(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2023년07월20일
(11) 등록번호 10-2558266
(24) 등록일자 2023년07월18일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) *G06F 21/64* (2013.01)
H04L 65/40 (2022.01)
(52) CPC특허분류
H04L 63/0823 (2013.01)
G06F 21/64 (2013.01)
(21) 출원번호 10-2021-7015357
(22) 출원일자(국제) 2020년04월05일
심사청구일자 2021년05월21일
(85) 번역문제출일자 2021년05월21일
(65) 공개번호 10-2021-0079352
(43) 공개일자 2021년06월29일
(86) 국제출원번호 PCT/CN2020/083396
(87) 국제공개번호 WO 2020/220938
국제공개일자 2020년11월05일
(30) 우선권주장
201910357610.X 2019년04월29일 중국(CN)
(56) 선행기술조사문헌
WO2018140628 A1
CN103460215 A
WO2018125989 A2
KR1020130091353 A

(73) 특허권자
후아웨이 테크놀러지 컴퍼니 리미티드
중국 518129 광동성 센젠 롱강 디스트릭트 반티안 후아웨이 어드미니스트레이션 빌딩
(72) 발명자
샤 량
중국 518129 광동성 센젠 롱강 디스트릭트 반티안 후아웨이 어드미니스트레이션 빌딩
왕 지타오
중국 518129 광동성 센젠 롱강 디스트릭트 반티안 후아웨이 어드미니스트레이션 빌딩
시 유린
중국 518129 광동성 센젠 롱강 디스트릭트 반티안 후아웨이 어드미니스트레이션 빌딩
(74) 대리인
유미특허법인

전체 청구항 수 : 총 39 항 심사관 : 천대식

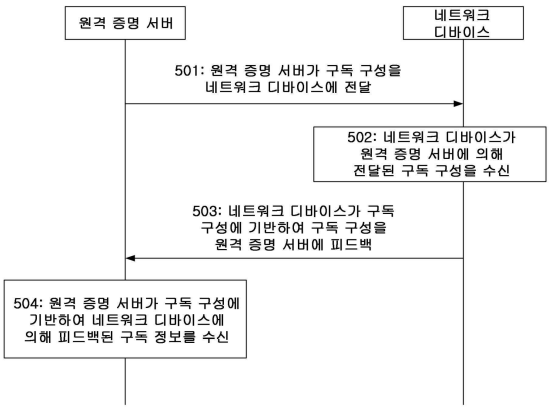
(54) 발명의 명칭 **데이터 수집 방법, 장치, 디바이스 및 컴퓨터가 판독 가능한 저장 매체**

(57) 요 약

본 출원은 데이터 수집 방법, 장치 및 디바이스 그리고 컴퓨터가 판독 가능 저장 매체를 개시한다. 데이터 수집 방법은 원격 증명 프로세스에 적용되며, 데이터 수집 방법은, 원격 증명 서버가 구독 구성을 네트워크 디바이스에 전달하는 것을 포함하며, 구독 구성은 네트워크 디바이스에 의해 수행되는 원격 증명 관련 정보를 구독하는

(뒷면에 계속)

대 표 도 - 도5



데 사용된다. 원격 증명 서버는 구독 구성에 기반하여 네트워크 디바이스에 의해 피드백된 구독 정보를 수신한다. 원격 증명 서버는 구독 구성을 네트워크 디바이스에 전달하고, 네트워크 디바이스는 구독 구성에 기반하여 구독 정보를 자동으로 피드백할 수 있다. 이러한 방식으로 원격 증명의 데이터 수집 모드가 더 유연하고 시기 적절하여, 보안 위험이 감소된다. 또한, 원격 증명 서버가 구독 구성을 여러 번 전달할 필요가 없기 때문에 추가 메시지 교환이 감소되어 데이터 수집 효율성이 향상된다.

(52) CPC특허분류
H04L 63/12 (2013.01)
H04L 67/51 (2022.05)

명 세 서

청구범위

청구항 1

데이터 수집 방법으로서,

상기 데이터 수집 방법은 원격 증명(remote attestation) 프로세스에 적용되며,

상기 데이터 수집 방법은,

원격 증명 서버가, 구독 구성(subscription configuration)을 네트워크 디바이스에 전달하는(deliver) 단계 - 상기 구독 구성은 상기 네트워크 디바이스에 의해 수행되는 원격 증명과 관련된 정보를 구독하는(subscribe) 데 사용됨 -; 및

상기 원격 증명 서버가, 상기 구독 구성에 기반하여 상기 네트워크 디바이스에 의해 피드백된 구독 정보를 수신하는 단계

를 포함하는 데이터 수집 방법.

청구항 2

제1항에 있어서,

상기 구독 구성은 데이터 스트림 구독 구성 또는 이벤트 구독 구성을 포함하는, 데이터 수집 방법.

청구항 3

제2항에 있어서,

상기 구독 구성이 상기 데이터 스트림 구독 구성을 포함하면, 상기 구독 정보는 다음 정보:

상기 네트워크 디바이스가 부팅될 때 기록되는 신뢰 체인(trust chain)의 각 계층에 있는 소프트웨어의 무결성(integrity) 정보;

상기 네트워크 디바이스가 실행될 때 기록되는 운영 체제의 동적 무결성 정보;

상기 네트워크 디바이스가 실행될 때 기록되는 소프트웨어의 동적 무결성 정보;

상기 네트워크 디바이스와 관련된 신원 인증서(identity certificate); 및

상기 네트워크 디바이스와 관련된 원격 증명 인증서

중 하나 이상을 포함하는, 데이터 수집 방법.

청구항 4

제2항에 있어서,

상기 구독 구성이 상기 이벤트 구독 구성을 포함하면, 상기 구독 정보는 다음 트리거된 이벤트:

디바이스 부팅 이벤트, 디바이스 업그레이드 이벤트, 특정 모드 공격 이벤트, 마스터/슬레이브 전환(switchover) 이벤트, 보드(board) 삽입/제거/전환 이벤트, 및 인증서 수명 주기(life cycle) 이벤트

중 하나 이상과 관련된 정보를 포함하는, 데이터 수집 방법.

청구항 5

제1항에 있어서,

상기 구독 구성은 구독 모드를 더 포함하고, 상기 구독 모드는 상기 구독 정보를 피드백하는 모드를 지시하는 데 사용되며, 상기 구독 모드는 주기적 피드백 기반 구독 모드 및 이벤트 트리거 피드백 기반 구독 모드 중 하

나 또는 조합을 포함하는, 데이터 수집 방법.

청구항 6

제5항에 있어서,

상이한 유형의 정보는 상이한 구독 모드에 대응하는, 데이터 수집 방법.

청구항 7

제1항에 있어서,

상기 구독 구성은 필터 구성을 더 포함하고, 상기 구독 정보는 상기 필터 구성에 기반하여 필터링이 수행된 후 획득된 정보를 포함하는, 데이터 수집 방법.

청구항 8

제1항에 있어서,

상기 데이터 수집 방법은,

데이터 처리 파라미터를 상기 네트워크 디바이스에 전달하는 단계

를 더 포함하고,

상기 구독 정보는 상기 데이터 처리 파라미터에 기반하여 처리가 수행된 후에 획득된 정보를 포함하는, 데이터 수집 방법.

청구항 9

제1항에 있어서,

상기 구독 구성을 네트워크 디바이스에 전달하는 단계는,

상기 네트워크 디바이스와 네트워크 구성 프로토콜 세션을 구축하고, 상기 네트워크 구성 프로토콜 세션에 기반하여 상기 구독 구성을 상기 네트워크 디바이스에 전달하는 단계

를 포함하는, 데이터 수집 방법.

청구항 10

데이터 수집 방법으로서,

상기 데이터 수집 방법은 원격 증명 프로세스에 적용되고,

상기 데이터 수집 방법은,

네트워크 디바이스가, 원격 증명 서버에 의해 전달된 구독 구성을 수신하는 단계 - 상기 구독 구성은 상기 네트워크 디바이스에 의해 수행된 원격 증명과 관련된 정보를 구독하는 데 사용됨 -; 및

상기 네트워크 디바이스가, 상기 구독 구성에 기반하여 구독 정보를 상기 원격 증명 서버에 피드백하는 단계

를 포함하는 데이터 수집 방법.

청구항 11

제10항에 있어서,

상기 구독 구성은 데이터 스트림 구독 구성 및 이벤트 구독 구성 중 하나 이상을 포함하는, 데이터 수집 방법.

청구항 12

제10항에 있어서,

상기 구독 구성이 데이터 스트림 구독 구성을 포함하면, 상기 구독 구성에 기반하여 구독 정보를 상기 원격 증명 서버에 피드백하는 단계는,

상기 데이터 스트림 구독 구성에 기반하여, 다음 정보:

상기 네트워크 디바이스가 부팅될 때 기록되는 신뢰 체인의 각 계층에 있는 소프트웨어의 무결성 정보;

상기 네트워크 디바이스가 실행될 때 기록되는 운영 체제의 동적 무결성 정보;

상기 네트워크 디바이스가 실행될 때 기록되는 소프트웨어의 동적 무결성 정보;

상기 네트워크 디바이스와 관련된 신원 인증서; 그리고

상기 네트워크 디바이스와 관련된 원격 증명 인증서

중 하나 이상을 상기 원격 증명 서버에 피드백하는 단계

를 포함하는, 데이터 수집 방법.

청구항 13

제11항에 있어서,

상기 구독 구성이 상기 이벤트 구독 구성을 포함하면, 상기 구독 구성에 기반하여 구독 정보를 상기 원격 증명 서버에 피드백하는 단계는,

다음 트리거된 이벤트:

디바이스 부팅 이벤트, 디바이스 업그레이드 이벤트, 특정 모드 공격 이벤트, 마스터/슬레이브 전환 이벤트, 보드 삽입/제거/전환 이벤트, 및 인증서 수명주기 이벤트

중 하나 이상과 관련된 정보를, 상기 이벤트 구독 구성에 기반하여 상기 원격 증명 서버에 피드백하는 단계

를 포함하는, 데이터 수집 방법.

청구항 14

제10항에 있어서,

상기 구독 구성은 구독 모드를 더 포함하고, 상기 구독 모드는 구독 정보를 피드백하는 모드를 지시하는 데 사용되며, 상기 구독 모드는 주기적 피드백 기반 구독 모드 및 이벤트 트리거 피드백 기반 구독 모드 중 하나 또는 조합을 포함하며,

상기 구독 구성에 기반하여 구독 정보를 상기 원격 증명 서버에 피드백하는 단계는,

상기 구독 구성에 포함된 상기 구독 모드에 기반하여 상기 구독 정보를 상기 원격 증명 서버에 피드백하는 단계

를 포함하는, 데이터 수집 방법.

청구항 15

제14항에 있어서,

상이한 유형의 정보는 상이한 구독 모드에 대응하는, 데이터 수집 방법.

청구항 16

제10항에 있어서,

상기 구독 구성은 필터 구성을 더 포함하고, 상기 구독 정보는 상기 필터 구성에 기반하여 필터링이 수행된 후에 획득된 정보를 포함하는, 데이터 수집 방법.

청구항 17

제10항에 있어서,

상기 데이터 수집 방법은

상기 원격 증명 서버에 의해 전달된 데이터 처리 파라미터를 수신하는 단계

를 더 포함하고,

상기 구독 정보는 상기 데이터 처리 파라미터에 기반하여 처리가 수행된 후에 획득된 정보를 포함하는, 데이터 수집 방법.

청구항 18

제10항에 있어서,

상기 원격 증명 서버에 의해 전달된 구독 구성을 수신하는 단계는,

상기 원격 증명 서버와 네트워크 구성 프로토콜 세션을 구축하고, 상기 네트워크 구성 프로토콜 세션에 기반하여 상기 원격 증명 서버에 의해 전달되는 상기 구독 구성을 수신하는 단계

를 포함하는, 데이터 수집 방법.

청구항 19

데이터 수집 장치로서,

상기 데이터 수집 장치는 원격 증명 프로세스에 적용되며,

상기 데이터 수집 장치는,

구독 구성을 네트워크 디바이스에 전달하도록 - 상기 구독 구성은 상기 네트워크 디바이스에 의해 수행되는 원격 증명과 관련된 정보를 구독하는 데 사용됨 - 구성된 송신 모듈; 및

상기 구독 구성에 기반하여 상기 네트워크 디바이스에 의해 피드백된 구독 정보를 수신하도록 구성된 수신 모듈

을 포함하는 데이터 수집 장치.

청구항 20

제19항에 있어서,

상기 구독 구성은 데이터 스트림 구독 구성 및 이벤트 구독 구성 중 하나 이상을 포함하는, 데이터 수집 장치.

청구항 21

제20항에 있어서,

상기 구독 구성이 상기 데이터 스트림 구독 구성을 포함하면, 상기 구독 정보는 다음 정보:

상기 네트워크 디바이스가 부팅될 때 기록되는 신뢰 체인의 각 계층에 있는 소프트웨어의 무결성 정보;

상기 네트워크 디바이스가 실행될 때 기록되는 운영 체제의 동적 무결성 정보;

상기 네트워크 디바이스가 실행될 때 기록되는 소프트웨어의 동적 무결성 정보;

상기 네트워크 디바이스와 관련된 신원 인증서; 및

상기 네트워크 디바이스와 관련된 원격 증명 인증서

중 하나 이상을 포함하는, 데이터 수집 장치.

청구항 22

제20항 또는 제21항에 있어서,

상기 구독 구성이 상기 이벤트 구독 구성을 포함하면, 상기 구독 정보는 다음 트리거된 이벤트:

디바이스 부팅 이벤트, 디바이스 업그레이드 이벤트, 특정 모드 공격 이벤트, 마스터/슬레이브 전환 이벤트, 보드 삽입/제거/전환 이벤트, 및 인증서 수명 주기 이벤트

중 하나 이상과 관련된 정보를 포함하는, 데이터 수집 장치.

청구항 23

제19항에 있어서,

상기 구독 구성은 구독 모드를 더 포함하고, 상기 구독 모드는 상기 구독 정보를 피드백하는 모드를 지시하는 데 사용되며, 상기 구독 모드는 주기적 피드백 기반 구독 모드 및 이벤트 트리거 피드백 기반 구독 모드 중 하나 또는 조합을 포함하는, 데이터 수집 장치.

청구항 24

제23항에 있어서,

상이한 유형의 정보는 상이한 구독 모드에 대응하는, 데이터 수집 장치.

청구항 25

제19항에 있어서,

상기 구독 구성은 필터 구성을 더 포함하고, 상기 구독 정보는 상기 필터 구성에 기반하여 필터링이 수행된 후 획득된 정보를 포함하는, 데이터 수집 장치.

청구항 26

제19항에 있어서,

상기 송신 모듈은 추가로, 데이터 처리 파라미터를 상기 네트워크 디바이스에 전달하도록 구성되고,

상기 구독 정보는 상기 데이터 처리 파라미터에 기반하여 처리가 수행된 후에 획득된 정보를 포함하는, 데이터 수집 장치.

청구항 27

제19항에 있어서,

상기 송신 모듈은, 상기 네트워크 디바이스와 네트워크 구성 프로토콜 세션을 구축하고, 상기 네트워크 구성 프로토콜 세션에 기반하여 상기 구독 구성을 상기 네트워크 디바이스에 전달하도록 구성되는, 데이터 수집 장치.

청구항 28

데이터 수집 장치로서,

상기 데이터 수집 장치는 원격 증명 프로세스에 적용되고,

상기 데이터 수집 장치는,

원격 증명 서버에 의해 전달된 구독 구성을 수신하도록 - 상기 구독 구성은 네트워크 디바이스에 의해 수행된 원격 증명과 관련된 정보를 구독하는 데 사용됨 - 구성된 수신 모듈; 및

상기 구독 구성에 기반하여 구독 정보를 상기 원격 증명 서버에 피드백하도록 구성된 송신 모듈

을 포함하는 데이터 수집 장치.

청구항 29

제28항에 있어서,

상기 구독 구성은 데이터 스트림 구독 구성 및 이벤트 구독 구성 중 하나 이상을 포함하는, 데이터 수집 장치.

청구항 30

제28항에 있어서,

상기 구독 구성이 데이터 스트림 구독 구성을 포함하면, 상기 송신 모듈은, 상기 데이터 스트림 구독 구성에 기반하여, 다음 정보:

상기 네트워크 디바이스가 부팅될 때 기록되는 신뢰 체인의 각 계층에 있는 소프트웨어의 무결성 정보;

상기 네트워크 디바이스가 실행될 때 기록되는 운영 체제의 동적 무결성 정보;

상기 네트워크 디바이스가 실행될 때 기록되는 소프트웨어의 동적 무결성 정보;

상기 네트워크 디바이스와 관련된 신원 인증서; 그리고

상기 네트워크 디바이스와 관련된 원격 증명 인증서

중 하나 이상을 상기 원격 증명 서버에 피드백하도록 구성되는, 데이터 수집 장치.

청구항 31

제29항에 있어서,

상기 구독 구성이 상기 이벤트 구독 구성을 포함하면, 상기 송신 모듈은, 다음 트리거된 이벤트:

디바이스 부팅 이벤트, 디바이스 업그레이드 이벤트, 특정 모드 공격 이벤트, 마스터/슬레이브 전환 이벤트, 보드 삽입/제거/전환 이벤트, 및 인증서 수명주기 이벤트

중 하나 이상과 관련된 정보를, 상기 이벤트 구독 구성에 기반하여 상기 원격 증명 서버에 피드백하도록 구성되는, 데이터 수집 장치.

청구항 32

제28항에 있어서,

상기 구독 구성은 구독 모드를 더 포함하고, 상기 구독 모드는 구독 정보를 피드백하는 모드를 지시하는 데 사용되며, 상기 구독 모드는 주기적 피드백 기반 구독 모드 및 이벤트 트리거 피드백 기반 구독 모드 중 하나 또는 조합을 포함하며,

상기 송신 모듈은, 상기 구독 구성에 포함된 상기 구독 모드에 기반하여 상기 구독 정보를 상기 원격 증명 서버에 피드백하도록 구성되는, 데이터 수집 장치.

청구항 33

제32항에 있어서,

상이한 유형의 정보는 상이한 구독 모드에 대응하는, 데이터 수집 장치.

청구항 34

제28항에 있어서,

상기 구독 구성은 필터 구성을 더 포함하고, 상기 구독 정보는 상기 필터 구성에 기반하여 필터링이 수행된 후에 획득된 정보를 포함하는, 데이터 수집 장치.

청구항 35

제28항에 있어서,

상기 송신 모듈은 추가로, 상기 원격 증명 서버에 의해 전달된 데이터 처리 파라미터를 수신하도록 구성되고,

상기 송신 모듈에 의해 피드백된 상기 구독 정보는 상기 데이터 처리 파라미터에 기반하여 처리가 수행된 후에 획득된 정보를 포함하는, 데이터 수집 장치.

청구항 36

제28항에 있어서,

상기 송신 모듈은 네트워크 디바이스와 네트워크 구성 프로토콜 세션을 구축하고, 상기 네트워크 구성 프로토콜 세션에 기반하여 상기 원격 증명 서버에 의해 전달되는 상기 구독 구성을 수신하도록 구성되는, 데이터 수집 장치.

청구항 37

데이터 수집 디바이스로서,

상기 데이터 수집 디바이스는,

메모리 및 프로세서

를 포함하고,

상기 메모리는 적어도 하나의 명령을 포함하고, 상기 적어도 하나의 명령이 상기 프로세서에 의해 로드되고 실행되어, 제1항 내지 제9항 중 어느 한 항에 따른 데이터 수집 방법을 구현하거나, 또는 제10항 내지 제18항 중 어느 한 항에 따른 데이터 수집 방법을 구현하는, 데이터 수집 디바이스.

청구항 38

컴퓨터가 판독 가능한 저장 매체로서,

상기 저장 매체는 적어도 하나의 명령을 포함하고, 상기 명령이 프로세서에 의해 로드되고 실행되어, 제1항 내지 제9항 중 어느 한 항에 따른 데이터 수집 방법을 구현하거나, 또는 제10항 내지 제18항 중 어느 한 항에 따른 데이터 수집 방법을 구현하는, 컴퓨터가 판독 가능한 저장 매체.

청구항 39

컴퓨터가 판독 가능한 저장 매체에 저장되어 있는 컴퓨터 프로그램으로서,

상기 컴퓨터 프로그램은 컴퓨터 프로그램 코드를 포함하고, 상기 컴퓨터 프로그램 코드가 컴퓨터에 의해 실행될 때, 상기 컴퓨터가 제1항 내지 제9항 중 어느 한 항에 따른 데이터 수집 방법을 수행하거나, 또는 제10항 내지 제18항 중 어느 한 항에 따른 데이터 수집 방법을 수행하도록 인에이블되는, 컴퓨터 프로그램.

발명의 설명

기 술 분 야

[0001] 본 출원은 컴퓨터 보안 기술 분야에 관한 것으로, 특히 데이터 수집 방법, 장치 및 디바이스 그리고 컴퓨터가 판독 가능 저장 매체에 관한 것이다.

배 경 기 술

[0002] 컴퓨터 보안 기술의 발전과 함께, 신뢰할 수 있는(trusted) 컴퓨팅에 대한 연구에 점점 더 많은 관심을 기울이고 있으며, 원격 증명(remote attestation)은 신뢰할 수 있는 컴퓨팅의 중요한 부분이다. 원격 증명을 수행하기 위해서, 원격 증명 서버는 네트워크 디바이스에 대한 데이터를 수집해야 한다. 따라서, 데이터 수집 모드가 특히 중요하다.

[0003] 관련 기술은 데이터 수집 중에 폴링 챌린지 응답(polling challenge-response) 메커니즘을 제공한다. 이 메커니즘에서, 원격 증명 서버는 요청을 시작하고(initiate), 네트워크 디바이스는 현재 신뢰할 수 있는 정보와 요청에 기반한 현재 상태로 응답한다.

[0004] 폴링 챌린지 응답 메커니즘에서, 네트워크 디바이스는 서버가 요청을 시작할 때까지 응답하지 않는다. 따라서, 이 데이터 수집 모드는 유연하지 않다.

발명의 내용

[0005] 본 출원의 실시 예는 관련 기술의 문제점을 해결하기 위해 데이터 수집 방법, 장치 및 디바이스 그리고 컴퓨터가 판독 가능한 저장 매체를 제공한다. 기술 적 솔루션은 다음과 같다.

[0006] 제1 측면에 따르면, 데이터 수집 방법이 제공된다. 상기 데이터 수집 방법은 원격 증명 프로세스이다. 상기 데이터 수집 방법에 따르면, 원격 증명 서버가 구독 구성(subscription configuration)을 네트워크 디바이스에 전달한다(deliver). 상기 구독 구성은 상기 네트워크 디바이스에 의해 수행되는 원격 증명과 관련된 정보를 구독하는(subscribe) 데 사용된다. 상기 원격 증명 서버는 상기 구독 구성에 기반하여 상기 네트워크 디바이스에 의해 피드백된 구독 정보를 수신한다. 상기 원격 증명 서버는 상기 구독 구성을 상기 네트워크 디바이스에 전달하고, 상기 네트워크 디바이스는 상기 원격 증명 서버의 구독에 기반하여 상기 구독 정보를 자동으로 피드백할 수

있다. 이러한 방식으로, 원격 증명에서 네트워크 디바이스의 데이터 수집 모드는 상대적으로 유연하다. 또한, 원격 증명 서버가 구독 구성을 여러 번 전달할 필요가 없기 때문에 추가(extra) 메시지 교환이 감소되어 데이터 수집 효율성이 향상된다.

[0007] 선택적으로, 상기 데이터 수집 방법은 다음을 더 포함한다: 상기 원격 증명 서버는 데이터 처리 파라미터를 상기 네트워크 디바이스에 전달하고, 상기 구독 정보는 처리가 상기 데이터 처리 파라미터에 기반하여 수행된 후에 획득된 정보를 포함한다. 상기 데이터 처리 파라미터는 상기 네트워크 디바이스가 정보를 피드백하기 위한 사용을 위해, 미리 상기 네트워크 디바이스에 전달된다. 이러한 방식으로, 상호 작용의 양이 감소되고 데이터 수집 효율성이 향상된다.

[0008] 선택적으로, 상기 구독 구성을 상기 네트워크 디바이스에 전달하는 것은 다음을 포함한다: 상기 원격 증명 서버는 상기 네트워크 디바이스와 네트워크 구성 프로토콜 세션을 구축하고, 상기 네트워크 구성 프로토콜 세션에 기반하여 상기 구독 구성을 상기 네트워크 디바이스에 전달한다. 정보 구독은 광범위한 애플리케이션 시나리오를 가질 뿐만 아니라 유연성, 고효율, 사전 알림(proactive notification) 및 시간 유효성과 같은 네트워크 구성 프로토콜의 장점을 상속하는 네트워크 구성 프로토콜을 사용하여 구현된다.

[0009] 제2 측면에 따르면, 데이터 수집 방법이 제공된다. 상기 데이터 수집 방법은, 상기 데이터 수집 방법은 원격 증명 프로세스에 적용되고, 상기 데이터 수집 방법은, 네트워크 디바이스가, 원격 증명 서버에 의해 전달된 구독 구성을 수신하는 것을 포함하며, 상기 구독 구성은 상기 네트워크 디바이스에 의해 수행된 원격 증명과 관련된 정보를 구독하는 데 사용된다. 상기 네트워크 디바이스는 상기 구독 구성에 기반하여 구독 정보를 상기 원격 증명 서버에 피드백한다.

[0010] 선택적으로, 상기 구독 구성은 데이터 스트림 구독 구성 및 이벤트 구독 구성 중 하나 이상을 포함한다.

[0011] 선택적으로, 상기 구독 구성이 상기 데이터 스트림 구독 구성을 포함하면, 상기 구독 구성에 기반하여 구독 정보를 상기 원격 증명 서버에 피드백하는 것은, 상기 데이터 스트림 구독 구성에 기반하여, 다음 정보:

[0012] 상기 네트워크 디바이스가 부팅될 때 기록되는 신뢰 체인의 각 계층에 있는 소프트웨어의 무결성 정보;

[0013] 상기 네트워크 디바이스가 실행될 때 기록되는 운영 체제의 동적 무결성 정보;

[0014] 상기 네트워크 디바이스가 실행될 때 기록되는 소프트웨어의 동적 무결성 정보;

[0015] 상기 네트워크 디바이스와 관련된 신원 인증서; 그리고

[0016] 상기 네트워크 디바이스와 관련된 원격 증명 인증서 중 하나 이상을 상기 원격 서버에 피드백하는 것을 포함한다.

[0017] 선택적으로, 상기 구독 구성이 상기 이벤트 구독 구성을 포함하면, 상기 구독 구성에 기반하여 구독 정보를 상기 원격 증명 서버에 피드백하는 것은, 다음 트리거된 이벤트: 디바이스 부팅 이벤트, 디바이스 업그레이드 이벤트, 특정 모드 공격 이벤트, 마스터/슬레이브 전환 이벤트, 보드 삽입/제거/전환 이벤트, 및 인증서 수명주기 이벤트 중 하나 이상과 관련된 정보를, 상기 이벤트 구독 구성에 기반하여 상기 원격 증명 서버에 피드백하는 것을 포함한다.

[0018] 선택적으로, 상기 구독 구성은 구독 모드를 더 포함하고, 상기 구독 모드는 구독 정보를 피드백하는 모드를 지시하는 데 사용되며, 상기 구독 모드는 주기적 피드백 기반 구독 모드 및 이벤트 트리거 피드백 기반 구독 모드 중 하나 또는 조합을 포함하며,

[0019] 상기 구독 구성에 기반하여 구독 정보를 상기 원격 증명 서버에 피드백하는 것은, 상기 구독 구성에 포함된 상기 구독 모드에 기반하여 상기 구독 정보를 상기 원격 증명 서버에 피드백하는 것을 포함한다.

[0020] 선택적으로, 전술한 상이한 유형의 정보는 상이한 구독 모드에 대응한다.

[0021] 선택적으로, 전술한 구독 구성은 필터 구성을 더 포함하고, 상기 구독 정보는 상기 필터 구성에 기반하여 필터링이 수행된 후에 획득된 정보를 포함한다.

[0022] 선택적으로, 상기 데이터 수집 방법은, 상기 원격 증명 서버에 의해 전달된 데이터 처리 파라미터를 수신하는 단계를 더 포함하고, 상기 구독 정보는 상기 데이터 처리 파라미터에 기반하여 처리가 수행된 후에 획득된 정보를 포함한다.

[0023] 선택적으로, 상기 원격 증명 서버에 의해 전달된 구독 구성을 수신하는 단계는, 상기 원격 증명 서버와 네트워

크 구성 프로토콜 세션을 구축하고, 상기 네트워크 구성 프로토콜 세션에 기반하여 상기 원격 증명 서버에 의해 전달되는 상기 구독 구성을 수신하는 단계를 포함한다.

[0024] 제3 측면에 따르면, 데이터 수집 장치가 제공된다. 상기 데이터 수집 장치는 원격 증명 프로세스에 적용되며, 상기 데이터 수집 장치는, 구독 구성을 네트워크 디바이스에 전달하도록 - 상기 구독 구성은 상기 네트워크 디바이스에 의해 수행되는 원격 증명과 관련된 정보를 구독하는 데 사용됨 - 구성된 송신 모듈; 및 상기 구독 구성에 기반하여 상기 네트워크 디바이스에 의해 피드백된 구독 정보를 수신하도록 구성된 수신 모듈을 포함한다.

[0025] 선택적으로, 상기 송신 모듈은 추가로, 데이터 처리 파라미터를 상기 네트워크 디바이스에 전달하도록 구성되고, 상기 구독 정보는 상기 데이터 처리 파라미터에 기반하여 처리가 수행된 후에 획득된 정보를 포함한다.

[0026] 선택적으로, 상기 송신 모듈은, 상기 네트워크 디바이스와 네트워크 구성 프로토콜 세션을 구축하고, 상기 네트워크 구성 프로토콜 세션에 기반하여 상기 구독 구성을 상기 네트워크 디바이스에 전달하도록 구성된다.

[0027] 제4 측면에 따르면, 데이터 수집 장치가 제공된다. 상기 데이터 수집 장치는 원격 증명 프로세스에 적용되고, 상기 데이터 수집 장치는, 원격 증명 서버에 의해 전달된 구독 구성을 수신하도록 - 상기 구독 구성은 상기 네트워크 디바이스에 의해 수행된 원격 증명과 관련된 정보를 구독하는 데 사용됨 - 구성된 수신 모듈; 및 상기 구독 구성에 기반하여 구독 정보를 상기 원격 증명 서버에 피드백하도록 구성된 송신 모듈을 포함한다.

[0028] 선택적으로, 상기 구독 구성이 데이터 스트림 구독 구성을 포함하면, 상기 송신 모듈은, 상기 데이터 스트림 구독 구성에 기반하여, 다음 정보:

[0029] 상기 네트워크 디바이스가 부팅될 때 기록되는 신뢰 체인의 각 계층에 있는 소프트웨어의 무결성 정보;

[0030] 상기 네트워크 디바이스가 실행될 때 기록되는 운영 체제의 동적 무결성 정보;

[0031] 상기 네트워크 디바이스가 실행될 때 기록되는 소프트웨어의 동적 무결성 정보;

[0032] 상기 네트워크 디바이스와 관련된 신원 인증서; 그리고

[0033] 상기 네트워크 디바이스와 관련된 원격 증명 인증서

[0034] 중 하나 이상을 상기 원격 서버에 피드백하도록 구성된다.

[0035] 선택적으로, 상기 구독 구성이 이벤트 구독 구성을 포함하면, 상기 송신 모듈은, 다음 트리거된 이벤트: 디바이스 부팅 이벤트, 디바이스 업그레이드 이벤트, 특정 모드 공격 이벤트, 마스터/슬레이브 전환 이벤트, 보드 삽입/제거/전환 이벤트, 및 인증서 수명주기 이벤트 중 하나 이상과 관련된 정보를, 상기 이벤트 구독 구성에 기반하여 상기 원격 서버에 피드백하도록 구성된다.

[0036] 선택적으로, 상기 구독 구성은 구독 모드를 더 포함하고, 상기 구독 모드는 구독 정보를 피드백하는 모드를 지시하는 데 사용되며, 상기 구독 모드는 주기적 피드백 기반 구독 모드 및 이벤트 트리거 피드백 기반 구독 모드 중 하나 또는 조합을 포함하며,

[0037] 상기 송신 모듈은, 상기 구독 구성에 포함된 상기 구독 모드에 기반하여 상기 구독 정보를 상기 원격 증명 서버에 피드백하도록 구성된다.

[0038] 선택적으로, 상기 수신 모듈은 추가로, 상기 원격 증명 서버에 의해 전달된 데이터 처리 파라미터를 수신하도록 구성되고, 상기 송신 모듈에 의해 피드백된 상기 구독 정보는 상기 데이터 처리 파라미터에 기반하여 처리가 수행된 후에 획득된 정보를 포함한다.

[0039] 선택적으로, 상기 수신 모듈은 상기 원격 증명 서버와 네트워크 구성 프로토콜 세션을 구축하고, 상기 네트워크 구성 프로토콜 세션에 기반하여 상기 원격 증명 서버에 의해 전달되는 상기 구독 구성을 수신하도록 구성된다.

[0040] 제5 측면에 따르면, 데이터 수집 디바이스가 제공된다. 상기 데이터 수집 디바이스는 메모리 및 프로세서를 포함한다. 상기 메모리는 적어도 하나의 명령을 포함하고, 상기 적어도 하나의 명령이 상기 프로세서에 의해 로드되고 실행되어, 본 출원의 제1 측면 또는 제2 측면의 임의의 가능한 구현에서의 방법을 구현한다.

[0041] 제6 측면에 따르면, 통신 장치가 제공된다. 상기 통신 장치는 트랜시버, 메모리 및 프로세서를 포함한다. 상기 트랜시버, 상기 메모리 및 상기 프로세서는 내부 연결 채널을 통해 서로 통신한다. 상기 메모리는 명령을 저장하도록 구성된다. 상기 프로세서는 상기 메모리에 저장된 명령을 실행하고, 상기 트랜시버가 신호를 수신하도록

제어하며, 상기 트랜시버가 신호를 송신하도록 제어하도록 구성된다. 또한, 상기 프로세서가 상기 메모리에 저장된 명령을 실행할 때, 상기 프로세서는 제1 측면 또는 제2 측면의 임의의 가능한 구현에서의 방법을 수행하도록 인에이블된다.

[0042] 선택적으로, 하나 이상의 프로세서가 있으며, 하나 이상의 메모리가 있다.

[0043] 선택적으로, 상기 메모리는 상기 프로세서와 통합될 수 있거나, 상기 메모리와 상기 프로세서는 별도로 배치될 수 있다.

[0044] 특정 구현 프로세스에서, 상기 메모리는 읽기 전용 메모리(read-only memory, ROM)와 같은 비 일시적(non-transitory) 메모리일 수 있다. 상기 메모리와 상기 프로세서는 하나의 칩으로 통합될 수 있거나 또는 상이한 칩에 배치될 수 있다. 상기 메모리의 유형과 상기 메모리와 상기 프로세서가 배치되는 모드는 본 출원의 실시예에서 한정되지 않는다.

[0045] 제7 측면에 따르면, 통신 시스템이 제공된다. 상기 통신 시스템은 제3 측면 또는 제3 측면의 임의의 가능한 구현에서의 장치 및 제4 측면 또는 제4 측면의 임의의 가능한 구현에서의 장치를 포함한다.

[0046] 제8 측면에 따르면, 컴퓨터 프로그램 (제품)이 제공된다. 상기 컴퓨터 프로그램 (제품)은 컴퓨터 프로그램 코드를 포함하고, 상기 컴퓨터 프로그램 코드가 컴퓨터에 의해 실행될 때, 상기 컴퓨터가 제1 측면 또는 제2 측면의 임의의 가능한 구현에서의 방법을 수행하도록 인에이블된다.

[0047] 제9 측면에 따르면, 판독 가능한 저장 매체가 제공된다. 상기 판독 가능한 저장 매체는 프로그램 또는 명령을 저장한다. 상기 프로그램 또는 상기 명령이 컴퓨터 상에서 실행될 때, 제1 측면 또는 제2 측면의 임의의 가능한 구현에서의 방법이 수행된다.

[0048] 제10 측면에 따르면, 프로세서를 포함하는 칩이 제공된다. 상기 프로세서가 메모리로부터 상기 메모리에 저장된 명령을 호출하고 실행하므로, 상기 칩이 설치된 통신 디바이스가 제1 측면 또는 제2 측면의 임의의 가능한 구현에서의 방법을 수행한다.

[0049] 제11측면에 따르면, 다른 칩이 제공되며, 상기 칩은 입력 인터페이스, 출력 인터페이스, 프로세서 및 메모리를 포함한다. 상기 입력 인터페이스, 상기 출력 인터페이스, 상기 프로세서 및 상기 메모리는 내부 연결 채널을 통해 서로 연결된다. 상기 프로세서가 상기 메모리에서의 코드를 실행하도록 구성되며, 상기 코드가 실행될 때, 상기 프로세서는 제1 측면 또는 제2 측면의 임의의 가능한 구현에서의 방법을 수행하도록 구성된다.

[0050] 본 출원의 실시 예의 기술 솔루션에 따르면, 원격 증명 서버는 구독 구성을 네트워크 디바이스에 전달하고, 네트워크 디바이스는 구독 구성에 기반하여 구독 정보를 자동으로 피드백할 수 있으므로, 원격 증명에서의 데이터 수집 모드는 더 유연하고 시기 적절(timely)하므로 보안 위험을 감소시킬 수 있다. 또한, 원격 증명 서버가 여러 번 구독 구성을 전달할 필요가 없기 때문에 추가 메시지 교환이 감소되어 데이터 수집 효율성이 향상된다.

도면의 간단한 설명

[0051] 도 1a는 본 출원의 실시 예에 따른 원격 증명 프로세스의 개략도이다.

도 1b는 본 출원의 실시 예에 따른 구현 환경의 개략도이다.

도 2는 본 출원의 실시 예에 따른 부팅 프로세스(boot process)의 개략도이다.

도 3은 본 출원의 실시 예에 따른 부팅 프로세스의 개략도이다.

도 4는 본 출원의 실시 예에 따른 원격 증명 프로세스의 개략도이다.

도 5는 본 출원의 실시 예에 따른 데이터 수집 방법의 흐름도이다.

도 6은 본 출원의 실시 예에 따른 구성 구독 데이터 모델의 트리 구조의 개략도이다.

도 7은 본 출원의 실시 예에 따른 세션 상호 작용의 개략도이다.

도 8은 본 출원의 실시 예에 따른 세션 상호 작용의 개략도이다.

도 9는 본 출원의 실시 예에 따른 동적 구독 데이터 모델의 트리 구조의 개략도이다.

도 10은 본 출원의 실시 예에 따른 동적 구독 데이터 모델의 트리 구조의 개략도이다.

도 11은 본 출원의 실시 예에 따른 세션 상호 작용의 개략도이다.

도 12는 본 출원의 실시 예에 따른 세션 상호 작용의 개략도이다.

도 13은 본 출원의 실시 예에 따른 동적 구독 데이터 모델의 트리 구조의 개략도이다.

도 14는 본 출원의 실시 예에 따른 데이터 수집 장치의 개략적인 구조도이다.

도 15는 본 출원의 실시 예에 따른 데이터 수집 장치의 개략적인 구조도이다.

도 16은 본 출원의 실시 예에 따른 데이터 수집 디바이스의 개략적인 구조도이다. 과

도 17은 본 출원의 실시 예에 따른 통신 장치의 개략적인 구조도이다.

발명을 실시하기 위한 구체적인 내용

[0052] 본 출원의 구현에 사용된 용어는 단지 본 출원의 실시 예를 설명하기 위해 사용된 것이며, 본 출원을 제한하려는 의도는 아니다.

[0053] 신뢰할 수 있는(trusted) 컴퓨팅 시스템에서, 신뢰할 수 있는 네트워크 시스템을 구축하려면 먼저 신뢰의 루트(root-of-trust, RoT)가 필요하고 신뢰의 체인(Chain of Trust)이 구축되어야 한다. 이러한 방식으로 네트워크 시스템의 각 모듈이 신뢰될 수 있다. 그러면, 전체 네트워크 시스템에 대한 신뢰가 구축될 수 있다. 이는 신뢰의 루트가 신뢰할 수 있는 구성 요소이어야 함을 보여준다. 일반적으로 신뢰할 수 있는 플랫폼 모듈(trusted platform module, TPM)과 기본 입/출력 시스템(basic input output system, BIOS)은 절대적으로 신뢰할 수 있는 것으로 간주되기 때문에, 각 네트워크 디바이스의 TPM 및 BIOS에 신뢰의 루트가 존재할 수 있다.

[0054] 신뢰할 수 있는 네트워크 디바이스는 측정을 위한 신뢰의 루트(root of trust for measurement, RTM), 스토리지를 위한 신뢰의 루트(root of trust for storage, RTS) 및 보고를 위한 신뢰의 루트(root of trust for reporting, RTR)인 3개의 신뢰할 수 있는 루트를 포함한다. RTM은 무결성(integrity) 측정을 완료하는 데 사용된다. 무결성 측정은 일반적으로 측정을 위한 신뢰의 코어 루트(core root of trust for measurement, CRTM)에 의해 제어되는 컴퓨팅 엔진을 사용하여 완료된다. CRTM은 네트워크 디바이스가 RTM을 실행할 때 사용되는 실행 코드를 포함하며, CRTM은 일반적으로 BIOS에 저장된다. RTM은 또한 신뢰 이전의 원천(origin of trust transfer)이다. RTS는 무결성 다이제스트(digest) 값과 다이제스트 시퀀스를 유지하는 엔진이며, RTS는 일반적으로 저장된 정보를 암호화하는 엔진과 암호화 키를 포함한다. RTR은 RTS가 보유한 데이터를 안정적으로 보고할 수 있는 컴퓨팅 엔진이다. 이 신뢰성(reliability)은 일반적으로 서명에 의해 보장된다.

[0055] 원격 증명(remote attestation, RA)은 전체적으로 신뢰할 수 있는 컴퓨팅 솔루션의 기술 중 하나이며, RA는 신뢰할 수 있는 서버의 신뢰할 수 있는 상태(trusted status)를 결정하는 데 사용된다. 도 1a에 도시된 바와 같이, 원격 증명 시스템은 RA 서버(RA server), RA 클라이언트(RA client) 및 프라이버시 인증 기관(privacy certificate authority, PCA)을 포함한다. RA 서버는 RA 클라이언트의 플랫폼 구성 레지스터(platform configure register, PCR)의 참조 값(reference value)을 저장하고, RA 클라이언트에 의해 송신된 PCR 값을 수신할 책임이 있으며, RA 클라이언트의 신뢰할 수 있는 상태를 제공한다. RA 클라이언트는 TPM을 가지며, 신뢰할 수 있는 부팅 기능을 지원하는 디바이스이다. RA 클라이언트는 PCA에 의해 할당된 증명 ID 키(attestation identity key, AIK) 인증서(certificate)를 PCA에 신청하고 획득한다. 일부 시나리오에서, RA 서버는 RA 클라이언트 상에서 원격 증명을 시작한다(initiate). RA 서버는 챌린지 요청(challenge request)을 RA 클라이언트에 송신한다. RA 클라이언트는 PCR 값을 수집하고, AIK 개인 키 서명(private key signature)을 사용하며, AIK 개인 키 서명이 사용된 후 획득된 AIK 인증서 및 PCR 값을 RA 서버에 송신한다. RA 서버는 RA 클라이언트로부터 송신된 AIK 인증서의 유효성(validity)을 PCA에 대해 검증한다(verify). PCA는 RA 클라이언트에 대응하는 PCR 참조 값을 RA 서버에 리턴한다. RA 서버는 RA 클라이언트의 PCR 참조 값과 RA 클라이언트에 의해 송신된 PCR 값을 비교하고, 비교 결과에 기반하여 RA 클라이언트의 신뢰할 수 있는 상태를 결정한다. 다시 말해서, RA 서버는 RA 클라이언트가 신뢰할 수 있는(trusted) 지를 판정한다.

[0056] 도 1b에 도시된 구현 환경에서, 신뢰할 수 있는 컴퓨팅 그룹(trusted computing group, TCG)이 제안한 신뢰할 수 있는 루트(trusted root)가 TPM에 존재하는 것을 예로 사용한다. 네트워크 관리 시스템(network management system, NMS) 및/또는 운영 지원 시스템(operations supporting system, OSS)은 RA 서버 및/또는 RA 서버들로 사용되며, 네트워크 디바이스는 RA 클라이언트로 기능하며, 네트워크 디바이스는 TPM을 포함한다. 네트워크 디바이스의 전원을 켜서 네트워크 디바이스의 BIOS를 부팅하고, 네트워크 디바이스 및 네트워크 디바이스의 시스

템 커널 상에 그랜드 통합 부트 로더(grand unified bootloader, GRUB)를 로딩하는 전체 프로세스에서, NMS/OSS는 레벨별로 신뢰 체인 레벨을 구축하기 위해 각 프로세스에서 원격 증명을 수행해야 한다. 네트워크 디바이스는 측정을 통해 획득된 동적 측정 값 및 정적 측정 값과 같은 측정 값을 TPM의 PCR에 저장한다. 네트워크 디바이스의 원격 증명 모듈은 이러한 측정 값을 RA 서버로 기능하는 NMS/OSS에 송신한다. NMS/OSS는 PCR 값과 측정 로그(log)에 기반하여 네트워크 디바이스의 현재 상태를 계산하고 획득하며, 그 다음에 현재 상태를 예상된 값과 비교하여 네트워크 디바이스의 신뢰성을 결정할 수 있다. 도 1b의 높은 보안 영역(security zone)은, 예를 들어, 시스템 커널, 신뢰할 수 있는 영역(trusted zone) 또는 인텔 소프트웨어 가드 확장(intel software guard extensions, SGX)을 포함할 수 있다. 도 1b의 단말은 디바이스 신원 조합 엔진(device identity composition engine, DICE)을 갖는다.

[0057] 네트워크 디바이스의 보안은 디바이스 상에서 실행되는 소프트웨어의 무결성에 크게 좌우된다. 신뢰 체인 모델은 통상적으로(usually) 소프트웨어 무결성을 보장하는 데 사용된다. 부팅 페이즈(boot phase) 동안, 각 페이즈가 실행되기 전에 다음 페이즈가 검사된다(check). 도 2에 도시된 바와 같이, RoT(Root of Trust)는 절대적으로 안전해야 한다. 디바이스 부팅 프로세스(boot process) 동안, 시스템 펌웨어(firmware)는 전체 하드웨어 시스템을 초기화하고 다음 페이즈에서 실행될 시스템 로더(loader)를 검사한다. 다시 말해서, 다음 페이즈에서 실행될 시스템 로더(loader)의 HASH 서명 비교를 수행한다. 시스템 로더의 측정 값이 시스템 로더의 참조 값과 매칭(match)하면, 시스템 로더가 부팅되고 시스템 로더는 다음 페이즈에서 실행될 시스템 커널(kernel)을 검사한다. 시스템 커널의 측정 값이 시스템 커널의 참조 값과 매칭하면 시스템 커널이 부팅된다. 모든 부팅 프로세스가 완료될 때까지 앞서 설명한 부팅 프로세스에 대한 검사 프로세스가 반복된다. 부팅에는 보안 부팅(Secure BOOT) 및 신뢰할 수 있는 부팅(Trusted BOOT)이 포함된다.

[0058] 보안 부팅은 통합 확장 가능한 펌웨어 인터페이스(Unified Extensible Firmware Interface, UEFI)의 일부(서브 규칙(sub-rule))이다. 둘은 부분과 전체 사이에 관계가 있다. UEFI는 인터페이스의 유형을 자세히 정의하는 사양이다. 인터페이스의 유형은 운영 체제가 사전 부팅 운영 환경에서 운영 체제로 자동 로드하는 데 사용된다. 확장 가능한 펌웨어 인터페이스(extensible firmware interface, EFI)는 펌웨어 아키텍처, 인터페이스 및 개인용 컴퓨터(personal computer, PC)의 서비스에 대해 인텔 ®에서 제안한 권장 사양이다. EFI의 주요 기능은 운영 체제(operating system, OS)가 로드되기(boots) 전에 모든 플랫폼에서 일관되고 올바르게 지정된 일련의 부팅 서비스를 제공하는 것이다. 보안 부팅은 멀웨어(malware) 침입을 방지하기 위해 키를 사용한다. UEFI는 일부 신뢰가능한(reliable) 공개 키가 전달 전에 메인 보드에 구축될 수 있음을 지정한다. 그런 다음, 메인 보드에 로드해야 하는 운영 체제 또는 하드웨어 드라이버 프로그램은 공개 키로 인증되어야 한다. 다시 말해서, 소프트웨어는 대응하는 개인 키로 서명되어야 한다. 그렇지 않으면, 메인 보드가 소프트웨어를 로드하기를 거부한다. 멀웨어는 성공적으로 인증될 수 없기 때문에, 멀웨어가 BOOT를 감염시킬 수 없다.

[0059] 신뢰할 수 있는 부팅은 다음을 포함한다: 디바이스 시스템 부팅 프로세스 동안 디바이스의 TPM은 디바이스의 주요 시스템 상태(key system status)를 기록한다. 디바이스 시스템이 부팅된 후 디바이스는 원격 증명 및 인증을 위해 보고서(report)를 원격 서버에 송신한다. 사용자는 원격 증명 및 인증의 결과에 기반하여 전체 시스템 환경의 상태를 신뢰할 수 있는지를 판정한다. 본 출원의 일부 실시 예에서, 디바이스의 원격 증명 기능 모듈은 원격 증명 및 인증을 위한 보고서를 원격 서버에 송신한다. 본 출원의 일부 실시 예에서, 네트워크 관리 시스템 또는 네트워크 컨트롤러는 미리 구성된 정책 또는 특정 모드에서 획득된 정책에 따라 그리고 원격 증명 및 인증의 결과의 기반하여 전체 시스템 환경의 상태를 신뢰할 수 있는지를 판정할 수 있다. 예를 들어, 디바이스의 액세스 허용 여부 또는 디바이스의 서비스 운반(carry) 허용 여부가, 미리 구성된 정책 또는 획득된 정책에 따라 그리고 원격 증명 및 인증의 결과에 기반하여, 네트워크 관리 시스템 또는 네트워크 컨트롤러에 의해 결정될 수 있다.

[0060] 도 3에 도시된 바와 같이, 파일 검사를 부팅하는 것과 파일 측정을 부팅하는 것이 함께 수행될 수 있다. 파일 검사가 실패하면 부팅이 중지되며; 그러나 파일 측정에서, 부팅 프로세스의 측정 값 또는 부팅 프로세스와 관련된 정보의 측정 값만 기록되며, 파일 측정은 부팅을 방해하지 않는다. 도 3에 도시된 바와 같이, 파일 검사가 부팅될 때, 시스템 펌웨어(firmware)가 전체 하드웨어 시스템을 초기화하고, 다음 페이즈에서 실행할 시스템 로더(loader)를 검사한다. 다시 말해서, 다음 페이즈에서 실행될 시스템 로더(loader)의 HASH 서명 비교를 수행한다. 시스템 로더의 측정 값이 시스템 로더의 참조 값과 매칭하지 않으면, 시스템 로더의 부팅이 중지된다. 시스템 로더의 측정 값이 시스템 로더의 참조 값과 매칭하면, 시스템 로더가 부팅되고 시스템 로더는 다음 페이즈에서 실행될 시스템 커널(kernel)을 검사한다. 시스템 커널의 측정 값이 시스템 커널의 참조 값과 매칭하지 않으면, 시스템 커널의 부팅이 중지된다. 시스템 커널의 측정 값이 시스템 커널의 참조 값과 매칭하면, 시스템 커널

이 부팅된다. 도 3에 도시된 바와 같이, 파일 측정이 부팅될 때, 시스템 로더와 시스템 커널도 검사된다. 그러나, 검사는 시스템 로더의 부팅과 시스템 커널의 부팅을 방해하지 않으며, 부팅 프로세스의 측정 값 또는 부팅 프로세스와 관련된 정보의 측정 값만 TPM에 기록된다.

[0061] 또한, 도 4에 도시된 바와 같이, 원격 증명 서버는 특정 포맷과 상호 작용 프로세스를 사용하여, 네트워크 디바이스 또는 노드에 의해 송신된 네트워크 디바이스 또는 노드의 보안 속성을 네트워크를 이용하여 수집하고, 그리고 챌린지 응답 상호 작용 메커니즘을 사용하여 보안 속성을 원격 증명 서버에 안전하게 송신하며, 특정 정책에 따라 검증(verification)을 수행하여 최종적으로 디바이스를 신뢰할 수 있는지를 증명한다(prove). 또한, 전체 원격 증명 프로토콜 상호 작용 프로세스 동안 디바이스 및 통신의 보안을 보장하기 위해, 인증서 적용(application) 및 철회(revocation)와 같은 인증서 메커니즘을 미리 배포하여, 프로토콜 상호 작용 프로세스 동안 인증서 검증 및 보기(viewing)와 같은 필요한 작동(operation)을 지원해야 한다. 네트워크 디바이스 또는 노드는 서버, 사물 인터넷(internet of things, IoT) 게이트웨이 또는 단말일 수 있다. 네트워크 디바이스 또는 노드의 보안 속성은 소프트웨어 및 하드웨어 무결성 값, 구성 정보, 노드 상태 등을 포함한다. 네트워크 디바이스 또는 노드는 중앙 처리 유닛(central processing unit, CPU) & TPM으로부터 BIOS, Grub, 시스템 커널(kernel), 그리고 최종적으로 애플리케이션(application, App)의 신뢰 체인까지의 무결성 값을 계산하고 기록할 수 있다. 도 4에 도시된 바와 같이, 신뢰할 수 있는 단말, 원격 증명, 그리고 디바이스 계층(layer), 통신 계층 및 관리 계층의 종단간 신뢰할 수 있는 실행 환경이, 단말, 게이트웨이, 그리고 클라우드 단말 상에서 구현될 수 있다.

[0062] 전술한 원격 증명 프로세스에서, 데이터 수집 모드는 챌린지 응답 상호 작용 메커니즘을 사용하여 구현된다. 이 모드에서, 원격 증명 서버가 먼저 요청을 네트워크 디바이스에 송신하며, 그 다음에 네트워크 디바이스가 네트워크 디바이스의 보안 속성과 같은 데이터를 원격 증명 서버에 피드백한다. 결과적으로, 이 데이터 수집 모드는 유연하지 않고 시기 적절하지 않아서 어느 정도 보안 위험을 초래한다. 또한, 서버가 요청을 시작해야 하기 때문에 추가 메시지 교환이 발생하고 효율성이 낮다.

[0063] 이를 고려하여 본 출원의 실시 예는 원격 증명 프로세스에 적용되는 데이터 수집 방법을 제공한다. 이 방법에서, 네트워크 구성 프로토콜(network configuration protocol, NETCONF)의 구독/게시(subscription/publishment) 및 푸시(push) 메커니즘에 기반하여 데이터를 수집하는 예를 사용한다. NETCONF는 네트워크 구성 관리 도구(tool)에서 사용되는 네트워크 구성 프로토콜이다. NETCONF는 네트워크 디바이스의 구성 파일을 설치(installing), 질의(querying), 읽기(reading), 쓰기 및 삭제하기 위한 메커니즘을 제공한다. 명령어 라인 인터페이스(command-line interface, CLI) 및 간단한 네트워크 관리 프로토콜(simple network management protocol, SNMP)과 비교하여, NETCONF는 더 유연하고 확장 가능하다. 또한, NETCONF는 원격 프로시저 호출(remote procedure call, RPC) 계층에 기반하여, 확장 가능한 마크업 언어(extensible markup language, XML) 데이터 포맷을 사용하여 네트워크 디바이스 구성을 위한 설치, 운영 및 삭제 메커니즘을 제공한다.

[0064] NETCONF 프로토콜은 다음 4개의 계층으로 나뉜다.

[0065] 콘텐츠(content) 계층은 관리되는 객체(object)의 집합을 나타낸다.

[0066] 작동 계층(operation layer)은 RPC에서 사용되는 일련의 기본 원시 작동 집합(basic primitive operation set)을 정의한다. 이러한 작동은 NETCONF의 기본 능력을 구성한다.

[0067] RPC 계층은 RPC 모듈을 인코딩하기 위한, 단순하고 전송 프로토콜에 독립적인 메커니즘(simple and transport-protocol-independent mechanism)을 제공한다.

[0068] 통신 프로토콜 계층: 연결 없는 사용자 데이터그램 프로토콜(user datagram protocol, UDP)을 전송 프로토콜로 사용하는 SNMP와 달리, NETCONF는 연결 지향적이며(connection-oriented), 통신 포트 간의 영구 연결을 필요로 한다. 또한, 이 연결은 안정적이고 순차적인 데이터 전송을 제공해야 한다. 현재 보안 쉘 프로토콜(Secure Shell, SSH), 전송 계층 보안(Transport Layer Security, TLS) 프로토콜 등이 지원된다.

[0069] 또한, 본 출원의 이 실시 예에서 제공되는 방법에서, Yang push는 표준 메커니즘을 제공하기 위해 사용되므로, 시스템에서 Yang 모델을 사용하여 기술된 모든 데이터를 구독할 수 있다. 구독 경로 및 구독 모드가 지정된 후, 주기적 피드백 기반 구독 모드(periodic feedback based subscription mode)가 선택될 때, 시스템은 지정된 기간(time period)이 만료된 후 지정된 데이터를 구독자에게 푸시한다. on-change 모드(on change mode)(즉, 이벤트 트리거 피드백 기반 구독 모드(event-triggered based subscription mode))가 선택되는 경우, 시스템은

구독 데이터가 변경될 때 구독자에게 데이터를 푸시한다.

[0070] 다음으로, 본 출원의 이 실시 예에서 제공되는 데이터 수집 방법이 설명을 위한 예로 사용된다. 도 5에 도시된 바와 같이, 데이터 수집 방법은 다음 단계를 포함한다.

[0071] 단계(501)에서, 원격 증명 서버는 구독 구성을 네트워크 디바이스에 전달하고, 여기서 구독 구성은 네트워크 디바이스에 의해 수행되는 원격 증명과 관련된 정보를 구독하는 데 사용된다.

[0072] 본 출원에서, 구독 모드가 사용된다. 원격 증명 서버는 네트워크 디바이스에 의해 수행되는 원격 증명과 관련된 정보를 구독하기 위해 구독 구성을 네트워크 디바이스에 전달한다. 선택적으로, 구독 구성은 데이터 스트림 구독 구성 및 이벤트 구독 구성 중 하나 이상을 포함한다. 예를 들어, 원격 증명 서버는 네트워크 디바이스에 의해 수행되는 원격 증명을 위해 데이터 스트림과 관련된 정보를 구독하기 위해, 데이터 스트림 구독 구성을 네트워크 디바이스에 전달한다. 다르게는, 원격 증명 서버는 네트워크 디바이스에 의해 수행되는 원격 증명을 위한 이벤트와 관련된 정보를 구독하기 위해, 이벤트 구독 구성을 네트워크 디바이스에 전달한다. 다르게는, 원격 증명 서버는 네트워크 디바이스에 의해 수행되는 원격 증명을 위한 데이터 스트림 및 이벤트와 관련된 정보를 구독하기 위해, 데이터 스트림 구독 구성 및 이벤트 구독 구성을 네트워크 디바이스에 전달한다. 원격 증명 서버는 데이터 스트림 구독 구성 및 이벤트 구독 구성을 동시에 네트워크 디바이스에 전달하거나 전달하지 않을 수 있다. 이것은 본 출원의 이 실시 예에서 제한되지 않는다.

[0073] 데이터 스트림과 관련된 정보는 네트워크 디바이스의 신뢰와 관련된 다양한 유형의 정보일 수 있으며, 다음 정보: 네트워크 디바이스가 부팅될 때 기록되는 신뢰 체인의 각 계층에 있는 소프트웨어의 무결성 정보, 네트워크 디바이스가 실행될 때 기록되는 운영 체제의 동적 무결성 정보, 네트워크 디바이스가 실행될 때 기록되는 소프트웨어의 동적 무결성 정보, 네트워크 디바이스와 관련된 신원 인증서, 및 네트워크 디바이스와 관련된 원격 증명 인증서 중 하나 이상을 포함하지만 이에 제한되지 않는다.

[0074] 이벤트는 디바이스 부팅 이벤트, 디바이스 업그레이드, 특정 모드 공격 이벤트, 마스터/슬레이브 전환(switchover), 보드 삽입/제거/전환 및 인증서 수명 주기(life cycle) 이벤트 중 하나 이상을 포함하지만, 이에 제한되지는 않는다. 보드 전환 이벤트는 서비스가 위치한 보드에서 전환을 수행하는 이벤트를 포함한다. 원격 증명 서버가 구독하는 데이터 스트림의 종류와 이벤트의 종류는 애플리케이션 시나리오에 기반하여 결정될 수 있다. 이것은 본 출원의 이 실시 예에서 제한되지 않는다.

[0075] 선택적으로, 구독 구성은 구독 모드를 더 포함할 수 있고, 구독 모드는 구독 정보를 피드백하는 모드를 지시하는 데 사용되며, 구독 모드는 주기적 피드백 기반 구독 모드 및 이벤트 트리거 피드백 기반 구독 모드 중 하나 또는 조합을 포함한다. 선택적으로, 서로 다른 유형의 정보는 서로 다른 구독 모드에 대응한다. 예를 들어, 일부 주요 보안 데이터 스트림의 경우, 이벤트 트리거 피드백 기반 구독 모드가 구성되므로, 구독 데이터가 변경될 때 네트워크 디바이스가 변경된 데이터를 원격 증명 서버에 즉시 피드백할 수 있다. 일반 보안 데이터 스트림의 경우, 주기적 피드백 기반 구독 모드가 구성될 수 있으므로, 기간이 만료된 후 네트워크 디바이스는 구독된 데이터를 원격 증명 서버로 피드백한다. 물론, 구독 모드는 다르게는, 다른 정책을 사용하여 결정될 수 있다. 예를 들어, 구독 모드는 애플리케이션 시나리오에 기반하여 결정된다. 이것은 본 출원의 이 실시 예에서 제한되지 않는다.

[0076] 선택적으로, 구독 구성은 필터 구성을 더 포함할 수 있다. 필터 구성은 데이터 스트림 또는 이벤트와 관련된 정보를 필터링하는 데 사용된다. 데이터 스트림 구독 구성 및 이벤트 구독 구성은 비교적 넓은 범위의 정보 구독이지만, 필터는 제한 조건으로 이해될 수 있음을 이해해야 한다. 구체적으로, 상대적으로 광범위한 정보에서 보다 상세한 정보를 선택하여 수집된 데이터가 보다 타깃이 된다(targeted).

[0077] 본 출원의 이 실시 예의 선택적 구현에서, 구독 구성에서 어느 콘텐츠가 구독을 위해 구성되는지에 관계없이, 구독 구성을 네트워크 디바이스에 전달하기 위해, 원격 증명 서버에 의해 구독 구성을 네트워크 디바이스에 전달하는 모드는 다음 모드: 네트워크 디바이스와 네트워크 구성 프로토콜 세션을 구축하고, 네트워크 구성 프로토콜 세션에 기반하여 구독 구성을 네트워크 디바이스에 전달하는 모드 중 하나 이상을 포함하지만 이에 제한되지는 않는다.

[0078] 선택적으로, 본 출원의 이 실시 예에서 제공되는 방법에서, 구독 구성의 시간 유효성은 추가로 네트워크 구성 프로토콜 세션의 시간 유효성에 바인딩될(bound) 수 있다. 네트워크 구성 프로토콜 세션에 기반하여 구독 구성이 전달된 후, 네트워크 구성 프로토콜 세션에 기반하여 동적 구독을 구현할 수 있다. 다시 말해서, 네트워크 구성 프로토콜 세션이 유효할 때, 구독 구성에 따라 구독을 계속할 수 있다. 네트워크 구성 프로토콜 세션의 연

결이 끊어지면, 구독 구성이 유효하지 않으며, 구독 구성에 기반하여 구독을 계속할 수 없으므로, 네트워크 디바이스의 상태를 동적으로 모니터링할 수 있다. 이 모드에서, 추가 정보 교환을 줄이기 위해 대응하는 동적 구독 RPC를 정의할 수 있다.

[0079] 물론, 구독 구성의 시간 유효성은 네트워크 구성 프로토콜 세션의 시간 유효성에 바인딩되지 않을 수 있다. 네트워크 구성 프로토콜 세션에 기반하여 구독 구성이 전달된 후, 구성 구독은 네트워크 구성 프로토콜 세션에 의존하지 않고 구현된다. 다시 말해서, 네트워크 구성 프로토콜 세션의 연결이 끊어졌는지에 관계없이 구독 구성에 기반하여 구독을 계속할 수 있으며, 네트워크 디바이스의 상태를 항상 모니터링할 수 있다.

[0080] 구독 구성의 시간 유효성이 네트워크 구성 프로토콜 세션의 시간 유효성에 바인딩되는지는 수집된 데이터의 유형에 따라 판정될 수 있다. 예를 들어, 일부 주요 보안 데이터의 경우, 구독 구성의 시간 유효성이 네트워크 구성 프로토콜 세션의 시간 유효성에 바인딩되지 않을 수 있으며, 모니터링은 on-change 모드(on-change mode)에서 항상 수행된다. 일반 보안 데이터의 경우, 구독 구성의 시간 유효성은 네트워크 구성 프로토콜 세션의 시간 유효성에 바인딩되어, NETCONF 세션의 부팅 프로세스 동안 관련 정보를 주기적으로 읽을 수 있다.

[0081] 단계(502)에서, 네트워크 디바이스는 원격 증명 서버에 의해 전달된 구독 구성을 수신한다.

[0082] 선택적으로, 네트워크 디바이스가 원격 증명 서버와 네트워크 구성 프로토콜 세션을 구축하면, 원격 증명 서버가 네트워크 구성 프로토콜 세션에 기반하여 구독 구성을 전달한 후, 네트워크 디바이스는 네트워크 구성 프로토콜 세션에 기반하여, 원격 증명 서버에 의해 전달되는 구독 구성을 수신한다.

[0083] 단계(503)에서, 네트워크 디바이스는 구독 구성에 기반하여 구독 정보를 원격 증명 서버에 피드백한다.

[0084] 원격 증명 서버에 의해 전달된 구독 구성을 수신한 후, 네트워크 디바이스는 구독 구성에 기반하여, 원격 증명 서버로 피드백되어야 하는 구독 정보를 획득할 수 있다.

[0085] 선택적으로, 구독 구성이 데이터 스트림 구독 구성을 포함하면, 구독 구성에 기반하여 구독 정보를 원격 증명 서버에 피드백하는 것은, 데이터 스트림 구독 구성에 기반하여, 다음 정보: 네트워크 디바이스가 부팅될 때 기록되는 신뢰 체인의 각 계층에 있는 소프트웨어의 무결성 정보, 네트워크 디바이스가 실행될 때 기록되는 운영 체제의 동적 무결성 정보, 네트워크 디바이스가 실행될 때 기록되는 소프트웨어의 동적 무결성 정보, 네트워크 디바이스와 관련된 신원 인증서, 및 네트워크 디바이스와 관련된 원격 증명 인증서 중 하나 이상을 원격 서버에 피드백하는 것을 포함한다. 피드백할 구독 정보 유형은 구독 구성의 구독 요건(requirement)에 기반하여 결정될 수 있다. 예를 들어, 구독 구성이 네트워크 디바이스에게, 네트워크 디바이스가 부팅될 때 기록되는 신뢰 체인의 각 계층에 있는 소프트웨어의 무결성 정보를 구독하기를 요구하면, 네트워크 디바이스는 네트워크 디바이스가 부팅될 때 기록되는 신뢰 체인의 각 계층에 있는 소프트웨어의 무결성 정보를, 구독 구성에 기반하여 원격 증명 서버에 피드백한다.

[0086] 선택적으로, 구독 구성이 이벤트 구독 구성을 포함하면, 구독 구성에 기반하여 구독 정보를 원격 증명 서버에 피드백하는 것은, 다음 트리거된 이벤트: 디바이스 부팅 이벤트, 디바이스 업그레이드 이벤트, 특정 모드 공격 이벤트, 마스터/슬레이브 전환 이벤트, 보드 삽입/제거/전환 이벤트 및 인증서 수명 주기 이벤트 중 하나 이상과 관련된 정보를 이벤트 구독 구성에 기반하여 원격 서버에 피드백하는 것을 포함한다. 피드백할 구독 정보 유형은 구독 구성의 구독 요건에 기반하여 결정될 수 있다. 예를 들어, 구독 구성이 디바이스 부팅과 관련된 정보를 구독하기를 요구하면, 네트워크 디바이스가 부팅된 후, 네트워크 디바이스는 구독 구성에 기반하여, 네트워크 디바이스가 부팅된 후 획득된 정보를 구독 정보로 하여 원격 증명 서버에 피드백한다.

[0087] 선택적으로, 구독 구성은 구독 모드를 더 포함하고, 구독 모드는 구독 정보를 피드백하는 모드를 지시하는 데 사용되며, 구독 모드는 주기적 피드백 기반 구독 모드, 이벤트 트리거 피드백 기반 구독 모드, 또는 주기적 피드백 기반 구독 모드와 이벤트 트리거 피드백 기반 구독 모드의 조합을 포함한다. 선택적으로, 서로 다른 유형의 정보는 구독 정보를 피드백하는 서로 다른 모드에 대응한다. 네트워크 디바이스는 구독 구성에 포함된 구독 모드에 기반하여, 구독 정보를 원격 증명 서버에 피드백한다. 구독 정보를 피드백하는 데 사용되는 특정 구독 모드는 구독 구성의 구독 요건에 기반하여 결정될 수 있다. 예를 들어, 구독 구성에 의해 요구되는 구독 모드가 주기적 피드백 기반 구독 모드이면, 네트워크 디바이스는 기간이 만료된 후 획득된 구독 정보를 원격 증명 서버에 피드백한다.

[0088] 구독 구성이 필터 구성을 더 포함하면, 구독 구성에서 구독하는 데이터 스트림 및 이벤트와 관련된 정보를 수집한 후, 네트워크 디바이스는 필터 구성에 기반하여, 수집된 정보를 필터링하고 그 다음에 구독 요건을 충족하는

구독 정보를 획득한다.

[0089] 단계(504)에서, 원격 증명 서버는 구독 구성에 기반하여 네트워크 디바이스에 의해 피드백된 구독 정보를 수신한다.

[0090] 네트워크 디바이스에 의해 피드백된 구독 정보를 수신한 후, 원격 증명 서버는 데이터 수집을 완료하고 구독 정보에 기반하여 원격 증명을 수행할 수 있다. 예를 들어, 특정 정책에 따라 검증을 수행하여 네트워크 디바이스가 신뢰할 수 있는지를 최종적으로 증명한다. 이러한 방식으로, 원격 증명은 네트워크 디바이스의 보안 속성을 동적으로 모니터링하여, 네트워크 디바이스가 변조되는(tampered), 교체(replaced) 또는 복사되는 것을 방지할 수 있다.

[0091] 본 출원의 이 실시 예에서, 원격 증명 서버는 구독 구성을 네트워크 디바이스에 전달하고, 네트워크 디바이스는 구독 구성에 기반하여 구독 정보를 자동으로 피드백할 수 있으므로, 원격 증명에서의 데이터 수집 모드가 더 유연해지고 시기 적절해지며, 이에 따라 보안 위험을 감소시킨다. 또한, 원격 증명 서버가 구독 구성을 여러 번 전달할 필요가 없기 때문에 추가 메시지 교환이 감소되어 데이터 수집 효율성이 향상된다.

[0092] 또한, 본 출원의 이 실시 예에서 제공되는 방법은: 원격 증명 서버가 데이터 처리 파라미터(data processing parameter)를 네트워크 디바이스에 전달하는 것을 더 포함한다. 네트워크 디바이스는 원격 증명 서버에 의해 전달된 데이터 처리 파라미터를 수신한다. 이에 기반하여, 네트워크 디바이스가 원격 증명 서버로 피드백한 구독 정보는, 데이터 처리 파라미터에 기반하여 처리가 수행된 후 획득된 정보이다. 이 모드에서, 원격 증명 서버는 nonce, 해시 서명 알고리즘 및 지정된 TPM 이름(name)과 같은 데이터 처리 파라미터를 나중에 사용하기 위해 네트워크 디바이스에 미리 전송한다.

[0093] 예를 들어, TPM의 PCR 값을 획득하기 위해, 데이터 처리 파라미터는 사용될 수 있는, nonce, PCR-list 어레이, 완전한 메시지의 서명 알고리즘 식별자 및 공개 키 식별자(public-key-identifier) 식별자를 포함한다. 각 파라미터의 콘텐츠는 다음과 같다.

[0094] Nonce는 매번 상이하다. 타임 스탬프를 이용하여 타임 넘버로 표현된 nonce의 값을 기록하거나 특정 숫자로 표현된 nonce의 값을 매번 증가시킨다. 원격 증명 서버 및 네트워크 디바이스는 nonce에 기반하여 수신된 메시지의 시간 유효성 및 비 반복(non-repetition)을 결정할 수 있다. nonce를 사용하여 메시지의 시간 유효성 및 비 반복을 확인(confirm)하는 것 외에도, 본 출원의 일부 실시 예에서 원격 증명 서버는 또한 시드(seed) 및 연속적으로 계산된 해시 알고리즘 식별자를 송신하며, 네트워크 디바이스 및 원격 증명 서버는 동기적으로 작동을 수행하여, 이에 따라 수신된 원격 증명 메시지의 시간 유효성과 비 반복을 공동으로 확인한다. 다르게는, 시간 기반 단방향 증명(time-based uni-directional attestation, RATS TUDA) 메커니즘을 사용하여 nonce와 유사한 기능을 구현할 수 있다. RATS TUDA 메커니즘은 기본적으로 단방향 원격 증명 프로토콜이다. 구체적으로, 증명자(attester)(네트워크 디바이스)는 증명자의 무결성 증거를 검증자(verifier)(원격 증명 서버)에게 단방향으로 송신하고, 검증자는 검증 기능을 완료한다. RATS TUDA 메커니즘은 주로 신뢰할 수 있는 제3자, 즉 신뢰할 수 있는 타임 스탬프 기관(trusted time stamp authority, TSA)을 도입한다. 검증자는 수신된 원격 증명 메시지에서 운반된 증명자의 타임 스탬프 정보와 TSA에 의해 제공된 타임 스탬프 토큰(time stamp token, TST)을 사용하여, 수신된 원격 증명 메시지의 시간 유효성과 비 반복을 공동으로 결정한다.

[0095] PCR-list 어레이는 복수의 PCR 정보를 포함한다. PCR 정보는 PCR 레지스터 번호 및 PCR 정보에 사용되는 특정 서명 알고리즘, 예를 들어 디지털 서명 알고리즘(digital signature algorithm, DSA), 타원 곡선 디지털 서명 알고리즘(elliptic curve digital signature algorithm, ECDSA), 또는 Edwards-curve 디지털 서명 알고리즘(Edwards-curve digital signature algorithm, EDDSA)을 포함한다.

[0096] 완전한 메시지의 서명 알고리즘은 DSA, ECDSA, EDDSA 등을 포함한다. 본 출원의 이 실시 예에서, 파라미터는 선택적 서명 알고리즘의 그룹이다. 증명자는 독립적으로 서명 알고리즘을 임의로 선택하고, 선택한 서명 알고리즘을 리턴된 메시지에서 지시할 수 있다.

[0097] 사용될 수 있는 공개 키 식별자(public-key-identifier)는 서명 및 확인에 사용되는 공개/개인 키 쌍을 지정한다. 본 출원의 이 실시 예에서, 파라미터는 선택적 공개 키 번호의 그룹이다. 증명자는 독립적으로 공개 키를 임의로 선택하고, 선택한 공개 키를 리턴된 메시지에서 지정할 수 있다.

[0098] 타깃 TPM 이름/번호는 TPM 이름의 그룹이다. 증명자는 일부 정책에 따라 결정을 내릴 수 있으며, 예를 들어, (1) 수집을 위한 TPM 선택; (2) PCR 값이 변경된 TPM을 송신, 및 (3) 특정 시퀀스에서 모든 TPM의 PCR 값을 송

신하는 것을 결정할 수 있다.

[0099] 다른 예로, 검증자가 증명자(네트워크 디바이스)에 저장되어 있는 저장된 관리 로그(stored management log, SML)의 PCR 값을 획득해야 하면, 송신된 데이터 처리 파라미터는 노드 이름, SML의 로그 레코드 선택 모드, 로그 유형 및 PCR-list 어레이를 포함한다. 각 파라미터의 콘텐츠는 다음과 같다.

[0100] 노드 이름: 본 출원의 이 실시 예에서, 파라미터는 노드 이름의 그룹이다. 검증자가 노드 이름을 증명자에게 전달한 후, 증명자는 일부 정책에 따라 결정을 내릴 수 있다. 예를 들어, (1) 증명자가 수집을 위한 노드를 선택하고, (2) SML 로그 파일이 변경된 노드를 송신하며, 및 (3) 특정 시퀀스에서 각 노드의 모든/업데이트된 SML 값을 송신한다.

[0101] SML의 로그 레코드 선택 모드는 다음과 같다: 마지막 로그 레코드가 획득된 후 로그 레코드를 선택하며, 로그 레코드가 지정된 번호에 따라 획득되거나 또는 로그 레코드가 지정된 시간에 따라 획득된다. 검증자가 SML의 로그 선택 모드를 증명자에게 전달한 후, 증명자는 독립적으로 선택 모드를 임의로 선택하고, 선택된 모드를 리턴된 메시지에서 지정할 수 있다.

[0102] 로그 유형은 BIOS 또는 무결성 측정 아키텍처(integrity measurement architecture, IMA)이다.

[0103] PCR-list 어레이는 복수의 PCR 정보를 포함한다. PCR 정보는 PCR 레지스터 번호와 PCR 정보에 사용되는 특정 서명 알고리즘, 예를 들어, DSA, ECDSA 또는 EDDSA를 포함한다.

[0104] 데이터 처리 파라미터의 전술한 두 가지 예는 본 출원의 이 실시 예에서 제공되는 방법의 예시적인 실시 예일 뿐이며, 다른 유형 또는 다른 콘텐츠를 가지는 데이터 처리 파라미터가 상이한 애플리케이션에 기반하여 추가로 전달될 수 있음을 이해해야 한다. 이것은 본 출원의 이 실시 예에서 제한되지 않는다. 어떤 유형의 데이터 처리 파라미터가 사용되는지에 관계없이, 원격 증명에 사용되는 관련 정보를 획득된 후, 네트워크 디바이스는 데이터 처리 파라미터에 기반하여 획득된 정보를 처리한 다음, 처리된 정보를 원격 증명 서버에 피드백할 수 있다. 예를 들어, 획득된 정보는 데이터 처리 파라미터의 암호화 알고리즘에 기반하여 암호화된다.

[0105] 결론적으로, 본 출원의 이 실시 예에서, NETCONF의 pub/sub 및 push 메커니즘에서, 널리 사용된 시나리오는 기존 고정 네트워크에 존재하며, 유연성, 고효율, 사전 알림, 시간 유효성과 같은 메커니즘의 효과는 상속된다. 또한, 디바이스 측 상의 이벤트에 의해 트리거되는 원격 증명 메커니즘은 네트워크 디바이스가 구독 정보를 사전에(proactively) 피드백하는 것에 의해 구현된다. 또한, nonce는 무작위적이고 동기적이므로, 정보가 본 출원의 이 실시 예에서 제공되는 상호 작용 메커니즘에서 사용될 수 있다.

[0106] 이해의 편의를 위해 다음 두 가지 예를 사용하여 설명한다.

[0107] (1) 구성 구독 모드에서 구독하는 이벤트의 경우

[0108] 1. 예를 들어, 구독 구성은 데이터 스트림 구독 구성, 이벤트 구독 구성, 필터 구독 구성 및 구독 모드를 포함하며, 원격 증명 서버는 데이터 처리 파라미터를 추가로 전달한다. 콘텐츠는 다음과 같다.

[0109] 데이터 스트림 구독 구성의 콘텐츠는:

[0110] 데이터 스트림: pcr-trust-evidence(PCR 신뢰 증거);

[0111] bios-log-trust-evidence(BIOS 로그 신뢰 증거); 및

[0112] ima-log-trust-evidence(IMA 로그 신뢰 증거)

[0113] 를 포함한다.

[0114] 이벤트 구독 구성의 콘텐츠는:

[0115] 이벤트 이름(1001); 및

[0116] 이벤트 유형: 디바이스 부팅 완료됨

[0117] 을 포함한다.

[0118] 데이터 스트림의 데이터 처리 파라미터는:

[0119] 원격 증명의 유형: tpm2-attestation-challenge;

[0120] pcr 라이브러리: aaa;

[0121] pcr-indices: 6;

[0122] 해시 알고리즘 id: 14; nonce-value: 0x564ac291;

[0123] signature-identifier-type: TPM_ALG-ID:2;

[0124] Key-id: public-key 0x784a22bf

[0125] 를 포함한다.

[0126] 필터 구독 구성은:

[0127] 벤더의 디바이스의 yang 모델: xxx-vendor-device; 및

[0128] 디바이스의 디바이스 id: 030DLA106C0522221111

[0129] 를 포함한다.

[0130] 구독 모드는:

[0131] 주기적 피드백: periodic;

[0132] 구독 주기: 500; 및

[0133] 푸시할 보안 데이터 스트림: 1001(이벤트 구독 구성의 디바이스 부팅 이벤트 ID와 동일)

[0134] 을 포함한다.

[0135] 이전 구독 구성에 기반하여, 구성 정보는 다음과 같다.

```
<rpcnetconf:message-id="101"
  xmlns:netconf="urn:ietf:params:xml:ns:netconf:base:1.0">
 <edit-config>
  <streams>
   <stream>
    <name>pcr-trust-evidence</name>
   </stream>
   <stream>
    <name>bios-log-trust-evidence</name>
   </stream>
   <stream>
    <name>ima-log-trust-evidence</name>
   </stream>
  </streams>
  <subscriptions
    xmlns="urn:ietf:params:xml:ns:yang:ietf-subscribed-notifications">
   <events>
    <event>
     <name>1001</name>
     <type>device-startup-ok</type>
    </event>
   </events>
   <subscription>
    <subscription-id>100</subscription-id>
    <rats-type>
     <tpm2-attestation-challenge>
      <pcr-list>
       <id>aaa</id>
       <pcr-indices>6</pcr-indices>
       <algo-registry-type>
        <ietf-ni-hash-algo-id>14</ietf-ni-hash-algo-id>
```

[0136]

```
                </algo-registry-type>
              </pcr-list>
              <nonce-value>0x564ac291</nonce-value>
              <signature-identifier-typ>
               <TPM_ALG-ID>2</TPM_ALG-ID>
              </signature-identifier-typ>
              <key-identifier>
               <public-key>0x784a22bf</public-key>
                </key-identifier>
              </tpm2-attestation-challenge>
            </rats-type>
            <stream-subtree-filter>
                <xxx-vendor-device
                 xmlns="urn:xxx:params:xml:ns:yang:xxx-vendor-device ">
                 <device-id>030DLA106C0522221111</device-id>
                </xxx-vendor-device>
            </stream-subtree-filter>
            <periodic xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-push:1.0">
              <sub-rats-event xmlns="urn:ietf:params:xml:ns:yang:ietf-rats-sub-push:1.0">
               1001</sub-rats-event>
              <period>500</period>
            </periodic>
          </subscription>
        </subscriptions>
      </edit-config>
    </rpc>
```

[0137]

[0138] yang 데이터 모델을 정의하고, 구독 데이터 스트림 유형과 구독 이벤트 유형을 설명하며, 구성 구독을 구현한다. 도 6은 관련 구성 구독 데이터 모델의 트리 구조를 나타낸다. 트리 구조의 예는 IETF RFC8340에 기반하여 작성된다.

[0139] 하위 계층 전송 프로토콜 NETCONF의 경우, 원격 증명 서버는 NETCONF 클라이언트(NETCONF client)이고, 네트워크 디바이스는 NETCONF 서버(NETCONF server)이다. 도 7에 도시된 바와 같이, NETCONF 클라이언트(원격 증명 서버)는 먼저 NETCONF 서버(네트워크 디바이스)와 netconf 세션을 구축하고, yang 데이터 모델을 사용하여 관련 원격 증명 구독 구성을 NETCONF 서버에 전달한다. NETCONF 서버는 주기적으로 알림(notification)을 송신하여, 관련 데이터, 즉 구독 정보를 NETCONF 클라이언트에 주기적으로 푸시한다. 구성 구독은 netconf 세션에 의존하지 않는다. 세션이 다운된(session is down) 후에, 구성 구독은 여전히 존재하며, NETCONF 서버는 여전히 주기적으로 알림을 NETCONF 클라이언트에 송신한다.

[0140] 2. 예를 들어, 구독 구성은 데이터 스트림 구독 구성, 이벤트 구독 구성, 필터 구독 구성 및 구독 모드를 포함하며, 원격 증명 서버는 데이터 처리 파라미터를 추가로 전달한다. 콘텐츠는 다음과 같다.

[0141] 데이터 스트림 구독 구성의 콘텐츠는: 데이터 스트림: pcr-trust-evidence(PCR-trust-evidence), bios-log-trust-evidence(BIOS-log-trust-evidence) 및 ima-log- trust-evidence(IMA-log-trust-evidence)를 포함한다.

[0142] 이벤트 구독 구성의 콘텐츠는:

[0143] 이벤트 이름: 1002; 및

[0144] 이벤트 유형: 마스터/슬레이브 전환

[0145] 을 포함한다.

[0146] 데이터 스트림의 데이터 처리 파라미터는:

[0147] 원격 증명의 유형: log-retrieval;

[0148] log-selector 구성: node-name이 aaa;

[0149] node-physical-index: 77;

[0150] index-type: last-entry-value으로서 선택됨: 010101;

[0151] log-type: bios; pcr 라이브러리: aaa; pcr-indices: 7;

[0152] 해시 알고리즘 id: 14; 및 log-entry-quantity: 69

[0153] 을 포함한다.

[0154] 필터 구독 구성은:

[0155] 벤더의 디바이스의 yang 모델: xxx-vendor-device; 및

[0156] 디바이스의 디바이스 id: xxxx

[0157] 를 포함한다.

[0158] 구독 모드는:

[0159] on-change 보고: on-change;

[0160] 푸시될 보안 데이터 스트림: 1002(마스터/슬레이브 전환 이벤트 ID와 동일)

[0161] 을 포함한다.

[0162] 이전 구독 구성에 기반하여, 구성 정보는 다음과 같다.

```
<rpcnetconf:message-id="101"
  xmlns:netconf="urn:ietf:params:xml:ns:netconf:base:1.0">
  <edit-config>
  <streams>
   <stream>
    <name>pcr-trust-evidence</name>
   </stream>
  <stream>
    <name>bios-log-trust-evidence</name>
  </stream>
  <stream>
    <name>ima-log-trust-evidence</name>
  </stream>
  </streams>
  <subscriptions
   xmlns="urn:ietf:params:xml:ns:yang:ietf-subscribed-notifications">
   <events>
    <event>
     <name>1002</name>
       <type>master-slave-swithover</type>
    </event>
   </events>
   <subscription>
     <subscription-id>100</subscription-id>
    <rats-type>
     <log-retrieval>
       <log-selector>
       <node-name>linkcard-2</node-name>
       <node-physical-index>77</node-physical-index>
        <index-type>
        <last-entry-value>67</last-entry-value>
```

[0163]

```
                    <index-type>
                    </log-selector>
                     <log-type>bios</log-type>
                     <pcr-list>
                      <id>aaa</id>
                     <pcr-indices>7</pcr-indices>
                     <algo-registry-type>
                     <ietf-ni-hash-algo-id>5</ietf-ni-hash-algo-id>
                     </algo-registry-type>
                     </pcr-list>
                    <log-entry-quantity>69</log-entry-quantity>
                  </log-retrieval>
                 </rats-type>

               <stream-subtree-filter>
                 <xxx-vendor-device
                        xmlns="urn:xxx:params:xml:ns:yang:xxx-vendor-device ">
                   <device-id>030DLA106C0522221111</device-id>
                 </xxx-vendor-device>
               </stream-subtree-filter>
             <on-change xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-push:1.0">
               <sub-rats-event xmlns="urn:ietf:params:xml:ns:yang:ietf-rats-sub-push:1.0">
                  1001</sub-rats-event>
               </on-change>
             </subscription>
           </subscriptions>
         </edit-config>
       </rpc>
```

[0164]

[0165] 도 8에 도시된 바와 같이, NETCONF 클라이언트는 NETCONF 서버와 netconf 세션을 구축하고, yang 데이터 모델을 사용하여 대응하는 원격 증명 구독 구성을 NETCONF 서버에 전달한다. 구독된 키 데이터가 변경될 때, NETCONF 서버는 알림을 송신하여, 관련 데이터, 즉 구독 정보를 NETCONF 클라이언트에 푸시한다. 구성 구독은 netconf 세션에 의존하지 않을 수 있다. 세션이 다운된 후에, 구성 구독은 여전히 존재하며, NETCONF 서버는 여전히 주기적으로 알림을 클라이언트에 송신한다.

[0166] 구독 이벤트가 트리거될 때, NETCONF 서버는 다음 포맷의 알림을 NETCONF 클라이언트에 송신한다. 도 9는 관련된 동적 구독 데이터 모델의 트리 구조를 나타낸다. 트리 구조의 예는 IETF RFC8340에 기반하여 작성된다.

[0167] (2) 동적 구독 모드에서 구독되는 증명 이벤트의 경우

[0168] 1. 예를 들어, 구독 구성은 데이터 스트림 구독 구성, 필터 구독 구성 및 구독 모드를 포함한다. 콘텐츠는 다음과 같다.

[0169] 데이터 스트림 구독 구성의 콘텐츠는:

[0170] 원격 증명의 유형: tpm2-attestation-challenge;

[0171] pcr 라이브러리: aaa; pcr-indices: 7;

[0172] 해시 알고리즘 id: 5;

[0173] nonce-value: 0xa45668b1;

[0174] signature-identifier-type: TPM_ALG-ID:2; 및

[0175] Key-id: public-key 0xad3567c3

[0176] 를 포함한다.

[0177] 필터 구독 구성은:

[0178] 벤더의 디바이스의 yang 모델: xxx-vendor-device; 및

[0179] 디바이스의 디바이스 id: xxxx

[0180] 를 포함한다.

[0181] 구독 모드는:

[0182] 주기적 보고: periodic;

[0183] 구독 주기: 500; 및

[0184] 푸시할 보안 데이터 스트림: 1001(이는 디바이스 부팅 이벤트 id와 동일함)

[0185] 을 포함한다.

[0186] 이전 구독 구성에 기반하여, 구성 정보는 다음과 같다.

```
<rpcnetconf:message-id="101"
 xmlns:netconf="urn:ietf:params:xml:ns:netconf:base:1.0">
  <establish-subscription
  xmlns="urn:ietf:params:xml:ns:yang:ietf-subscribed-notifications">
 <rats-type>
 <tpm2-attestation-challenge>
                <pcr-list>
          <id>aaa</id>
                <pcr-indices>7</pcr-indices>
                <algo-registry-type>
               <ietf-ni-hash-algo-id>5</ietf-ni-hash-algo-id>
              </algo-registry-type>
              </pcr-list>
              <nonce-value>0xa45668b1</nonce-value>
              <signature-identifier-typ>
               <TPM_ALG-ID>2</TPM_ALG-ID>
               </signature-identifier-typ>
              <key-identifier>
                <public-key>0xad3567c3</public-key>
              </key-identifier>
             </tpm2-attestation-challenge>
              </rats-type>
                  <stream-subtree-filter>
                    <xxx-vendor-device xmlns="urn:xxx:params:xml:ns:yang:xxx-vendor
-device ">
                     device-id>xxxxx</device-id>
                     </xxx-vendor-device>
          </stream-subtree-filter>
          <periodic xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-push:1.0">
          <sub-rats-event xmlns="urn:ietf:params:xml:ns:yang:ietf-rats-sub-
push:1.0">1001</sub-rats-event>
            <period>500</period>
           </periodic>
      </establish-subscription>
  </rpc>
```

[0187]

[0188] yang 데이터 모델을 정의하고, 구독 데이터 스트림 유형과 구독 이벤트 유형을 설명하며, 동적 구독을 구현한다. 도 10은 관련된 동적 구독 데이터 모델의 트리 구조를 나타낸다. 트리 구조의 예는 IETF RFC8340에 기반하여 작성된다.

[0189] 동적 구독에서, NETCONF 클라이언트는 netconf 세션이 시작될 때 구독 RPC를 NETCONF 서버에 송신한다. NETCONF 서버는 netconf 세션이 존재하는 주기 내에서 구독 정보를 주기적으로 푸시하거나 on-change 모드의 구독 정보를 NETCONF 클라이언트로 푸시한다. 예를 들어, 도 11에 도시된 바와 같이, NETCONF 클라이언트는 NETCONF 서버와 netconf 세션을 구축하고, RPC를 사용하여 대응하는 원격 증명 구독 구성을 NETCONF 서버에 전달한다. NETCONF 서버는 주기적으로 알림을 송신하여, 관련 데이터, 즉 구독 정보를 NETCONF 클라이언트에 주기적으로 푸시한다. 동적 구독은 netconf 세션에 의존한다. 세션이 다운될 때, 구독이 사라진다(disappear).

[0190] 2. 예를 들어, 구독 구성은 데이터 스트림 구독 구성, 필터 구독 구성 및 구독 모드를 포함한다. 콘텐츠는 다음과 같다.

[0191] 데이터 스트림 구독 구성의 콘텐츠는:

[0192] 원격 증명의 유형: log-retrieval;

[0193] log-selector 구성: 노드 이름은 linecard-2;

[0194] node-physical-index: 77;

[0195] index-type: last-entry-value으로 선택됨: 28;

[0196] log-type: bios; pcr 라이브러리: aaa; pcr-indices: 7;

[0197] 해시 알고리즘 id: 5; 및

[0198] log-entry-quantity: 69

[0199] 를 포함한다.

[0200] 이벤트 구독 구성의 콘텐츠는:

[0201] 이벤트 이름: 1008; 및

[0202] 이벤트 유형: 디바이스 업그레이드

[0203] 를 포함한다.

[0204] 필터 구독 구성의 콘텐츠는:

[0205] 벤더의 디바이스의 yang 모델: xxx-vendor-device; 및

[0206] 디바이스의 디바이스 id: xxxx

[0207] 를 포함한다.

[0208] 구독 모드는:

[0209] on-change 보고: on-change;

[0210] 푸시할 보안 데이터 스트림: 1008(이는 디바이스 업그레이드 이벤트 id와 동일함)

[0211] 을 포함한다.

[0212] 이전 구독 구성에 기반하여, 구성 정보는 다음과 같다.

```
<rpcnetconf:message-id="101"
  xmlns:netconf="urn:ietf:params:xml:ns:netconf:base:1.0">
    <establish-subscription
      xmlns="urn:ietf:params:xml:ns:yang:ietf-subscribed-notifications">
     <rats-type>
      <log-retrieval>
      <log-selector>
       <node-name>aaa</node-name>
       <node-physical-index>77</node-physical-index>
       <index-type>
          <last-entry-value>010101</last-entry-value>
          <index-type>
      </log-selector>
      <log-type>bios</log-type>
              <pcr-list>
              <id>aaa</id>
              <pcr-indices>73</pcr-indices>
              <algo-registry-type>
              <ietf-ni-hash-algo-id>14</ietf-ni-hash-algo-id>
              </algo-registry-type>
              </pcr-list>
              <log-entry-quantity>69</log-entry-quantity>
          </log-retrieval>
         </rats-type>
       <stream-subtree-filter>
          <xxx-vendor-device    xmlns="urn:xxx:params:xml:ns:yang:xxx-vendor-device
">
          device-id>xxxxx</device-id>
       </xxx-vendor-device>
       </stream-subtree-filter>
    <on-change xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-push:1.0">
    <sub-rats-event
xmlns="urn:ietf:params:xml:ns:yang:ietf-rats-sub-push:1.0">1008</sub-rats-event>
    </on-change>
  </establish-subscription>
</rpc>
```

[0213]

[0214] 도 12에 도시된 바와 같이, NETCONF 클라이언트는 NETCONF 서버와 netconf 세션을 구축하고, RPC를 사용하여 관련 원격 증명 구독 구성을 NETCONF 서버에 전달한다. 구독된 키 데이터가 변경될 때 NETCONF 서버는 알림을 송신하여, 관련 데이터, 즉 구독 정보를 NETCONF 클라이언트에 푸시한다. 동적 구독은 netconf 세션에 의존한다. 세션이 다운될 때 구독이 사라진다.

[0215] 구독 이벤트가 트리거될 때, NETCONF 서버는 다음 포맷으로 알림을 NETCONF 클라이언트에 송신한다. 도 13은 관련된 동적 구독 데이터 모델의 트리 구조를 나타낸다. 트리 구조의 예는 국제 표준 RFC8340에 기반하여 작성된다.

[0216] 결론적으로, 본 출원의 이 실시 예에서 제공되는 방법에서, 최신 netconf/대표 상태 전송 구성 프로토콜(representational state transfer configuration protocol, RESCONF) pub(publication)/sub((subscription) 및 push(push) 메커니즘이 사용되며, 상기 방법은 기존의 고정 네트워크에서 널리 사용된다. 이 메커니즘은, 예를 들어, RESCONF + JS 객체 표기법(javascript object notation, JSON)/확장 가능한 마크업 언어(extensible markup language, XML) 및 제약 애플리케이션 프로토콜(constrained application protocol, CoAP) + 간결한 이진 객체 표현(concise binary object representation, CBOR)과 같은, 다른 프로토콜 및 메시지 인코딩 포맷으

로 쉽게 변환될 수 있음을 이해해야 한다. 이러한 방식으로, 메커니즘이 웹(인터넷), IoT 및 모바일 디바이스와 같은 시나리오에 쉽게 이식될 수 있다. 다른 프로토콜의 데이터 수집 방법은 NETCONF와 동일한 원리를 가지고 있다. 자세한 내용은 여기서 다시 설명하지 않는다.

[0217] 동일한 기술적 개념에 기반하여, 본 출원의 실시 예는 데이터 수집 장치를 더 제공한다. 데이터 수집 장치는 원격 증명 프로세스에 사용된다. 도 14를 참조하며, 데이터 수집 장치는:

[0218] 구독 구성을 네트워크 디바이스에 전달하도록 구성된 송신 모듈(141) - 구독 구성은 네트워크 디바이스에 의해 수행된 원격 증명과 관련된 정보를 구독하는 데 사용됨 -; 및

[0219] 구독 구성에 기반하여 네트워크 디바이스에 의해 피드백되는 구독 정보를 수신하도록 구성된 수신 모듈(142)을 포함한다.

[0220] 선택적으로, 송신 모듈(141)은 추가로, 데이터 처리 파라미터를 네트워크 디바이스에 전달하도록 구성되며, 여기서 구독 정보는 데이터 처리 파라미터에 기반하여 처리가 수행된 후에 획득된 정보를 포함한다.

[0221] 선택적으로, 송신 모듈(141)은 네트워크 디바이스와 네트워크 구성 프로토콜 세션을 구축하고, 네트워크 구성 프로토콜 세션에 기반하여 구독 구성을 네트워크 디바이스에 전달하도록 구성된다.

[0222] 동일한 기술적 개념에 기반하여, 본 출원의 실시 예는 데이터 수집 장치를 더 제공한다. 데이터 수집 장치는 원격 증명 프로세스에 사용된다. 도 15를 참조하며, 데이터 수집 장치는:

[0223] 원격 증명 서버에 의해 전달된 구독 구성을 수신하도록 구성된 수신 모듈(151) - 구독 구성은 네트워크 디바이스에 의해 수행된 원격 증명과 관련된 정보를 구독하는 데 사용됨 -; 및

[0224] 구독 구성에 기반하여 구독 정보를 원격 증명 서버에 피드백하도록 구성된 송신 모듈(152)을 포함한다.

[0225] 선택적으로, 구독 구성이 데이터 스트림 구독 구성을 포함하면, 송신 모듈(152)은 데이터 스트림 구독 구성에 기반하여 다음 정보:

[0226] 네트워크 디바이스가 부팅될 때 기록되는 신뢰 체인의 각 계층에 있는 소프트웨어의 무결성 정보;

[0227] 네트워크 디바이스가 실행될 때 기록되는 운영 체제의 동적 무결성 정보;

[0228] 네트워크 디바이스가 실행될 때 기록되는 소프트웨어의 동적 무결성 정보;

[0229] 네트워크 디바이스와 관련된 신원 인증서; 및

[0230] 네트워크 디바이스와 관련된 원격 증명 인증서

[0231] 중 하나 이상을 원격 서버에 피드백하도록 구성된다.

[0232] 선택적으로, 구독 구성이 이벤트 구독 구성을 포함하면, 송신 모듈(152)은 다음 트리거된 이벤트: 디바이스 부팅 이벤트, 디바이스 업그레이드 이벤트, 특정 모드 공격 이벤트, 마스터/슬레이브 전환 이벤트, 보드 삽입/제거/전환 이벤트 및 인증서 수명주기 이벤트 중 하나 이상과 관련된 정보를, 이벤트 구독 구성에 기반하여 원격 서버에 피드백하도록 구성된다.

[0233] 선택적으로, 구독 구성은 구독 모드를 더 포함하고, 구독 모드는 구독 정보를 피드백하는 모드를 지시하는 데 사용되며, 구독 모드는 주기적 피드백 기반 구독 모드 및 이벤트 트리거 기반 구독 모드 중 하나 또는 조합을 포함하며; 그리고

[0234] 송신 모듈(152)은 구독 구성에 포함된 구독 모드에 기반하여 구독 정보를 원격 증명 서버에 피드백하도록 구성된다.

[0235] 선택적으로, 수신 모듈(151)은 추가로, 원격 증명 서버에 의해 전달된 데이터 처리 파라미터를 수신하도록 구성되고, 송신 모듈에 의해 피드백되는 구독 정보는 데이터 처리 파라미터에 기반하여 처리가 수행된 후에 획득된 정보를 포함한다.

[0236] 선택적으로, 수신 모듈(151)은 원격 증명 서버와 네트워크 구성 프로토콜 세션을 구축하고, 네트워크 구성 프로토콜 세션에 기반하여 원격 증명 서버에 의해 전달된 구독 구성을 수신하도록 구성된다.

[0237] 위에 제공된 장치가 장치의 기능을 구현하는 경우, 전술한 기능 모듈로의 분할은 설명을 위한 예일뿐이다. 실제 애플리케이션에서, 전술한 기능은 요건에 따라 서로 다른 기능 모듈에 의해 할당 및 구현될 수 있으며, 즉, 디

바이스의 내부 구조는 전술한 기능의 전부 또는 일부를 구현하기 위해 서로 다른 기능 모듈로 분할된다. 또한, 전술한 실시 예에서 제공된 장치 및 방법 실시 예는 동일한 개념에 속한다. 구체적인 구현 과정은 방법 실시 예를 참조한다. 자세한 내용은 여기서 다시 설명하지 않는다.

[0238] 동일한 개념에 기반하여, 본 출원의 실시 예는 데이터 수집 디바이스를 추가로 제공한다. 도 16을 참조하면, 데이터 수집 디바이스는 메모리(161) 및 프로세서(162)를 포함한다. 메모리(161)는 적어도 하나의 명령을 저장하고, 적어도 하나의 명령은 프로세서(162)에 의해 로드되고 실행되어 본 출원의 실시 예에서 제공된 전술한 데이터 수집 방법 중 어느 하나를 구현한다.

[0239] 본 출원의 실시 예는 통신 장치를 더 제공한다. 도 17에 도시된 바와 같이, 통신 장치는 트랜시버(transceiver)(171), 메모리(172) 및 프로세서(173)를 포함한다. 트랜시버(171), 메모리(172) 및 프로세서(173)는 내부 연결 채널을 통해 서로 통신한다. 메모리(172)는 명령을 저장하도록 구성된다. 프로세서(173)는 메모리에 저장된 명령을 실행하고, 트랜시버(171)가 신호를 수신하도록 제어하고, 트랜시버(171)가 신호를 전송하도록 제어하도록 구성된다. 또한, 프로세서(173)가 메모리(172)에 저장된 명령을 실행할 때, 프로세서(173)는 전술한 데이터 수집 방법 중 어느 하나를 수행할 수 있다.

[0240] 본 출원의 실시 예는 통신 시스템을 더 제공한다. 통신 시스템은 도 14에 도시된 장치와 도 15에 도시된 장치를 포함한다.

[0241] 본 출원의 데이터 수집 디바이스는 개인용 컴퓨터(personal computer, PC), 서버 또는 네트워크 디바이스일 수 있다. 예를 들어, 데이터 수집 디바이스는 라우터, 스위치, 서버 등일 수 있다.

[0242] 동일한 개념에 기반하여, 본 출원의 실시 예는 컴퓨터가 판독 가능 저장 매체를 더 제공한다. 저장 매체는 적어도 하나의 명령을 저장하고, 이 명령은 본 출원의 실시 예에서 제공된 전술한 데이터 수집 방법 중 어느 하나를 구현하기 위해 프로세서에 의해 로드되고 실행된다.

[0243] 본 출원의 실시 예는 프로세서를 포함하는 칩을 더 제공한다. 프로세서는 메모리에 저장된 명령을 메모리로부터 호출하고 실행하도록 구성되므로, 칩이 설치된 통신 디바이스가 전술한 데이터 수집 방법 중 하나를 수행한다.

[0244] 본 출원의 실시 예는 입력 인터페이스, 출력 인터페이스, 프로세서 및 메모리를 포함하는 칩을 더 제공한다. 입력 인터페이스, 출력 인터페이스, 프로세서 및 메모리는 내부 연결 채널을 통해 연결된다. 프로세서는 메모리에서 코드를 실행하도록 구성된다. 코드가 실행될 때, 프로세서는 전술한 데이터 수집 방법 중 하나를 수행하도록 구성된다.

[0245] 프로세서는 중앙 처리 유닛(Central Processing Unit, CPU)이거나 다른 범용 프로세서, 디지털 신호 프로세서(digital signal processor, DSP) 또는 애플리케이션 특정 집적 회로(application specific integrated circuit, ASIC), 필드 프로그래밍 가능 게이트 어레이(field-programmable gate array, FPGA) 또는 다른 프로그래밍 가능 로직 디바이스, 개별 게이트 또는 트랜지스터 로직 디바이스, 개별 하드웨어 구성 요소 등일 수 있다. 범용 프로세서는 마이크로 프로세서, 임의의 통상적인 프로세서 등일 수 있다. 프로세서는 고급 RISC 머신(advanced RISC machines, ARM) 아키텍처를 지원하는 프로세서일 수 있다.

[0246] 또한, 선택적 실시 예에서, 하나 이상의 프로세서가 있고, 하나 이상의 메모리가 있다. 선택적으로, 메모리는 프로세서와 통합될 수 있거나, 또는 메모리와 프로세서는 별도로 배치될 수 있다. 메모리는 읽기 전용 메모리 및 랜덤 액세스 메모리를 포함할 수 있으며, 명령 및 데이터를 프로세서에 제공할 수 있다. 메모리는 비 휘발성 랜덤 액세스 메모리를 더 포함할 수 있다. 예를 들어, 메모리는 디바이스 유형에 대한 정보를 더 저장할 수 있다.

[0247] 메모리는 휘발성 메모리 또는 비 휘발성 메모리일 수 있거나, 휘발성 메모리와 비 휘발성 메모리를 모두 포함할 수 있다. 비 휘발성 메모리는 읽기 전용 메모리(read-only memory, ROM), 프로그래밍 가능한 읽기 전용 메모리(programmable ROM, PROM), 소거 가능한 프로그래밍 가능한 읽기 전용 메모리(erasable PROM, EPROM), 전기적으로 소거 가능한 프로그래밍 가능 읽기 전용 메모리(electrically EPROM, EEPROM) 또는 플래시 메모리일 수 있다. 휘발성 메모리는 랜덤 액세스 메모리(random access memory, RAM)일 수 있으며, 외부 캐시로 사용된다. 예를 들어, 제한은 아니지만 정적 랜덤 액세스 메모리(static RAM, SRAM), 동적 랜덤 액세스 메모리(dynamic random access memory, DRAM), 동기식 동적 랜덤 액세스 메모리(synchronous DRAM, SDRAM), 이중 데이터 속도 동기식 동적 랜덤 액세스 메모리(double data rate SDRAM, DDR SDRAM), 향상된 동기식 동적 랜덤 액세스 메모리(enhanced SDRAM, ESDRAM), 동기화 링크 동적 랜덤 액세스 메모리(synchlink DRAM, SLDRAM) 및 직접 rambus

임의 액세스 메모리(direct rambus RAM, DR RAM)와 같은 다양한 형태의 RAM을 사용할 수 있다.

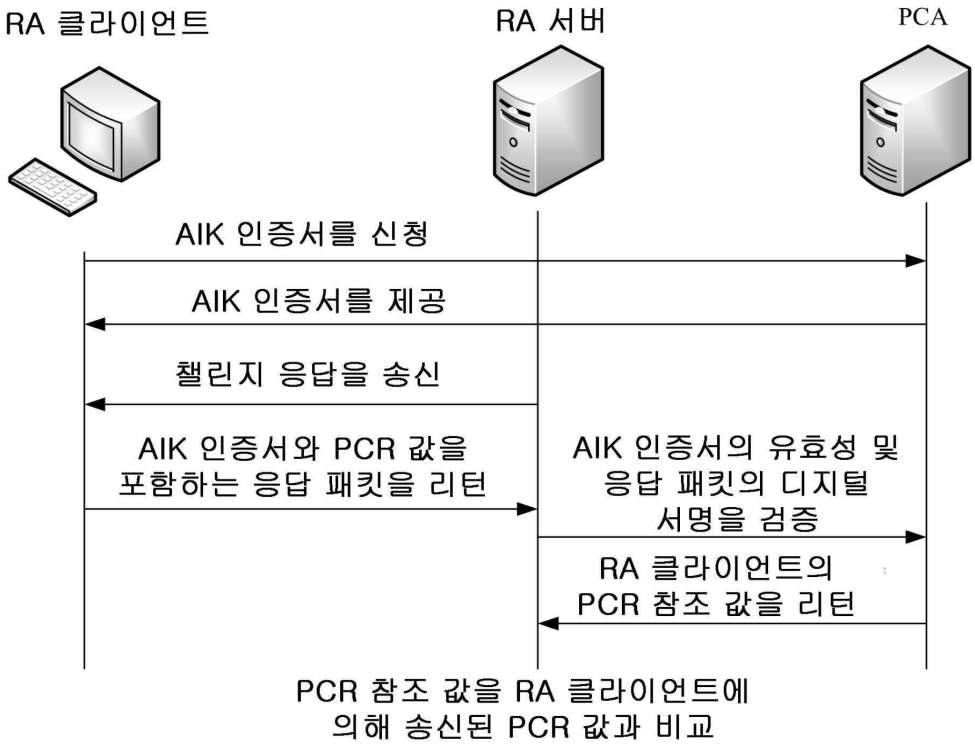
[0248] 본 출원은 컴퓨터 프로그램을 제공한다. 컴퓨터 프로그램이 컴퓨터에 의해 실행될 때, 프로세서 또는 컴퓨터는 전술한 방법 실시 예에서 대응하는 단계 및/또는 절차를 수행할 수 있다.

[0249] 전술한 실시 예의 전부 또는 일부는 소프트웨어, 하드웨어, 펌웨어, 또는 이들의 임의의 조합을 사용하여 구현될 수 있다. 소프트웨어가 실시 예를 구현하는 데 사용될 때, 실시 예의 전부 또는 일부는 컴퓨터 프로그램 제품의 형태로 구현될 수 있다. 컴퓨터 프로그램 제품은 하나 이상의 컴퓨터 명령을 포함한다. 컴퓨터 프로그램 명령이 로드되어 컴퓨터 상에서 실행될 때 본 출원에 따른 절차 또는 기능의 전부 또는 일부가 생성된다. 컴퓨터는 범용 컴퓨터, 전용 컴퓨터, 컴퓨터 네트워크 또는 다른 프로그램 가능한 장치일 수 있다. 컴퓨터 명령은 컴퓨터가 판독 가능 저장 매체에 저장되거나, 컴퓨터가 판독 가능 저장 매체로부터 다른 컴퓨터가 판독 가능 저장 매체로 전송될 수 있다. 예를 들어, 컴퓨터 명령은 웹 사이트, 컴퓨터, 서버 또는 데이터 센터에서 유선(예: 동축 케이블, 광섬유 또는 디지털 가입자 라인) 또는 무선(예: 적외선, 라디오 또는 마이크로파) 모드에서 다른 웹 사이트, 컴퓨터, 서버 또는 데이터 센터로 전송될 수 있다. 컴퓨터가 판독 가능 저장 매체는 컴퓨터에 의해 액세스 가능한 임의의 사용 가능한 매체, 또는 하나 이상의 사용 가능한 매체를 통합하는 서버 또는 데이터 센터와 같은 데이터 저장 디바이스일 수 있다. 사용 가능한 매체는 자기 매체(예를 들어, 플로피 디스크, 하드 디스크 또는 자기 테이프), 광학 매체(예를 들어, DVD) 또는 반도체 매체(예: 솔리드 스테이트 드라이브(solid state drive))일 수 있다.

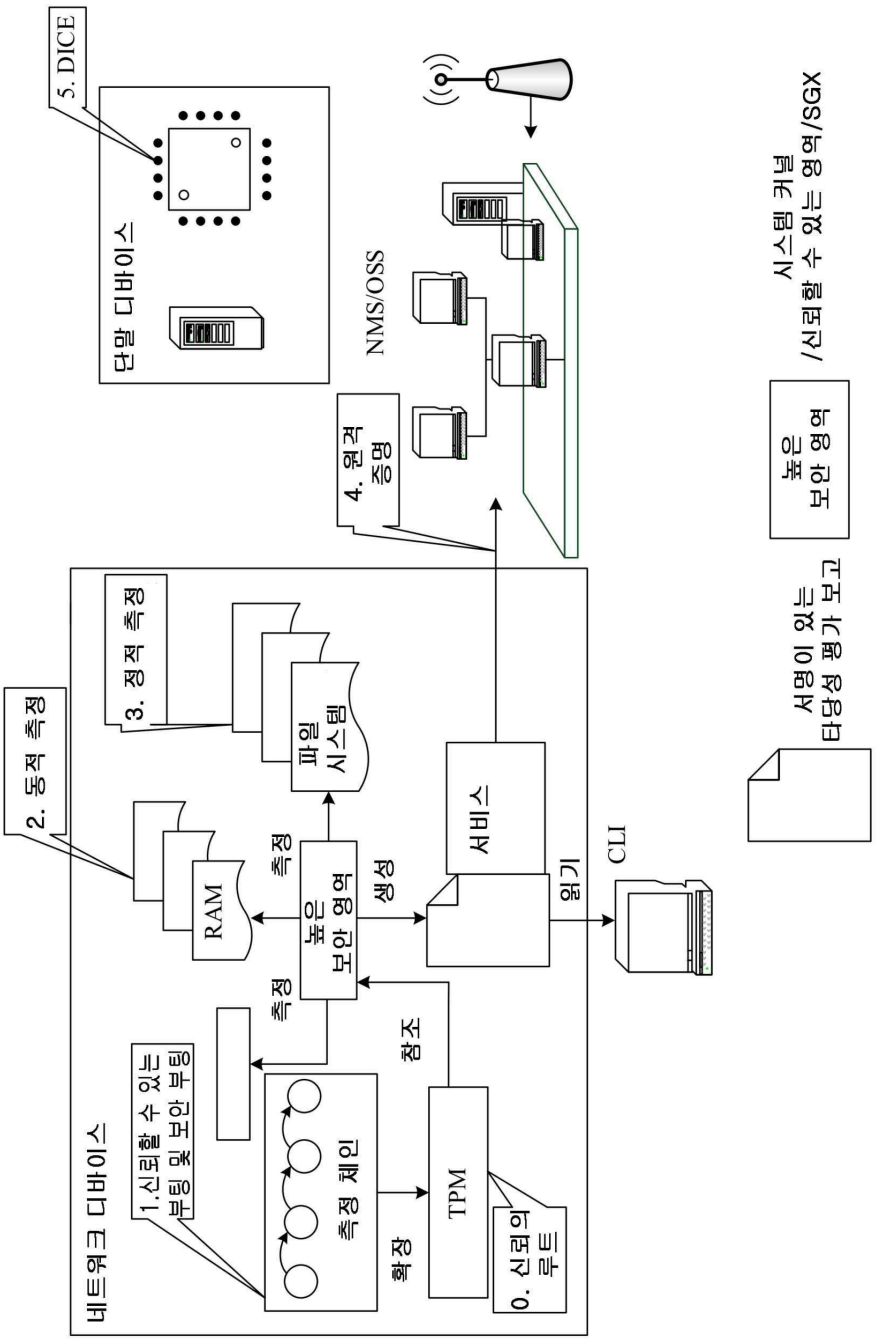
[0250] 전술한 설명은 단지 본 출원의 실시 예일뿐, 본 출원을 제한하려는 의도는 아니다. 본 출원의 원칙을 벗어나지 않고 수정, 동등한 대체 또는 개선이 이루어진 경우에는 본 출원의 보호 범위 내에 있어야 한다.

도면

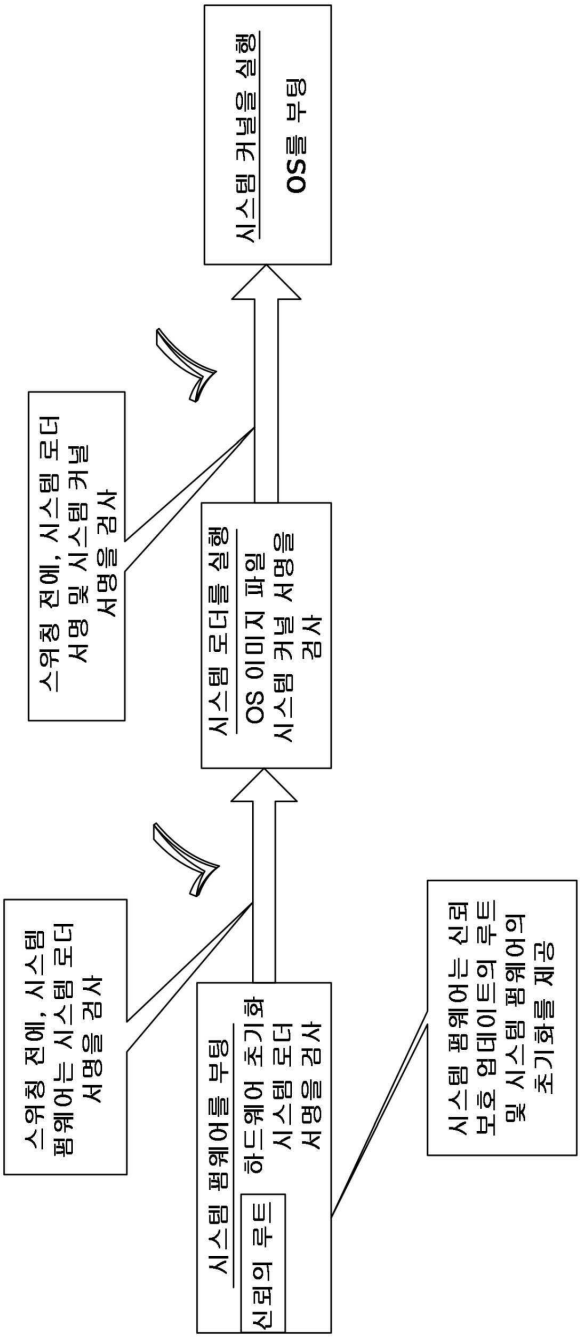
도면1a



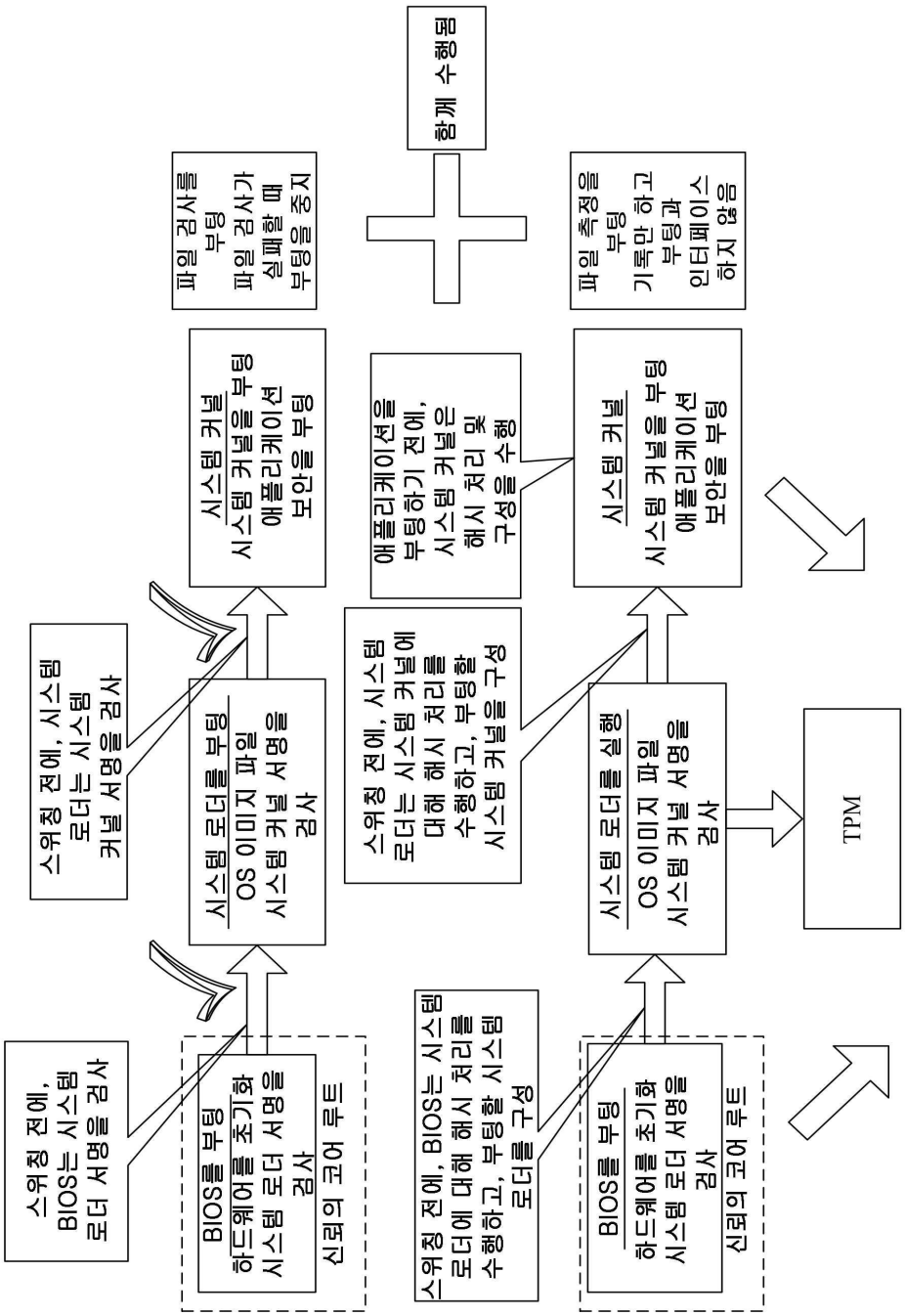
도면1b


5. DICE
단말 디바이스
NMS/OSS
4. 원격 증명
시스템 커널
/신뢰할 수 있는 영역/SGX
높은 보안 영역
서명이 있는
타당성 평가 보고
네트워크 디바이스
2. 동적 측정
3. 정적 측정
RAM
파일 시스템
측정
높은 보안 영역
생성
서비스
읽기
CLI
측정
참조
1.신뢰할 수 있는 부팅 및 보안 부팅
측정 체인
확장
TPM
0. 신뢰의 루트

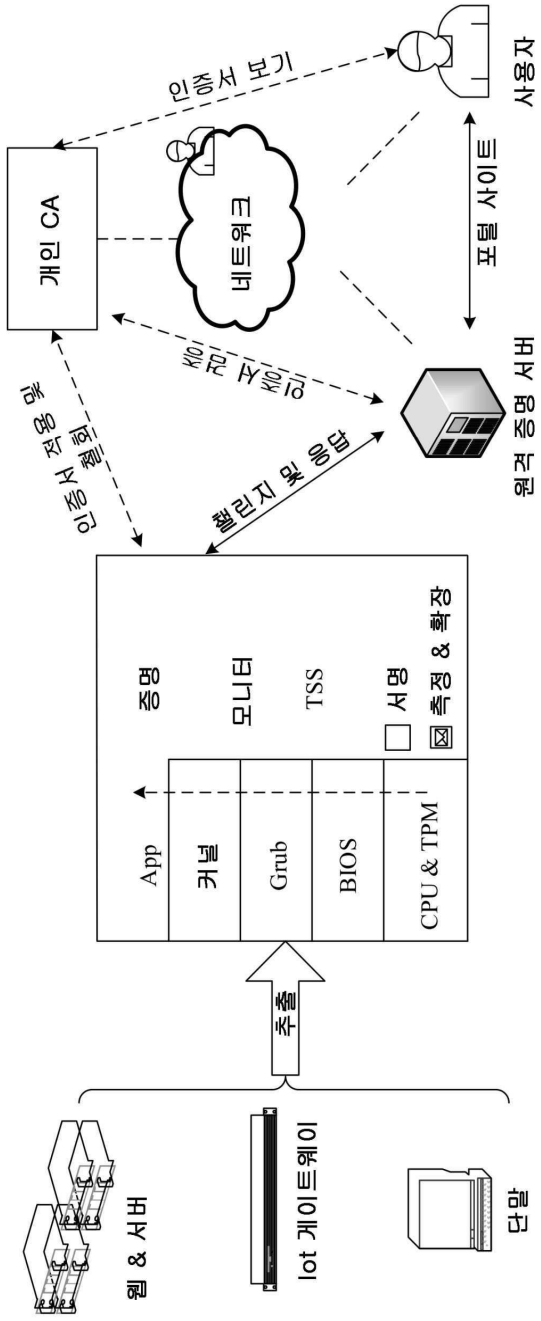
도면2


시스템 펌웨어를 부팅
신뢰의 루트
하드웨어 초기화
시스템 로더
서명을 검사
스위칭 전에, 시스템
펌웨어는 시스템 로더
서명을 검사
시스템 펌웨어는 신뢰
보호 업데이트의 루트
및 시스템 펌웨어의
초기화를 제공
시스템 로더를 실행
OS 이미지 파일
시스템 커널 서명을
검사
스위칭 전에, 시스템 로더
서명 및 시스템 커널
서명을 검사
시스템 커널을 실행
OS를 부팅

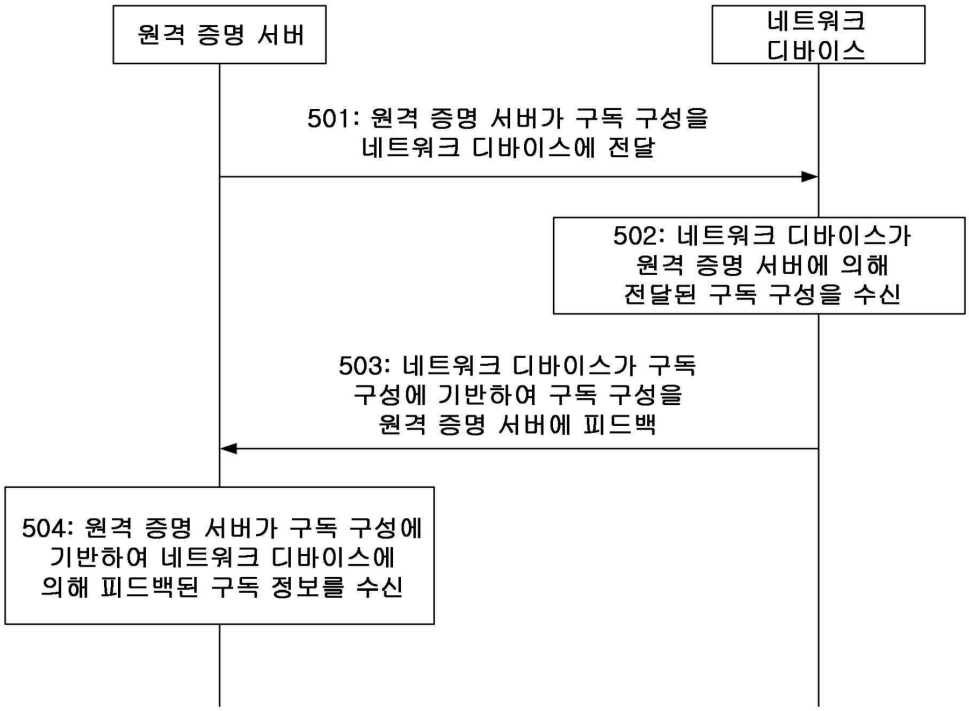
도면3


스위칭 전에,
BIOS는 시스템
로더 서명을 검사
BIOS를 부팅
하드웨어를 초기화
시스템 로더 서명을
검사
신뢰의 코어 루트
스위칭 전에, 시스템
로더는 시스템
커널 서명을 검사
시스템 로더를 부팅
OS 이미지 파일
시스템 커널 서명을
검사
시스템 커널
시스템 커널을 부팅
애플리케이션
보안을 부팅
파일 검사를
부팅
파일 검사가
실패할 때
부팅을 중지
함께 수행됨
스위칭 전에, BIOS는 시스템
로더에 대해 해시 처리를
수행하고, 부팅할 시스템
로더를 구성
스위칭 전에, 시스템
로더는 시스템 커널에
대해 해시 처리를
수행하고, 부팅할
시스템 커널을 구성
애플리케이션을
부팅하기 전에,
시스템 커널은
해시 처리 및
구성을 수행
BIOS를 부팅
하드웨어를 초기화
시스템 로더 서명을
검사
신뢰의 코어 루트
시스템 로더를 실행
OS 이미지 파일
시스템 커널 서명을
검사
시스템 커널
시스템 커널을 부팅
애플리케이션
보안을 부팅
파일 측정을
부팅
기록만 하고
부팅과
인터페이스
하지 않음
TPM

도면4


사용자
인증서 보기
개인 CA
네트워크
포털 사이트
원격 증명 서버
인증서 검증
챌린지 및 응답
인증서 생성 및 전송
증명
모니터
TSS
서명
측정 & 확장
App
커널
Grub
BIOS
CPU & TPM
추출
웹 & 서버
Iot 게이트웨이
단말

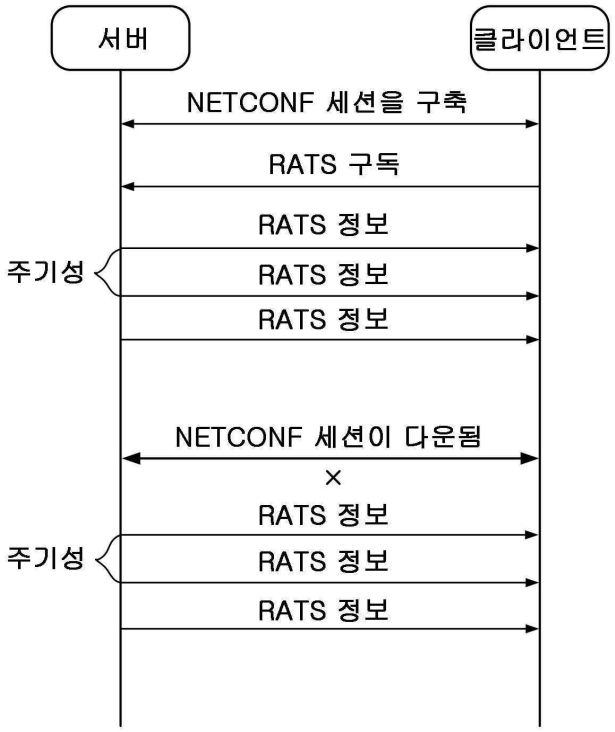
도면5


원격 증명 서버
네트워크 디바이스
501: 원격 증명 서버가 구독 구성을 네트워크 디바이스에 전달
502: 네트워크 디바이스가 원격 증명 서버에 의해 전달된 구독 구성을 수신
503: 네트워크 디바이스가 구독 구성에 기반하여 구독 구성을 원격 증명 서버에 피드백
504: 원격 증명 서버가 구독 구성에 기반하여 네트워크 디바이스에 의해 피드백된 구독 정보를 수신

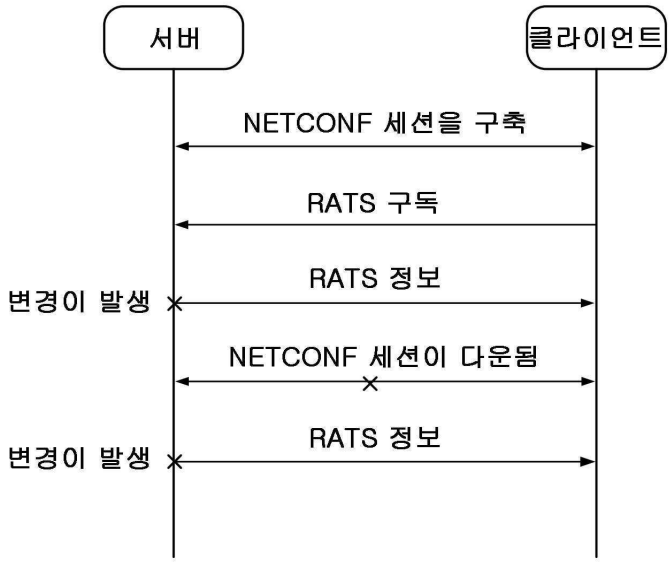
도면6

```
module: ietf-rats-sub-push
  augment /sn:streams/sn:stream:
    +--ro type?   identityref
  augment /sn:subscriptions:
    +--rw events
       +--rw event* [name]
          +--rw name    string
          +--rw type?   identityref
  augment /sn:subscriptions/sn:subscription:
    +--rw (rats-type)?
       +--:(tpm2-attestation-challenge)
       |  +--rw tpm2-attestation-challenge
       |     +--rw pcr-list* [id]
       |     |  +--rw id     string
       |     |  +--rw pcr
       |     |     +--rw pcr-indices*                  uint8
       |     |     +--rw (algo-registry-type)
       |     |        +--:(tcg)
       |     |        |  +--rw tcg-hash-algo-id?       uint16
       |     |        +--:(ietf)
       |     |           +--rw ietf-ni-hash-algo-id?   uint8
       |     +--rw nonce-value?                  binary
       |     +--rw (signature-identifier-type)
       |     |  +--:(TPM_ALG_ID)
       |     |  |  +--rw TPM_ALG_ID-value?       uint16
       |     |  +--:(COSE_Algorithm)
       |     |     +--rw COSE_Algorithm-value?   int32
       |     +--rw (key-identifier)?
       |        +--:(public-key)
       |        |  +--rw pub-key-id?             binary
       |        +--:(uuid)
       |           +--rw uuid-value?             binary
       +--:(log-retrieval)
          +--rw log-retrieval
             +--rw log-selector* [node-name]
             |  +--rw node-name                string
             |  +--ro node-physical-index?     int32
             |  +--rw (index-type)?
             |     +--:(last-entry)
             |     |  +--rw last-entry-value?   binary
             |     +--:(index)
             |     |  +--rw index-number?       uint64
             |     +--:(timestamp)
             |        +--rw timestamp?          yang:date-and-time
             +--rw log-type?             identityref
             +--rw pcr-list* [id]
             |  +--rw id     string
             |  +--rw pcr
             |     +--rw pcr-indices*                  uint8
             |     +--rw (algo-registry-type)
             |        +--:(tcg)
             |        |  +--rw tcg-hash-algo-id?       uint16
             |        +--:(ietf)
             |           +--rw ietf-ni-hash-algo-id?   uint8
             +--rw log-entry-quantity?   uint16
  augment /sn:subscriptions/sn:subscription/yp:update-trigger/yp:periodic:
    +--rw sub-rats-event*   -> /sn:subscriptions/rsp:events/event/name
  augment /sn:subscriptions/sn:subscription/yp:update-trigger/yp:on-change:
    +--rw sub-rats-event*   -> /sn:subscriptions/rsp:events/event/name
  augment /sn:establish-subscription/sn:input:
```

도면7


서버
클라이언트
NETCONF 세션을 구축
RATS 구독
RATS 정보
주기성
RATS 정보
RATS 정보
NETCONF 세션이 다운됨
×
RATS 정보
주기성
RATS 정보
RATS 정보

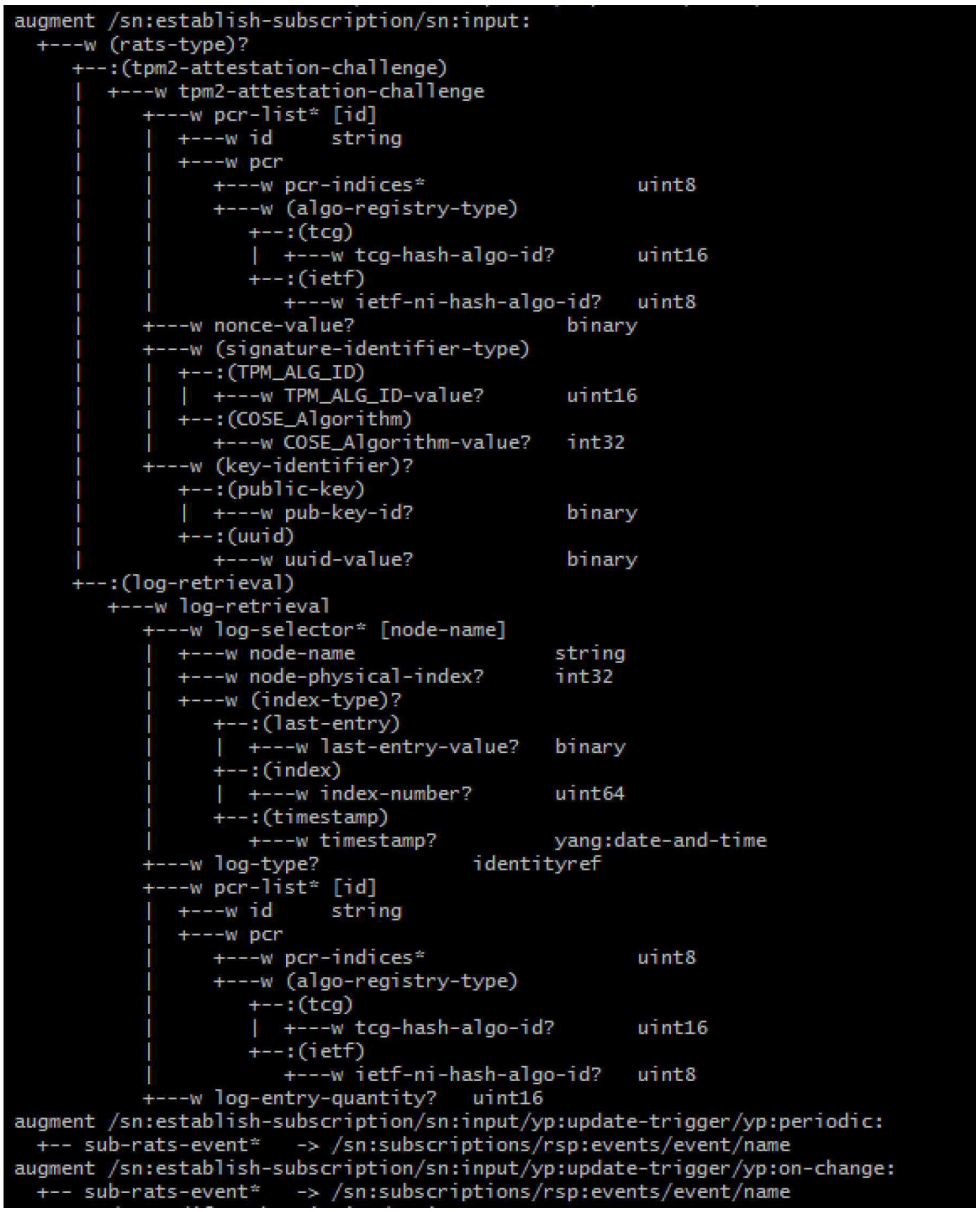
도면8


서버
클라이언트
NETCONF 세션을 구축
RATS 구독
RATS 정보
변경이 발생
NETCONF 세션이 다운됨
×
RATS 정보
변경이 발생

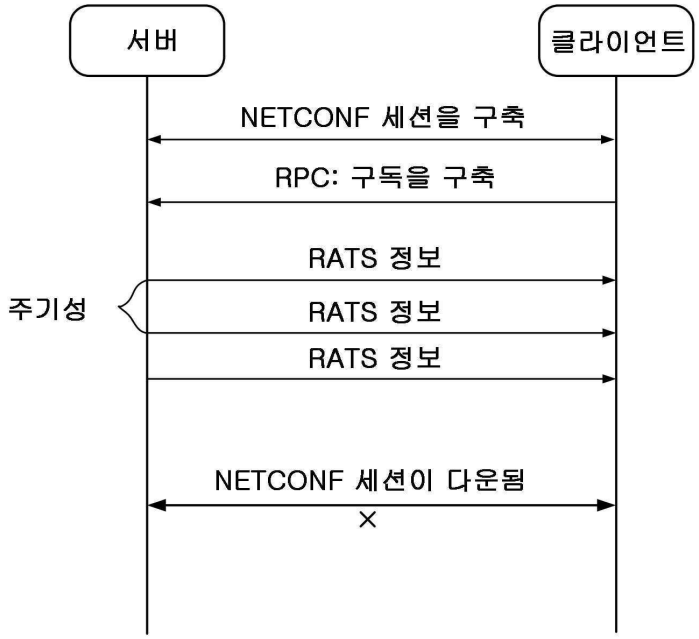
도면9

```
notifications:
  +---n tpm2-attestation-challenge
  |  +--ro tpm2-attestation-response* [tpm_name]
  |     +--ro tpm_name                string
  |     +--ro tpm-physical-index?     int32
  |     +--ro up-time?                uint32
  |     +--ro node-name?              string
  |     +--ro node-physical-index?    int32
  |     +--ro tpms-attest
  |     |  +--ro pcrdigest?                    binary
  |     |  +--ro tpms-attest-result?           binary
  |     |  +--ro tpms-attest-result-length?    uint32
  |     +--ro tpmt-signature?         binary
  +---n log-retrieval
     +--ro system-event-logs
        +--ro node-data* [node-name]
           +--ro node-name               string
           +--ro node-physical-index?    int32
           +--ro up-time?                uint32
           +--ro tpm-updated* [tpm_name]
           |  +--ro tpm_name               string
           |  +--ro tpm-physical-index?    int32
           +--ro log-result
              +--ro (log-type)?
                 +--:(bios)
                 |  +--ro bios-event-logs
                 |     +--ro bios-event-entry* [event-number]
                 |        +--ro event-number    string
                 +--:(ima)
                    +--ro ima-event-logs
                       +--ro ima-event-entry* [event-number]
                          +--ro event-number    string
```

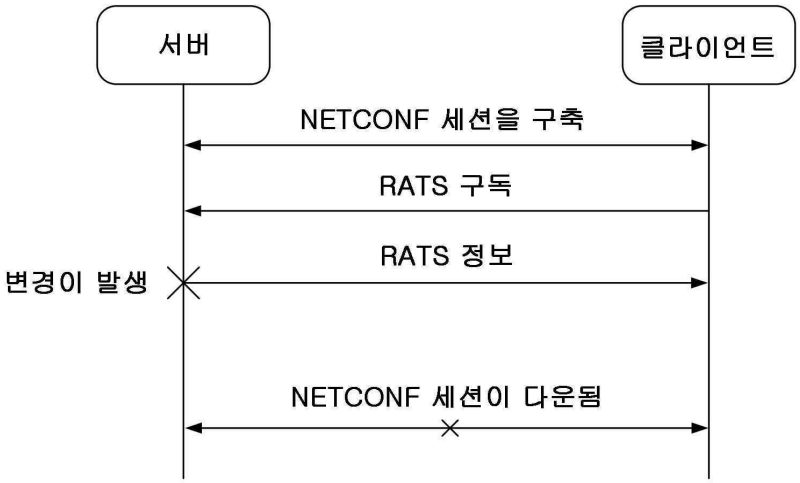
도면10


augment /sn:establish-subscription/sn:input:
+---w (rats-type)?
+--:(tpm2-attestation-challenge)
| +---w tpm2-attestation-challenge
| +---w pcr-list* [id]
| | +---w id string
| | +---w pcr
| | +---w pcr-indices* uint8
| | +---w (algo-registry-type)
| | +--:(tcg)
| | | +---w tcg-hash-algo-id? uint16
| | +--:(ietf)
| | +---w ietf-ni-hash-algo-id? uint8
| +---w nonce-value? binary
| +---w (signature-identifier-type)
| | +--:(TPM_ALG_ID)
| | | +---w TPM_ALG_ID-value? uint16
| | +--:(COSE_Algorithm)
| | +---w COSE_Algorithm-value? int32
| +---w (key-identifier)?
| +--:(public-key)
| | +---w pub-key-id? binary
| +--:(uuid)
| +---w uuid-value? binary
+--:(log-retrieval)
+---w log-retrieval
+---w log-selector* [node-name]
| +---w node-name string
| +---w node-physical-index? int32
| +---w (index-type)?
| +--:(last-entry)
| | +---w last-entry-value? binary
| +--:(index)
| | +---w index-number? uint64
| +--:(timestamp)
| +---w timestamp? yang:date-and-time
+---w log-type? identityref
+---w pcr-list* [id]
| +---w id string
| +---w pcr
| +---w pcr-indices* uint8
| +---w (algo-registry-type)
| +--:(tcg)
| | +---w tcg-hash-algo-id? uint16
| +--:(ietf)
| +---w ietf-ni-hash-algo-id? uint8
+---w log-entry-quantity? uint16
augment /sn:establish-subscription/sn:input/yp:update-trigger/yp:periodic:
+-- sub-rats-event* -> /sn:subscriptions/rsp:events/event/name
augment /sn:establish-subscription/sn:input/yp:update-trigger/yp:on-change:
+-- sub-rats-event* -> /sn:subscriptions/rsp:events/event/name

도면11


서버
클라이언트
NETCONF 세션을 구축
RPC: 구독을 구축
RATS 정보
주기성
RATS 정보
RATS 정보
NETCONF 세션이 다운됨

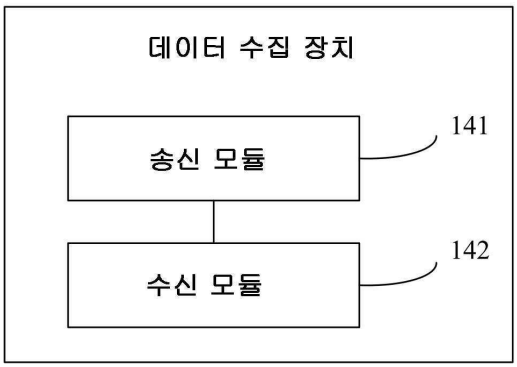
도면12


서버
클라이언트
NETCONF 세션을 구축
RATS 구독
RATS 정보
변경이 발생
NETCONF 세션이 다운됨

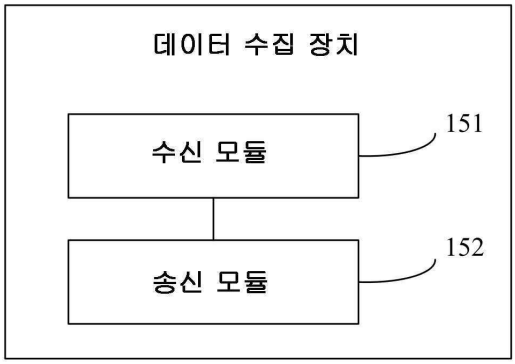
도면13

```
notifications:
  +---n tpm2-attestation-challenge
  |  +--ro tpm2-attestation-response* [tpm_name]
  |     +--ro tpm_name                string
  |     +--ro tpm-physical-index?     int32
  |     +--ro up-time?                uint32
  |     +--ro node-name?              string
  |     +--ro node-physical-index?    int32
  |     +--ro tpms-attest
  |     |  +--ro pcrdigest?                    binary
  |     |  +--ro tpms-attest-result?           binary
  |     |  +--ro tpms-attest-result-length?    uint32
  |     +--ro tpmt-signature?         binary
  +---n log-retrieval
     +--ro system-event-logs
        +--ro node-data* [node-name]
           +--ro node-name               string
           +--ro node-physical-index?    int32
           +--ro up-time?                uint32
           +--ro tpm-updated* [tpm_name]
           |  +--ro tpm_name                string
           |  +--ro tpm-physical-index?     int32
           +--ro log-result
              +--ro (log-type)?
                 +--:(bios)
                 |  +--ro bios-event-logs
                 |     +--ro bios-event-entry* [event-number]
                 |        +--ro event-number    string
                 +--:(ima)
                    +--ro ima-event-logs
                       +--ro ima-event-entry* [event-number]
                          +--ro event-number    string
```

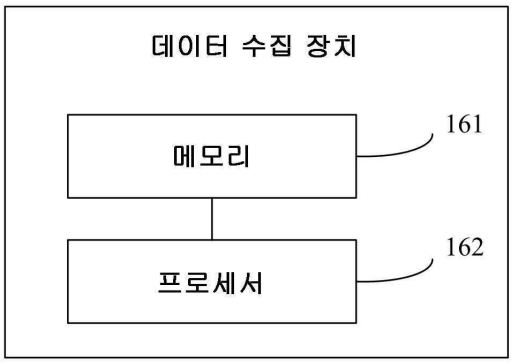
도면14



도면15



도면16



도면17