(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년11월12일
(11) 등록번호 10-0926822
(24) 등록일자 2009년11월06일

(51) Int. Cl.
G06F 15/00 (2006.01)
(21) 출원번호 10-2007-0125164
(22) 출원일자 2007년12월04일
심사청구일자 2007년12월04일
(65) 공개번호 10-2009-0058405
(43) 공개일자 2009년06월09일
(56) 선행기술조사문헌
KR1020030085270 A
KR1020070037782 A
JP2001350534 A
KR1020020070689 A
전체 청구항 수 : 총 18 항

(73) 특허권자
(주)유디피
서울 강서구 등촌동 684-2 우리벤처타운 11층
(72) 발명자
심재술
경기 고양시 일산구 일산3동 후곡마을아파트 1510동 302호
최진용
서울시 강서구 가양1동 150-37번지 202호
(74) 대리인
특허법인무한

심사관 : 천대식

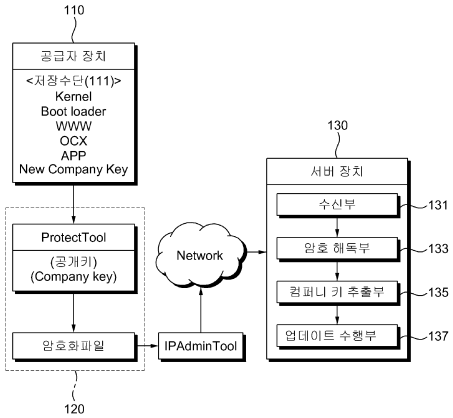
(54) 소프트웨어 보호수단 제공 방법 및 이를 수행하기 위한네트워크 시스템

(57) 요 약

소프트웨어 보호 수단 제공 방법 및 이를 수행하기 위한 네트워크 장치를 개시한다.

공개키 암호화 방식으로 암호화된 업데이트 정보를 수신하는 단계와, 상기 수신된 업데이트 정보를 미리 저장된 개인키에 의하여 해독하는 단계와, 상기 해독된 정보로부터 컴퍼니 키를 추출하는 단계 및 상기 추출된 컴퍼니 키와 미리 저장된 컴퍼니 키를 비교하여 운용 소프트웨어의 업데이트를 결정하는 단계를 포함하는 운용 소프트웨어의 보호 수단 제공 방법을 제공한다.

대 표 도 - 도1



특허청구의 범위

청구항 1

네트워크 장치의 운용 소프트웨어 및 판매업체에 고유하게 할당되는 컴퍼니 키를 생성하는 단계;

상기 운용 소프트웨어의 업데이트 정보 및 상기 컴퍼니 키를 공개키 암호화 방식으로 암호화 하여 원격지에 설치된 네트워크 장치로 전송하는 단계;

상기 네트워크 장치에 미리 저장된 개인키로 수신된 암호화 파일을 해독하여 상기 업데이트 정보 및 상기 컴퍼니 키를 추출하는 단계; 및

상기 추출된 컴퍼니 키와 상기 네트워크 장치에 미리 저장된 컴퍼니 키를 비교하여 동일한 경우에는 상기 업데이트 정보에 따라서 운용 소프트웨어를 업데이트 하는 단계를 포함하는 소프트웨어 보호수단 제공 방법.

청구항 2

제 1 항에 있어서,

상기 네트워크 장치의 운용 소프트웨어는 웹 페이지, 판매 업체의 브랜드 정보, 커널, 어플리케이션 프로그램, 액티브 X 중 적어도 하나를 포함하는 것을 특징으로 하는 소프트웨어 보호수단 제공 방법.

청구항 3

제 1 항에 있어서,

상기 업데이트 정보 및 컴퍼니 키는 하나의 파일로 랩핑되고, 상기 랩핑된 하나의 파일은 공개키 암호화 방식으로 암호화되는 것을 특징으로 하는 소프트웨어 보호수단 제공 방법.

청구항 4

제 1 항에 있어서,

상기 판매업체에 고유하게 할당되는 컴퍼니 키는 임의로 변경할 수 없는 고정된 값임을 특징으로 하는 소프트웨어 보호수단 제공 방법.

청구항 5

제 1 항에 있어서,

상기 추출된 컴퍼니 키와 상기 네트워크 장치에 미리 저장된 컴퍼니 키를 비교하여 동일하지 않은 경우에는 운용 소프트웨어의 업데이트를 거부하는 것을 특징으로 하는 소프트웨어 보호수단 제공 방법.

청구항 6

IP 카메라를 원격지에서 제어 할 수 있는 웹페이지를 제공하는 네트워크 장치에서 상기 웹페이지를 포함하는 운용 소프트웨어의 보호 수단 제공 방법으로서,

공개키 암호화 방식으로 암호화된 업데이트 정보를 수신하는 단계;

상기 수신된 업데이트 정보를 미리 저장된 개인키에 의하여 해독하는 단계;

상기 해독된 정보로부터 컴퍼니 키를 추출하는 단계; 및

상기 추출된 컴퍼니 키와 미리 저장된 컴퍼니 키를 비교하여 운용 소프트웨어의 업데이트를 결정하는 단계를 포함하는 운용 소프트웨어의 보호 수단 제공 방법.

청구항 7

제 6 항에 있어서,

상기 추출된 컴퍼니 키와 상기 미리 저장된 컴퍼니 키가 동일한 경우에는 상기 업데이트 정보에 따라서 운용 소프트웨어의 업데이트를 수행하는 것을 특징으로 하는 운용 소프트웨어의 보호 수단 제공 방법.

청구항 8

제 6 항에 있어서,

상기 추출된 컴퍼니 키와 상기 미리 저장된 컴퍼니 키가 동일하지 않은 경우에는 상기 업데이트 정보를 송신한 송신단으로 업데이트 거부 메시지를 전송하는 것을 특징으로 하는 운용 소프트웨어의 보호 수단 제공 방법.

청구항 9

네트워크 장치의 운용 소프트웨어 및 상기 운용 소프트웨어의 보호 수단을 제공하기 위한 유틸리티를 생성하는 단계;

상기 유틸리티에 의하여 제1 컴퍼니 키를 생성하는 단계;

상기 생성된 제1 컴퍼니 키에 따라서 네트워크 장치에 저장된 제2 컴퍼니 키를 변경하는 단계;

상기 운용 소프트웨어의 업데이트 정보 및 상기 제1 컴퍼니 키를 공개키 암호화 방식으로 암호화 하여 원격지에 설치된 네트워크 장치로 전송하는 단계;

상기 네트워크 장치에 미리 저장된 개인키로 수신된 암호화 파일을 해독하여 상기 업데이트 정보 및 상기 제1 컴퍼니 키를 추출하는 단계; 및

상기 추출된 제1 컴퍼니 키와 상기 네트워크 장치에 미리 저장된 제2 컴퍼니 키를 비교하여 동일한 경우에는 상기 업데이트 정보에 따라서 운용 소프트웨어를 업데이트 하는 단계를 포함하는 소프트웨어 보호수단 제공 방법.

청구항 10

제 9 항에 있어서,

상기 네트워크 장치의 운용 소프트웨어는 웹 페이지, 판매 업체의 브랜드 정보, 커널, 어플리케이션 프로그램, 액티브 X 중 적어도 하나를 포함하는 것을 특징으로 하는 소프트웨어 보호수단 제공 방법.

청구항 11

제 9 항에 있어서,

상기 업데이트 정보 및 컴퍼니 키는 하나의 파일로 랩핑되고, 상기 랩핑된 하나의 파일은 공개키 공개키 암호화 방식으로 암호화되는 것을 특징으로 하는 소프트웨어 보호수단 제공 방법.

청구항 12

제 9 항에 있어서,

상기 추출된 제1 컴퍼니 키와 상기 네트워크 장치에 미리 저장된 제2 컴퍼니 키를 비교하여 동일하지 않은 경우에는 운용 소프트웨어의 업데이트를 거부하는 것을 특징으로 하는 소프트웨어 보호수단 제공 방법.

청구항 13

네트워크 장치의 운용 소프트웨어 및 판매업체에 고유하게 할당되는 컴퍼니 키를 저장하기 위한 저장 수단;

상기 운용 소프트웨어의 업데이트 정보 및 상기 컴퍼니 키를 공개키 암호화 방식으로 암호화 하여 원격지에 설치된 네트워크 장치로 전송하기 위한 판매자 장치; 및

상기 네트워크 장치에 미리 저장된 개인키로 수신된 암호화 파일을 해독하여 상기 업데이트 정보 및 상기 컴퍼니 키를 추출하고 상기 추출된 컴퍼니 키와 미리 저장된 컴퍼니 키를 비교하여 운용 소프트웨어의 업데이트를 결정하는 서버 장치를 포함하는 소프트웨어 보호수단을 제공하기 위한 네트워크 시스템.

청구항 14

제 13 항에 있어서,

상기 서버 장치는 상기 추출된 컴퍼니 키와 상기 미리 저장된 컴퍼니 키가 동일하지 않은 경우에는 상기 업데이트 정보를 송신한 송신단으로 업데이트 거부 메시지를 전송하는 것을 특징으로 하는 소프트웨어 보호수단을 제

공하기 위한 네트워크 시스템.

청구항 15

공개키 암호화 방식으로 암호화된 업데이트 정보를 수신하는 수신부;

상기 수신된 업데이트 정보를 미리 저장된 개인키에 의하여 해독하는 암호 해독부;

상기 해독된 정보로부터 컴퍼니 키를 추출하는 컴퍼니 키 추출부; 및

상기 추출된 컴퍼니 키와 미리 저장된 컴퍼니 키를 비교하여 운용 소프트웨어의 업데이트를 결정하는 업데이트 수행부를 포함하는 네트워크 시스템.

청구항 16

제 15 항에 있어서,

상기 업데이트 수행부는 상기 추출된 컴퍼니 키와 상기 미리 저장된 컴퍼니 키가 동일하지 않은 경우에는 상기 업데이트 정보를 송신한 송신단으로 업데이트 거부 메시지를 전송하는 것을 특징으로 하는 소프트웨어 보호수단을 제공하기 위한 네트워크 시스템.

청구항 17

네트워크 장치의 운용 소프트웨어 및 상기 운용 소프트웨어의 보호 수단을 제공하기 위한 유틸리티를 저장하기 위한 저장 수단;

상기 유틸리티에 의하여 제1 컴퍼니 키를 생성하고 상기 운용 소프트웨어의 업데이트 정보 및 상기 제1 컴퍼니 키를 공개키 암호화 방식으로 암호화 하여 원격지에 설치된 네트워크 장치로 전송하는 판매자 장치; 및

상기 네트워크 장치에 미리 저장된 개인키로 수신된 암호화 파일을 해독하여 상기 업데이트 정보 및 상기 제1 컴퍼니 키를 추출하고 상기 추출된 제1 컴퍼니 키와 미리 저장된 제2 컴퍼니 키를 비교하여 운용 소프트웨어의 업데이트를 결정하는 서버 장치를 포함하는 소프트웨어 보호수단을 제공하기 위한 네트워크 시스템.

청구항 18

제 17 항에 있어서,

상기 서버 장치는 상기 추출된 제1 컴퍼니 키와 상기 네트워크 장치에 미리 저장된 제2 컴퍼니 키를 비교하여 동일하지 않은 경우에는 운용 소프트웨어의 업데이트를 거부하는 것을 특징으로 하는 소프트웨어 보호수단을 제공하기 위한 네트워크 시스템.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 소프트웨어 보호 수단 제공 방법 및 이를 수행하기 위한 네트워크 장치에 관한 것이다. 보다 구체적으로, 본 발명은 네트워크 장치(IP카메라, 비디오 인코더 등) 및 네트워크 장치를 운용하기 위한 소프트웨어 공급 업체가 상기 네트워크 장치의 판매 업체에게 소프트웨어 보호 수단을 함께 제공하기 위한 방법 및 이를 수행하기 위한 네트워크 시스템에 관한 것이다.

배 경 기 술

<2> 네트워크 장치는 네트워크 카메라 또는 네트워크 비디오 서버를 포함하는 개념이다.

<3> 상기 네트워크 카메라 및 네트워크 비디오 서버는 주로 보안을 필요로 하는 지역에 다수의 카메라를 설치하여 건물의 안팎이나, 주차장, 은행 등의 보안상태를 점검 하는데 사용된다.

<4> 또한, 상기 네트워크 비디오 서버는 다양한 어플리케이션 소프트웨어에 의하여 네트워크에 연결된 카메라를 원격지에서 제어하고, 카메라에 의하여 획득되는 영상 데이터 및 음성데이터를 저장/가공/처리 할 수 있다.

<5> 상기 네트워크 비디오 서버는 네트워크를 통하여 누구나 접근 가능하기 때문에 네트워크 어플리케이션 소프트웨어가 임의로 변경될 수 있는 위험이 있다.

<6> 즉, 네트워크 비디오 서버는 그 특성 상 서버의 기능 향상, 버그 수정, 사용자 인터페이스 변경 등의 이유로 업데이트가 빈번하게 요구된다.

<7> 그러나, 일반적인 아이디/암호 체계는 서버의 사용권을 제한하기 위한 것일 뿐, 서버내의 프로그램의 업데이트는 '관리자' 권한을 가진 사람이면 누구나 가능하다. 그런데, 서버의 '관리자' 권한을 획득하는 것은 서버의 운용을 책임지는 사람이라면 언제든지 획득 가능하다.

<8> 따라서, 네트워크 비디오 서버는 서버의 '관리자' 권한을 획득한 자에 의한 어플리케이션 소프트웨어의 변경의 위험에 쉽게 노출된다.

<9> 특히, 네트워크 장치의 제조 업체와 판매 업체가 구분되어 있는 경우(예를 들어, OEM 생산/공급의 경우)에는 더욱 문제가 될 수 있다.

<10> 즉, 네트워크 장치의 제조업체(이하, "네트워크 장치 공급 업체"라 칭함)가 다수의 네트워크 장치 판매 업체에게 네트워크 장치 및 어플리케이션 소프트웨어를 공급하는 경우에, 각각의 판매 업체가 갖고 있는 소프트웨어가 동일 기종의 다른 판매 업체가 판매하는 장치에서 동작할 수 없도록 하여야 한다.

발명의 내용

해결 하고자하는 과제

<11> 따라서, 본 발명은 네트워크 장치 판매 업체마다 고유한 암호화 키를 부여함으로써, 네트워크 장치를 운용하기 위한 소프트웨어를 보호할 수 있는 방법 및 이를 수행하기 위한 네트워크 시스템을 제안하고자 한다.

<12> 또한, 본 발명은 네트워크 장치의 제조 업체와 판매 업체가 구분되어 있는 경우에 각각의 판매 업체가 갖고 있는 소프트웨어가 동일 기종의 다른 판매 업체가 판매하는 장치에서 동작할 수 없도록 하기 위한 보호 수단 제공 방법 및 이를 수행하기 위한 네트워크 시스템을 제안하고자 한다.

과제 해결수단

<13> 상기한 과제를 해결하기 위한 본 발명에 따른 실시예는 네트워크 장치의 운용 소프트웨어 및 판매업체에 고유하게 할당되는 컴퍼니 키를 생성하는 단계와, 상기 운용 소프트웨어의 업데이트 정보 및 상기 컴퍼니 키를 공개키 암호화 방식으로 암호화 하여 원격지에 설치된 네트워크 장치로 전송하는 단계와, 상기 네트워크 장치에 미리 저장된 개인키로 수신된 암호화 파일을 해독하여 상기 업데이트 정보 및 상기 컴퍼니 키를 추출하는 단계 및 상기 추출된 컴퍼니 키와 상기 네트워크 장치에 미리 저장된 컴퍼니 키를 비교하여 동일한 경우에는 상기 업데이트 정보에 따라서 운용 소프트웨어를 업데이트 하는 단계를 포함하는 소프트웨어 보호수단 제공 방법을 제공한다.

<14> 또한, 본 발명의 다른 실시예는 공개키 암호화 방식으로 암호화된 업데이트 정보를 수신하는 단계와, 상기 수신된 업데이트 정보를 미리 저장된 개인키에 의하여 해독하는 단계와, 상기 해독된 정보로부터 컴퍼니 키를 추출하는 단계 및 상기 추출된 컴퍼니 키와 미리 저장된 컴퍼니 키를 비교하여 운용 소프트웨어의 업데이트를 결정하는 단계를 포함하는 운용 소프트웨어의 보호 수단 제공 방법을 제공한다.

<15> 또한, 본 발명의 또 다른 실시예는 네트워크 장치의 운용 소프트웨어 및 상기 운용 소프트웨어의 보호 수단을 제공하기 위한 유틸리티를 생성하는 단계와, 상기 유틸리티에 의하여 제1 컴퍼니 키를 생성하는 단계와, 상기 생성된 제1 컴퍼니 키에 따라서 네트워크 장치에 저장된 제2 컴퍼니 키를 변경하는 단계와, 상기 운용 소프트웨어의 업데이트 정보 및 상기 제1 컴퍼니 키를 공개키 암호화 방식으로 암호화 하여 원격지에 설치된 네트워크 장치로 전송하는 단계와, 상기 네트워크 장치에 미리 저장된 개인키로 수신된 암호화 파일을 해독하여 상기 업데이트 정보 및 상기 제1 컴퍼니 키를 추출하는 단계 및 상기 추출된 제1 컴퍼니 키와 상기 네트워크 장치에 미리 저장된 제2 컴퍼니 키를 비교하여 동일한 경우에는 상기 업데이트 정보에 따라서 운용 소프트웨어를 업데이트 하는 단계를 포함하는 소프트웨어 보호수단 제공 방법을 제공한다.

<16> 상기한 본 발명의 실시예를 수행하기 위한 네트워크 시스템은 네트워크 장치의 운용 소프트웨어 및 판매업체에 고유하게 할당되는 컴퍼니 키를 저장하기 위한 저장 수단과, 상기 운용 소프트웨어의 업데이트 정보 및 상기 컴퍼니 키를 공개키 암호화 방식으로 암호화 하여 원격지에 설치된 네트워크 장치로 전송하기 위한 판매자 장치

및 상기 네트워크 장치에 미리 저장된 개인키로 수신된 암호화 파일을 해독하여 상기 업데이트 정보 및 상기 컴퍼니 키를 추출하고 상기 추출된 컴퍼니 키와 미리 저장된 컴퍼니 키를 비교하여 운용 소프트웨어의 업데이트를 결정하는 서버 장치를 포함한다.

<17> 또한, 본 발명의 다른 네트워크 시스템은 공개키 암호화 방식으로 암호화된 업데이트 정보를 수신하는 수신부와, 상기 수신된 업데이트 정보를 미리 저장된 개인키에 의하여 해독하는 암호 해독부와, 상기 해독된 정보로부터 컴퍼니 키를 추출하는 컴퍼니 키 추출부 및 상기 추출된 컴퍼니 키와 미리 저장된 컴퍼니 키를 비교하여 운용 소프트웨어의 업데이트를 결정하는 업데이트 수행부를 포함한다.

<18> 또한 본 발명의 또 다른 네트워크 시스템은 네트워크 장치의 운용 소프트웨어 및 상기 운용 소프트웨어의 보호 수단을 제공하기 위한 유틸리티를 저장하기 위한 저장 수단과, 상기 유틸리티에 의하여 제1 컴퍼니 키를 생성하고 상기 운용 소프트웨어의 업데이트 정보 및 상기 제1 컴퍼니 키를 공개키 암호화 방식으로 암호화 하여 원격지에 설치된 네트워크 장치로 전송하는 판매자 장치 및 상기 네트워크 장치에 미리 저장된 개인키로 수신된 암호화 파일을 해독하여 상기 업데이트 정보 및 상기 제1 컴퍼니 키를 추출하고 상기 추출된 제1 컴퍼니 키와 미리 저장된 제2 컴퍼니 키를 비교하여 운용 소프트웨어의 업데이트를 결정하는 서버 장치를 포함한다.

효 과

<19> 본 발명의 실시예에 따르면, 네트워크 장치 판매 업체마다 고유한 암호화 키를 부여함으로써, 네트워크 장치를 운용하기 위한 소프트웨어를 보호할 수 있게 된다.

<20> 또한 본 발명의 실시예에 따르면, 네트워크 장치의 제조 업체와 판매 업체가 구분되어 있는 경우에 각각의 판매 업체가 갖고 있는 소프트웨어가 동일 기종의 다른 판매 업체가 판매하는 장치에서 동작할 수 없도록 할 수 있게 된다.

발명의 실시를 위한 구체적인 내용

<21> 이하에서는 첨부된 도면을 참조하여 본 발명의 실시예를 상세히 설명하기로 한다. 본 발명을 설명함에 있어서, 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고, 본 명세서에서 사용되는 용어(terminology)들은 본 발명의 바람직한 실시예를 적절히 표현하기 위해 사용된 용어들로서, 이는 사용자, 운용자의 의도 또는 본 발명이 속하는 분야의 관례 등에 따라 달라질 수 있다. 따라서, 본 용어들에 대한 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

<22> 도 1은 본 발명의 실시예에 따른 네트워크 시스템의 구조를 나타내는 블록도이다.

<23> 도 1을 참조하면, 네트워크 시스템은 공급자 장치(110), 판매자 장치(120) 및 서버 장치(130)를 포함하여 구성된다.

<24> 상기 공급자 장치(110)는 네트워크 장치(서버 장치 또는 IP 카메라)를 제조하여 판매자에게 공급하는 공급자가 운용하는 컴퓨터 장치일 수 있다.

<25> 상기 공급자 장치(110)는 네트워크 장치를 운용하기 위한 어플리케이션 프로그램, 커널, Boot loader, 웹 페이지 구성요소, OCX, Active X 등의 원본 파일을 저장하기 위한 저장수단(111)을 포함하여 구성될 수 있다.

<26> 참고적으로, 커널, boot loader, web pages, ActiveX (OCX), configuration file 은 원본 파일이다.

<27> 상기 커널은 서버 장치의 OS, 파일 시스템, 어플리케이션 프로그램 등 서버 정치가 동작하기 위한 모든 실행 가능한 프로그램의 집합을 통틀어 일컫는다.

<28> 상기 boot loader는 서버 장치에 전원이 인가되었을 때 최초로 실행이 되며, boot loader의 실행이 완료되고 나서야 서버 장치의 커널이 동작을 개시한다. boot loader는 서버 장치의 하드웨어를 구성 및 설정하여 커널이 동작하는데 필요한 최소한의 환경을 구성한다.

<29> 상기 web pages는 HTML, 자바 스크립트, 그림 파일들로 구성되어 있다. 웹 브라우저를 이용해서 서버 장치의 여러 가지 설정 값을 변경하는데 필요한 웹 환경을 제공한다. 판매자의 목적에 따라 web pages의 구성 요소를 수정할 수 있다. Web pages는 어느 한 판매자와 다른 판매자를 시각적으로 구분지을 수 있는 가장 중요한 부분이다.

<30> 상기 ActiveX는 OCX라고도 부른다. ActiveX는 서버 장치에서 end-user의 피씨로 다운로드되어 end-user의 피씨에서 실행이 된다. 주 목적은 서버 장치가 생성한 MPEG-4 및 MJPEG 스트림을 end-user의 피씨에서 decompression하고 decompression된 영상을 보여준다.

<31> 상기 configuration file은 제품 이름, 제품 설명, 제품의 브랜드 이름과 같이 제품을 구분지을 수 있는 문자열을 가지고 있다. 각 판매자는 자기가 원하는 제품의 이름을 configuration file을 통해 설정할 수 있다.

<32> 이때, 상기 저장수단(111)은 컴퓨터 판독 가능한 외부 저장 매체 또는 FTP 접속 프로그램일 수 있다. 또한, 상기 저장수단(111)은 운용 소프트웨어의 보호 수단을 제공하기 위한 유틸리티 및 판매업체에 고유하게 할당되는 컴퍼니 키를 저장하고 있다.

<33> 상기 판매자 장치(120)는 네트워크 장치를 공급 받아 자신의 브랜드로 이를 판매하는 판매자가 운용하는 컴퓨터 장치일 수 있다.

<34> 상기 판매자 장치(120)는 상기 공급자 장치(110) 또는 저장 수단(111)으로부터 운용 소프트웨어의 원본 파일, 컴퍼니 키 및 운용 소프트웨어의 보호 수단을 제공하기 위한 유틸리티를 수신할 수 있다.

<35> 상기 판매자 장치(120)는 상기 운용 소프트웨어의 업데이트 정보 및 상기 컴퍼니 키를 공개키 암호화 방식으로 암호화 하여 원격지에 설치된 서버 장치(130)로 전송한다.

<36> 상기 서버 장치(130)는 미리 저장된 개인키로 수신된 암호화 파일을 해독하여 상기 업데이트 정보 및 상기 컴퍼니 키를 추출하고 상기 추출된 컴퍼니 키와 미리 저장된 컴퍼니 키를 비교하여 운용 소프트웨어의 업데이트를 결정한다.

<37> 또한, 상기 서버 장치(130)는 공개키 암호화 방식으로 암호화된 업데이트 정보를 수신하는 수신부(131)와, 상기 수신된 업데이트 정보를 미리 저장된 개인키에 의하여 해독하는 암호 해독부(133)와, 상기 해독된 정보로부터 컴퍼니 키를 추출하는 컴퍼니 키 추출부(135) 및 상기 추출된 컴퍼니 키와 미리 저장된 컴퍼니 키를 비교하여 운용 소프트웨어의 업데이트를 결정하는 업데이트 수행부(137)를 포함하여 구성될 수 있다.

<38> 이하, 상기 도 1에 도시된 네트워크 시스템에 의한 소프트웨어 보호 수단 제공 방법을 설명하기로 한다.

<39> 도 2는 본 발명의 실시예에 따른 소프트웨어 보호수단 제공 방법을 나타내는 흐름도이다.

<40> 상기 도 2를 참조하면, 소프트웨어 보호수단 제공 방법은 네트워크 장치의 운용 소프트웨어 및 판매업체에 고유하게 할당되는 컴퍼니 키를 생성하는 단계(S10)와, 상기 운용 소프트웨어의 업데이트 정보 및 상기 컴퍼니 키를 공개키 암호화 방식으로 암호화 하여 원격지에 설치된 네트워크 장치로 전송하는 단계(S20)와, 상기 네트워크 장치에 미리 저장된 개인키로 수신된 암호화 파일을 해독하여 상기 업데이트 정보 및 상기 컴퍼니 키를 추출하는 단계(S30) 및 상기 추출된 컴퍼니 키와 상기 네트워크 장치에 미리 저장된 컴퍼니 키를 비교하여 동일한 경우에는 상기 업데이트 정보에 따라서 운용 소프트웨어를 업데이트 하는 단계(S40, S50)를 포함한다.

<41> 상기 단계(S10)에서 네트워크 장치 공급자는 공급자 장치(110)에 의하여 네트워크 장치의 운용 소프트웨어 및 판매업체에 고유하게 할당되는 컴퍼니 키를 생성한다.

<42> 한편, 네트워크 장치 공급자는 상기 판매업체에 고유하게 할당되는 컴퍼니 키에 대응하는 고유한 컴퍼니 키를 미리 네트워크 장치에 저장한다. 이때, 상기 네트워크 장치에 저장되는 컴퍼니 키는 상기 판매업체에 고유하게 할당되는 컴퍼니 키와 동일한 값을 갖거나 미리 설정된 한 쌍을 이루는 값일 수 있다.

<43> 본 실시예에서 상기 판매업체에 고유하게 할당되는 컴퍼니 키 및 네트워크 장치에 미리 저장되는 컴퍼니 키는 임의로 변경할 수 없는 고정된 값이다.

<44> 상기 단계(S20)에서 판매자 장치(120)는 운용 소프트웨어의 업데이트 필요시 업데이트 정보를 생성하고, 운용 소프트웨어의 보호 수단을 제공하기 위한 유틸리티를 사용하여 업데이트 정보 및 컴퍼니 키를 암호화 하여 서버 장치(130)로 전송한다.

<45> 상기 업데이트 정보 및 컴퍼니 키의 암호화 과정은 도 3에 도시된 바와 같이, 업데이트 정보 및 컴퍼니 키를 하나의 파일로 랩핑(Wrapping)하고(S70, S80), 상기 랩핑된 하나의 파일을 공개키 암호화 방식으로 암호화하는 것(S90)이다.

<46> 상기 단계(S30)에서, 서버 장치(130)는 공개키 암호화 방식으로 암호화된 업데이트 정보를 수신하여 이를 해독하고 업데이트 정보 및 컴퍼니 키를 추출한다.

<47> 상기 단계(S30)에서, 서버 장치(130)는 수신된 업데이트 정보를 미리 저장된 개인키에 의하여 해독할 수 있다.

<48> 상기 단계(S40)에서, 서버 장치(130)는 상기 추출된 컴퍼니 키와 미리 저장된 컴퍼니 키를 비교한다.

<49> 상기 추출된 컴퍼니 키와 미리 저장된 컴퍼니 키가 동일한 경우에, 상기 서버 장치(130)는 해독된 업데이트 정보에 따라서 운용 소프트웨어를 업데이트 한다(S50).

<50> 만일, 상기 추출된 컴퍼니 키와 미리 저장된 컴퍼니 키가 동일하지 않은 경우에는 운용 소프트웨어의 업데이트를 거부한다(S60).

<51> 본 발명의 실시예에 따르면, 서버 장치(130)는 업데이트 거부 메시지를 판매자 장치로 전송할 수 있다.

<52> 한편, 본 발명의 실시예에 따르면, 상기 서버 장치(130)는 운용 소프트웨어 보호 수단을 제공하기 위하여, 공개키 암호화 방식으로 암호화된 업데이트 정보를 수신하고, 상기 수신된 업데이트 정보를 미리 저장된 개인키에 의하여 해독하고, 상기 해독된 정보로부터 컴퍼니 키를 추출하고, 그리고 상기 추출된 컴퍼니 키와 미리 저장된 컴퍼니 키를 비교하여 운용 소프트웨어의 업데이트를 결정할 수 있다.

<53> 도 4는 본 발명의 다른 실시예에 따른 소프트웨어 보호수단 제공 방법을 나타내는 흐름도이다.

<54> 상기 도 4를 참조하면, 소프트웨어 보호수단 제공 방법은 운용 소프트웨어의 보호 수단을 제공하기 위한 유틸리티에 의하여 제1 컴퍼니 키를 생성하는 단계(S110)와, 상기 생성된 제1 컴퍼니 키에 따라서 네트워크 장치에 저장된 제2 컴퍼니 키를 변경하는 단계(S120)와, 상기 운용 소프트웨어의 업데이트 정보 및 상기 제1 컴퍼니 키를 공개키 암호화 방식으로 암호화 하여 원격지에 설치된 네트워크 장치로 전송하는 단계(S130)와, 상기 네트워크 장치에 미리 저장된 개인키로 수신된 암호화 파일을 해독하여 상기 업데이트 정보 및 상기 제1 컴퍼니 키를 추출하는 단계(S140) 및 상기 추출된 제1 컴퍼니 키와 상기 네트워크 장치에 미리 저장된 제2 컴퍼니 키를 비교하여 동일한 경우에는 상기 업데이트 정보에 따라서 운용 소프트웨어를 업데이트 하는 단계(S150, S160)를 포함한다.

<55> 상기 단계(S110)에서, 판매자 장치(120)는 임의의 값으로 제1 컴퍼니 키를 생성할 수 있다.

<56> 이때, 상기 단계(S120)에서, 상기 네트워크 장치의 판매자는 서버장치(130)에 저장된 컴퍼니 키를 상기 제1 컴퍼니 키에 대응하는 값으로 변경할 수 있다.

<57> 상기 단계(S130) 내지 단계(S170)는 상기한 단계(S20) 내지 단계(S60)와 동일한 동작을 수행하는 것이다.

<58> 상기한 본 발명의 실시예들에 따라서, 네트워크 장치의 제조 업체와 판매 업체가 구분되어 있는 경우에도 각각의 판매 업체가 갖고 있는 소프트웨어가 동일 기종의 다른 판매 업체가 판매하는 장치에서 동작할 수 없고, 운용 소프트웨어의 보호가 가능하게 된다.

<59> 또한, 본 발명의 실시예에 따르면, 판매자가 직접 네트워크 장치를 제조하지 않는 경우에도 판매자 자신만의 브랜드를 사용할 수 있고, 동일한 공급자로부터 네트워크 장치를 공급 받은 다른 판매자에 의하여 브랜드 정보가 변경되는 것을 방지할 수 있다.

<60> 한편, 상기한 컴퍼니 키는 예를 들어 6byte 길이를 갖는 숫자 값이나 그 이상의 길이를 갖는 숫자 및 문자로 구성된 값일 수 있다.

<61> 그리고, 상기한 보호 수단을 제공하기 위한 유틸리티는 도 5에 도시한 바와 같이, 업데이트 대상 운용 소프트웨어를 선택하고, 컴퍼니 키와 업데이트 정보를 하나의 파일로 생성(Wrapping)하고, 생성된 하나의 파일을 암호화하기 위한 인터페이스를 제공하도록 구성될 수 있다.

<62> 도 6a는 도 5에 도시된 유틸리티의 인터페이스 예에서 "companykey" 가 선택된 경우에, 컴퍼니 키를 생성하기 위한 인터페이스를, 도 6b는 "Packaging" 가 선택된 경우에 저장 경로 및 파일 정보를 지정하기 위한 인터페이스를, 도 6c는 "Encrypt"가 선택된 경우에 해당 정보를 나타내고 암호화 명령을 수행하기 위한 인터페이스를 각각 나타낸다.

<63> 본 발명에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media),

CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 상기 매체는 프로그램 명령, 데이터 구조 등을 지정하는 신호를 전송하는 반송파를 포함하는 광 또는 금속선, 도파관 등의 전송 매체일 수도 있다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

<64> 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

<65> 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

도면의 간단한 설명

<66> 도 1은 본 발명의 실시예에 따른 네트워크 시스템의 구조를 나타내는 블록도이다.

<67> 도 2는 본 발명의 실시예에 따른 소프트웨어 보호수단 제공 방법을 나타내는 흐름도이다.

<68> 도 3은 업데이트 정보 및 컴퍼니 키의 암호화 과정을 보여주는 도면이다.

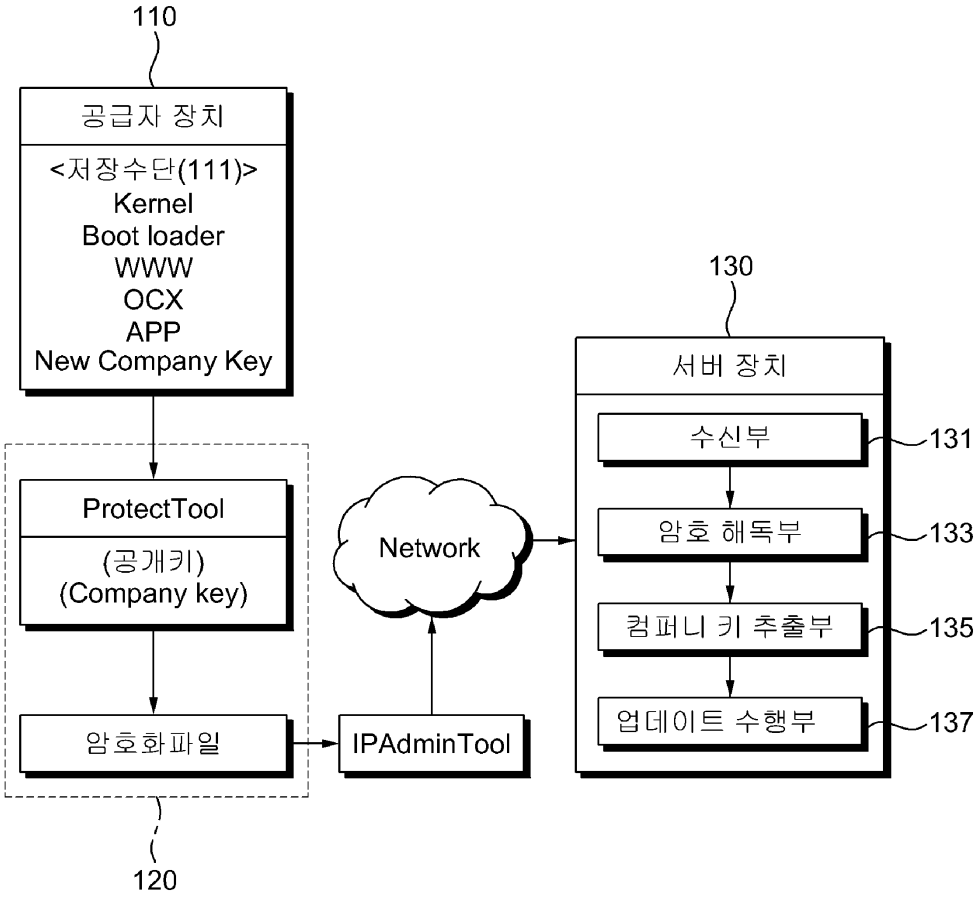
<69> 도 4는 본 발명의 다른 실시예에 따른 소프트웨어 보호수단 제공 방법을 나타내는 흐름도이다.

<70> 도 5는 보호 수단을 제공하기 위한 유틸리티의 구성예를 보여주는 도면이다.

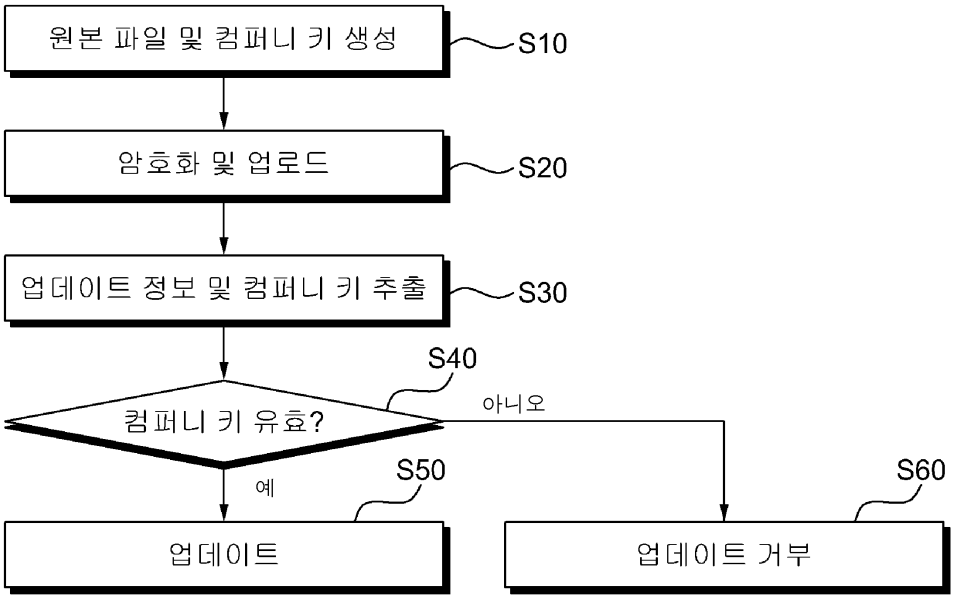
<71> 도 6a 내지 도 6c는 도 5에 예시된 유틸리티 구성의 부가 구성을 보여주는 도면이다.

도면

도면1


110
공급자 장치
<저장수단(111)>
Kernel
Boot loader
WWW
OCX
APP
New Company Key
ProtectTool
(공개키)
(Company key)
암호화파일
120
Network
IPAdminTool
130
서버 장치
수신부
131
암호 해독부
133
컴퍼니 키 추출부
135
업데이트 수행부
137

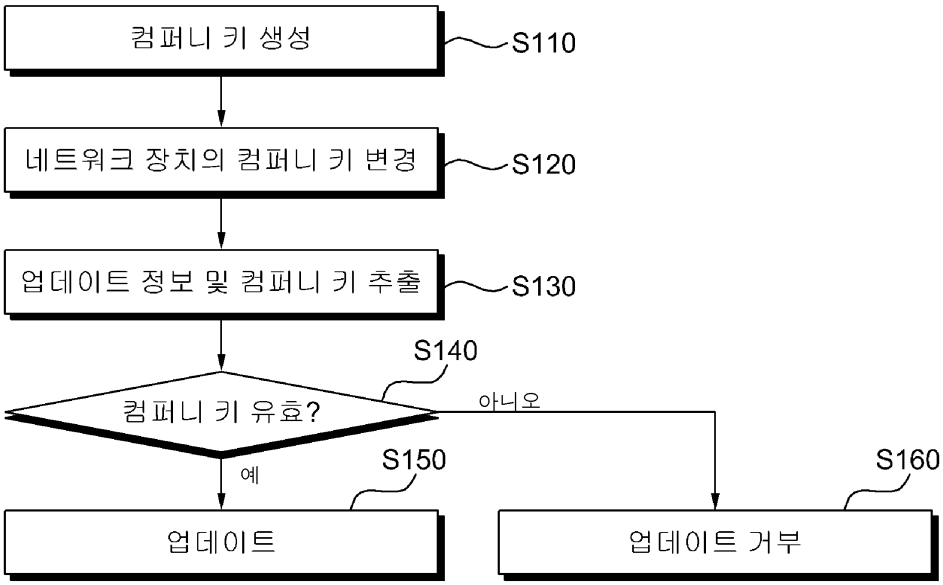
도면2


원본 파일 및 컴퍼니 키 생성
S10
암호화 및 업로드
S20
업데이트 정보 및 컴퍼니 키 추출
S30
S40
컴퍼니 키 유효?
아니오
예
S50
S60
업데이트
업데이트 거부

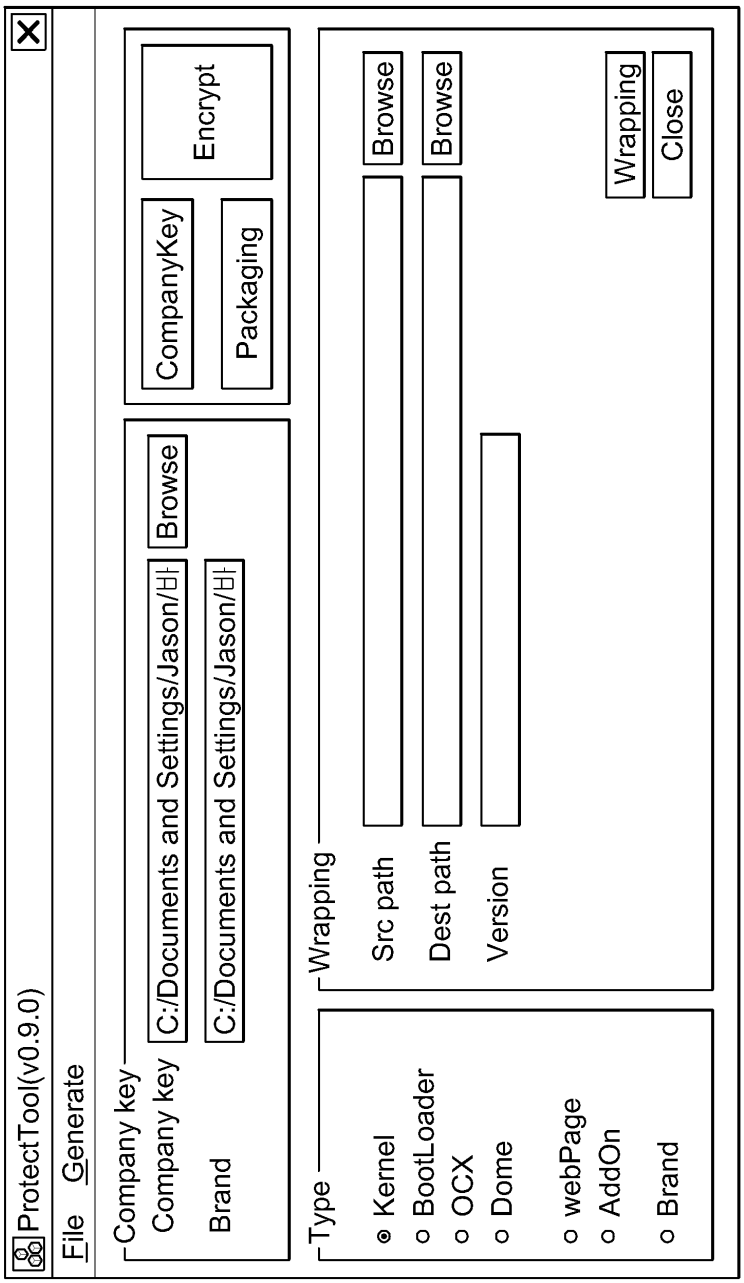
도면3


S70
S80
S90
업데이트 정보 생성
컴퍼니 키를
포함하여 랩핑
공개키 기반
암호화

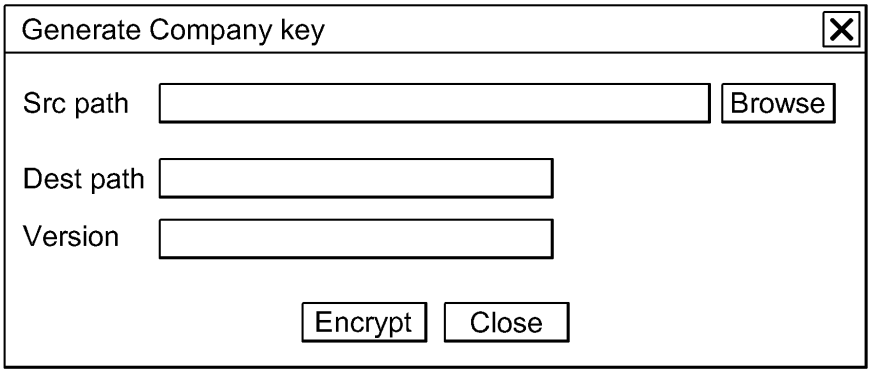
도면4


컴퍼니 키 생성
S110
네트워크 장치의 컴퍼니 키 변경
S120
업데이트 정보 및 컴퍼니 키 추출
S130
S140
컴퍼니 키 유효?
아니오
예
S150
S160
업데이트
업데이트 거부

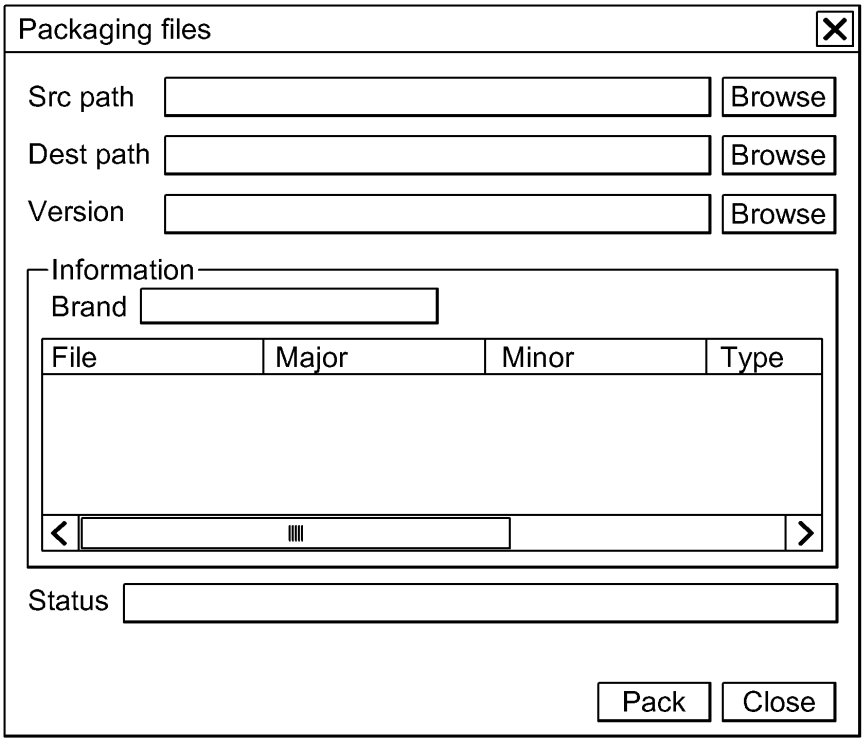
도면5


ProtectTool(v0.9.0)
File Generate
Company key
Company key
C:/Documents and Settings/Jason/바
Browse
Brand
C:/Documents and Settings/Jason/바
CompanyKey
Encrypt
Packaging
Type
Kernel
BootLoader
OCX
Dome
webPage
AddOn
Brand
Wrapping
Src path
Browse
Dest path
Browse
Version
Wrapping
Close

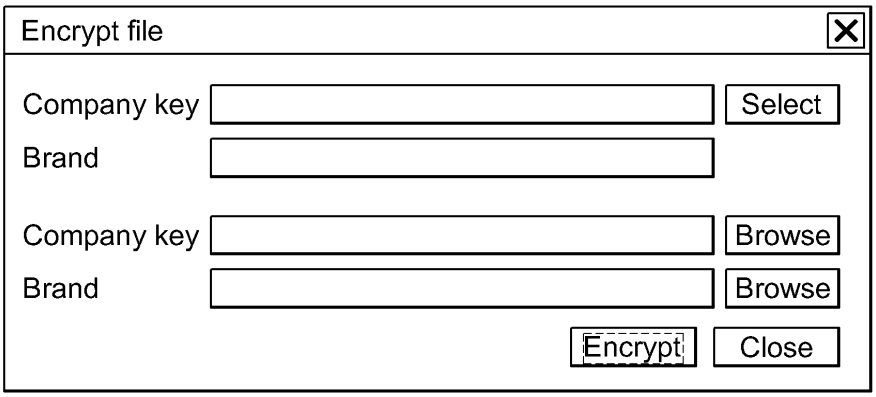
도면6a


Generate Company key
Src path
Browse
Dest path
Version
Encrypt
Close

도면6b


Packaging files
Src path
Browse
Dest path
Browse
Version
Browse
Information
Brand
File
Major
Minor
Type
Status
Pack
Close

도면6c


Encrypt file
Company key
Select
Brand
Company key
Browse
Brand
Browse
Encrypt
Close