년02월18일
(11) 등록번호 10-2768835
(24) 등록일자 2025년02월12일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) *G06F 21/64* (2013.01)
(52) CPC특허분류
H04L 63/123 (2013.01)
G06F 21/645 (2013.01)
(21) 출원번호 10-2021-7014616
(22) 출원일자(국제) 2019년11월13일
심사청구일자 2022년11월10일
(85) 번역문제출일자 2021년05월14일
(65) 공개번호 10-2021-0092745
(43) 공개일자 2021년07월26일
(86) 국제출원번호 PCT/IL2019/051238
(87) 국제공개번호 WO 2020/105032
국제공개일자 2020년05월28일
(30) 우선권주장
263181 2018년11월21일 이스라엘(IL)
(56) 선행기술조사문헌
US20070244974 A1*
US20180097829 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
카주아르 어드밴스드 테크놀로지스 리미티드
이스라엘 텔아비브 6744332 이갈 알론 스트리트 126
(72) 발명자
핀첼스타인 다니엘 몬디
이스라엘 7583160 리숀 레지온 하히트야쉬붓 스트리트 10
포랏 유발 모쉐
이스라엘 6200932 텔아비브-야파 스데롯 스무츠 스트리트 20
펜스터 야콥
이스라엘 4960326 페탁 티크바 브란데 스트리트 58
(74) 대리인
특허법인와이에스장

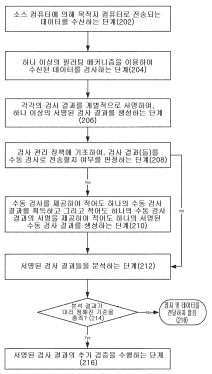
전체 청구항 수 : 총 14 항 심사관 : 문형섭

(54) 발명의 명칭 **보안 통신 방법 및 그 시스템**

(57) 요 약

소스 컴퓨터와 목적지 컴퓨터 사이의 보안 통신을 위한 컴퓨터화된 방법이 제공되며, 이 방법은 검사 컴퓨터에 의해 수행되고, 소스 컴퓨터에 의해 목적지 컴퓨터로 전송되는 데이터를 수신하는 단계; 하나 이상의 필터링 메커니즘을 사용하여 수신된 데이터를 검사하여 하나 이상의 검사 결과를 생성하는 단계; 하나 이상의 검사 결과 각각에 개별적으로 서명하는 단계; 검사 관리 정책에 기초하여 검사 결과 및/또는 그것의 파생물 중 적어도 일부를 수동 검사를 위해 전송할지 여부를 판정하는 단계; 긍정적인 판정 시, 적어도 일부의 검사 결과 및/또는 그것의 파생물의 수동 검사를 제공하고, 적어도 하나의 수동 검사 결과에 서명을 제공하는 단계; 및 상기 분석 결과가 상기 검사 관리 정책에 규정된 사전 정의된 기준을 충족하는 경우 서명된 검사 결과를 분석하고 서명된 검사 결과의 추가 검증을 수행하는 단계를 포함한다.

대 표 도 - 도2



(52) CPC특허분류
H04L 63/0227 (2013.01)
H04L 63/0471 (2013.01)
H04L 63/20 (2013.01)

명 세 서

청구범위

청구항 1

소스 컴퓨터와 목적지 컴퓨터 사이의 보안 통신을 위한 컴퓨터화된 방법으로서, 상기 방법은:

상기 소스 컴퓨터 및 상기 목적지 컴퓨터를 검사 컴퓨터와 작동 가능하게 연결할 때, 상기 소스 컴퓨터에 의해 상기 목적지 컴퓨터로 전송되는 데이터를 상기 검사 컴퓨터가 수신하는 단계;

상기 검사 컴퓨터에 의해, 하나 이상의 필터링 메커니즘을 사용하여 수신된 데이터를 검사하여, 각각의 필터링 메커니즘에 각각 대응하는 하나 이상의 검사 결과를 생성하는 단계로서, 각각의 검사 결과는 상기 수신된 데이터의 검사된 상태를 나타내는 것인 상기 하나 이상의 검사 결과를 생성하는 단계;

상기 검사 컴퓨터에 의해, 상기 하나 이상의 검사 결과 각각에 개별적으로 서명하여, 하나 이상의 서명된 검사 결과를 생성하는 단계;

상기 검사 컴퓨터에 의해, 검사 관리 정책에 기초하여 상기 수신된 데이터의 상기 검사 결과 및/또는 그것의 파생물 중 적어도 일부를 수동 검사를 위해 전송할지 여부를 판정하는 단계로서, 상기 검사 관리 정책은 상기 수신된 데이터와 연관된 하나 이상의 속성에 대해 규정되는 것인, 상기 판정하는 단계;

긍정적인 판정 시, 상기 검사 컴퓨터에 의해 전송된 적어도 일부의 검사 결과 및/또는 그것의 파생물에 대한 수동 검사를 제공하여, 승인 상태를 나타내는 적어도 하나의 수동 검사 결과를 생성하고, 그리고 상기 적어도 하나의 수동 검사 결과의 서명을 제공하여, 적어도 하나의 서명된 수동 검사 결과를 생성하는 단계; 및

상기 검사 컴퓨터에 의해, 상기 검사 관리 정책에 의해 규정된 사전 정의된 기준에 기반하여, i) 상기 하나 이상의 서명된 검사 결과 및 ii) 상기 적어도 하나의 서명된 수동 검사 결과 중 적어도 하나를 포함하는 서명된 검사 결과를 분석하고, 상기 사전 정의된 기준은 승인을 나타내는 서명된 검사 결과의 수 및/또는 가중치가 적용된 승인을 나타내는 서명된 검사 결과의 합계에 기반하고, 그리고 그 분석 결과가 상기 사전 정의된 기준을 충족하는 경우 상기 서명된 검사 결과에 대한 추가 검증을 수행하는 단계를 포함하고, 상기 추가 검증은 상기 하나 이상의 서명된 검사 결과 및/또는 상기 적어도 하나의 서명된 수동 검사 결과의 완전성 및 정확성을 검증하여, 상기 수신된 데이터에 대응하는 검사된 데이터를 상기 목적지 컴퓨터로 전송할지 여부를 판정하는 것을 특징으로 하는 소스 컴퓨터와 목적지 컴퓨터 사이의 보안 통신을 위한 컴퓨터화된 방법.

청구항 2

제 1 항에 있어서, 상기 검사 컴퓨터는 하나 이상의 필터링 메커니즘을 갖도록 구성되고 하나 이상의 보안 서명 메커니즘과 연관된 하나 이상의 검사자를 포함하고, 그리고 상기 수신된 데이터는 각 검사자의 각각의 필터링 메커니즘을 사용하여 각 검사자에 의해 개별적으로 검사되고, 상기 하나 이상의 검사 결과 각각은 대응하는 검사자의 각각의 보안 서명 메커니즘을 사용하여 대응하는 검사자에 의해 개별적으로 서명되는 것을 특징으로 하는 소스 컴퓨터와 목적지 컴퓨터 사이의 보안 통신을 위한 컴퓨터화된 방법.

청구항 3

제 1 항에 있어서, 상기 하나 이상의 필터링 메커니즘은 멀웨어 탐지, 데이터 유출 방지, 표현 인식, 형식 변환, 리댁팅 변경(redactiong modification) 및 데이터 필터링을 포함하는 필터링 메커니즘 그룹에서 선택되는 것을 특징으로 하는 소스 컴퓨터와 목적지 컴퓨터 사이의 보안 통신을 위한 컴퓨터화된 방법.

청구항 4

제 3 항에 있어서, 상기 선택은 상기 검사 관리 정책 및 상기 수신된 데이터를 기반으로 하는 것을 특징으로 하는 소스 컴퓨터와 목적지 컴퓨터 사이의 보안 통신을 위한 컴퓨터화된 방법.

청구항 5

제 1 항에 있어서, 상기 검사 결과 중 적어도 하나는 상기 수신된 데이터의 검사된 상태 및 상기 수신된 데이터

에 대응하는 검사된 데이터를 포함하는 것을 특징으로 하는 소스 컴퓨터와 목적지 컴퓨터 사이의 보안 통신을 위한 컴퓨터화된 방법.

청구항 6

제 2 항에 있어서, 상기 수동 검사는 보안 서명 메커니즘과 각각 연관된 적어도 하나의 수동 검사자에 의해 수행되고, 상기 적어도 하나의 수동 검사 결과의 서명은 상기 적어도 하나의 수동 검사자 각각에 의해 검사자와 연관된 상기 보안 서명 메커니즘을 사용하여 개별적으로 수행되는 것을 특징으로 하는 소스 컴퓨터와 목적지 컴퓨터 사이의 보안 통신을 위한 컴퓨터화된 방법.

청구항 7

제 6 항에 있어서, i) 상기 하나 이상의 검사자와 연관된 상기 보안 서명 메커니즘 및 ii) 상기 적어도 하나의 수동 검사자 각각과 연관된 상기 보안 서명 메커니즘 중 적어도 일부는 보안 환경에서 실행되는 암호화 서명인 것을 특징으로 하는 소스 컴퓨터와 목적지 컴퓨터 사이의 보안 통신을 위한 컴퓨터화된 방법.

청구항 8

제 7 항에 있어서, 상기 암호화 서명은 보호된 메모리 영역의 지정된 보안 엔클레이브에서 실행되는 것을 특징으로 하는 소스 컴퓨터와 목적지 컴퓨터 사이의 보안 통신을 위한 컴퓨터화된 방법.

청구항 9

제 7 항에 있어서, 상기 하나 이상의 검사자 및 상기 적어도 하나의 수동 검사자 각각은 검사자에 지정된 각각의 보안 엔클레이브를 갖고, 그 지정된 보안 엔클레이브에서 실행되는 암호화 서명인, 검사자와 연관된 보안 서명 메커니즘을 갖는 것을 특징으로 하는 소스 컴퓨터와 목적지 컴퓨터 사이의 보안 통신을 위한 컴퓨터화된 방법.

청구항 10

제 1 항에 있어서, 상기 수신된 데이터와 연관된 하나 이상의 속성은 상기 수신된 데이터의 하나 이상의 속성, 상기 데이터를 전송하는 상기 소스 컴퓨터의 하나 이상의 속성 및 상기 데이터가 전송되는 환경의 하나 이상의 속성으로 구성된 그룹에서 선택되는 것을 특징으로 하는 소스 컴퓨터와 목적지 컴퓨터 사이의 보안 통신을 위한 컴퓨터화된 방법.

청구항 11

제 1 항에 있어서, 상기 검사 컴퓨터에 의해, 상기 하나 이상의 검사 결과를 집계된 검사 결과로 집계하고 상기 집계된 검사 결과를 수동 검사로 보낼지 여부를 판정하는 단계를 더 포함하고, 상기 수동 검사는 상기 집계된 검사 결과에 대해 수행되는 것을 특징으로 하는 소스 컴퓨터와 목적지 컴퓨터 사이의 보안 통신을 위한 컴퓨터화된 방법.

청구항 12

제 2 항에 있어서, 상기 검사 관리 정책은 상기 하나 이상의 검사자의 사전 정의된 오더의 목록을 포함하고, 상기 수신된 데이터는 상기 사전 정의된 오더의 목록 중 하나에서 상기 하나 이상의 검사자에 의해 검사되고 서명되어, 제 1 검사자를 제외한 각 검사자가 상기 수신된 데이터 및 이전에 서명을 수행한 한 명 이상의 이전 검사자의 하나 이상의 서명을 포함하는 콘텐츠에 서명하여, 서명 체인을 생성하고, 그리고 상기 추가 검증은 상기 서명 체인 내의 각 서명의 완전성 및 정확성의 검증 및 상기 서명 체인의 오더가 상기 사전 정의된 오더의 목록에 속하는지 여부의 검증을 포함하는 것을 특징으로 하는 소스 컴퓨터와 목적지 컴퓨터 사이의 보안 통신을 위한 컴퓨터화된 방법.

청구항 13

소스 컴퓨터 및 목적지 컴퓨터에 동작 가능하게 연결된 검사 컴퓨터로서, 상기 검사 컴퓨터는 제 1 항 내지 제 12 항 중 어느 한 항의 방법 단계들을 수행하도록 구성된 것을 특징으로 하는 소스 컴퓨터 및 목적지 컴퓨터에 동작 가능하게 연결된 검사 컴퓨터.

청구항 14

컴퓨터에 의해 실행될 때 컴퓨터로 하여금 제 1 항 내지 제 12 항 중 어느 한 항의 방법 단계를 수행하게 하는 명령들의 프로그램을 실체적으로 구현하는 것을 특징으로 하는 비 일시적 컴퓨터 판독 가능 저장 매체.

청구항 15

삭제

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 일반적으로 데이터 통신 분야에 관한 것이며, 더욱 상세하게는 소스 컴퓨터와 목적지 컴퓨터 간의 통신 보호에 관한 것이다.

배 경 기 술

[0002] 현대 정보 시대에, 개인 정보 및 기관 정보를 포함하는 방대한 양의 데이터가 전 세계에 걸친 네트워크에 침투하고 있다. 그러나, 컴퓨터 장치 및 컴퓨터 네트워크에 대한 정보 보안 위반 및 공격은 점점 더 정교해지면서 놀라운 속도로 증가하고 있어 원치 않는 데이터 유출과 조직 자산에 대한 잠재적인 위험/손상을 일으킨다.

[0003] 보안 산업은 신규성, 효율성, 기능 세트 및 보안에 대한 전반적인 접근 방식의 측면에서 데이터 보안 제품의 급속한 발전을 이루었다. 현재, 예컨대, 바이러스 백신 소프트웨어 설치, 방화벽 사용, 데이터 보호 정책 수립, 데이터 분류, ID 및 액세스 관리 등과 같은 데이터 보안 및 무결성을 보장하기 위해 특정 기술과 조치가 사용된다.

[0004] 그러나, 데이터 보안 및 무결성을 보장하고 보존하기 위한 안전한 데이터 통신이 여전히 필요하다.

발명의 내용

과제의 해결 수단

[0005] (일반적인 설명)

[0006] 현재 개시된 주제의 특정 양태에 따라, 소스 컴퓨터와 목적지 컴퓨터 사이의 보안 통신을 위한 컴퓨터화된 방법이 제공되며, 이 방법은: 소스 컴퓨터 및 목적지 컴퓨터를 검사 컴퓨터와 작동 가능하게 연결할 때, 소스 컴퓨터에 의해 목적지 컴퓨터로 전송되는 데이터를 검사 컴퓨터에 의해 수신하는 단계; 검사 컴퓨터에 의해, 하나 이상의 필터링 메커니즘을 사용하여 수신된 데이터를 검사하여, 각각의 필터링 메커니즘에 각각 대응하는 하나 이상의 검사 결과(각각의 검사 결과는 수신된 데이터의 검사된 상태를 나타냄)를 생성하는 단계; 검사 컴퓨터에 의해 하나 이상의 검사 결과 각각에 개별적으로 서명하여 하나 이상의 서명된 검사 결과를 생성하는 단계; 검사 컴퓨터에 의해, 검사 관리 정책에 기초하여 검사 결과 및/또는 그것의 파생물 중 적어도 일부를 수동 검사를 위해 전송할지 여부를 판정하는 단계로서, 이 검사 관리 정책은 수신된 데이터와 연관된 하나 이상의 속성에 대해 규정된 것인, 상기 판정하는 단계; 긍정적인 판정 시, 검사 컴퓨터에 의해 전송된 적어도 일부의 검사 결과 및/또는 그것의 파생물에 대한 수동 검사를 제공하여 승인 상태를 나타내는 적어도 하나의 수동 검사 결과를 생성하고, 그리고 적어도 하나의 수동 검사 결과의 서명을 제공하여 적어도 하나의 서명된 수동 검사 결과를 생성하는 단계; 및 검사 컴퓨터에 의해 i) 하나 이상의 서명된 검사 결과 및 ii) 적어도 하나의 서명된 수동 검사 결과 중 적어도 하나를 포함하는 서명된 검사 결과를 분석하고, 그리고 분석 결과가 검사 관리 정책에 의해 규정된 사전 정의된 기준을 충족하는 경우 서명된 검사 결과에 대한 추가 검증을 수행하는 단계를 포함하고, 추가 검증은 수신된 데이터에 대응하는 검사된 데이터를 목적지 컴퓨터로 전송할지 여부를 판정한다.

[0007] 상기 특징에 더하여, 현재 개시된 주제의 이 양태에 따른 방법은 기술적으로 가능한 임의의 원하는 조합 또는 순열로 아래 나열된 특징 (i) 내지 (xiii) 중 하나 이상을 포함할 수 있다:

[0008] (i). 검사 컴퓨터는 하나 이상의 필터링 메커니즘으로 구성되고 하나 이상의 보안 서명 메커니즘과 연관된 하나 이상의 검사자를 포함할 수 있다. 수신된 데이터는 각각의 필터링 메커니즘을 사용하여 각 검사자에 의해 개별적으로 검사될 수 있으며, 하나 이상의 검사 결과 각각은 각각의 보안 서명 메커니즘을 사용하여 대응하는 검사자에 의해 개별적으로 서명될 수 있다.

[0009] (ii). 하나 이상의 필터링 메커니즘은 멀웨어 탐지, 데이터 유출 방지, 표현 인식, 형식 변환, 리댁팅 변경(redactiong modification) 및 데이터 필터링을 포함하는 필터링 메커니즘 그룹에서 선택될 수 있다.

[0010] (iii). 선택은 검사 관리 정책 및 수신된 데이터를 기반으로 할 수 있다.

[0011] (iv). 검사 결과 중 적어도 하나는 수신 데이터의 검사 상태 및 수신 데이터에 대응하는 검사 데이터를 포함할 수 있다.

[0012] (V). 수동 검사는 각각 보안 서명 메커니즘과 연관된 적어도 하나의 수동 검사자에 의해 수행될 수 있으며, 적어도 하나의 수동 검사 결과의 서명은 그것과 연관된 보안 서명 메커니즘을 사용하여 적어도 하나의 수동 검사자 각각에 의해 개별적으로 수행될 수 있다.

[0013] (vi) 하나 이상의 검사자와 연관된 보안 서명 메커니즘 및 ii) 적어도 하나의 수동 검사자 각각과 연관된 보안 서명 메커니즘 중 적어도 일부는 보안 환경에서 실행되는 암호화 서명일 수 있다.

[0014] (vii). 암호화 서명은 보호된 메모리 영역의 지정된 보안 영역에서 실행될 수 있다.

[0015] (viii). 하나 이상의 검사자 및 적어도 하나의 수동 검사자 각각은 그것에 지정된 각각의 보안 엔클레이브(enclave)를 가질 수 있고, 지정된 보안 엔클레이브에서 실행되는 암호화 서명인 그것과 연관된 보안 서명 메커니즘을 가질 수 있다.

[0016] (ix). 수신된 데이터와 연관된 하나 이상의 속성은 수신된 데이터의 하나 이상의 속성, 데이터를 전송하는 소스 컴퓨터의 하나 이상의 속성, 및 데이터가 전송되는 환경의 하나 이상의 속성을 포함하는 그룹으로부터 선택될 수 있다.

[0017] (x). 이 방법은 검사 컴퓨터에 의해 하나 이상의 검사 결과를 집계된 검사 결과로 집계하고, 집계된 검사 결과를 수동 검사를 위해 전송할지 여부를 판정하는 단계를 더 포함할 수 있다. 수동 검사는 집계된 검사 결과에 대해 수행될 수 있다.

[0018] (xi). 사전 정의된 기준은 검사 관리 정책에 규정된 가중치 서명 검사 결과의 합계를 기반으로 할 수 있다.

[0019] (xii). 추가 검증은 하나 이상의 서명된 검사 결과 및/또는 적어도 하나의 서명된 수동 검사 결과의 완전성과 정확성을 검증하는 것을 포함할 수 있다.

[0020] (xiii). 검사 관리 정책은 하나 이상의 검사자의 사전 정의된 오더(order)의 목록을 포함하고, 수신된 데이터는 사전 정의된 오더의 목록 중 하나에서 상기 하나 이상의 검사자에 의해 검사되고 서명되어, 제 1 검사자를 제외한 각 검사자가 수신된 데이터와 이전에 서명을 수행한 한 명 이상의 이전 검사자의 하나 이상의 서명을 포함한 콘텐츠에 서명하여 서명 체인을 생성하고, 그리고 추가 검증은 서명 체인의 각 서명의 완전성 및 정확성의 검증 및 서명 체인의 주문이 사전 정의된 오더의 목록에 속하는지 여부의 검증을 포함한다.

[0021] 현재 개시된 주제의 다른 양태에 따라, 소스 컴퓨터와 작동 가능하게 연결된 검사 컴퓨터 및 검사 컴퓨터를 갖는 목적지 컴퓨터가 제공되며, 이 검사 컴퓨터는: 소스 컴퓨터에 의해 목적지 컴퓨터로 전송되는 데이터를 수신하고; 하나 이상의 필터링 메커니즘을 사용하여 수신된 데이터를 검사하여, 각각의 필터링 메커니즘에 각각 대응하는 하나 이상의 검사 결과(각각의 검사 결과는 수신된 데이터의 검사된 상태를 나타냄)를 발생시키고; 하나 이상의 검사 결과 각각에 개별적으로 서명하여 하나 이상의 서명된 검사 결과를 생성하고; 수신된 데이터와 연관된 하나 이상의 속성과 관련하여 규정된 검사 관리 정책에 기초하여, 수동 검사를 위해 검사 결과 및/또는 그것의 파생물의 적어도 일부를 전송할지 여부를 판정하고; 긍정적인 판정시, 검사 컴퓨터에 의해 전송된 적어도 일부의 검사 결과 및/또는 그것의 파생물에 대한 수동 검사를 제공하여, 승인 상태를 나타내는 적어도 하나의 수동 검사 결과를 생성하고, 그리고 적어도 하나의 수동 검사 결과의 서명을 제공하여 적어도 하나의 서명된 수동 검사 결과를 제공하고; 그리고 검사 컴퓨터에 의해, i) 하나 이상의 서명된 검사 결과 및 ii) 적어도 하나의 서명된 수동 검사 결과 중 적어도 하나를 포함하는 서명된 검사 결과를 분석하고, 그리고 분석 결과가 검사 관리 정책에 의해 규정된 사전 정의된 기준을 충족하는 경우 서명된 검사 결과에 대한 추가 검증을 수행하도록 구성되고, 추가 검증은 수신된 데이터에 대응하는 검사된 데이터를 목적지 컴퓨터로 전송할지 여부를 판정한다.

[0022] 개시된 주제의 이러한 양태는 기술적으로 가능한 임의의 원하는 조합 또는 순열로 필요한 부분만 약간 수정하여 방법과 관련하여 위에 나열된 특징 (i) 내지 (xiii) 중 하나 이상을 포함할 수 있다.

[0023] 현재 개시된 주제의 다른 양태에 따라, 컴퓨터에 의해 실행될 때 컴퓨터가 소스 컴퓨터와 목적지 컴퓨터 사이의 보안 통신 방법을 수행하게 하는 명령들의 프로그램을 실체적으로 구현하는 비 일시적 컴퓨터 판독 가능 저장 매체가 제공되며, 이 방법은: 소스 컴퓨터 및 목적지 컴퓨터를 검사 컴퓨터와 작동 가능하게 연결할 때, 소스 컴퓨터에 의해 목적지 컴퓨터로 전송되는 데이터를 검사 컴퓨터에 의해 수신하는 단계; 검사 컴퓨터에 의해, 하나 이상의 필터링 메커니즘을 사용하여 수신된 데이터를 검사하여 각각의 필터링 메커니즘에 각각 대응하는 하나 이상의 검사 결과를 발생시키는 단계(각각의 검사 결과는 수신된 데이터의 검사된 상태를 나타냄); 검사 컴퓨터에 의해, 하나 이상의 검사 결과 각각에 개별적으로 서명하여 하나 이상의 서명된 검사 결과를 생성하는 단계; 검사 컴퓨터에 의해 그리고 검사 관리 정책에 기초하여, 수동 검사를 위해 검사 결과 및/또는 그것의 파생

물 중 적어도 일부를 전송할지 여부를 판정하는 단계로서, 검사 관리 정책은 수신된 데이터와 연관된 하나 이상의 속성과 연관지어 규정된 것인 상기 판정하는 단계; 긍정적인 판정 시, 검사 컴퓨터에 의해 전송된 적어도 일부의 검사 결과 및/또는 파생물에 대한 수동 검사를 제공하여, 승인 상태를 나타내는 적어도 하나의 수동 검사 결과를 생성하고, 그리고 적어도 하나의 수동 검사 결과의 서명을 제공하여 적어도 하나의 서명된 수동 검사 결과를 제공하는 단계; 및 검사 컴퓨터에 의해, i) 하나 이상의 서명된 검사 결과 및 ii) 적어도 하나의 서명된 수동 검사 결과 중 적어도 하나를 포함하는 서명된 검사 결과를 분석하고 그리고 분석 결과가 검사 관리 정책에 규정된 사전 정의된 기준을 충족하는 경우 서명된 검사 결과의 추가 검증을 수행하는 단계를 포함하고, 추가 검증은 수신된 데이터에 대응하는 검사된 데이터를 목적지 컴퓨터로 전송할지 여부를 판정한다.

[0024] 개시된 주제의 이러한 양태는 기술적으로 가능한 임의의 원하는 조합 또는 순열로 필요한 부분만 약간 수정하여 방법과 관련하여 위에 나열된 특징 (i) 내지 (xiii) 중 하나 이상을 포함할 수 있다.

도면의 간단한 설명

[0025] 이제, 본 발명을 이해하고 그것이 실제로 실시될 수 있는 방법을 보기 위해, 실시예들이 첨부된 도면을 참조하여 비 제한적인 예로서 설명될 것이다.

도 1은 현재 개시된 본 발명의 특정 실시예에 따른 검사 컴퓨터 시스템의 개략적인 블록도를 도시한다.

도 2는 현재 개시된 본 발명의 특정 실시예에 따른 소스 컴퓨터와 목적지 컴퓨터 사이의 보안 통신의 일반화된 흐름도를 도시한다.

도 3은 현재 개시된 본 발명의 특정 실시예에 따른 클라이언트-서버 통신 아키텍처에서 클라이언트-서버 경로 및 서버-클라이언트 경로에 대한 보안 통신을 보장하는 개략도이다.

발명을 실시하기 위한 구체적인 내용

[0026] 아래의 상세한 설명에서, 본 발명의 완전한 이해를 제공하기 위해 많은 특정 세부사항이 설명된다. 그러나, 현재 개시된 본 발명은 이러한 특정 세부사항 없이도 실시될 수 있다는 것을 당업자는 이해할 것이다. 다른 예에서, 현재 개시된 본 발명을 모호하게 하지 않도록 잘 알려진 방법, 절차, 구성 요소 및 회로는 상세히 설명되지 않았다.

[0027] 달리 구체적으로 언급되지 않는 한, 다음 논의로부터 명백한 바와 같이, 명세서 논의 전반에 걸쳐 "수신하는 것", "연결하는 것", "송신하는 것", "검사하는 것", "필터링하는 것", "서명하는 것", "판정하는 것", "제공하는 것", "분석하는 것", "수행하는 것", "검증하는 것", "집계하는 것" 등은 데이터를 조작하고 및/또는 다른 데이터로 변환하는 컴퓨터의 작업(들) 및/또는 프로세스(들)를 의미한다는 것을 이해해야 하며, 상기 데이터는 전자, 수량과 같이 물리적으로 표현되고, 및/또는 상기 데이터는 물리적 대상을 나타낸다. 본 명세서에서 사용되는 "컴퓨터"라는 용어는 비 제한적인 예로서 검사 컴퓨터 및 그것의 일부분, 뿐만 아니라 그 내부에 포함된 처리 및 메모리 장치 및 프로세서를 포함하여 데이터 처리 기능을 갖춘 모든 종류의 하드웨어 기반 전자 장치를 포함하도록 광범위하게 해석되어야 한다.

[0028] 본 명세서에서 사용되는 "비 일시적 메모리" 및 "비 일시적 저장 매체"라는 용어는 현재 개시된 본 발명에 적합한 임의의 휘발성 또는 비 휘발성 컴퓨터 메모리를 포함하도록 광범위하게 해석되어야 한다.

[0029] 현재 개시된 본 발명의 실시예는 임의의 특정 프로그래밍 언어를 참조하여 설명되지 않는다. 본 명세서에 설명된 현재 개시된 본 발명의 교시를 구현하기 위해 다양한 프로그래밍 언어가 사용될 수 있다는 것이 이해될 것이다.

[0030] 본 명세서에서 사용된 바와 같이, "예를 들어", "~와 같은", "예컨대" 및 이의 변형은 현재 개시된 본 발명의 비 제한적인 실시예를 설명한다. 명세서에서 "일 경우", "일부 경우", "다른 경우" 또는 그 변형에 대한 언급은 실시예(들)와 관련하여 설명된 특정 특징, 구조 또는 특성이 현재 개시된 본 발명의 적어도 하나의 실시예에 포함된다는 것을 의미한다. 따라서, "일 경우", "일부 경우", "다른 경우" 또는 그 변형의 표현이 반드시 동일한 실시예(들)를 지칭하는 것은 아니다.

[0031] 달리 구체적으로 언급되지 않는 한, 별도의 실시예의 맥락에서 설명된 현재 개시된 본 발명의 특정 특징이 단일 실시예에서 조합되어 제공될 수도 있다는 것이 이해될 것이다. 반대로, 단일 실시예의 맥락에서 설명된 현재 개시된 본 발명의 다양한 특징은 또한 개별적으로 또는 임의의 적절한 하위 조합으로 제공될 수 있다. 아래의

상세한 설명에서, 방법 및 장치에 대한 완전한 이해를 제공하기 위해 다수의 특정 세부사항이 설명된다.

[0032] 이를 염두에 두고, 현재 개시된 주제의 특정 실시예에 따른 검사 컴퓨터 시스템의 개략적인 블록도를 도시하는 도 1에 주의를 기울인다.

[0033] 도 1에 도시된 시스템(100)은 소스 컴퓨터(101) 및 목적지 컴퓨터(120)에 작동 가능하게 연결된 검사 컴퓨터를 지칭한다. 검사 컴퓨터는 소스 컴퓨터(101)와 목적지 컴퓨터(120) 사이의 안전한 데이터 통신을 보장하기 위해 사용될 수 있다. 특정 실시예에 따르면, 소스 컴퓨터는 목적지 컴퓨터로의 데이터 전송을 초기화하는 요청 컴퓨터화된 엔티티를 지칭하고, 목적지 컴퓨터는 전송된 데이터를 수신하는 수신 컴퓨터화된 엔티티를 지칭한다.

[0034] 소스 컴퓨터 및 목적지 컴퓨터는 임의의 적절한 데이터 통신 방식 및 구조에서 서로 연결 및 통신할 수 있는 임의의 컴퓨터화된 엔티티를 지칭할 수 있으며, 본 개시는 각 엔티티의 특정 유형, 구조 및/또는 기능/역할에 제한되지 않는다는 점에 유의해야 한다. 일부 실시예에서, 소스 컴퓨터 및 목적지 컴퓨터는 클라이언트-서버 통신 아키텍처에서 작동할 수 있다. 예를 들어, 소스 컴퓨터는 서버 역할을 하는 목적지 컴퓨터로 정보를 가져오는 요청을 개시하는 클라이언트를 의미할 수 있다. 다른 예로서, 소스 컴퓨터는 목적지 컴퓨터로 정보를 제공하거나 내보내는 서버를 의미할 수 있으며, 이에 따라 목적지 컴퓨터는 클라이언트 역할을 한다. 이러한 경우 중 한 예시적인 예는 로컬-원격 연결 체계일 수 있다. 예를 들어, 보험 회사와 같은 조직은 원격 사용자/에이전트가 자신의 내부 시스템에 연결하고 보험 견적을 받을 수 있도록 허용할 수 있다. 그러나 원격 사용자가 회사의 귀중한 정보를 유출하거나 내부 시스템에 멀웨어를 도입하지 않도록 조치를 취해야 한다. 따라서, 본 명세서에서 제안하는 검사 컴퓨터 시스템은 클라이언트-서버 경로 및/또는 서버-클라이언트 경로에 대한 보안 통신을 보장하기 위해 활용될 수 있다. 이러한 양태에 대한 자세한 내용은 도 3을 참조하여 아래에서 더 자세히 설명한다.

[0035] 도시된 바와 같이, 시스템(100)은 하드웨어 기반 I/O 인터페이스(126) 및 저장 유닛(122)에 동작 가능하게 연결된 프로세싱 및 메모리 유닛(PMU, 프로세싱 유닛이라고도 함)(102)을 포함할 수 있다. PMU(102)는 도 2를 참조하여 아래에서 더 상세히 설명되는 바와 같이 운영 체제(100)에 필요한 모든 처리를 제공하도록 구성된다. PMU(102)는 프로세서(별도로 도시되지 않음) 및 메모리(별도로 도시되지 않음)를 포함한다. PMU(102)의 프로세서는 PMU에 포함된 비 일시적 컴퓨터 판독 가능 메모리 상에 구현된 컴퓨터 판독 가능 명령에 따라 여러 기능 모듈을 실행하도록 구성될 수 있다. 이러한 기능 모듈은 이하 PMU에 포함된 것으로 언급된다. 본 명세서에서 언급된 프로세서라는 용어는 데이터 처리 능력을 갖는 임의의 처리 회로를 포괄하도록 광범위하게 해석되어야하며, 본 개시는 그 유형 또는 플랫폼, 또는 그 안에 포함된 처리 코어의 수로 제한되지 않는다는 점에 유의해야 한다.

[0036] PMU(102)에 포함된 기능 모듈은 하나 이상의 검사자(104), 정책 시행자(108), 및 검사자 및 정책 시행자와 작동 가능하게 연결된 컨트롤러(106)를 포함할 수 있다. 소스 컴퓨터(101)에 의해 목적지 컴퓨터(120)로 전송된 데이터를 I/O 인터페이스(126)를 통해 PMU가 수신하면, 하나 이상의 검사자(104)는 하나 이상의 필터링 메커니즘을 사용하여 수신된 데이터를 검사하도록 구성될 수 있으며, 각각의 필터링 메커니즘에 각각 대응하는 하나 이상의 검사 결과를 발생시킨다. 각각의 검사 결과는 수신된 데이터의 검사 상태를 나타낼 수 있다. 하나 이상의 검사자(104)는 하나 이상의 검사 결과 각각에 개별적으로 서명하도록 추가로 구성되어 하나 이상의 서명된 검사 결과를 생성할 수 있다. 컨트롤러(106)는 검사 관리 정책에 기초하여 수동 검사를 위해 검사 결과 및/또는 그것의 파생물 중 적어도 일부를 전송할지 여부를 판정하도록 구성될 수 있다. 검사 관리 정책은 수신된 데이터와 연관된 하나 이상의 속성과 관련하여 규정될 수 있다. 본 명세서에서 언급된 하나 이상의 검사자는 아래에서 더 설명되는 수동 검사자와 비교하여 PMU에 포함된 컴퓨터화된 기능 모듈이라는 점에 유의해야 한다.

[0037] 긍정적인 판정 시(즉, 컨트롤러가 수동 검사가 필요하다고 판정한 때), 수동 검사 모듈(110)은 검사 컴퓨터(예를 들어, 컨트롤러(106)에 의해 전송된 적어도 일부 검사 결과 및/또는 그것의 파생물의 수동 검사를 제공하여 승인 상태를 나타내는 적어도 하나의 수동 검사 결과를 생성하고, 적어도 하나의 수동 검사 결과의 서명을 제공하여 적어도 하나의 서명된 수동 검사 결과를 발생시키도록 구성될 수 있다. 컨트롤러(106)는 i) 하나 이상의 서명된 검사 결과 및 ii) 적어도 하나의 서명된 수동 검사 결과 중 적어도 하나를 포함하는 서명된 검사 결과를 분석하고 분석 결과가 검사 관리 정책에 규정된 사전 정의된 기준을 충족하는 경우 서명된 검사 결과의 추가 검증을 수행하도록 더 구성될 수 있다. 추가 검증은 수신된 데이터에 대응하는 검사된 데이터를 (예를 들어, I/O 인터페이스(126)를 통해) 목적지 컴퓨터로 전송할지 여부를 판정할 수 있다.

[0038] 특정 실시예에 따라, 시스템(100)은 저장 유닛(122)을 포함할 수 있다. 저장 유닛(122)은 운영 체제(100)에 필요한 임의의 데이터, 예를 들어 시스템(100)의 입력 및 출력과 연관된 데이터 및 시스템(100)에 의해 생성된 중

간 처리 결과를 저장하도록 구성될 수 있다. 예로서, 저장 유닛(122)은 소스 컴퓨터(101)로부터 수신된 데이터, 검사 결과(들), 검사된 데이터, 수동 검사 결과 및 서명된 검사 결과 등을 저장하도록 구성될 수 있다.

[0039] 일부 실시예에서, 시스템(100)은 시스템(100)과 연관된 사용자 지정 입력 및/또는 출력을 가능하게 하도록 구성된 컴퓨터 기반 그래픽 사용자 인터페이스(GUI)(124)를 선택적으로 포함할 수 있다. 예를 들어, 사용자는 수신된 데이터 및/또는 GUI에서 일부 검사 결과를 볼 수 있다. 선택적으로, 사용자는 GUI를 통해 시스템(100)의 특정 동작 파라미터를 정의하는 옵션을 제공받을 수 있다.

[0040] 본 기술 분야에 정통한 사람들은 현재 개시된 주제의 교시가 도 1에 도시된 시스템에 의해 구속되지 않는다는 것을 쉽게 이해할 것이다. 동등한 및/또는 수정된 기능은 통합되거나 다른 방식으로 분할될 수 있으며 소프트웨어와 펌웨어 및 하드웨어의 적절한 조합으로 구현될 수 있다.

[0041] 도 1에 도시된 시스템은 분산 컴퓨팅 환경에서 구현될 수 있으며, 여기서 하나 이상의 검사자(104) 또는 그 일부와 같은 도 1에 도시되고 전술한 기능 모듈 중 하나 이상이 정책 시행자(108) 및 컨트롤러(106)는 여러 로컬 및/또는 원격 장치를 통해 분산될 수 있고 통신 네트워크를 통해 연결될 수 있다. 또한, 저장 유닛(122) 및 GUI(124)가 도 1에서 시스템(100)의 일부인 것으로 도시되었지만, 일부 다른 실시예에서, 전술한 유닛 중 적어도 일부는 시스템(100)의 외부인 것으로 구현될 수 있고 I/O 인터페이스(126)를 통해 시스템(100)과 데이터 통신으로 동작하도록 구성된다.

[0042] 또한 일부 경우에 검사 컴퓨터는 독립형 컴퓨터(들)로 구현될 수 있고(예시적으로 도 1에 도시된 바와 같이) 소스 컴퓨터 및 목적지 컴퓨터에 작동 가능하게 연결되어 그것들과 함께 작동할 수도 있다. 일부 다른 경우에, 검사 컴퓨터 또는 그 기능의 적어도 일부는 소스 컴퓨터 및/또는 목적지 컴퓨터와 통합되어 그 기능을 용이하게 하고 향상시킬 수 있다. 그러한 경우에, 시스템(100)의 구성 요소 또는 그 적어도 일부는 소스 컴퓨터 및/또는 목적지 컴퓨터의 일부를 형성할 수 있다.

[0043] 이제, 현재 개시된 주제의 특정 실시예에 따른 소스 컴퓨터와 목적지 컴퓨터 사이의 보안 통신의 일반화된 흐름도를 도시하는 도 2를 참조한다.

[0044] 소스 컴퓨터와 목적지 컴퓨터를 검사 컴퓨터(예를 들어, 도 1에 도시된 검사 컴퓨터(100))와 작동 가능하게 연결하면, 데이터는(예를 들어, I/O 인터페이스(126)를 통해 PMU(102)에 의해) 검사 컴퓨터에 의해 수신되고(202), 이 데이터는 소스 컴퓨터에서 검사 컴퓨터를 통해 목적지 컴퓨터로 전송된다.

[0045] 전술한 바와 같이, 소스 컴퓨터 및 목적지 컴퓨터는 임의의 적절한 데이터 통신 방식 및 구조에서 서로 연결하고 통신할 수 있는 임의의 컴퓨터화된 엔티티를 지칭할 수 있다. 본 명세서에서 언급되는 바와 같이, 소스 컴퓨터에 의해 전송되는 데이터는 임의의 적절한 포맷 및/또는 구조로 표현될 수 있는 특정 정보를 나타내는 임의의 유형의 데이터를 포함할 수 있다. 예를 들어, 일부 경우에, 데이터는, 예를 들어, 이미지 파일, 텍스트 파일, 오디오 및/또는 비디오 파일 등과 같은 다른 가능한 파일 형식을 가진 파일 형식으로 표현될 수 있으며, 그 중 특정 형식은 이러한 파일과 연관된 특정 프로그램에 의해 결정될 수 있다. 그러나, 본 개시 내용은 그 표현의 특정 유형에 의해 제한되지 않는다. 또한, 예를 들어 인스턴트 메시지와 같은 전형적인 파일 형식과 연관되지 않고 전송되는 임의의 데이터도 본 개시 내용에 포함되는 것으로 해석되어야 한다.

[0046] 어떤 경우에 소스 컴퓨터와 목적지 컴퓨터가 이러한 검사를 인식하지 않고 기본적으로 검사 컴퓨터가 수신된 데이터의 검사를 수행할 수 있으며, 다른 경우에 검사 컴퓨터는 수신된 데이터를 검사하기 위해 소스 컴퓨터로부터 특정 요청을 수신하면 검사를 수행할 수 있다. 특정 실시예에 따르면, 일부 경우에, 소스 컴퓨터는 아래에 설명된 다른 동작을 진행하도록 허용되기 전에(예를 들어, 검사 컴퓨터에 의해) 인증되고 건강 검사를 받아야 할 필요가 있을 수 있다.

[0047] 수신된 데이터는 하나 이상의 필터링 메커니즘을 사용하여 검사 컴퓨터에 의해 검사될 수 있으며(204), 각각의 필터링 메커니즘에 각각 대응하는 하나 이상의 검사 결과를 발생시킨다. 하나 이상의 검사 결과 각각은 검사 컴퓨터에 의해 개별적으로 서명될 수 있으며(206), 서명된 하나 이상의 검사 결과가 발생한다. 특정 실시예에 따르면, 검사 컴퓨터는 하나 이상의 검사자(예를 들어, 도 1에 도시된 PMU에 포함된 하나 이상의 검사자(104))를 포함할 수 있다. 하나 이상의 검사자는 각각 하나 이상의 필터링 메커니즘으로 구성되고 하나 이상의 보안 서명 메커니즘과 연관될 수 있다. 수신된 데이터는 각각의 필터링 메커니즘을 사용하여 각 검사자에 의해 개별적으로 검사될 수 있다. 각각의 검사 결과는 각각의 보안 서명 메커니즘을 사용하여 해당 검사자가 별도로 서명할 수 있다.

[0048] 본 명세서에서 "필터링" 및 "필터링 메커니즘(들)"이라는 용어가 사용되지만, 수신된 데이터에서 원치 않는 특

징 또는 구성 요소를 단순히 제거하는 것으로 제한되는 것으로 해석되어서는 안되며, 수신된 데이터의 유효성을 검사하는데 사용할 수 있는 적절한 검사 메커니즘을 포함한다. 특정 실시예에 따르면, 하나 이상의 검사자의 하나 이상의 필터링 메커니즘은 멀웨어 탐지, 데이터 누출 방지, 표현 인식, 형식 변환, 리댁팅 변경 및 데이터 정리를 포함하는 필터링 메커니즘의 그룹으로부터 선택될 수 있다. 이러한 필터링 메커니즘의 예시적인 설명은 예시의 목적으로만 여기에 제공되며 어떤 방식으로든 본 개시 내용을 제한하려는 의도는 없다. 멀웨어 감지는 수신된 데이터에 포함된 악성 코드(예컨대, 안티 바이러스 소프트웨어에 사용되는 메커니즘)를 검색하는 것을 의미할 수 있다. 데이터 유출 방지란 귀중한 정보가 유출되는 것을 확인하고 방지하는 것을 의미한다. 표현 인식은 지정된 정규식/패턴과 일치하는 데이터를 감지할 수 있는 정규식 엔진을 참조할 수 있다. 형식 변환은 마이크로소프트 워드(Microsoft Word)를 PDF 또는 이미지 형식으로 변환하는 것과 같은 보안 목적을 위해 수신된 데이터의 형식을 서로 변환하는 것을 의미할 수 있다. 리댁팅 변경은 데이터 수정(예컨대, 보안 목적을 위해 특정 콘텐츠를 검열하거나 가리기 위해 데이터를 수정하는 등)을 위해 소스 컴퓨터에서 자동으로 전송된 데이터를 수정하는 것을 의미할 수 있다. 데이터 클렌징(Data cleansing)은 필요하지 않은 구성 요소를 감지하고 수정(또는 제거)하는 것을 의미하며, 예를 들어 데이터를 구성 요소로 분해하고 재구성하는 방식으로 원하지 않는 데이터를 전송하는데 사용될 수 있다.

[0049] 특정 실시예에 따르면, 주어진 수신 데이터에 사용될 하나 이상의 필터링 메커니즘 또는 하나 이상의 검사자의 선택은 검사 관리 정책 및 주어진 수신 데이터에 기초하여(예를 들어, 도 1에 도시된 바와 같은 컨트롤러(106)에 의해) 수행될 수 있다. 여기서 사용되는 검사 관리 정책은 검사 컴퓨터(특히, 컨트롤러)가 수신된 데이터의 검사를 수행하기 위해 구성되는 일련의 검사 규칙 및 구성을 의미할 수 있다. 검사 관리 정책은 블록(208)을 참조하여 아래에서 상세히 설명되는 바와 같이 검사될 각각의 수신된 데이터에 대해 구체적으로 판정된다.

[0050] 대응하는 검사자로부터의 각각의 검사 결과는 수신된 데이터의 검사 상태를 나타낼 수 있다. 일부 실시예에서, 검사 결과 중 적어도 하나는 수신된 데이터의 검사된 상태 및 수신된 데이터에 대응하는 검사된 데이터를 포함할 수 있다. 다양한 필터링 메커니즘과 수신된 데이터에 따라 다양한 유형의 검사 상태가 있을 수 있다. 예를 들어, 검사된 상태의 한 가지 유형은 문제가 발견되지 않았기 때문에 데이터가 무해하다는 긍정적인 표시를 제공한다. 또 다른 유형의 검사 상태는 발견된 문제와 연관된 설명 정보와 함께 하나 이상의 문제가 발견된 것일 수 있다. 이러한 경우, 추가 하위 카테고리가 있을 수 있다. 예를 들어, 클리닝이 수행되지 않아서 해결되지 않은 문제가 여전히 존재하는 상태, 또는 해결되지 않은 문제가 검사자에 의해 처리/해결되었으므로 더 이상 존재하지 않는 상태. 또 다른 유형의 검사 상태는 수신된 데이터에 대해 특정 수정이 수행되어 수신된 데이터의 수정된 버전인 검사된 데이터가 생성된 것일 수 있다. 기타 가능한 검사 상태 유형은 데이터를 처리할 수 없음, 데이터 판독 오류, 필터의 내부 오류, 필터링을 수행하기 위한 리소스 부족 등을 포함할 수 있다(그러나 이에 국한되지는 않는다).

[0051] 전술한 바와 같이, 하나 이상의 검사자는 각각 하나 이상의 보안 서명 메커니즘과 연관될 수 있다. 본 명세서에서 사용되는 용어 "서명"또는 "서명 메커니즘"은 메시지 또는 문서와 같은 디지털 데이터의 신뢰성 및 무결성을 제시하기 위해 디지털 서명을 제공하는데 사용되는 컴퓨팅 방식을 지칭한다. 유효한 디지털 서명은 전송된 메시지가 청구된 발신자(예컨대, 인증)에 의해 생성되었으며 메시지가 전송 중에 변경되지 않았음을(즉, 무결성) 믿을 수 있는 이유를 수신자에게 제공할 수 있으므로 위조 및/또는 변조를 감지하는데 사용할 수 있다. 하나 이상의 검사자와 연관된 보안 서명 메커니즘은 암호화 기반이다. 일반적으로 디지털 서명 또는 디지털 서명은 비대칭 암호화(예컨대, 공개 키 암호화)를 사용한다. 서명 메커니즘 또는 서명 체계를 사용하면 공개 키와 개인 키의 키 쌍을 소유 한 발신자가 개인 키를 사용하여 데이터에 서명할 수 있으며 수신자가 해당 공개 키를 사용하여 서명된 데이터(데이터와 함께 서명 포함)를 확인할 수 있다. 가능한 서명 메커니즘의 한 예는 RSA 알고리즘을 기반으로 할 수 있다.

[0052] 서명을 보호하기 위해서는 개인 키에 접근할 수 있는 사람은 누구나 소유자의 서명을 위조할 수 있기 때문에 개인 키를 비밀로 유지하기 위한 조치가 취해져야 한다. 키 보존을 위한 보안 환경을 제공하는 한 가지 예는 물리적 캐리어를 사용하는 것이다. 물리적 캐리어는 개인 키를 저장하는 하드웨어(예컨대, USB 동글/어댑터 등)이며, 장치에 연결되었을 때만 장치가 개인 키를 사용하여 서명을 수행할 수 있도록 한다. 따라서, 데이터에 서명하려면 물리적으로 동글이 있어야 하며, 이는 보안 서명 메커니즘에 대한 또 다른 보호 계층을 제공한다. 특정 실시예에서, 물리적 캐리어는 코딩될 수 있고 일부 경우에는 추가적인 보호 기능을 제공하기 위한 자체 프로세서를 갖는다.

[0053] 보안 환경을 제공하는 또 다른 예는 보안 엔클레이브를 사용하는 것이다. 보안 엔클레이브(본 명세서에서 SE 또는 엔클레이브라고도 함)는 애플리케이션이 코드를 실행하고 내부에 데이터를 저장할 수 있는 보안 영역(예를

들어, 분리 및 암호화 됨)을 제공하는 애플리케이션 또는 프로세스에 내장된 신뢰할 수 있는 실행 환경이다. 보안 엔클레이브는 보안 엔클레이브 명령과 연관된 프로세서에 의해 제공되는 액세스 제어 메커니즘을 사용하여 데이터가 보호되는 보호 메모리 영역에서 실행될 수 있다.

[0054] 예를 들어, 보안 엔클레이브는 인텔에 의해 SGX(Software Guard Extensions)로 구현된다. SGX는 해당 메모리 보호 의미 체계와 관리에 사용되는 명령을 사용하여 프로세서에서 실행되는 새로운 모드이다. SGX는 보호된 메모리 페이지를 원하는 코드와 데이터로 채우고, 코드와 데이터를 엔클레이브에 잠그고, 그 안에서 측정을 수행하여 보안 엔클레이브를 생성할 수 있다. 프로세서는 엔클레이브 내부에서 코드를 실행할 수 있다. 커널(링 0), 하이퍼 바이저(링 "-1"), SMM(링 "-2") 또는 AMT(링 "-3")를 포함한 다른 엔티티는 엔클레이브에 속하는 메모리 페이지를 읽거나 쓸 권한이 없다.

[0055] 다른 예로서, 보안 엔클레이브 또는 유사한 데이터 보안 및 액세스 제어 메커니즘(상이하게 지칭될 수 있음)은 예를 들어, AMD의 SEV(Secure Encrypted Virtualization) 및 ARM의 트러스트존(TrustZone) 등과 같은 다른 플랫폼 및/또는 벤더의 기술에 의해 구현된다.

[0056] 단지 예시의 목적으로, 아래 설명의 특정 실시예가 용어 보안 엔클레이브(들) 및 SGX와 관련하여 제공된다. 마찬가지로, 실시예는 위에서 예시된 바와 같이 상이한 플랫폼 및/또는 기술에서 구현되는 다른 유사한 데이터 보안 및 액세스 제어 메커니즘에 적용될 수 있다.

[0057] 특정 실시예에 따르면, 전술한 보안 엔클레이브는 개인 키를 보존하고 /하거나 키를 사용하여 서명을 실행하기 위한 보안 환경으로 사용될 수 있으며, 따라서 키에 대한 추가적인 보안 보호 및/또는 장치가 손상된 경우에도 현재 권한 수준 및 CPU 모드에 관계없이 다른 엔티티가 액세스할 수 있는 권한이 없는 서명의 실행을 제공할 수 있다. 이는 엔클레이브가 입력될 때 액세스 제어 메커니즘이 해당 엔클레이브에 속하는 엔클레이브 메모리 페이지를 엔클레이브 외부에서 읽거나 쓸 수 없도록 보장하기 때문이다.

[0058] 본 개시의 특정 실시예에 따르면, 하나 이상의 검사자(또는 그 적어도 일부) 각각은 검사자가 코드를 실행하고 그 안에 데이터를 저장할 수 있는 보안 환경을 제공하는 각각의 보안 엔클레이브를 가질 수 있다. 따라서 각 검사자는 다른 개체가 액세스할 수 없는 지정된 엔클레이브를 사용하여 자신의 코드와 데이터를 안전하게 보호할 수 있다. 예를 들어, 각 검사자는 개인 키를 보호하고/또는 지정된 엔클레이브에서 서명을 실행하도록 선택할 수 있다. 어떤 경우에는 검사자와 연관된 전체 검사 기능이 지정된 엔클레이브에서 실행될 수 있다고 판정할 수 있다(즉, 검사자가 실제로 엔클레이브에서 실행 중이다).

[0059] 도 2의 설명을 계속하면, 하나 이상의 검사 결과가 하나 이상의 검사자에 의해 별도로 서명되고 하나 이상의 서명된 검사 결과가 획득되면, (예를 들어, 컨트롤러(106)에 의해) 검사 관리 정책에 따라 검사 결과 및/또는 파생 항목 중 적어도 일부를 수동 검사를 위해 보낼지 여부가 판정될 수 있다(208).

[0060] 전술한 바와 같이, 검사 관리 정책은 검사할 수신 데이터 각각에 대해 구체적으로 판정된다. 수신된 각 데이터에 대해 정책은 그와 연관된 하나 이상의 속성에 대해 지정될 수 있다. 일부 실시예에서, 수신된 데이터와 연관된 하나 이상의 속성은 수신된 데이터의 하나 이상의 속성, 데이터를 전송하는 소스 컴퓨터의 하나 이상의 속성 및 데이터가 전송되는 환경의 하나 이상의 속성을 포함하는 그룹으로부터 선택될 수 있다.

[0061] 예로서, 수신된 데이터의 속성은 데이터의 유형 및 데이터의 내용을 포함할 수 있다. 소스 컴퓨터의 속성은 사용자(즉, 소스 컴퓨터를 사용하는 직원/직위) 이름, 사용자 유형, 소스 컴퓨터 유형, 운영 체제의 유형 및 버전, 설치된 신뢰할 수 있는 엔티티 애플리케이션/지원 버전, 존재한다면 현재 건강 상태(예컨대, 유효한 보안 경고), 최근 검사 내역, 물리적 위치 및 IP 주소 등을 포함할 수 있다. 환경의 속성은 데이터를 수신 한 날짜 및/또는 시간, 검사자로부터 반환된 검사 상태의 수 및 유형 등을 포함할 수 있다.

[0062] 특정 실시예에 따르면, 검사 관리 정책은 상기 나열된 속성 중 하나 이상에 기초한 하나 이상의 사전 정의된 기준을 포함할 수 있다. 사전 정의된 기준 중 적어도 일부는 검사 결과 또는 그것의 파생물의 수동 검사가 필요한지 여부를 판정하는데 사용될 수 있다. 예를 들어, 영업 사원의 사용자로부터 받은 엑셀(Excel) 파일은 VBA(Visual Basic for Applications) 매크로를 포함하며, 이 매크로는 검사자 중 한 명만 무해한지 여부를 판정할 수 있다. 파일 유형, 파일의 내용, 반환된 검사 상태 수(예컨대, 검사를 수행할 수 있는 검사자 수)에 따라 수동 검사를 위해 파일을 전송해야 하는지 여부를 판정할 수 있다. 또 다른 예를 들어, 오토캐드(AutoCAD) 파일은 관리 보조원으로부터 수신된다. 이러한 포지션의 유형은 일반적으로 이러한 유형의 파일을 처리하는 것을 수반하지 않기 때문에 파일 유형 및 사용자 유형에 따라 수동 검사를 위해 파일을 전송해야 하는지를 판정한다. 추가 예로서, 스프레드 시트 파일은 CFO인 사용자로부터 수신된다. 모든 검사자(및 최소 2 명)는 그것이

무해하다고 판단하고 아무도 악성이라고 판단하지 않는다. 파일 유형 및 사용자 유형에 따라 수동 검사없이 파일을 자동으로 전송할 수 있는지(예컨대, 정책 시행자에게) 판정할 수 있다.

[0063] 전술한 바와 같이, 경우에 따라 검사 결과는 수신된 데이터의 검사 상태 및 수신된 데이터에 대응하는 검사된 데이터를 포함할 수 있다. 특정 경우에 따라, 컨트롤러는 수동 검사를 위해 정확히 무엇을 보낼지 판정할 수 있다. 일부 실시예에서, 수동 검사가 일부 검사 결과(예를 들어, 일부 특정 검사자(들)의 선택된 검사 결과(들))에 대해서만 필요하다고 판정할 수 있다. 선택된 각각의 검사 결과에 대해 검사된 데이터, 검사된 상태, 원래 수신된 데이터 및 서명된 검사 결과와 같은 파생 항목 중 하나 이상이 수동 검사를 위해 전송되도록 판정할 수 있다. 예를 들어, 위의 수신 데이터가 엑셀 파일 또는 오토캐드 파일인 경우 원본 파일은 검사된 상태와 함께 검사된 파일을 수동 검사를 위해 보낼 수 있다. 다른 예에서, 수신된 데이터가 검사자 중 하나에 의해 검사시에 필터링/정화/수정된 경우, 수신된 데이터에 대응하는 검사된 데이터는 수신된 데이터의 필터링/수정된 버전일 수 있다. 컨트롤러는 수정 승인을 위해 수동 검사를 위해 검사된 데이터를 전송하도록 판정할 수 있다.

[0064] 일부 실시예에서, 선택적으로, 하나 이상의 검사 결과, 또는 그 적어도 일부(예를 들어, 선택된 검사 결과)는 (예를 들어, 컨트롤러에 의해) 집계된 검사 결과로 집계될 수 있고, 집계된 검사는 검사 결과의 파생된 결과로서, 수동 검사를 위해 전송될 수 있다. 예를 들어, 일부 경우에 집계된 검사 결과는 원래 수신된 데이터와 함께 하나 이상의 검사된 상태를 기반으로 생성된 집계된 검사 상태를 포함할 수 있다. 일부 다른 경우에는 하나 이상의 검사자이 검사ㄴ한 검사 데이터와 함께 집계된 검사 상태를 포함할 수 있다.

[0065] 블록(208)에서 긍정적인 판정시, 검사 컴퓨터(예컨대, 컨트롤러에 의해)에 의해 전송된 검사 결과 및/또는 그것의 파생물 중 적어도 일부에 대한 수동 검사가(예컨대, 수동 검사 모듈(110)에 의해) 제공될 수 있고(210), 이는 승인 상태를 나타내는 적어도 하나의 수동 검사 결과를 발생시킨다. 또한, 적어도 하나의 수동 검사 결과의 서명이 제공될 수 있으며(210)(예를 들어, 수동 검사 모듈(110)에 의해 컨트롤러(106)에) 적어도 하나의 서명된 수동 검사 결과가 발생한다. 특정 실시예에 따르면, 수동 검사는 각각 보안 서명 메커니즘과 연관된 적어도 하나의 수동 검사자에 의해 수행될 수 있고, 적어도 하나의 수동 검사 결과의 서명은 연관된 보안 서명 메커니즘을 사용하여 적어도 하나의 수동 검사자 각각에 의해 개별적으로 수행될 수 있다. 여기서 사용되는 수동 검사자란 용어는 검사 컴퓨터로부터 검사 결과 및/또는 그것의 파생물을 수신한 후 수신된 정보를 승인할지 여부를 판정하기 위해 추가 검사/검증을 수행하는 승인자(컴퓨터 장치를 장착함)인 사람을 지칭한다. 여기서 언급되는 수동 검사 모듈(110)은 추가 검사/검증을 수행하기 위해 적어도 하나의 수동 검사자가 운영하는 적어도 하나의 컴퓨터 장치(또는 컴퓨터 장치의 전용 검사 모듈)를 포함하는 것으로 해석되어야 한다.

[0066] 적어도 하나의 수동 검사자에 의해 사용되는 서명 메커니즘은 하나 이상의 검사자(위의 블록(206)을 참조하여 설명된 바와 같이)와 연관된 서명 메커니즘을 참조하여 전술한 것과 유사한 방식으로 구현될 수 있다. 특히, 본 개시의 일부 실시예에서, 적어도 하나의 수동 검사자 각각과(또는 적어도 하나의 수동 검사자 중 적어도 일부와) 연관된 보안 서명 메커니즘은 보안 환경에서 실행되는 암호화 서명이다. 예로서, 적어도 하나의 수동 검사자(또는 적어도 그 일부) 각각에는 수동 검사 프로세스를 수행하기 위한 전용 검사 모듈을 포함하는 컴퓨터 장치가 장착될 수 있다. 검사 모듈은 검사 모듈이 코드를 실행하고 그 안에 데이터를 저장할 수 있는 보안 환경을 제공하는 각각의 보안 엔클레이브를 가지고 있다. 예를 들어, 검사 모듈은 자신의 개인 키를 보호하거나 지정된 엔클레이브에서 서명을 실행하도록 선택할 수 있다. 어떤 경우에는 검사 모듈과 연관된 전체 수동 검사 프로세스가 지정된 엔클레이브에서 실행될 수 있다고 판정될 수 있다.

[0067] 설명의 목적으로, 이제 수동 검사 프로세스를 보여주는 비 제한적인 예를 설명한다. 회사의 CFO는 지정된 컴퓨터 장치를 사용하여 승인자 역할을 할 수 있다. 컴퓨터 장치는 그 검사 모듈에 구현된 검사 기능으로 특별히 구성된다. CFO가 검사 컴퓨터로부터 받은 검사 결과를 확인하고 수동 검사 결과를 제공하면, 검사 모듈에 지정된 보안 구역에서 수행되는 수동 검사 결과에 서명하여 다른 기관이 서명, 특히 서명에 사용되는 개인 키에 액세스할 수 있다. 서명된 수동 검사 결과는 추가 판정을 내리기 위해 검사 컴퓨터의 컨트롤러에 제공될 수 있다.

[0068] 일부 실시예에서, 수동 검사 결과는 승인 상태(즉, 검사 컴퓨터에 의해 전송된 검사 결과 및/또는 그것의 파생물의 수신된 적어도 일부가 승인되었는지 여부)를 나타낼 수 있다 . 선택적으로, 수동 검사자가 검사시 데이터의 특정 수정을 수행하는 경우 수동 검사 결과에는 수동 검사 데이터도 포함될 수 있다.

[0069] 계속해서 도 2의 설명으로, 서명된 검사 결과는 검사 컴퓨터(예를 들어, 컨트롤러(106)에 의해)에 의해 분석될 수 있다(212). 서명된 검사 결과는 i) 하나 이상의 서명된 검사 결과 및 ii) 서명된 하나 이상의 수동 검사 결

과 중 적어도 하나를 포함할 수 있다. 일부 실시예에서, 블록(208)에서 수동 검사가 필요하지 않다고 판정될 때, 여기서 서명된 검사 결과는 하나 이상의 검사자에 의해 제공되는 하나 이상의 서명된 검사 결과만을 포함할 수 있다. 일부 다른 실시예에서, 블록(208)에서 수동 검사가 필요하다고 판정될 때(즉, 위에서 언급한 바와 같은 긍정적인 판정 시), 그리고 적어도 하나의 서명된 수동 검사 결과가 수동 검사 모듈에 의해 컨트롤러에 제공되면, 여기에서 서명된 검사 결과에는 서명된 하나 이상의 수동 검사 결과 또는 하나 이상의 검사자가 제공한 하나 이상의 서명된 검사 결과 및 서명된 하나 이상의 수동 검사 결과가 포함될 수 있다.

[0070] 특정 실시예에 따르면, 분석은 검사 관리 정책에 의해 지정된 바와 같이 사전 정의된 기준에 기초할 수 있다. 경우에 따라, 하나 이상의 검사자 및/또는 적어도 하나의 수동 검사자에게 각각의 가중치 요소가 할당될 수 있으며, 서명된 검사 결과는 해당 검사 결과에 가중치 요소를 적용하여 컨트롤러에 의해 분석/평가될 수 있고, 이는 가중 합계/총계(즉, 가중 서명된 검사 결과의 합계)를 발생시킨다. 예를 들어, 사전 정의된 기준은 승인을 나타내는 서명된 검사 결과의 수(예컨대, 서명된 검사 결과에 포함된 서명에 기반) 또는 승인 또는 이들의 조합을 나타내는 가중 서명된 검사 결과의 합계를 기반으로 할 수 있다. 이전 예를 계속하여, 오토캐드 파일이 수동 검사를 위해 전송되었을 때, 사전 정의된 기준은 승인을 나타내는 수동 검사자의 서명을 적어도 2 개 얻어야 한다는 것, 또는 5의 총 가중치를 나타내는 승인을 나타내는 서명을 적어도 2 개 얻어야 한다는 것일 수 있다. 예를 들어, 파일은 조직 내 직위/책임에 따라 가중치가 다른 여러 수동 검사자에게 전송될 수 있다. 예를 들어, CEO는 4의 가중치를 할당받을 수 있고, 부서 관리자는 2의 가중치를 할당받을 수 있고, 기술 엔지니어와 영업 사원은 1의 가중치를 할당 받을 수 있다. 이 경우 승인을 나타내는 두 서명이 5의 가중치와 함께 수신되면, 예를 들어 CEO 및 기술 엔지니어의 서명을 수신하면, 사전 정의된 기준이 충족된 것으로 간주될 수 있다. 수동 검사를 위해 엑셀 파일이 전송될 때, 사전 정의된 기준은 7의 총 가중치를 가진 승인을 나타내는 적어도 3개의 서명을 받아야 하고, 3개의 서명 중 적어도 하나는 기술 부서로부터 받아야 한다는 것일 수 있다. 다른 예에서, 수동 검사가 수행되지 않는 경우, 사전 정의된 기준은 하나 이상의 검사자 모두의 검사 결과가 데이터가 무해하다는 긍정적인 표시를 제공하는 것일 수 있다.

[0071] 분석 결과가 사전 정의된 기준을 충족하면(214), 서명된 검사 결과의 추가 검증이 검사 컴퓨터(예를 들어, 정책 시행자(108)에 의해)에 의해 수행될 수 있다(216). 추가 검증은 수신된 데이터에 해당하는 검사된 데이터를 목적지 컴퓨터로 보낼지 여부를 판정할 수 있다. 일부 실시예에서, 추가 검증은 하나 이상의 서명된 검사 결과 및/또는 적어도 하나의 서명된 수동 검사 결과의 완전성 및 정확성을 검증하는 것을 포함할 수 있다. 정책 시행자는 컨트롤러로부터 서명된 모든 검사 결과를 수신하고 데이터를 목적지 컴퓨터로 보낼지 여부에 대한 최종 판정을 내리도록 구성되어 컨트롤러 외에 추가 보호 계층을 제공한다(즉, 리던던시를 제공하고 시스템의 신뢰도를 증가시킨다). 정책 시행자는 한 명 이상의 검사자 및/또는 적어도 한 명의 수동 검사자가 검사를 실행했는지(즉, 완전성), 서명이 올바른지(즉, 정확성) 여부를 확인한다.

[0072] 한편, 분석 결과가 사전 정의된 기준을 충족하지 못하는 경우(214), 서명된 검사 결과에 대한 추가 검증을 수행할 필요가 없다. 검사 프로세스는 중지될 수 있으며(218) 데이터가 목적지 컴퓨터로 전송되지 않을 것임을 판정할 수 있다.

[0073] 특정 실시예에 따르면, 각각의 검사 결과에 개별적으로 서명하는 하나 이상의 검사자 각각 대신에, 컨트롤러는 "서명 체인" 메커니즘(검사 관리 정책에 명시된대로)을 유지할 수 있고, 서명 체인 메커니즘에서 각 검사자는 이전에 실행된 검사자의 서명을 포함하는 콘텐츠에 서명한다. 구체적으로, 검사 관리 정책은 하나 이상의 검사자의 사전 정의된 오더의 목록을 포함할 수 있으며, 수신된 데이터는 사전 정의된 오더의 목록 중 하나에서 하나 이상의 검사자에 의해 검사되고 서명될 수 있으며, 제 1 서명자를 제외한 각각의 검사자는 수신된 데이터와 이전에 서명을 수행한 한 명 이상의 이전 검사자의 하나 이상의 서명을 포함하는 콘텐츠에 서명하여 서명 체인을 생성한다. 이러한 경우, 추가 검증은 서명 체인에 있는 각 서명의 완전성과 정확성을 검증하고, 서명 체인의 오더가 사전 정의된 오더의 목록에 속하는지 여부를 검증하는 것을 포함할 수 있다. 이를 통해 악의적인 당사자가 컨트롤러를 인수하여 문제가 있는 데이터가 통과할 수 있는 상황을 효과적으로 방지할 수 있다.

[0074] 특정 실시예에 따르면, 컨트롤러는 또한 검사 관리 정책에 따라 검사 결과를 분석하는 것을 용이하게 하기 위해 정책 시행자를 참조하여 전술한 것과 유사한 방식으로 검사자의 서명을 검증하도록 구성될 수 있다. 어떤 경우에는, 검사자가 손상되었는지 여부를 감지하기 위해 검사자가 올바르게 작동하는지 확인/검사하도록 컨트롤러를 구성할 수 있다(예컨대, 검사자 중 일부는 항상 잘못된 응답을 반환하는 공격자에게 공격을 받을 수 있다). 이러한 검증의 한 가지 예는 검사자를 조사하는 것이다. "프로브"또는 "프로빙"이라는 용어는 데이터 수집 및/또는 엔티티의 상태 또는 활동을 모니터링하기 위해 취한 조치 또는 서비스를 의미한다.

[0075] 전술한 바와 같이, 하나 이상의 검사자(104) 또는 그 일부, 정책 시행자(108) 및 제어기(106)와 같은 전술한 기능 모듈(또는 적어도 그 일부) 각각은 로컬 및/또는 원격 엔티티를 통해 분산된 별도의 장치에서 구현되며 통신 네트워크를 통해 서로 작동 가능하게 연결될 수 있음을 이해해야 한다. 또한, 이들 모듈 각각은 개인 키 저장 및/또는 서명 프로세스 실행 및/또는 검증 등을 수행하기 위해 지정된 개별 보안 엔클레이브를 가질 수 있다. 어떤 경우에는, 모듈의 전체 기능이 지정된 엔클레이브에서 실행될 수 있다(즉, 모듈이 엔클레이브에서 실행되는 것으로 간주 됨).

[0076] 이제 도 3으로 돌아가면, 현재 개시된 주제의 특정 실시예에 따라 클라이언트-서버 통신 아키텍처에서 클라이언트-서버 경로 및 서버-클라이언트 경로에 대한 보안 통신을 보장하는 개략도가 도시되어 있다.

[0077] 도시된 바와 같이, 클라이언트(304)는 통신 네트워크를 통해 서버(302)와 통신하고있다. 클라이언트(304)는 서버(302)로 정보를 가져오기 위한 요청을 개시할 수 있으며(따라서 클라이언트-서버 경로는 가져오기 경로라고도 함), 서버(302)는 정보를 클라이언트(304)에 제공하거나 내보낼 수 있다(따라서 서버-클라이언트 경로는 또한 내보내기 경로라고도 지칭됨). 여기에서 제안되고 도 2를 참조하여 위에서 설명된 검사 메커니즘은 가져오기 경로 및/또는 내보내기 경로에서 통신을 보호하는데 사용될 수 있으며, 이에 따라 클라이언트와 서버 사이에 보안 가져오기 및/또는 보안 내보내기 통신 경로를 제공한다. 두 경로에서 보안 통신을 수행하는 목적은 다를 수 있지만, 예를 들어, 보안 가져오기는 서버에 대한 입력 정보가 무해한지 확인하는 것을 목표로 할 수 있지만, 보안 내보내기는 중요한 정보가 유출되는 것을 확인하고 방지하는 것을 목표로 할 수 있으며, 여기에서 제안된 컴퓨터 시스템 및 검사 메커니즘은 두 경로 모두에 유사하게 적용될 수 있다. 구체적으로, 도 3의 좌측 다이어그램(306)은 보안 가져오기 검사 시스템을 보여준다. 가져오기 요청자는 클라이언트(304)로부터 검사 요청을 수신하고 요청을 가져오기 컨트롤러(즉, 위에서 설명한 컨트롤러의 역할에 해당하는 가져오기 컨트롤러)로 전송하는 인터페이스 역할을 한다. 가져오기 컨트롤러는 위에서 설명한 것과 유사한 방식으로 가져오기 검사자, 수동 검사 모듈 및 가져오기 정책 시행자 사이를 조정한다. 마지막 보호 계층 역할을 하는 가져오기 시행자는 데이터를 서버로 전달할지 여부를 판정한다. 유사하게, 오른쪽 다이어그램(308)은 유사한 방식으로 구현되는 보안 내보내기 검사 시스템을 보여준다. 두 경로의 다른 목적으로 인해, 어느 한 경로의 검사자는 다른 필터링 메커니즘과 연관될 수 있고 컨트롤러는 특정 목적을 제공하기 위해 다른 검사 관리 정책으로 구성될 수 있다.

[0078] 도면에 도시되고 위에서 설명된 예는 단지 예시적인 목적을 위한 것이며 어떠 방식으로든 본 개시를 제한하는 것으로 간주되어서는 안된다는 점에 유의해야 한다. 당업자라면 임의의 다른 적절한 구현 또는 예시가 도시된 예에 추가로 또는 그 대신에 사용될 수 있음을 쉽게 이해할 것이다.

[0079] 또한, 도 2에 도시된 흐름도가 시스템(100)의 요소를 참조하여 설명되었지만, 이것은 결코 구속되지 않으며, 동작은 여기에 설명된 요소 이외의 요소에 의해 수행될 수 있다는 점에 유의한다.

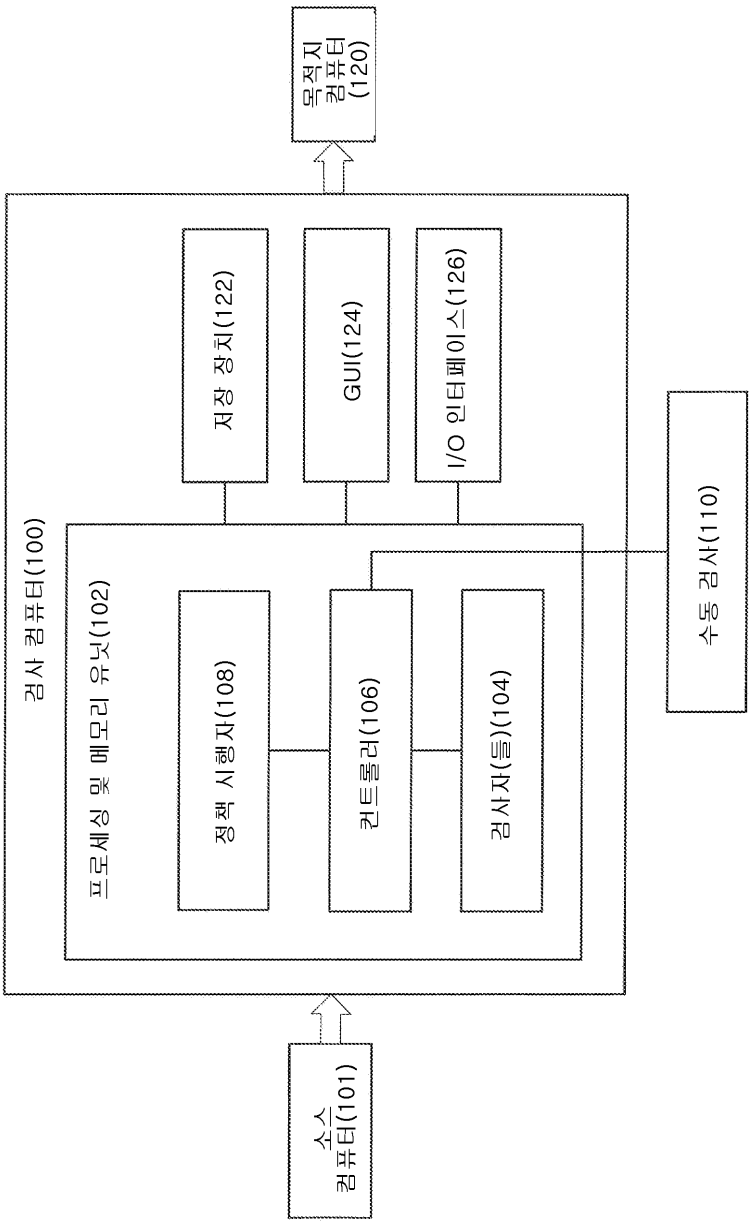
[0080] 본 발명은 본 명세서에 포함된 설명 또는 도면에 도시된 세부사항에 적용되는 것으로 제한되지 않음을 이해해야 한다. 본 발명은 다른 실시예가 가능하고 다양한 방식으로 실행 및 수행될 수 있다. 따라서, 여기에 사용된 어법 및 용어는 설명을 위한 것이며 제한하는 것으로 간주되어서는 안된다는 것을 이해해야 한다. 이와 같이, 당업자는 본 개시의 기초가 되는 개념이 현재 개시된 주제의 여러 목적을 수행하기 위한 다른 구조, 방법 및 시스템을 설계하기 위한 기초로서 쉽게 이용될 수 있음을 인식할 것이다.

[0081] 또한, 본 발명에 따른 시스템은 적절하게 프로그래밍된 컴퓨터에서 적어도 부분적으로 구현될 수 있음을 이해할 것이다. 마찬가지로, 본 발명은 본 발명의 방법을 실행하기 위해 컴퓨터에 의해 판독 가능한 컴퓨터 프로그램을 고려한다. 본 발명은 또한 본 발명의 방법을 실행하기 위해 컴퓨터에 의해 실행 가능한 명령어 프로그램을 유형적으로 구현하는 비 일시적 컴퓨터 판독 가능 저장 매체를 고려한다.

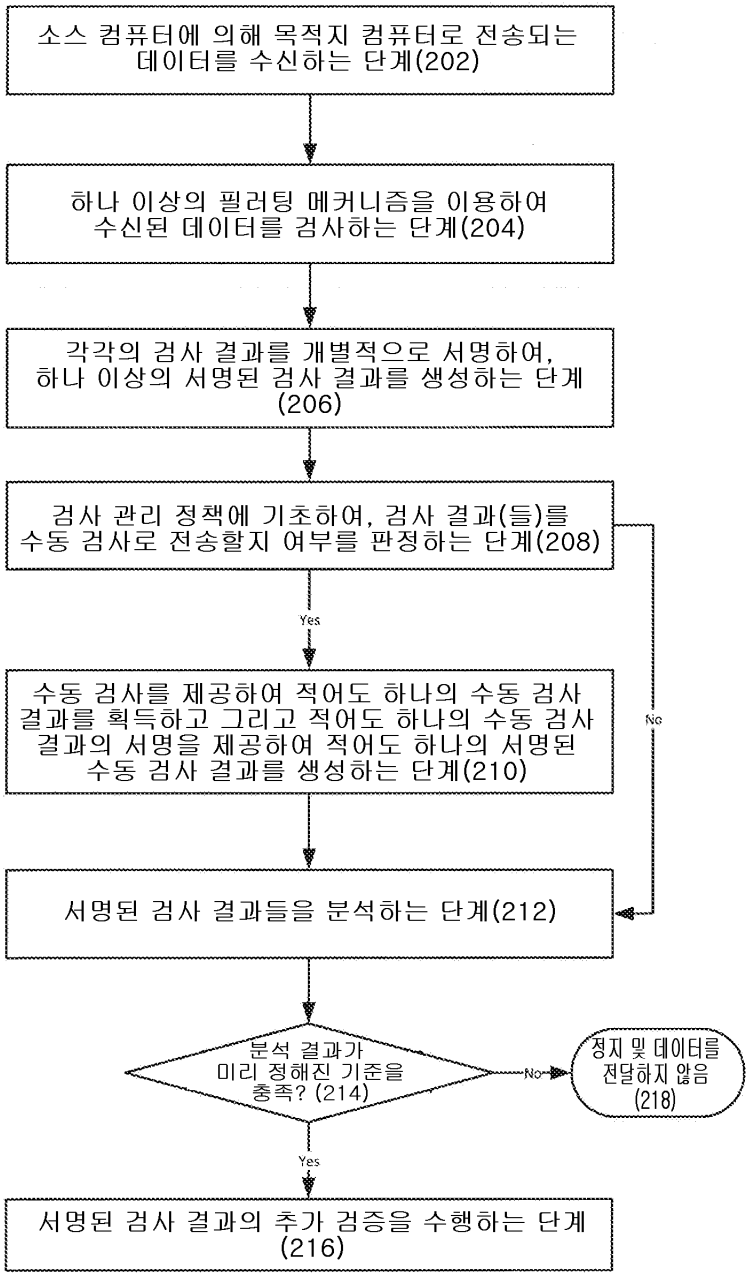
[0082] 당업자는 첨부된 청구 범위에 의해 정의된 범위를 벗어나지 않고 본 명세서에 기술된 바와 같이 본 발명의 실시예에 다양한 수정 및 변경이 적용될 수 있음을 쉽게 이해할 것이다.

도면

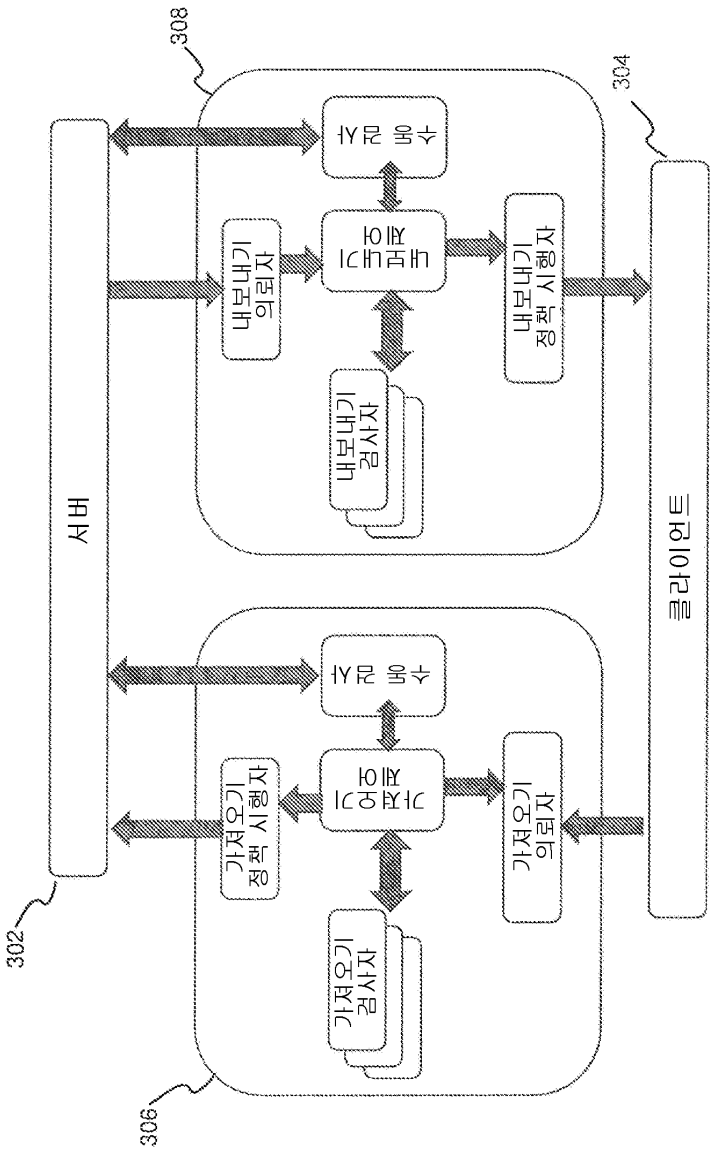
도면1


목적지 컴퓨터 (120)
검사 컴퓨터(100)
프로세싱 및 메모리 유닛(102)
저장 장치(122)
GUI(124)
I/O 인터페이스(126)
정책 시행자(108)
컨트롤러(106)
검사자(들)(104)
수동 검사(110)
소스 컴퓨터(101)

도면2


소스 컴퓨터에 의해 목적지 컴퓨터로 전송되는 데이터를 수신하는 단계(202)
하나 이상의 필러팅 메커니즘을 이용하여 수신된 데이터를 검사하는 단계(204)
각각의 검사 결과를 개별적으로 서명하여, 하나 이상의 서명된 검사 결과를 생성하는 단계(206)
검사 관리 정책에 기초하여, 검사 결과(들)를 수동 검사로 전송할지 여부를 판정하는 단계(208)
Yes
No
수동 검사를 제공하여 적어도 하나의 수동 검사 결과를 획득하고 그리고 적어도 하나의 수동 검사 결과의 서명을 제공하여 적어도 하나의 서명된 수동 검사 결과를 생성하는 단계(210)
서명된 검사 결과들을 분석하는 단계(212)
분석 결과가 미리 정해진 기준을 충족? (214)
No
정지 및 데이터를 전달하지 않음 (218)
Yes
서명된 검사 결과의 추가 검증을 수행하는 단계(216)

도면3


308
304
302
306
서버
클라이언트
수동 관사
내보내기 제어
내보내기 의뢰자
내보내기 정책 시행자
내보내기 검사자
수동 관사
가져오기 제어
가져오기 정책 시행자
가져오기 의뢰자
가져오기 검사자