(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년06월04일
(11) 등록번호 10-1153073
(24) 등록일자 2012년05월29일

(51) 국제특허분류(Int. Cl.)
G06F 15/00 (2006.01)
(21) 출원번호 10-2005-0079871
(22) 출원일자 2005년08월30일
심사청구일자 2010년08월25일
(65) 공개번호 10-2006-0050799
(43) 공개일자 2006년05월19일
(30) 우선권주장
10/953,020 2004년09월29일 미국(US)
(56) 선행기술조사문헌
US20030149749 A1
US20030079216 A1

(73) 특허권자
마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
왓슨, 콜린
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내
홀라데이, 마틴 엘.
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내
카르키, 무케쉬
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내
(74) 대리인
제일특허법인

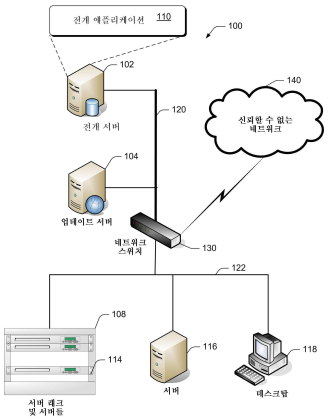
전체 청구항 수 : 총 26 항 심사관 : 복진요

(54) 발명의 명칭 **외부 악성 공격으로부터 네트워크를 통한 소프트웨어전개의 격리**

(57) 요 약

여기에서는, 베어 컴퓨터(예를 들어, 서버)가 악성 네트워크-기반 공격에 영향받지 않도록, 네트워크를 통한 베어 컴퓨터로의 소프트웨어(예를 들어, 오퍼레이팅 시스템) 및 업데이트들의 안전한 전개를 위한 구현이 설명된다.

대 표 도 - 도1



특허청구의 범위

청구항 1

프로세서에 의해 실행되는 경우,

전개 서버에 의해, 네트워크 상의 베어 컴퓨터를 신뢰할 수 없는 네트워크로부터 격리시키기 위한 명령어들을 네트워크 스위치에 송신하는 단계;

상기 명령어들에 응답하여, 상기 네트워크 스위치에 의해, 상기 네트워크 상의 베어 컴퓨터를 상기 신뢰할 수 없는 네트워크로부터 격리시키는 단계 - 상기 신뢰할 수 없는 네트워크는 상기 베어 컴퓨터가 상기 신뢰할 수 없는 네트워크로부터 격리되지 않을 때, 상기 베어 컴퓨터로 악성 공격을 통신할 수 있음-;

상기 베어 컴퓨터를 격리시키기 위한 명령어들을 송신한 후에, 상기 전개 서버에 의해, 소프트웨어 제품을 상기 네트워크를 통하여 상기 베어 컴퓨터에 전개하는 단계;

상기 베어 컴퓨터가 여전히 격리된 상태에서 상기 네트워크를 통하여 상기 소프트웨어 제품에 대한 업데이트를 수신하도록, 상기 전개 서버에 의해, 상기 네트워크를 통하여 상기 베어 컴퓨터에 명령하는 단계;

상기 베어 컴퓨터가 여전히 격리된 상태에서 상기 소프트웨어 제품에 대한 업데이트를 적용하도록, 상기 전개 서버에 의해, 상기 네트워크를 통하여 상기 베어 컴퓨터에 명령하는 단계;

상기 베어 컴퓨터로부터 상기 소프트웨어 제품이 업데이트되었다는 통신을 상기 전개 서버에서 수신하는 단계; 및

그 후 상기 베어 컴퓨터의 격리를 중단하도록, 상기 전개 서버에 의해, 상기 네트워크 스위치에 명령하는 단계

를 포함하는 동작들을 수행하는 프로세서-실행 가능 명령어들을 가진 하나 이상의 프로세서-판독 가능 기록 매체.

청구항 2

제1항에 있어서,

상기 소프트웨어 제품은 오퍼레이팅 시스템, 응용 프로그램, 또는 소프트웨어 서비스를 포함하는 그룹으로부터 선택되는 하나 이상의 프로세서-판독 가능 기록 매체.

청구항 3

제1항에 있어서,

상기 베어 컴퓨터가 상기 업데이트를 수신한 후, 상기 베어 컴퓨터가 상기 신뢰할 수 없는 네트워크를 통해 통신할 수 있도록, 상기 격리를 제거하는 단계를 더 포함하는 하나 이상의 프로세서-판독 가능 기록 매체.

청구항 4

제1항에 있어서,

상기 베어 컴퓨터는 베어 서버를 포함하는 하나 이상의 프로세서-판독 가능 기록 매체.

청구항 5

제1항에 있어서,

상기 베어 컴퓨터는 가상 베어 컴퓨터를 포함하고 상기 네트워크는 적어도 일부가 가상 네트워크인 하나 이상의 프로세서-판독 가능 기록 매체.

청구항 6

제1항에 있어서,

상기 격리시키는 단계는 물리적 네트워크 스위치에 의해 수행되는 하나 이상의 프로세서-판독 가능 기록

매체.

청구항 7

제1항에 있어서,

상기 격리시키는 단계는 가상 네트워크 스위치에 의해 수행되고 상기 네트워크는 적어도 일부가 가상 네트워크인 하나 이상의 프로세서-판독 가능 기록 매체.

청구항 8

제1항에 있어서,

상기 신뢰할 수 없는 네트워크는 하나 이상의 신뢰할 수 없는 네트워크-결합형 장치들을 포함하는 하나 이상의 프로세서-판독 가능 기록 매체.

청구항 9

제1항에 있어서,

상기 소프트웨어 제품은 이미지로서 수신되는 하나 이상의 프로세서-판독 가능 기록 매체.

청구항 10

제1항에 있어서,

상기 격리시키는 단계, 상기 전개하는 단계 및 상기 명령하는 단계의 동작들은 사용자 상호 작용 없이 수행되는 하나 이상의 프로세서-판독 가능 기록 매체.

청구항 11

제1항에 따른 하나 이상의 프로세서-판독 가능 기록 매체를 포함하는 컴퓨터.

청구항 12

전개 서버에 의해, 네트워크 상의 베어 컴퓨터를 신뢰할 수 없는 네트워크로부터 격리시키기 위한 명령어들을 네트워크 스위치에 송신하는 단계;

상기 명령어들에 응답하여, 상기 네트워크 스위치에 의해, 상기 네트워크 상의 베어 컴퓨터를 상기 신뢰할 수 없는 네트워크로부터 격리시키는 단계 - 상기 신뢰할 수 없는 네트워크는 상기 베어 컴퓨터가 상기 신뢰할 수 없는 네트워크로부터 격리되지 않을 때, 상기 베어 컴퓨터로 악성 공격을 통신할 수 있음-;

상기 베어 컴퓨터를 격리시키기 위한 명령어들을 송신한 후에, 상기 전개 서버에 의해, 소프트웨어 제품을 상기 네트워크를 통하여 상기 베어 컴퓨터에 전개하는 단계;

상기 베어 컴퓨터가 여전히 격리된 상태에서 상기 네트워크를 통하여 상기 소프트웨어 제품에 대한 업데이트를 수신하도록, 상기 전개 서버에 의해, 상기 네트워크를 통하여 상기 베어 컴퓨터에 명령하는 단계;

상기 베어 컴퓨터가 여전히 격리된 상태에서 상기 소프트웨어 제품에 대한 업데이트를 적용하도록, 상기 전개 서버에 의해, 상기 네트워크를 통하여 상기 베어 컴퓨터에 명령하는 단계;

상기 베어 컴퓨터로부터 상기 소프트웨어 제품이 업데이트되었다는 통신을 상기 전개 서버에서 수신하는 단계; 및

그 후 상기 베어 컴퓨터의 격리를 중단하도록, 상기 전개 서버에 의해, 상기 네트워크 스위치에 명령하는 단계

를 포함하는 방법.

청구항 13

제12항에 있어서, 상기 소프트웨어 제품은 오퍼레이팅 시스템, 응용 프로그램, 또는 소프트웨어 서비스를 포함하는 그룹으로부터 선택되는 방법.

청구항 14

제12항에 있어서,

상기 베어 컴퓨터가 상기 업데이트를 수신한 후, 상기 베어 컴퓨터가 상기 신뢰할 수 없는 네트워크를 통해 통신할 수 있도록, 상기 격리를 제거하는 단계를 더 포함하는 방법.

청구항 15

제12항에 있어서,

상기 베어 컴퓨터는 베어 서버를 포함하는 방법.

청구항 16

제12항에 있어서,

상기 베어 컴퓨터는 가상 베어 컴퓨터를 포함하고 상기 네트워크는 적어도 일부가 가상 네트워크인 방법.

청구항 17

제12항에 있어서,

상기 신뢰할 수 없는 네트워크는 하나 이상의 신뢰할 수 없는 네트워크-결합형 장치들을 포함하는 방법.

청구항 18

제12항에 있어서,

상기 소프트웨어 제품은 이미지로서 수신되는 방법.

청구항 19

제12항에 있어서,

상기 격리시키는 단계, 상기 전개하는 단계 및 상기 명령하는 단계의 동작들은 사용자 상호작용 없이 수행되는 방법.

청구항 20

전개 수단;

업데이트 수단; 및

격리 수단을 포함하는 시스템으로서,

상기 전개 수단은,

네트워크 상의 베어 컴퓨터를 신뢰할 수 없는 네트워크로부터 격리시키기 위한 명령어들을 상기 격리 수단에 송신하고;

상기 베어 컴퓨터를 격리시키기 위한 명령어들을 송신한 후 상기 네트워크를 통해 상기 베어 컴퓨터에 소프트웨어 제품을 전개하고;

상기 베어 컴퓨터가 여전히 격리된 상태에서 상기 네트워크를 통하여 상기 업데이트 수단으로부터 상기 소프트웨어 제품에 대한 업데이트를 수신하도록 상기 네트워크를 통하여 상기 베어 컴퓨터에 명령하고;

상기 베어 컴퓨터가 여전히 격리된 상태에서 상기 소프트웨어 제품에 대한 업데이트를 적용하도록 상기 네트워크를 통하여 상기 베어 컴퓨터에 명령하고;

상기 베어 컴퓨터로부터 상기 소프트웨어 제품이 업데이트되었다는 통신을 수신하며;

그 후 상기 베어 컴퓨터의 격리를 중단하도록 상기 격리 수단에 명령하도록 구성되며,

상기 격리 수단은,

상기 전개 수단으로부터 상기 명령들을 수신하는 것에 응답하여, 상기 신뢰할 수 없는 네트워크로부터 상기

네트워크 상의 상기 베어 컴퓨터를 격리시키도록 구성되며, 상기 신뢰할 수 없는 네트워크는, 상기 베어 컴퓨터가 상기 신뢰할 수 없는 네트워크로부터 격리되지 않았을 때, 상기 베어 컴퓨터로 악성 공격을 통신할 수 있는 시스템.

청구항 21

제20항에 있어서, 상기 소프트웨어 제품은 오퍼레이팅 시스템, 응용 프로그램 또는 소프트웨어 서비스를 포함하는 그룹으로부터 선택되는 시스템.

청구항 22

제20항에 있어서,

상기 베어 컴퓨터가 상기 신뢰할 수 없는 네트워크를 통해 통신할 수 있도록, 상기 베어 컴퓨터가 상기 업데이트를 수신한 후, 상기 격리를 제거하기 위한 격리-해제(un-isolation) 수단을 더 포함하는 시스템.

청구항 23

제20항에 있어서,

상기 베어 컴퓨터는 베어 서버를 포함하는 시스템.

청구항 24

제20항에 있어서,

상기 베어 컴퓨터는 가상 베어 컴퓨터를 구비하고 상기 네트워크는, 적어도 일부가, 가상 네트워크인 시스템.

청구항 25

제20항에 있어서,

상기 신뢰할 수 없는 네트워크는 하나 이상의 신뢰할 수 없는 네트워크-결합형 장치들을 포함하는 시스템.

청구항 26

제20항에 있어서,

상기 소프트웨어 제품은 이미지로서 전개되는 시스템.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[0016] **기술 분야**

[0017] 본 발명은 일반적으로 네트워크의 컴퓨터들에 대한 오퍼레이팅 시스템들 및 여타 소프트웨어에 관한 것이다.

[0018] **배경**

[0019] 오퍼레이팅 시스템을 갖추지 않은 서버인 "베어 서버(bare server)"를 네트워크에 새로이 추가하는 가장 빠르고 간단한 방법들 중 하나는 베어 서버를 네트워크에 플러그하고 전개 서버(deployment server)를 사용해 오퍼레이팅 시스템의 디스크 "이미지" 또는 셋업 파일들을 베어 서버에 전개하는 것이다. 베어 서버는 이 이미지를 자신의 하드 디스크 드라이브 또는 등가의 저장 공간에 저장한 다음 리부팅한다. 베어 서버가 리부팅하고 나면, 베어 서버는 새롭게 전개된 오퍼레이팅 시스템으로 실행될 것이다.

[0020] 오퍼레이팅 시스템들에 대한 패치들이 빈번하게 전개된다. 베어 서버들이 처음으로 부팅될 때 이들이 최신 패치들을 포함하도록, 베어 서버들에 전개할 새로운 이미지들 또는 셋업 파일들을 재생하는 것은 시간 소모적이다.

[0021] 따라서, 다른 경우라면 "스테일(stale)인" 오퍼레이팅 시스템을 갖는 새롭게 전개된 서버들은 제1 의 사후전개(post-deployment) 리부팅시에 즉시 업데이트되는 것이 바람직하다. 제1 의 사후전개 리부팅 후, 일반적으로 (인터넷과 같은) 공중 네트워크로부터 또는 인트라넷 서버로부터, 네트워크를 통해 필요한 업데이트들을 획득하는 것이 보통이다.

[0022] 그러나, 네트워크(특히 인터넷과 같은 신뢰할 수 없는 네트워크)는, 바이러스, 트로이 목마, 또는 여타 네트워크-기반 공격과 같은, 악성 공격에 감염되기 쉽다. 새롭게 전개된 "스테일" 서버가 그것을 이와 같은 공격들로부터 보호해 줄 필요한 업데이트들을 획득할 수 있기도 전에 네트워크를 통해 (바이러스 또는 트로이 목마와 같은) 악성 코드에 의해 "공격"받는 것은 드문 일이 아니다.

[0023] 많은 악성 프로그램들이 구식 오퍼레이팅 시스템을 실행 중인 서버를 손상시키는데 1초도 걸리지 않으므로, 이것은 실제적인 가능성이다. 예를 들어, MS 블라스터(Blaster) 바이러스는 수 십분의 1초 내에 스테일 및 비보호 서버를 손상시킬 수 있다.

[0024] 이러한 문제에 부분적으로 대처하기 위해, 베어 서버는, 네트워크에 접속되지 않은 상태로, 수동으로 양쪽 서버들에 케이블을 플러그하는 것에 의한 것과 같이, 전개 서버에 접속될 수 있다. 이 케이블을 통해, 전개 서버는 오퍼레이팅 시스템 이미지를 베어 서버에 전개할 수 있다. 그 다음, 서버는 오퍼레이팅 시스템으로써 리부팅될 수 있다. 이것이 수행되고 나면, 대개는 CD들로써 손수, 오퍼레이팅 시스템을 최적 안전화하기 위한 업데이트들이 설치될 수 있다. 업데이트되고 나면, 서버는 네트워크에 플러그될 수 있다.

[0025] 이러한 부분적 솔루션이 공격에 대한 서버의 취약성을 감소시킬 수는 있지만, 이것은 시간 소모적이다. 정보기술 전문가는 베어 서버들을 전개 서버에 직접적으로 접속하고, 이미지들을 전개하며, 업데이트들을 설치하고, 전개 서버로부터 서버들을 분리한 다음, 서버들을 네트워크에 접속시키는데 많은 시간을 소모할 수 있다. 여러 가지 점에서, 이것은 자동 소프트웨어 전개의 목적을 무효화한다.

[0026] 또한, 이러한 문제에 부분적으로 대처하기 위해, 서버를 네트워크에 접속시키기 전에, 대개는 다수의 CD들로써, 오퍼레이팅 시스템 및 업데이트들이 베어 서버에 수동으로 설치될 수 있다. 그러나, 오퍼레이팅 시스템 및 업데이트들을 수동으로 설치하는 것 또한 시간 소모적이며 지루한 일로서, 각각의 서버에 대해 수 시간이 걸릴 수 있다. 이것 또한 자동 소프트웨어 전개의 목적을 무효화한다.

[0027] 따라서, 베어 서버가 악성 네트워크-기반 공격에 감염되지 않도록, 네트워크를 통해, 오퍼레이팅 시스템 및 업데이트들을 베어 서버에 안전하게 전개하기 위한 방법이 필요하다.

발명이 이루고자 하는 기술적 과제

[0028] 여기에서는, 베어 컴퓨터(예를 들어, 서버)가 악성 네트워크-기반 공격에 감염되지 않도록, 네트워크를 통한 베어 컴퓨터로의 소프트웨어(예를 들어, 오퍼레이팅 시스템) 및 업데이트들의 안전한 전개를 위한 구현이 설명된다.

발명의 구성 및 작용

[0029] 유사한 요소들 및 사양들을 언급하기 위해, 도면들 전체에 걸쳐 동일한 번호들을 사용한다.

[0030] **상세한 설명**

[0031] 다음 설명은, 베어 서버가 악성 네트워크-기반 공격에 감염되지 않도록, 네트워크를 통한 베어 서버로의 오퍼레이팅 시스템 및 업데이트들의 안전한 전개를 위한 기술들을 서술한다. 이 기술들은, 프로그램 모듈들, 범용- 및 특수-목적 컴퓨팅 시스템들, 네트워크 서버들과 장비, 전용 전자 장치들과 하드웨어를 포함하는(그러나 이에 한정되지는 않음), 다수의 방법들로, 그리고 하나 이상의 컴퓨터 네트워크들의 일부로서 구현될 수 있다.

[0032] 이러한 기술들의 예시적 구현을, 새롭게 전개된 취약한 소프트웨어의 예시적 아이솔레이터 또는 단순히 "예시적 아이솔레이터(exemplary isolator)"라고 할 수 있다.

[0033] **예시적 동작 환경**

[0034] 자동 소프트웨어 전개 서비스를 통해, 데이터 센터들은 네트워크를 통해 기준 "이미지들"을 전송하는 것에 기초해 소프트웨어(예를 들어, 오퍼레이팅 시스템들)를 빠르게 전개하는 능력을 갖추게 된다. 빠른 시스템 전개들이 데이터 센터 조작자들에게는 상당한 이점이지만, 새로운 서버를 빠르게 전개함으로써 그것이 즉시 공

격받게 되는 것은 심각한 단점이다.

[0035] 도 1은, 소프트웨어가 자동적으로 전개되는 동작 환경(100;또는 "아키텍처")을 개시한다. 이것은 또한, 예시적 아이솔레이터가 동작할 수 있는 예시적 동작 환경이기도 하다.

[0036] 이러한 예시적 동작 환경(100)은 중심이 되는 안전한 네트워크(120)를 통해 결합되어 있는 몇 개의 컴포넌트들을 갖춘 것으로 도시되어 있다. 그러한 네트워크-결합된 컴포넌트들은 전개 서버(102), 업데이트 서버(104), 및 네트워크 스위치(130)를 포함한다. 이러한 동작 환경(100)은 또한, 전환 가능하며 안전할 수도 있는 네트워크(122)를 통해 결합되어 있는 몇 개의 컴포넌트들을 갖춘 것으로 도시되어 있으며, 그러한 컴포넌트들은 래크-탑재형 베어 서버(114;래크(108)에 탑재되어 있는 하나 또는 수 개의 서버들), 베어 서버(116), 및 베어 데스크탑 컴퓨터(118)이다. 더 나아가, 이러한 환경은 네트워크 스위치(130)를 통해 2개의 다른 네트워크들(120 및 122)에 전환 가능하게 결합되어 있는 신뢰할 수 없는 네트워크(140;예를 들어, 인터넷)도 갖춘 것으로 도시되어 있다.

[0037] 전개 서버(102)는 소프트웨어 전개 동작을 수행한다. 전개 서버(102)는 후술되는 프로세스들 중 하나 이상을 수행할 수 있는 컴퓨터-판독 가능 매체들을 구비한다. 이러한 매체들은, 예를 들어, 전개 애플리케이션(110)을 구비할 수 있다.

[0038] 도 1에 도시된 바와 같이, 예시적 아이솔레이터는 전개 서버(102)의 전개 애플리케이션(110)에 의해 구현된다. 이것은 또한, 적어도 부분적으로는, 네트워크 스위치(130)에 의해 구현된다.

[0039] 또한, 업데이트 서버(104)는, 구식 오퍼레이팅 시스템의 동작, 예를 들어, 그것의 보안 기능들을 향상시키기 위해 구식 오퍼레이팅 시스템을 업데이트하기 위한 것과 같이, 소프트웨어 패치들, 수정들(fixes) 등을 전개할 수 있는 컴퓨터-판독 가능 매체들을 구비한다. 이러한 업데이트들은, 다음에서 부연되는 바와 같이, 베어 서버에 의해 나중에 수신되는 다양한 악성 코드에 대한 저항성을 향상시킬 수 있다.

[0040] 또한, 래크(108)의 베어 서버(114), 베어 독립형 서버(116), 및 베어 데스크탑(118)의 예시적인 3개의 베어 컴퓨터들이 도시되어 있다. 베어 컴퓨터들 각각은 베어 컴퓨터로 하여금, 예를 들면, 전개 애플리케이션(110)으로부터, 기본 명령들을 요청하고, 수신하며, 따를 수 있게 하기에 충분한 소프트웨어 또는 하드웨어 애플리케이션을 가진다.

[0041] 동작 환경(100)은 네트워크(120 및 122)를 통해 통신한다. 이러한 네트워크들은, 네트워크-기반 공격들과 같은, 악성 통신에 감염될 수 있는 통신 네트워크들이다. 특히, 이와 같은 악성 통신은 (네트워크를 통해 악성 코드를 송신할 수 있는 손상된 컴퓨터와의 인터넷 또는 인트라넷과 같은) 신뢰할 수 없는 네트워크(140)로부터 유래할 수 있다.

[0042] 이러한 네트워크들(120, 122, 및 140)은 네트워크 스위치(130)를 통해 전환 가능하도록 다같이 결합된다. 이 스위치는 (전개 서버(102)와 같은) 서버로부터, 어떤 네트워크들(및 실제로는 그러한 네트워크들상의 어떤 장치들)이 서로 통신할 수 있는지를 선택하기 위한 명령들을 수신할 수 있다.

[0043] 예를 들어, 네트워크 스위치(130)는 신뢰할 수 없는 네트워크(140)로부터 네트워크(122)를 격리시키도록 지시될 수 있다. 그런 식으로, 네트워크(122)의 장치들은 네트워크(120)의 장치들과는 통신할 수 있지만, 신뢰할 수 없는 네트워크(140)의 장치들과는 통신할 수 없으며 그 반대도 마찬가지이다.

[0044] **방법적 구현**

[0045] 도 2a 및 도 2b는 새롭게 전개된 취약한 소프트웨어에 대한 예시적 아이솔레이터의 방법적 구현을 도시한다. 이러한 방법적 구현은 소프트웨어, 하드웨어, 또는 그들의 조합으로 수행될 수 있다. 용이한 이해를 위해, 방법 단계들이 별도의 단계들로서 서술되지만, 이처럼 별도로 서술된 단계들이 그들의 수행에 있어서 반드시 순서 의존적인 것으로 해석되어서는 안된다.

[0046] 도 2a 및 도 2b의 방법은 (예를 들면, 전개 애플리케이션(110)을 갖춘) 전개 서버(102), 네트워크 스위치(130), 및 베어 서버(예를 들어, 서버(116))에 의해 수행되는 개개 연산들 또는 동작들을 표현하는 일련의 블록들로서 도시되어 있다.

[0047] 업데이트 이전 및 업데이트 동안, 비보호인 상태에서, 새롭게 전개된 베어 서버를 효과적으로 격리시키기 위하여, 전개 서버(102)에 의해 수행되는 그러한 예시적 연산들 및 동작들은 "전개 서버/전개 애플리케이션"이라는 제목 아래에 도시되어 있다.

[0048] 전개된 이미지를 안전하게 수신하여 오퍼레이팅 시스템을 안전하게 업데이트하기 위하여, 베어 서버(예를 들어, 서버(116))에 의해 수행되는 그러한 예시적 연산들 및 동작들은 "베어 서버"라는 제목 아래에 도시되어 있다.

[0049] 업데이트 이전 및 업데이트 동안, 비보호인 상태에서, 새롭게 전개된 베어 서버를 선택적으로 격리시키기 위하여(그렇게 하라는 명령들에 응답하여), 네트워크 스위치(130)에 의해 수행되는 그러한 예시적 연산들 및 동작들은 "네트워크 스위치"라는 제목 아래에 도시되어 있다.

[0050] 도 2a의 202에서는, 베어 컴퓨터가 네트워크(122)에 접속된다. 독립형 서버(116) 또는 데스크탑(118)과 같은, 다른 베어 컴퓨터들이 네트워크에 대신 접속될 수도 있지만, 예를 들어, 베어 서버(114)가 래크(108)를 통해 네트워크에 플러그된다.

[0051] 204에서는, 베어 서버가, 오퍼레이팅 시스템을 요청하며, 네트워크들(예를 들어, 스위치(130)를 통한 네트워크(122 및 120))을 통해 통신한다. 오퍼레이팅 시스템이 없는 상태라면, 베어 서버가 통상적으로, 아직까지는 네트워크의 악성 코드에 취약하지 않다.

[0052] 206에서는, 전개 서버(102)가 오퍼레이팅 시스템을 위한 요청을 수신한다. 208에서, 전개 서버(102)는, (신뢰할 수 없는 네트워크(140)와 같은) 불안전한 네트워크들로부터 베어 서버를 효과적으로 격리시키는 명령들을 네트워크 스위치로 송신한다.

[0053] 도 2a의 210에서, 네트워크 스위치(140)는 명령을 수신하고, 212에서, (신뢰할 수 없는 네트워크(140)와 같은) 불안전한 네트워크들로부터 베어 서버를 효과적으로 격리시킨다.

[0054] 스위치가 이것을 실현할 수 있는 여러 방법들이 존재한다. 완력적인 일 방법은 신뢰할 수 없는 네트워크(140)로부터의 모든 수신 트래픽을 차단하는 것이다. 다른 접근 방법은 네트워크(122)와 신뢰할 수 없는 네트워크(140)간의 통신을 방지하는 것이 될 것이다. 좀더 복잡한 접근 방법은 스위치를 통과한 트래픽의 모니터링 및 신뢰할 수 없는 네트워크(140)로부터/신뢰할 수 없는 네트워크(140)로 전개중인 베어 서버로부터/서버로의 트래픽 차단을 수반한다.

[0055] 신뢰할 수 있는 네트워크를 통해, 새롭게 전개된 베어 서버는 전개 서버, 업데이트 서버 및, DHCP(Dynamic Host Configuration Protocol) 및 DNS(Domain Name System) 서버들과 같은, 가능한 여타 네트워크 인프라스트럭처 서비스들과 통신할 수 있다.

[0056] 214에서, 전개 서버는, 전개 애플리케이션(110)을 통해, 오퍼레이팅 시스템 이미지를 갖는 이미지를 안전하게 베어 서버로 전개한다.

[0057] 도 2a의 216에서, 베어 서버는 네트워크를 통해 이미지를 안전하게 수신하여 그것을 메모리에 저장한다. 218에서, 베어 서버는, 베어 서버가 이미지를 수신했다는 것을 전달한다. 220에서, 전개 서버는 베어 서버로부터, 베어 서버가 이미지를 수신했다는 것을 나타내는 통지를 수신한다. 222에서, 전개 서버는, 전개 애플리케이션을 통해, 이미지를 부팅할 것을 베어 서버에 지시한다.

[0058] 도 2a의 224에서, 베어 서버는 재부팅함으로써, 오퍼레이팅 시스템 및 그것의 구성 설정들로 이미지를 실행시킨다. 부팅 프로세스가 끝난 후에는, 오퍼레이팅 시스템을 가지고 있으므로, 더 이상 베어가 아닌, 베어 서버가 실행되어 동작한다.

[0059] 네트워크 스위치(130)가 신뢰할 수 없는 네트워크들로부터 그것을 효과적으로 격리시킨다는 것을 제외하면, 구식 오퍼레이팅 시스템을 갖춘 베어 서버는 네트워크를 통해 송신되는 악성 혼신 및 통신에 취약할 수 있을 것이다. 베어 서버의 어떤 것도 악성 공격으로부터 그것을 보호하지 못한다. 대신, 외부 컴포넌트들(즉, 전개 서버 및 스위치)의 동작들은, 그것이 여전히 취약할 수 있는 동안에도 그것을 격리시켜왔다.

[0060] 이 방법은 이제 도 2b로 이어진다.

[0061] 도 2b의 226에서, 베어 서버(114)는 오퍼레이팅 시스템이 실행 중이며 그리고/또는 부팅이 성공적이었다는 것을 전개 서버에 통지한다.

[0062] 228에서, 전개 서버(102)는 이 정보를 수신한다. 230에서, 전개 서버는, 전개 애플리케이션(110)을 통해, 업데이트들을 수신하고 그리고/또는 설치할 것을 베어 서버에 지시한다.

[0063] 일 실시예에서, 전개 서버는 업데이트 서버(104)와 통신을 개시할 것을 베어 서버에 지시한다. 다른 실시예에서, 전개 서버는 베어 서버의 오퍼레이팅 시스템에 업데이트들을 송신하고 이러한 업데이트들을 추가할 것

을 지시한다.

[0064] 도 2b의 232에서, 베어 서버는 업데이트들을 수신하라는 명령을 수신한다. 234에서, 베어 서버는 업데이트들을 수신하기 위한 통신을 개시한다. 예를 들어, 베어 서버는 업데이트 서버(104)로부터의 통신을 요청한다.

[0065] 236에서, 베어 서버는 업데이트들을 수신하고 오퍼레이팅 시스템에 적용한다. 이러한 업데이트들은, 예를 들어, 블록 234에서 요청된 업데이트 서버로부터 또는 전개 서버로부터 직접적으로 네트워크를 통해 수신될 수 있다.

[0066] 도 2b의 238에서, 베어 서버는, 그 오퍼레이팅 시스템을 업데이트했다는 것을 통지한다. 240에서, 전개 서버는 이러한 통지를 수신한다.

[0067] 242에서, 전개 서버는 베어 서버의 격리를 중단할 것을 네트워크 스위치에 지시한다. 다시 말해, 베어 서버는, 그것이 완전히 업데이트되어 더 이상 악성 공격들에 취약하지 않을 것이므로, 인터넷과 같은, 불안전한 네트워크를 통한 자유로운 지배가 허용되어야 한다.

[0068] 도 2b의 244에서, 네트워크 스위치(140)는 명령을 수신한다. 246에서, 스위치는 베어 서버를 그것의 격리로부터 해제시킨다. 스위치는 이제 베어 서버와 (신뢰할 수 없는 네트워크(140)와 같은) 불안전한 네트워크들 간의 트래픽을 허용한다.

[0069] 여기에서, 전부는 아니라 할지라도, 전개 서버, 전개 애플리케이션, 및 네트워크 스위치의 동작들 대부분은 사용자 개입없이 자동적으로 수행될 수 있다.

[0070] 이것은 사용자로 하여금, 오퍼레이팅 시스템이 업데이트되기 전에 네트워크를 통하여 악성 코드에 베어 서버가 영향받게 하지 않으면서, 베어 서버 또는 다른 베어 컴퓨터를 네트워크에 접속할 수 있게 하며, 추가적 상호 작용 없이, 업데이트된 오퍼레이팅 시스템으로 베어 서버가 동작하게 한다.

[0071] **대안의 동작 환경**

[0072] 도 3은, 예시적 아이솔레이터가 동작할 수 있는 또 다른 예시적 동작 환경(300;또는 "아키텍처")을 개시한다. 이러한 동작 환경(300)은 네트워크(320)를 통해 결합되어 있는 몇 개의 컴포넌트들을 갖춘 것으로 도시되어 있다.

[0073] 그러한 네트워크-결합형 컴포넌트들은 전개 서버(302) 및 업데이트 서버(304)를 포함한다. 또한, 네트워크(320)에는 신뢰할 수 없는 네트워크(140;예를 들어, 인터넷)가 첨부되어 있다. 또한, 도시되지 않은 여타의 다수 네트워크-결합형 장치들이 존재할 수 있다.

[0074] "가상 서버"(350)는 네트워크(320)에 결합되어 있는 것으로 도 3에 도시되어 있는 다른 컴포넌트이다. 가상 서버는 가상 머신들의 하나 이상의 인스턴스들을 호스팅하는 서버이다. 이러한 가상 서버는 "가상 LAN"(virtual local area network;360)에 대한 홈이다. 이러한 가상 LAN은 물리적으로 존재하는 것이 아니라, 가상 서버(350)에 의해 시뮬레이션된다. 명료화를 위해, 실제의 물리적 네트워크(320)를 여기에서는 "외부" 네트워크라고 하고, 가상 LAN(360)을 여기에서는 "내부" 네트워크라고 한다.

[0075] 다른 방법으로, 전개 서버(302) 및 업데이트 서버(304)는 가상 서버(350)내의 가상 머신들 및 내부 네트워크(360)내의 신뢰되는 가상 네트워크의 일부일 수 있다.

[0076] 이러한 내부 네트워크(360)는 (도 1에 도시된 스위치(130)의 시뮬레이션 버전인) 가상 네트워크 스위치(462) 및 다수의 가상 머신들(예를 들어, 366 및 368)을 가진다. 더 나아가, 내부 네트워크(360) 또한, 내부 네트워크(360)의 나머지에 가상적으로 전환 가능하게 결합되어 있는 신뢰할 수 없는 가상 네트워크(364)를 갖춘 것으로 도시되어 있다.

[0077] 신뢰할 수 없는 가상 네트워크(364)는, 가상 스위치(362)가 신뢰할 수 없는 가상 네트워크(364)로의 액세스를 가상적으로 스위치 온/오프할 수 있다는 것을 보여주기 위한 목적을 위해 내부 네트워크(360)와 관련되어 있는 것으로 도 3에 도시되어 있다. 그러나, 도 3에 도시되어 있는 신뢰할 수 없는 가상 네트워크(364)는 신뢰할 수 없는 실제 네트워크(340)의 표현일 뿐이다. 스위치는 신뢰할 수 없는 실제 네트워크(340)로의/신뢰할 수 없는 실제 네트워크(340)로부터의 액세스를 가상적으로 전환(또는 필터링)할 수 있다.

[0078] 이러한 다른 실시예에서, 목표 베어 서버는 (서버(368)와 같은) 가상 서버이다. 하나의 물리적 네트워크 및 물리적 베어 서버의 맥락에서 상술된 연산들 및 동작은 도 3에 나타낸 실시예에서의 내부 네트워크(360)와 관련된 동작과 직접적으로 유사하다.

[0079] **예시적인 컴퓨팅 시스템 및 환경**

[0080] 도 4는, 여기에서 설명되는 예시적 아이솔레이터가 (완전하게 또는 부분적으로) 구현될 수 있는 적당한 컴퓨팅 환경(400)의 일례를 도시한다. 컴퓨팅 환경(400)은 여기에서 설명되는 컴퓨터 및 네트워크 아키텍처들에 이용될 수 있다.

[0081] 예시적 컴퓨팅 환경(400)은 컴퓨팅 환경의 일례일 뿐이며 컴퓨터 및 네트워크 아키텍처들의 사용 또는 기능 범위에 대해 어떤 제한을 두려는 것은 아니다. 컴퓨팅 환경(400)이 예시적 컴퓨팅 환경(400)에 도시된 컴포넌트들 중의 어느 하나 또는 컴포넌트들의 조합과 관련하여 어떠한 의존성이나 요구 사항을 갖는 것으로 해석되어서도 안된다.

[0082] 예시적 아이솔레이터는 다수의 여타 범용 또는 특수 목적 컴퓨팅 시스템 환경들 또는 구성들로써 구현될 수 있다. 사용에 적당할 수 있는 주지의 컴퓨팅 시스템들, 환경들, 및/또는 구성들로는 퍼스널 컴퓨터들, 서버 컴퓨터들, 씬 클라이언트들(thin clients), 씩 클라이언트들(thick clients), 핸드-헬드 또는 랩탑 장치들, 멀티-프로세서 시스템들, 마이크로프로세서-기반 시스템들, 셋톱 박스들, PDA들(personal digital assistants), 어플라이언스들, 특수-목적 전자 장치들(예를 들어, DVD 플레이어), 프로그램 가능한 상용 전자 장치들, 네트워크 PC들, 미니컴퓨터들, 메인프레임 컴퓨터들, 상기 시스템들 또는 장치들 중 어느 하나를 포함하는 분산 컴퓨팅 환경들 등을 들 수 있지만, 이에 한정되는 것은 아니다.

[0083] 예시적 아이솔레이터는, 컴퓨터에 의해 실행되는, 프로그램 모듈들과 같은, 프로세서-실행 가능 명령어들의 일반적인 맥락에서 설명될 수 있다. 일반적으로, 프로그램 모듈들은 특정한 태스크들을 수행하거나 특정한 추상적 데이터형들을 구현하는 루틴들, 프로그램들, 오브젝트들, 컴포넌트들, 데이터 구조들 등을 포함한다. 예시적 아이솔레이터는, 태스크들이 통신 네트워크를 통해 링크되어 있는 원격 프로세싱 장치들에 의해 수행되는 분산 컴퓨팅 환경들에서도 실시될 수도 있다. 분산 컴퓨팅 환경에서, 프로그램 모듈들은 메모리 저장 장치들을 포함하는 로컬 및 원격 컴퓨터 저장 매체들 모두에 배치될 수 있다.

[0084] 컴퓨팅 환경(400)은 컴퓨터(402) 형태의 범용 컴퓨팅 장치를 포함한다. 컴퓨터(402)의 컴포넌트들은 하나 이상의 프로세서들 또는 프로세싱 유닛들(404), 시스템 메모리(406), 및 프로세서(404)를 포함하여, 다양한 시스템 컴포넌트들을 시스템 메모리(406)에 결합시키는 시스템 버스(408)를 들 수 있지만, 이에 한정되는 것은 아니다.

[0085] 시스템 버스(408)는, 메모리 버스 또는 메모리 컨트롤러, 주변 장치 버스, 가속 그래픽 포트, 및 다양한 버스 아키텍처들 중 어느 하나를 사용하는 프로세서 또는 로컬 버스를 포함하여, 몇가지 유형의 버스 구조들 중 하나 이상을 표현한다. 일례로써, 이와 같은 아키텍처들로는 CardBus, PCMCIA(Personal Computer Memory Card International Association), AGP(Accelerated Graphics Port), SCSI(Small Computer System Interface), USB(Universal Serial Bus), IEEE 1394, VESA(Video Electronics Standards Association) 로컬 버스, 및 (Mezzanine 버스라고도 하는) PCI(peripheral Component Interconnects) 버스를 들 수 있다.

[0086] 컴퓨터(402)는 통상적으로 다양한 프로세서-판독 가능 매체들을 포함한다. 이러한 매체들은 컴퓨터(402)에 의해 액세스될 수 있는 이용 가능한 임의의 매체일 수 있으며, 휘발성 및 비휘발성 매체들, 분리형 및 비분리형 매체들 모두를 포함한다.

[0087] 시스템 메모리(406)는 RAM(random access memory;410)과 같은 휘발성 메모리 및/또는 ROM(read only memory;412)과 같은 비휘발성 메모리 형태의 프로세서-판독 가능 매체들을 포함한다. 스타트-업(start-up) 동안과 같은 때에, 컴퓨터(402)내의 요소들 사이에서 정보 전달을 돕는 기본적 루틴들을 포함하는 BIOS(basic input/output system;414)는 ROM(412)에 저장된다. RAM(410)은 통상적으로, 프로세싱 유닛(404)으로 즉시 액세스될 수 있거나 그리고/또는 프로세싱 유닛(404)에 의해 현재 연산되는 프로그램 모듈들 및/또는 데이터를 포함한다.

[0088] 컴퓨터(402)는 다른 분리형/비분리형, 휘발성/비휘발성 컴퓨터 저장 매체들도 포함할 수 있다. 일례로써, 도 4는 비분리형, 비휘발성 자기 매체들(도시하지 않음)로부터 판독하고 그에 기입하기 위한 하드 디스크 드라이브(416), 분리형, 비휘발성 자기 디스크(420;예를 들어, "플로피 디스크")로부터 판독하고 그에 기입하기 위한 자기 디스크 드라이브(418) 및, CD-ROM, DVD-ROM, 또는 다른 광학 매체들과 같은, 분리형, 비휘발성 광학 디스크(424)로부터 판독하고 그리고/또는 그에 기입하기 위한 광학 디스크 드라이브(422)를 도시한다. 하드 디스크 드라이브(416), 자기 디스크 드라이브(418), 및 광학 디스크 드라이브(422)는 하나 이상의 데이터 미디어 인터페이스들(425)에 의해 시스템 버스(408)에 각각 접속된다. 다른 방법으로, 하드 디스크 드라이브

(416), 자기 디스크 드라이브(418), 및 광학 디스크 드라이브(422)는 하나 이상의 인터페이스(도시하지 않음)들에 의해 시스템 버스(408)에 접속될 수도 있다.

[0089] 디스크 드라이브들 및 그들과 관련된 프로세서-판독 가능 매체들은 컴퓨터(402)에 컴퓨터 판독 가능 명령어들, 데이터 구조들, 프로그램 모듈들, 및 다른 데이터의 비휘발성 저장을 제공한다. 본 예는 하드 디스크(416), 분리형 자기 디스크(420), 및 분리형 광학 디스크(424)를 도시하지만, 컴퓨터에 의해 액세스될 수 있는 데이터를 저장할 수 있는, 자기 카세트들이나 다른 자기 저장 장치들, 플래시 메모리 카드들, CD-ROM, DVD(digital versatile disks)나 다른 광학 저장 장치, RAM, ROM, EEPROM(electrically erasable programmable read-only memory) 등과 같은, 프로세서-판독 가능 매체들의 다른 유형들이 예시적인 컴퓨팅 시스템 및 환경을 구현하는데 이용될 수도 있다는 것이 이해된다.

[0090] 예로써, 오퍼레이팅 시스템(426), 하나 이상의 애플리케이션 프로그램들(428), 다른 프로그램 모듈들(430), 및 프로그램 데이터(432)를 포함하여, 임의 갯수의 프로그램 모듈들이 하드 디스크(416), 자기 디스크(420), 광학 디스크(424), ROM(412), 및/또는 RAM(410)에 저장될 수 있다.

[0091] 사용자는 키보드(434) 및 포인팅 장치(436;예를 들어, "마우스")와 같은 입력 장치들을 통해 명령들 및 정보를 컴퓨터(402)에 입력할 수 있다. (구체적으로 나타내지 않은) 다른 입력 장치들(438)로는 마이크로폰, 조이스틱, 게임 패드, 위성 안테나, 직렬 포트, 스캐너 등을 들 수 있다. 이들 및 다른 입력 장치들은 시스템 버스(408)에 결합되어 있는 입/출력 인터페이스들(440)을 통해 프로세싱 유닛(404)에 접속되어 있지만, 병렬 포트, 게임 포트, 또는 USB(universal serial bus)와 같은, 다른 인터페이스 및 버스 구조들에 의해 접속될 수도 있다.

[0092] 모니터(442) 또는 다른 유형의 디스플레이 장치 또한, 비디오 어댑터(444)와 같은, 인터페이스를 통해 시스템 버스(408)에 접속될 수 있다. 모니터(442) 이외에, 다른 주변 출력 장치들로는, 스피커들(도시하지 않음) 및 프린터(446)와 같은, 컴포넌트들을 들 수 있는데, 이들은 입/출력 인터페이스들(440)을 통해 컴퓨터(402)에 접속될 수 있다.

[0093] 컴퓨터(402)는, 원격 컴퓨팅 장치(448)와 같은, 하나 이상의 원격 컴퓨터들로의 논리 접속들을 사용하는 네트워킹 환경에서 동작할 수도 있다. 일례로써, 원격 컴퓨팅 장치(448)는 퍼스널 컴퓨터, 포터블 컴퓨터, 서버, 라우터, 네트워크 컴퓨터, 피어 장치 또는 다른 공통 네트워크 노드, 전개 서버(102), 업데이트 서버(104) 등일 수 있다. 원격 컴퓨팅 장치(448)는, 컴퓨터(402)와 관련하여 여기에서 설명된 요소들 및 특징들 중 많은 것을 또는 그 전부를 포함할 수 있는 포터블 컴퓨터로서 도시되어 있다.

[0094] 컴퓨터(402)와 원격 컴퓨터(448) 간의 논리 접속들은 LAN(local area network;450) 및 일반적 WAN(general wide area network;452)으로서 묘사되어 있다. 이러한 네트워킹 환경들은 사무실들, 기업-범위의 컴퓨터 네트워크들, 인트라넷들, 및 인터넷에서 흔히 볼 수 있다. 이러한 네트워킹 환경들은 유선 또는 무선일 수 있다.

[0095] LAN 네트워킹 환경에서 구현될 경우, 컴퓨터(402)는 네트워크 인터페이스 또는 어댑터(454)를 통해 LAN(450)에 접속된다. WAN 네트워킹 환경에서 구현될 경우, 컴퓨터(402)는 통상적으로, 모뎀(456) 또는 WAN(452)을 통해 통신을 구축하기 위한 다른 수단을 포함한다. 컴퓨터(402) 내장형이거나 외장형일 수 있는 모뎀(456)은 입/출력 인터페이스들(440) 또는 여타의 적합한 메커니즘들을 통해 시스템 버스(408)에 겁속될 수 있다. 도시된 네트워크 접속들은 예시적인 것이며 컴퓨터들(402 및 448)간에 통신 링크(들)를 구축하는 다른 수단이 이용될 수도 있다는 것을 알 수 있을 것이다.

[0096] 컴퓨팅 환경(400)으로써 도시되어 있는 바와 같은, 네트워킹 환경에서, 컴퓨터(402)와 관련하여 도시된 프로그램 모듈들 또는 그 일부분들은 원격 메모리 저장 장치에 저장될 수도 있다. 예로써, 원격 애플리케이션 프로그램들(458)은 원격 컴퓨터(448)의 메모리 장치에 상주한다. 설명을 위해, 애플리케이션 프로그램들 및, 오퍼레이팅 시스템과 같은, 다른 실행 가능 프로그램 컴포넌트들이 여기에서는 이산 블록들로서 도시되어 있지만, 이러한 프로그램들 및 컴포넌트들이 다양한 시점에 컴퓨팅 장치(402)의 상이한 저장 컴포넌트들에 상주하며 컴퓨터의 데이터 프로세서(들)에 의해 실행된다는 것을 알 수 있을 것이다.

[0097] **프로세서-실행 가능 명령어들**

[0098] 예시적 아이솔레이터의 구현을, 하나 이상의 컴퓨터들 또는 다른 장치들에 의해 실행되는, 프로그램 모듈들과 같은, 프로세서-실행 가능 명령어들의 일반적인 맥락에서 설명할 수 있다. 일반적으로, 프로그램 모듈들은 특정한 태스크들을 수행하거나 특정한 추상적 데이터형들을 구현하는 루틴들, 프로그램들, 오브젝트들, 컴포

넌트들, 데이터 구조들 등을 포함한다. 통상적으로, 프로그램 모듈들의 기능은 다양한 실시예들에서의 필요에 따라 조합되거나 분산될 수 있다.

[0099] **예시적 동작 환경**

[0100] 도 4는 예시적 아이솔레이터가 구현될 수 있는 적합한 동작 환경(400)의 일례를 도시한다. 구체적으로, 여기에서 설명되는 예시적 아이솔레이터(들)는 임의의 프로그램 모듈들(428-430) 및/또는 도 4의 오퍼레이팅 시스템(426) 또는 그 일부에 의해 (전체적으로 또는 부분적으로) 구현될 수 있다.

[0101] 동작 환경은 적당한 동작 환경의 일례일 뿐이며 여기에서 설명되는 예시적 아이솔레이터(들)의 기능 범위 또는 사용에 대해 어떤 제한을 두려는 것은 아니다. 사용하기에 적합할 수 있는 주지의 다른 컴퓨팅 시스템들, 환경들, 및/또는 구성들로는 퍼스널 컴퓨터들(PC들), 서버 컴퓨터들, 핸드-헬드 또는 랩탑 장치들, 멀티-프로세서 시스템들, 마이크로프로세서-기반 시스템들, 프로그램 가능한 상용 전자 장치들, 무선 전화기들과 장비, 범용 또는 특수-목적 어플라이언스들, ASIC들(application-specific integrated circuits), 네트워크 PC들, 미니컴퓨터들, 메인프레임 컴퓨터들, 상기 시스템들 또는 장치들 중 어느 하나를 포함하는 분산 컴퓨팅 환경들 등을 들 수 있지만, 이에 한정되는 것은 아니다.

[0102] **프로세서-판독 가능 매체들**

[0103] 예시적 아이솔레이터의 구현은 소정 형태의 프로세서-판독 가능 매체들에 저장되거나 그를 통해 전송될 수 있다. 프로세서-판독 가능 매체들은, 컴퓨터에 의해 액세스될 수 있는 이용 가능한 임의의 매체들일 수 있다. 예로써, 프로세서-판독 가능 매체들은 "컴퓨터 저장 매체들" 및 "통신 매체들"을 구비할 수 있지만, 이에 한정되는 것은 아니다.

[0104] "컴퓨터 저장 매체들"은 컴퓨터 판독 가능 명령어들, 데이터 구조들, 프로그램 모듈들, 또는 다른 데이터와 같은 정보의 저장을 위해 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체들을 포함한다. 컴퓨터 저장 매체들은 RAM, ROM, EEPROM, 플래시 메모리 또는 다른 메모리 기술, CD-ROM, DVD(digital versatile disks) 또는 다른 광학 저장 장치, 자기 카세트들, 자기 테이프, 자기 디스크 저장 장치 또는 다른 자기 저장 장치들, 또는 소정 정보를 저장하는데 사용될 수 있으며 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체를 포함하지만, 이에 한정되는 것은 아니다.

[0105] "통신 매체들"은 통상적으로 프로세서-판독 가능 명령어들, 데이터 구조들, 프로그램 모듈들 또는, 반송파나 다른 전송 메커니즘과 같은, 변조 데이터 신호의 다른 데이터를 구현한다. 또한, 통신 매체들은 임의의 정보 전달 매체들을 포함한다.

[0106] **결론**

[0107] 하나 이상의 상술된 구현들이 구조적 특징들 및/또는 방법적 단계들에 특징적인 언어로 설명되었지만, 다른 구현들이, 설명된 구체적 특징들 또는 단계들 없이 실시될 수도 있다는 것이 이해되어야 한다. 오히려, 구체적 특징들 및 단계들은 하나 이상의 구현들에 대한 바람직한 형태로서 개시되어 있다.

발명의 효과

[0108] 따라서, 본 발명에 따르면, 베어 컴퓨터(예를 들어, 서버)가 악성 네트워크-기반 공격에 영향받지 않도록, 네트워크를 통한 베어 컴퓨터로의 소프트웨어(예를 들어, 오퍼레이팅 시스템) 및 업데이트들의 안전한 전개를 위한 구현이 제공된다.

도면의 간단한 설명

[0001] 도 1은 여기에서 설명되는 구현을 위한 예시적인 동작 환경이다. 예시적인 동작 환경은 예시적인 서버들, 악성 공격에 감염되기 쉬운 네트워크, 및 베어 컴퓨터들을 갖춘 것으로 도시되어 있다.

[0002] 도 2a 및 도 2b는 여기에서 설명되는 방법 구현을 나타내는 흐름도를 도시한다.

[0003] 도 3은 여기에서 설명되는 구현을 위한 예시적인 다른 동작 환경의 블록도이다.

[0004] 도 4는 여기에서 설명되는 하나 이상의 실시예를 (전체적으로 또는 부분적으로) 구현할 수 있는 컴퓨팅 동작 환경의 일례이다.

[0005] <도면의 주요 부분에 대한 부호의 설명>

[0006] 100 : 예시적 동작 환경

[0007] 102 : 전개 서버

[0008] 104 : 업데이트 서버

[0009] 108 : 서버 래크

[0010] 110 : 전개 애플리케이션

[0011] 114, 116 : 서버

[0012] 118 : 데스크탑

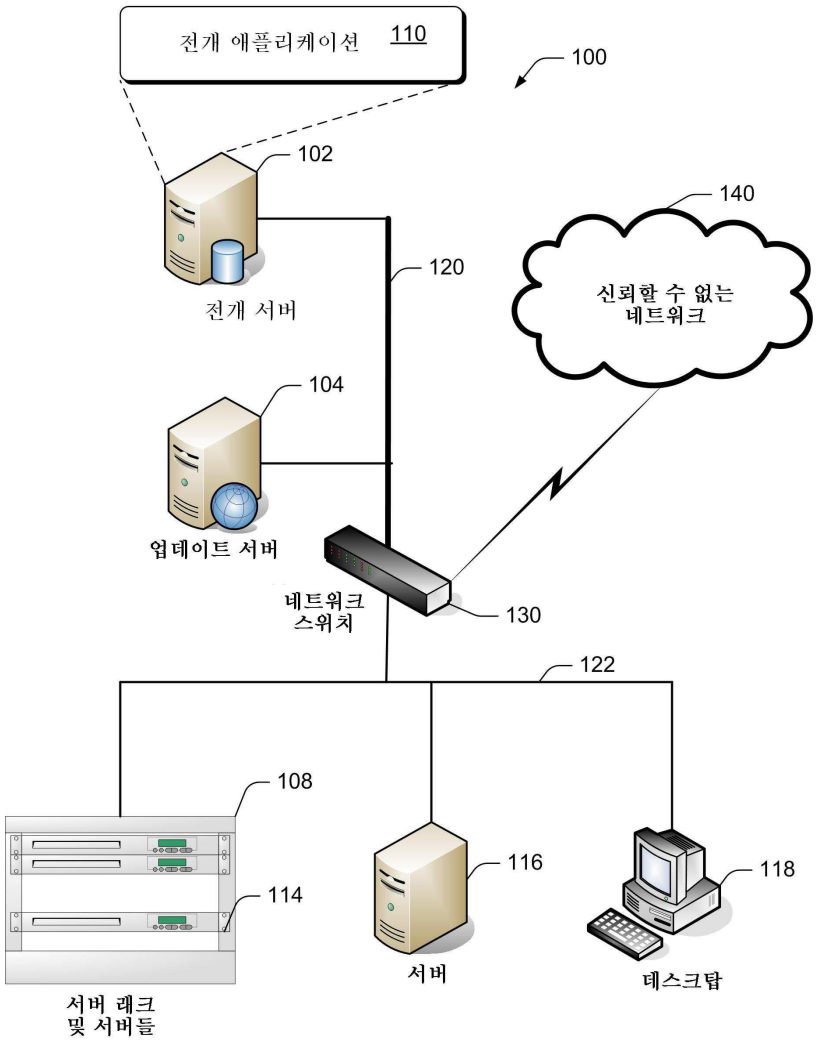
[0013] 120, 122 : (안전한) 네트워크

[0014] 130 : 네트워크 스위치

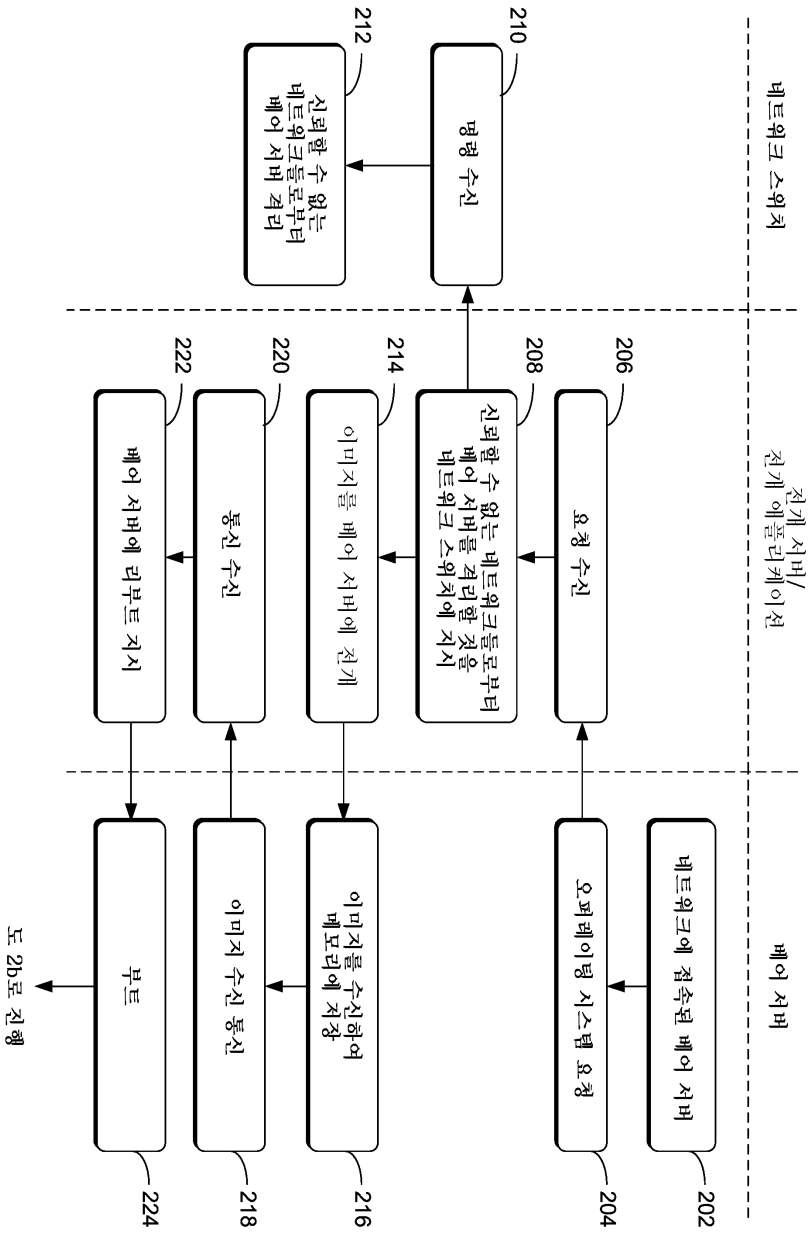
[0015] 140 : 신뢰할 수 없는 네트워크

도면

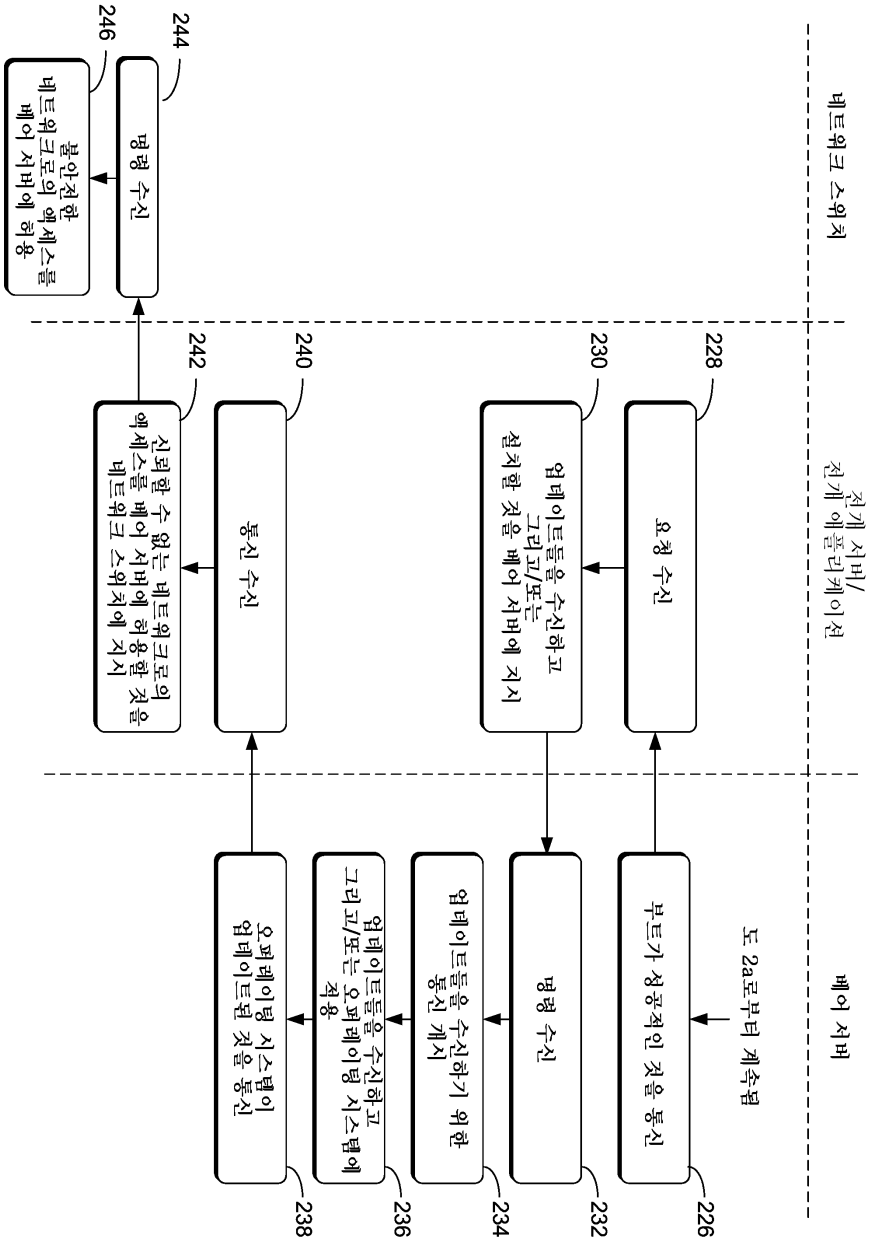
도면1



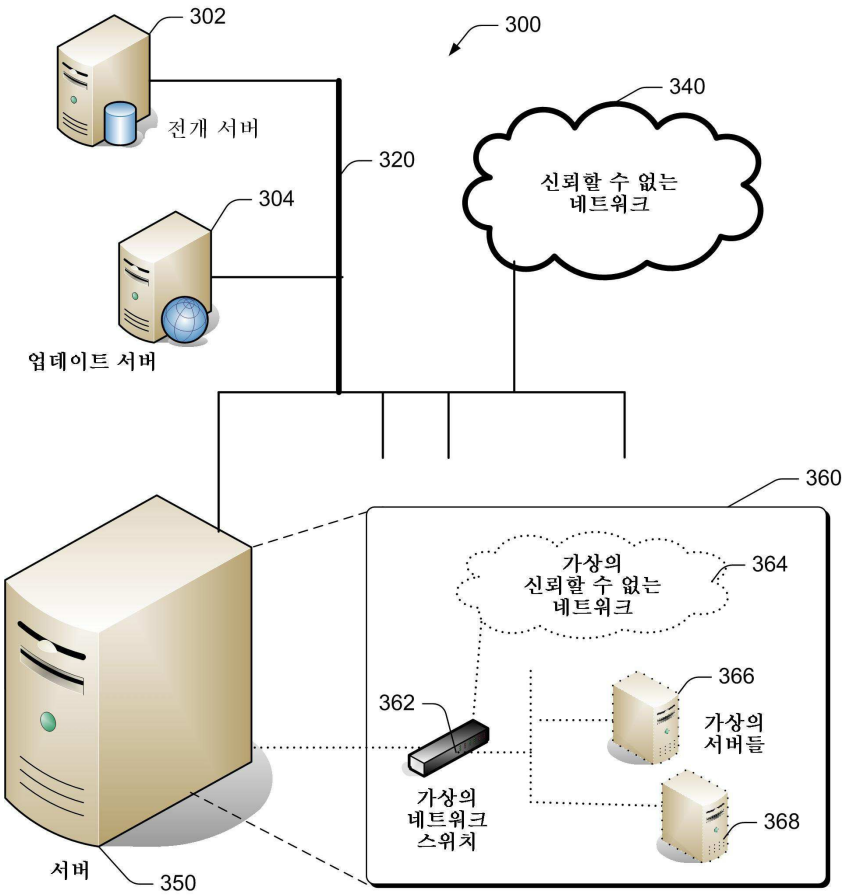
도면2a


네트워크 스위치
전개 서버/
전개 애플리케이션
베어 서버
210
명령 수신
212
신뢰할 수 없는
네트워크들로부터
베어 서버 격리
206
요청 수신
208
신뢰할 수 없는 네트워크들로부터
베어 서버를 격리할 것을
네트워크 스위치에 지시
214
이미지를 베어 서버에 전개
220
통신 수신
222
베어 서버에 리부트 지시
202
네트워크에 접속된 베어 서버
204
오퍼레이팅 시스템 요청
216
이미지를 수신하여
메모리에 저장
218
이미지 수신 통신
224
부트
도 2b로 진행

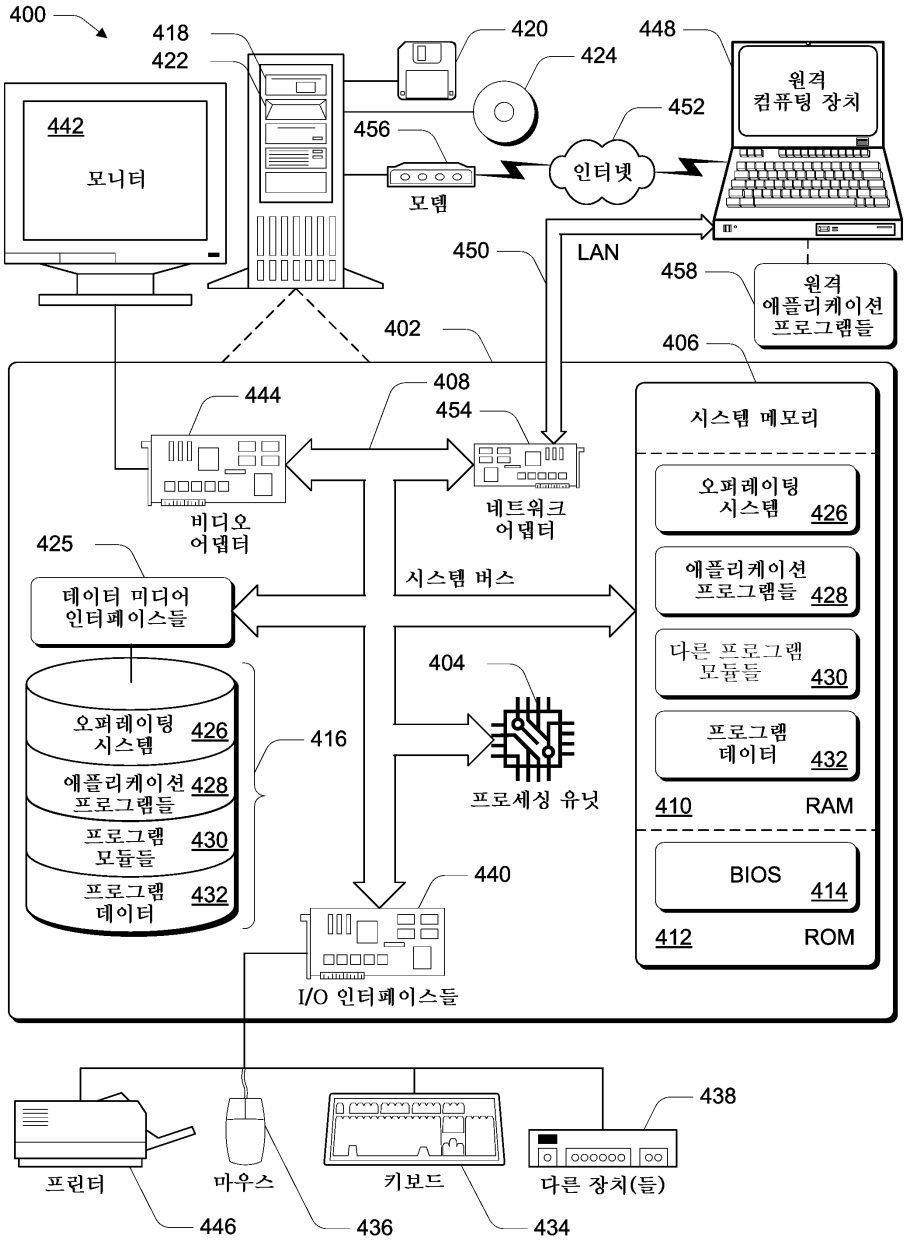
도면2b


네트워크 스위치
전개 서버/
전개 애플리케이션
베어 서버
도 2a로부터 계속됨
부트가 성공적인 것을 통신
226
요청 수신
228
업데이트들을 수신하고
그리고/또는
철치할 것을 베어 서버에 지시
230
명령 수신
232
업데이트들을 수신하기 위한
통신 개시
234
업데이트들을 수신하고
그리고/또는 오퍼레이팅 시스템에
적용
236
오퍼레이팅 시스템이
업데이트된 것을 통신
238
통신 수신
240
신뢰할 수 없는 네트워크로의
액세스를 베어 서버에 허용할 것을
네트워크 스위치에 지시
242
명령 수신
244
불안전한
네트워크로의 액세스를
베어 서버에 허용
246

도면3


302
300
340
전개 서버
320
신뢰할 수 없는
네트워크
304
업데이트 서버
360
가상의
신뢰할 수 없는
네트워크
364
362
366
가상의
서버들
가상의
네트워크
스위치
368
서버
350

도면4


400
418
422
420
424
448
원격
컴퓨팅 장치
442
모니터
456
452
인터넷
모뎀
450
LAN
458
원격
애플리케이션
프로그램들
402
406
444
408
454
시스템 메모리
오퍼레이팅
시스템 426
비디오
어댑터
네트워크
어댑터
425
애플리케이션
프로그램들 428
시스템 버스
데이터 미디어
인터페이스들
다른 프로그램
모듈들 430
404
오퍼레이팅
시스템 426
416
애플리케이션 428
프로그램들
프로그램
데이터 432
410
RAM
프로그램 430
모듈들
프로세싱 유닛
프로그램 432
데이터
440
BIOS
414
412
ROM
I/O 인터페이스들
438
프린터
마우스
키보드
다른 장치(들)
446
436
434