(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년05월20일
(11) 등록번호 10-1623266
(24) 등록일자 2016년05월16일

(51) 국제특허분류(Int. Cl.)
G06F 12/14 (2006.01)
(21) 출원번호 10-2014-0123694
(22) 출원일자 2014년09월17일
심사청구일자 2014년09월17일
(65) 공개번호 10-2016-0032928
(43) 공개일자 2016년03월25일
(56) 선행기술조사문헌
KR1020130078093 A
KR1020100100488 A
KR100663034 B1
KR1020090021985 A

(73) 특허권자
(주)스마일게이트엔터테인먼트
경기도 성남시 분당구 판교역로 220, 5층(삼평동, 쏠리드스페이스)
(72) 발명자
손형곤
경기도 용인시 수지구 성복1로 157 버들치마을경남아너스빌1차아파트 102동 2003호
이창선
경기도 광주시 오포읍 능평로 46-15, 아트리움 402호
권혁빈
경기도 성남시 분당구 판교역로 220, 5층(삼평동, 쏠리드스페이스)
(74) 대리인
특허법인 다해

전체 청구항 수 : 총 14 항 심사관 : 최봉묵

(54) 발명의 명칭 **CRC 알고리즘을 이용한 메모리 보호 파일의 위변조 검출 방법 및 서버**

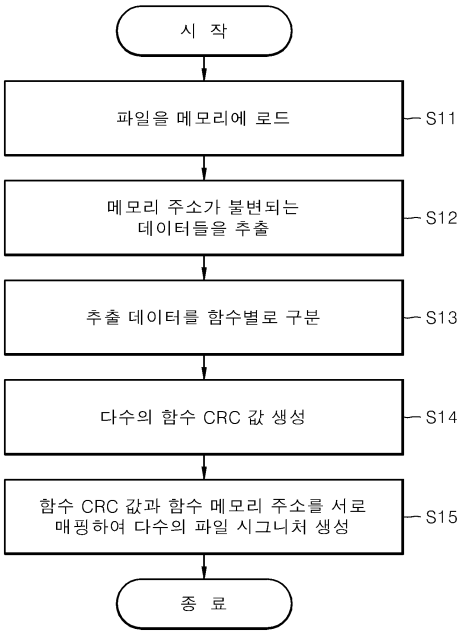
(57) 요 약

본 발명은 메모리 보호 기능이 적용된 파일에 대해서도 CRC 알고리즘을 이용한 파일 위변조 검출 동작을 수행할 수 있도록 하는 CRC 알고리즘을 이용한 메모리 보호 파일의 위변조 검출 방법 및 서버에 관한 것으로,

상기 CRC를 이용한 메모리 보호 파일의 위변조 검출 방법은 상기 메모리 보호 파일을 메모리 로드한 후, 메모리

(뒷면에 계속)

대 표 도 - 도3



주소가 변화되지 않는 데이터를 추출하는 단계; 상기 추출된 데이터를 함수별로 구분하고 함수별 CRC 값을 생성한 후 메모리 주소를 매핑하여, 다수의 파일 시그니처를 생성 및 저장하는 단계; 상기 클라이언트 단말에 상기 메모리 보호 파일을 제공하는 단계; 다수의 파일 시그니처 중 하나를 랜덤 선택한 후, 상기 랜덤 선택된 파일 시그너처에 포함된 메모리 주소를 상기 클라이언트 단말에 통보하고, 상기 클라이언트 단말로부터 상기 통보한 메모리 주소에 저장된 데이터에 대한 CRC 값을 피드백받는 단계; 및 상기 피드백받은 CRC 값과 상기 랜덤 선택된 파일 시그너처에 포함된 CRC 값을 비교 분석하여, 상기 메모리 보호 파일의 위변조 여부를 확인하는 단계를 포함할 수 있다.

명 세 서

청구범위

청구항 1

클라이언트 단말에 메모리 보호 파일을 제공하는 서버의 CRC를 이용한 메모리 보호 파일의 위변조 검출 방법에 있어서,

상기 메모리 보호 파일을 메모리 로드한 후, 메모리 주소가 변화되지 않는 데이터를 추출하는 단계;

상기 추출된 데이터를 함수별로 구분하고 함수별 CRC 값을 생성한 후 메모리 주소를 매핑하여, 다수의 파일 시그니처를 생성 및 저장하는 단계;

상기 클라이언트 단말에 상기 메모리 보호 파일을 제공하는 단계;

다수의 파일 시그니처 중 하나를 랜덤 선택한 후, 상기 랜덤 선택된 파일 시그너처에 포함된 메모리 주소를 상기 클라이언트 단말에 통보하고, 상기 클라이언트 단말로부터 상기 통보한 메모리 주소에 저장된 데이터에 대한 CRC 값을 피드백받는 단계; 및

상기 피드백받은 CRC 값과 상기 랜덤 선택된 파일 시그너처에 포함된 CRC 값을 비교 분석하여, 상기 메모리 보호 파일의 위변조 여부를 확인하는 단계를 포함하는 CRC를 이용한 메모리 보호 파일의 위변조 검출 방법.

청구항 2

제1항에 있어서, 상기 메모리 보호 파일은

파일 실행을 위해 메모리 로드될 때마다 메모리 주소가 변경되는 함수들을 구비한 파일인 것을 특징으로 하는 CRC를 이용한 메모리 보호 파일의 위변조 검출 방법.

청구항 3

제1항에 있어서, 상기 추출된 데이터는

메모리 로드 동작을 기 설정횟수 반복 수행한 후 메모리 주소가 변경되지 않는 데이터를 선별하는 방식으로 추출되거나, 메모리 보호 함수로 기 등록된 함수들에 대응되는 데이터를 선별하는 방식으로 추출되거나, 또는 메모리 보호 주소로 기 등록된 메모리 주소들에 저장된 데이터를 선별하는 방식으로 추출되는 것을 특징으로 하는 CRC를 이용한 메모리 보호 파일의 위변조 검출 방법.

청구항 4

제1항에 있어서, 상기 CRC 값을 피드백받는 단계는

상기 클라이언트 단말이 파일 실행을 요청하는 경우, 상기 클라이언트 단말로부터 해킹 가능성이 있음을 통보받는 경우, 서버 관리자가 파일 위변조 감시를 수동 요청하는 경우, 및 기 설정된 파일 위변조 감시 주기가 도래되는 경우 중 적어도 하나의 경우에 수행되는 것을 특징으로 하는 CRC를 이용한 메모리 보호 파일의 위변조 검출 방법.

청구항 5

제1항 내지 제 4항 중 어느 한 항에 따른 CRC를 이용한 메모리 보호 파일의 위변조 검출 방법을 구현하기 위한 프로그램 명령어가 기록된, 컴퓨터가 판독 가능한 기록매체.

청구항 6

클라이언트 단말에 메모리 보호 파일을 제공하는 서버의 CRC를 이용한 메모리 보호 파일의 위변조 검출 방법에 있어서,

메모리 보호 파일을 메모리 로드한 후, 메모리 주소가 변화되지 않는 데이터를 추출하는 단계;

상기 추출된 데이터에 대한 CRC 값을 생성한 후 상기 추출된 데이터가 로드된 메모리 주소들을 매핑하여 저장하는 단계;

상기 클라이언트 단말에 상기 메모리 보호 파일을 제공하는 단계;

상기 추출된 데이터의 메모리 주소들을 상기 클라이언트 단말에 통보하고, 상기 클라이언트 단말로부터 상기 추출된 데이터의 메모리 주소에 대한 CRC 값을 피드백받는 단계; 및

상기 피드백받은 CRC 값과 상기 추출된 데이터에 대한 CRC 값을 비교 분석하여, 상기 메모리 보호 파일의 위변조 여부를 확인하는 단계를 포함하는 CRC를 이용한 메모리 보호 파일의 위변조 검출 방법.

청구항 7

제6항에 있어서, 상기 메모리 보호 파일은

파일 실행을 위해 메모리 로드될 때마다 메모리 주소가 변경되는 함수들을 구비한 파일인 것을 특징으로 하는 CRC를 이용한 메모리 보호 파일의 위변조 검출 방법.

청구항 8

제6항에 있어서, 상기 추출된 데이터는

메모리 로드 동작을 기 설정횟수 반복 수행한 후 메모리 주소가 변경되지 않는 데이터를 선별하는 방식으로 추출되거나, 메모리 보호 함수로 기 등록된 함수들에 대응되는 데이터를 선별하는 방식으로 추출되거나, 또는 메모리 보호 주소로 기 등록된 메모리 주소들에 저장된 데이터를 선별하는 방식으로 추출되는 것을 특징으로 하는 CRC를 이용한 메모리 보호 파일의 위변조 검출 방법.

청구항 9

삭제

청구항 10

제6항 내지 제 8항 중 어느 한 항에 따른 CRC를 이용한 메모리 보호 파일의 위변조 검출 방법을 구현하기 위한 프로그램 명령어가 기록된, 컴퓨터가 판독 가능한 기록매체.

청구항 11

메모리 보호 파일을 메모리 로드한 후, 메모리 주소가 변화되지 않는 데이터를 추출하고, 상기 추출된 데이터의 CRC 값과 메모리 주소를 포함하는 파일 시그니처를 생성 및 저장하는 파일 시그니처 관리부;

클라이언트 단말에 상기 메모리 보호 파일을 제공하는 파일 제공부; 및

상기 파일 시그니처에 포함된 메모리 주소를 상기 클라이언트 단말에 통보한 후, 상기 클라이언트 단말로부터 피드백되는 CRC 값과 상기 파일 시그니처에 포함된 CRC 값을 비교 분석하여, 상기 메모리 보호 파일의 위변조 여부를 확인하는 파일 위변조 감지부를 포함하는 파일 제공 서버.

청구항 12

삭제

청구항 13

제11항에 있어서, 상기 파일 시그니처 관리부는

상기 추출된 데이터를 함수별로 구분하여 CRC 값과 메모리 주소를 획득함으로써, 다수의 파일 시그니처를 생성 및 저장하는 것을 특징으로 하는 파일 제공 서버.

청구항 14

제13항에 있어서, 상기 파일 위변조 감지부는

상기 다수의 파일 시그니처 중 하나를 랜덤 선택하고, 상기 랜덤 선택된 파일 시그니처에 포함된 메모리 주소를 상기 클라이언트 단말에 제공하여, 상기 클라이언트 단말에 상기 메모리 주소에 대응되는 CRC 값의 제공을 요청하는 것을 특징으로 하는 파일 제공 서버.

청구항 15

제11항에 있어서, 상기 파일 시그니처 관리부는

상기 추출된 데이터에 대한 CRC 값을 생성한 후 상기 추출된 데이터가 로드된 메모리 주소들을 매핑하여 파일 시그니처를 생성 및 저장하는 것을 특징으로 하는 파일 제공 서버.

청구항 16

제15항에 있어서, 상기 파일 위변조 감지부는

상기 파일 시그니처에 포함된 메모리 주소들을 상기 클라이언트 단말에 제공하여, 상기 클라이언트 단말에 상기 메모리 주소들에 대응되는 CRC 값의 제공을 요청하는 것을 특징으로 하는 파일 제공 서버.

발명의 설명

기 술 분 야

[0001] 본 발명은 순환 중복 검사(CRC; Cyclic Redundancy Check) 알고리즘을 이용한 파일 위변조 검출 방법에 관한 것으로, 특히 메모리 보호 기술이 적용된 파일에 대해서도 CRC 알고리즘을 이용한 파일 위변조 동작을 수행할 수 있도록 하는 CRC 알고리즘을 이용한 메모리 보호 파일의 위변조 검출 방법 및 서버에 관한 것이다.

배 경 기 술

[0002] CRC(cyclic redundancy check)는 파일 변경 사항을 확인하기 위한 알고리즘으로, 이는 파일 실행 전후의 CRC 값을 획득 및 비교 분석함으로써, 공격자에 의한 파일 위변조 여부를 간단하게 확인할 수 있도록 해준다(국내공개특허 제10-2010-0100488호 참고).

[0003] 한편, 근래에 게임 등의 프로그램을 해킹하기 위한 툴(Tool)로써, 프로그램(또는 파일)이 실행될 때, 프로그램이 동작되는 클라이언트 단말의 메모리 상에 위치한 코드를 수정하여 게임의 원래 동작방식과 다르게 동작하도록 하는 해킹 툴들이 많이 유포되고 있다.

[0004] 이러한 메모리 조작 방식의 해킹 기술은 실행 파일 자체의 크랙(Crack)과 동일한 효과를 낼 뿐만 아니라, 파일 실행 도중에도 메모리 해킹 동작이 수행될 수 있도록 하므로, 실행 프로그램 자체의 크랙보다 실질적으로는 더

큰 피해를 주게 되는 문제가 있다.

[0005] 이에 최근에는 해킹에 의한 메모리 조작이 발생하는 것을 사전에 방지하기 위해, 파일이 로드되는 메모리 주소를 메모리 로드시마다 랜덤하게 변경시켜 주는 ASLR(Address Space Layout Randomization)이 제안되었다.

[0006] 그런데, 이와 같이 ASLR이 적용된 파일이 메모리 로드시마다 메모리 주소가 변경되면, 해당 파일에 대응되는 CRC 값 또한 메모리 로드시마다 수시로 변경되는 현상이 발생하게 된다.

[0007] 따라서 종래의 CRC 체크를 이용한 파일 위변조 검출 방법은 ASLR이 적용된 파일에 대해서는 파일 위변조 검출 동작을 수행할 수 없게 되는 문제가 발생하게 된다. 즉, ASLR이 적용된 파일은 메모리 로드시마다 CRC 값이 변경되는 특성으로 인해, 동일 파일에 대해서는 서로 상이한 CRC 값이 생성될 수 있고, 이에 따라 파일 위변조 여부와 상관없이 무조건적으로 파일이 위변조되었다고 판단하게 되는 오류가 발생하게 된다.

발명의 내용

해결하려는 과제

[0008] 본 발명의 목적은 ASLR 이 적용된 파일과 같이 메모리 로드시마다 메모리 주소가 임의 변경되는 특징을 가지는 파일에 대해서도 CRC 알고리즘을 이용한 파일 위변조 검출 동작을 수행할 수 있도록 하는 CRC 알고리즘을 이용한 메모리 보호 파일의 위변조 검출 방법 및 서버를 제공하고자 한다.

[0009] 본 발명의 목적은 이상에서 언급한 목적으로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 본 발명이 속하는 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0010] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 클라이언트 단말에 메모리 보호 파일을 제공하는 서버의 CRC를 이용한 메모리 보호 파일의 위변조 검출 방법은, 상기 메모리 보호 파일을 메모리 로드한 후, 메모리 주소가 변화되지 않는 데이터를 추출하는 단계; 상기 추출된 데이터를 함수별로 구분하고 함수별 CRC 값을 생성한 후 메모리 주소를 매핑하여, 다수의 파일 시그니처를 생성 및 저장하는 단계; 상기 클라이언트 단말에 상기 메모리 보호 파일을 제공하는 단계; 다수의 파일 시그니처 중 하나를 랜덤 선택한 후, 상기 랜덤 선택된 파일 시그너처에 포함된 메모리 주소를 상기 클라이언트 단말에 통보하고, 상기 클라이언트 단말로부터 상기 통보한 메모리 주소에 저장된 데이터에 대한 CRC 값을 피드백받는 단계; 및 상기 피드백받은 CRC 값과 상기 랜덤 선택된 파일 시그너처에 포함된 CRC 값을 비교 분석하여, 상기 메모리 보호 파일의 위변조 여부를 확인하는 단계를 포함할 수 있다.

[0011] 상기 메모리 보호 파일은 파일 실행을 위해 메모리 로드될 때마다 메모리 주소가 변경되는 함수들을 구비한 파일인 것을 특징으로 한다.

[0012] 상기 추출된 데이터는 메모리 로드 동작을 기 설정횟수 반복 수행한 후 메모리 주소가 변경되지 않는 데이터를 선별하는 방식으로 추출되거나, 메모리 보호 함수로 기 등록된 함수들에 대응되는 데이터를 선별하는 방식으로 추출되거나, 또는 메모리 보호 주소로 기 등록된 메모리 주소들에 저장된 데이터를 선별하는 방식으로 추출되는 것을 특징으로 한다.

[0013] 상기 CRC 값을 피드백받는 단계는 상기 클라이언트 단말이 파일 실행을 요청하는 경우, 상기 클라이언트 단말의 파일 실행 결과치가 비정상적인 경우, 상기 클라이언트 단말로부터 해킹 가능성이 있음을 통보받는 경우, 서버 관리자가 파일 위변조 감시를 수동 요청하는 경우, 및 기 설정된 파일 위변조 감시 주기가 도래되는 경우 중 적어도 하나의 경우에 수행되는 것을 특징으로 한다.

[0014] 상기 목적을 달성하기 위한 본 발명의 다른 실시예에 따른 클라이언트 단말에 메모리 보호 파일을 제공하는 서버의 CRC를 이용한 메모리 보호 파일의 위변조 검출 방법은, 메모리 보호 파일을 메모리 로드한 후, 메모리 주소가 변화되지 않는 데이터를 추출하는 단계; 상기 추출된 데이터에 대한 CRC 값을 생성한 후 상기 추출된 데이터가 로드된 메모리 주소들을 매핑하여 저장하는 단계; 상기 클라이언트 단말에 상기 메모리 보호 파일을 제공하는 단계; 상기 추출된 데이터의 메모리 주소들을 상기 클라이언트 단말에 통보하고, 상기 클라이언트 단말로부터 상기 추출된 데이터의 메모리 주소에 대한 CRC 값을 피드백받는 단계; 및 상기 피드백받은 CRC 값과 상기 추출된 데이터에 대한 CRC 값을 비교 분석하여, 상기 메모리 보호 파일의 위변조 여부를 확인하는 단계를 포함

할 수 있다.

[0015] 상기 메모리 보호 파일은 파일 실행을 위해 메모리 로드될 때마다 메모리 주소가 변경되는 함수들을 구비한 파일인 것을 특징으로 한다.

[0016] 상기 추출된 데이터는 메모리 로드 동작을 기 설정횟수 반복 수행한 후 메모리 주소가 변경되지 않는 데이터를 선별하는 방식으로 추출되거나, 메모리 보호 함수로 기 등록된 함수들에 대응되는 데이터를 선별하는 방식으로 추출되거나, 또는 메모리 보호 주소로 기 등록된 메모리 주소들에 저장된 데이터를 선별하는 방식으로 추출되는 것을 특징으로 한다.

[0017] 상기 CRC 값을 피드백받는 단계는 상기 클라이언트 단말이 파일 실행을 요청하는 경우, 상기 클라이언트 단말의 파일 실행 결과치가 비정상적인 경우, 상기 클라이언트 단말로부터 해킹 가능성이 있음을 통보받는 경우, 서버 관리자가 파일 위변조 감시를 수동 요청하는 경우, 및 기 설정된 파일 위변조 감시 주기가 도래되는 경우 중 적어도 하나의 경우에 수행되는 것을 특징으로 한다.

[0018] 상기 목적을 달성하기 위한 본 발명의 또 다른 실시예에 따른 파일 제공 서버는, 메모리 보호 파일을 메모리 로드한 후, 메모리 주소가 변화되지 않는 데이터를 추출하고, 상기 추출된 데이터의 CRC 값과 메모리 주소를 포함하는 파일 시그니처를 생성 및 저장하는 파일 시그니처 관리부; 상기 클라이언트 단말에 상기 메모리 보호 파일을 제공하는 파일 제공부; 및 상기 파일 시그니처에 포함된 메모리 주소를 상기 클라이언트 단말에 통보한 후, 상기 클라이언트 단말로부터 피드백되는 CRC 값과 상기 파일 시그니처에 포함된 CRC 값을 비교 분석하여, 상기 메모리 보호 파일의 위변조 여부를 확인하는 파일 위변조 감지부를 포함할 수 있다.

[0019] 상기 메모리 보호 파일은 파일 실행을 위해 메모리 로드될 때마다 메모리 주소가 변경되는 함수들을 구비한 파일인 것을 특징으로 한다.

[0020] 상기 파일 시그니처 관리부는 상기 추출된 데이터를 함수별로 구분하여 CRC 값과 메모리 주소를 획득함으로써, 다수의 파일 시그니처를 생성 및 저장하는 것을 특징으로 한다.

[0021] 상기 파일 위변조 감지부는 상기 다수의 파일 시그니처 중 하나를 랜덤 선택하고, 상기 랜덤 선택된 파일 시그니처에 포함된 메모리 주소를 상기 클라이언트 단말에 제공하여, 상기 클라이언트 단말에 상기 메모리 주소에 대응되는 CRC 값의 제공을 요청하는 것을 특징으로 한다.

[0022] 상기 파일 시그니처 관리부는 상기 추출된 데이터에 대한 CRC 값을 생성한 후 상기 추출된 데이터가 로드된 메모리 주소들을 매핑하여 파일 시그니처를 생성 및 저장하는 것을 특징으로 한다.

[0023] 상기 파일 위변조 감지부는 상기 파일 시그니처에 포함된 메모리 주소들을 상기 클라이언트 단말에 제공하여, 상기 클라이언트 단말에 상기 메모리 주소들에 대응되는 CRC 값의 제공을 요청하는 것을 특징으로 한다.

발명의 효과

[0024] 본 발명에 따른 메모리 로드시마다 메모리 주소가 임의 변경되는 메모리 보안 파일이 항상 고정된 값의 CRC를 생성할 수 있도록 함으로써, 메모리 보안 파일 또한 CRC 알고리즘을 이용하여 파일 위변조 검출 동작을 간단히 수행할 수 있도록 한다.

[0025] 또한, 서버와 클라이언트 단말이 연동하여 파일 위변조 검출 동작을 수행함으로써, 공격자는 파일 위변조 검출 동작 수행 여부를 검출하기가 어렵고, 또한 분석자가 현재 어느 부분에 대한 분석을 수행하는지도 검출하기가 어려지도록 한다. 즉, 공격자가 인지하지 못하는 상태에서 파일 위변조 검출 동작을 수행할 수 있도록 해준다.

도면의 간단한 설명

[0026] 도1은 본 발명의 일 실시예에 따른 CRC 알고리즘을 이용한 메모리 보호 파일의 위변조 검출 시스템을 도시한 도면이다.

도2는 본 발명의 일 실시예에 따른 CRC를 이용한 메모리 보호 파일의 위변조 검출 방법을 개략적으로 설명하기

위한 도면이다.

도3은 본 발명의 일 실시예에 따른 파일 시그니처 생성 단계를 보다 상세히 설명하기 위한 도면이다.

도4는 본 발명의 일 실시예에 따른 파일 위변조 확인 단계를 보다 상세히 설명하기 위한 도면이다.

도5는 본 발명의 다른 실시예에 따른 CRC를 이용한 메모리 보호 파일의 위변조 검출 방법을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0027] 이하, 첨부된 도면을 참조하여 본 발명의 각 실시예에 따른 온라인 게임 등급 표시 아이콘 크기 제어방법 및 제어장치 에 대하여 설명하기로 한다.

[0028] 이하의 실시 예는 본 발명의 이해를 돕기 위한 상세한 설명이며, 본 발명의 권리 범위를 제한하는 것이 아님은 당연할 것이다. 따라서, 본 발명과 동일한 기능을 수행하는 균등한 발명 역시 본 발명의 권리 범위에 속할 것이다.

[0029] 또한 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.

[0030] 도1은 본 발명의 일 실시예에 따른 CRC 알고리즘을 이용한 메모리 보호 파일의 위변조 검출 시스템을 도시한 도면이다.

[0031] 도1을 참고하면, 본 발명의 시스템은 크게 클라이언트 단말(200)에게 메모리 보호 파일을 제공하고, 이와 더불어 메모리 보호 파일이 클라이언트 단말(200)상에서 위변조되었는지를 체크할 수 있도록 하는 서버(100)와, 서버(100)로부터 제공되는 파일을 실행하는 클라이언트 단말(200)을 포함하여 구성될 수 있다.

[0032] 이때, 메모리 보호 파일은 ASLR와 같은 메모리 보호 기술이 적용된 파일로, 파일 실행을 위해 메모리 로드될 때마다 메모리 주소가 랜덤하게 변경되는 파일로, 더욱 자세하게는, Image Base, Stack, Heap, PEB(Process Environment Block), TEB(Thread Environment Block) 등의 함수에 대응되는 메모리 주소가 랜덤하게 변화되고, 나머지 함수들을 고정된 메모리 주소를 가지게 되는 특징을 가진다.

[0033] 그러나 종래에는 이러한 함수 구별 없이 메모리 보호 파일의 CRC 값을 생성하였으며, 이에 따라 메모리 로드시마다 CRC 값이 변화되는 현상이 발생하게 된다.

[0034] 이에 본 발명에서는 고정된 메모리 주소를 가지는 함수만을 이용하여 CRC 값을 생성하도록 함으로써, ASLR 기술이 적용된 파일 또한 고정된 CRC 값을 가지도록 하고, 이를 기반으로 파일 위변조 여부를 검출할 수 있도록 하고자 한다.

[0035] 본 발명의 서버(100)는 파일 시그니처 생성부(110), 파일 제공부(120), 파일 위변조 감시부(130), 파일 DB(DataBase)(140), 메모리(150) 및 통신부(160) 등을 포함할 수 있다.

[0036] 파일 시그니처 생성부(110)는 ASLR 기술이 적용된 파일(이하, 보호대상 파일)을 메모리 로드한 후, 메모리 로드된 데이터 중에서 메모리 로드함과 동시에 메모리 주소가 변하지 않는 주소불변 데이터를 추출하도록 한다. 그리고 주소불변 데이터를 함수마다 끊어서 다수의 CRC 값을 생성하고, 다수의 CRC 값 각각에 해당 함수가 저장된 메모리 주소를 매핑하여 보호대상 파일에 대응되는 다수의 파일 시그니처를 생성 및 저장하도록 한다.

[0037] 참고로, 파일 실행을 위해 메모리에 로드된 데이터는 핵사 코드 또는 어셈블리 언어와 같이 서버내 중앙 처리장치가 직접 읽고 쓸 수 있는 기계어로, 동일 함수에 대응되는 데이터라 할지라도 메모리 주소값에 따라 데이터 값이 달라지는 특징을 가진다.

[0038] 파일 제공부(120)는 보호대상 파일을 저장 및 관리하고, 클라이언트 단말(200)의 필요시에 보호대상 파일을 선택 및 제공하도록 한다.

[0039] 파일 위변조 감시부(130)는 보호대상 파일에 대한 위변조 감시 이벤트가 발생하면, 보호대상 파일에 대응되는 다수의 파일 시그니처 중 하나를 랜덤 선택한 후, 랜덤 선택된 파일 시그니처에 포함된 메모리 주소를 클라이언트 단말(200)에 제공하도록 한다. 이에 클라이언트 단말(200)이 해당 메모리 영역에 저장된 데이터에 대응되는 CRC 값을 생성하여 전송하면, 전송된 CRC 값과 랜덤 선택된 파일 시그니처에 포함된 CRC 값을 비교 분석하여, 파일 위변조 여부를 검출하도록 한다.

[0040] 이때, 파일 위변조 감시 이벤트는 클라이언트 단말(200)이 파일 실행을 요청하는 경우, 클라이언트 단말(200)의 파일 실행 결과치가 비정상적인 경우, 클라이언트 단말(200)로부터 해킹 가능성이 있음을 통보받는 경우, 서버 관리자가 파일 위변조 감시를 수동 요청하는 경우, 및 기 설정된 파일 위변조 감시 주기가 도래되는 경우 등에서 다양하게 발생될 수 있을 것이다.

[0041] 파일 DB(DataBase)(140)는 클라이언트 단말(200)에 제공될 다수의 파일을 저장 및 관리한다.

[0042] 메모리(150)는 RAM, ROM 등의 반도체 기억 장치로 구현되며, 사용자에 의해 실행 요청한 파일이 기계 언어화(예를 들어, 핵사 코드, 어셈블리 언어)되어 로드되어, 서버(200)의 중앙처리장치(미도시)가 메모리 로드된 파일을 직접 읽기나 쓰기를 할 수 있도록 한다.

[0043] 통신부(160)는 클라이언트 단말(200)과의 유선 또는 무선 통신 채널을 형성하고, 이를 통해 각종 데이터를 송수신하도록 한다.

[0044] 계속하여, 본 발명의 클라이언트 단말(200)는 통신부(210), 파일 수신부(220), 파일 실행부(230), 및 CRC 생성부(240) 등을 포함할 수 있다.

[0045] 통신부(210)는 서버(100)과의 유선 또는 무선 통신 채널을 형성하고, 이를 통해 각종 데이터를 송수신하도록 한다.

[0046] 파일 수신부(220)는 서버(100)로부터 제공되는 파일을 수신 및 저장한다.

[0047] 파일 실행부(230)는 서버(100)로부터 제공된 파일을 실제 실행하되, 파일 실행이 요청되거나, 파일 실행 결과치가 비정상적이거나, 또는 해킹 가능성이 있으면, CRC 생성부(240)를 통해 파일의 CRC 값을 획득한 후 서버(100)에 제공하여 파일 위변조 확인받도록 한다. 만약, 실행 요청된 또는 실행 중인 파일이 위변조된 파일임이 확인되면, 파일 실행을 종료하는 등의 후속 조치를 취하여 이로 인한 부가적인 피해가 발생하지 않도록 해준다.

[0048] CRC 생성부(240)는 서버(100)가 통보한 메모리 주소에 접근한 후, CRC 알고리즘을 통해 해당 메모리 영역에 저장된 데이터에 대한 CRC 값을 생성하도록 한다. 이때, CRC 알고리즘은 서버(100)가 사용하는 CRC 알고리즘과 동일한 알고리즘인 것이 바람직할 것이다.

[0049] 도2는 본 발명의 일 실시예에 따른 CRC를 이용한 메모리 보호 파일의 위변조 검출 방법을 개략적으로 설명하기 위한 도면이다.

[0050] 도2를 참고하면, 본 발명의 방법은 크게 보호대상 파일에 대응되는 다수의 파일 시그니처를 생성하는 단계(S10), 보호대상 파일을 클라이언트 단말(200)에 제공하는 단계(S20), 및 다수의 파일 시그니처 중 하나를 통해 파일 위변조 여부를 확인하는 단계(S30) 등을 포함할 수 있다.

[0051] 이하, 도3 내지 도4를 참고하여 본 발명의 파일 위변조 검출 방법을 보다 상세히 설명하면 다음과 같다.

[0052] 도3은 본 발명의 일 실시예에 따른 파일 시그니처 생성 단계를 보다 상세히 설명하기 위한 도면이다.

[0053] 먼저, 보호대상 파일을 메모리 로드하고(S11), 메모리 로드된 데이터 중에서 메모리 주소가 변하지 않는 데이터를 추출하도록 한다(S12).

[0054] 단계 S12에서는 메모리 로드 동작을 기 설정횟수 반복 수행한 후 메모리 주소가 변경되지 않는 데이터만을 선별하는 방식으로 데이터를 추출하거나, 사용자에 의해 메모리 보호 함수로 등록된 함수들에 대응되는 데이터를 주소불변 데이터로 획득하는 방식으로 데이터를 추출하거나, 사용자에 의해 메모리 보호 주소로 등록된 메모리 주소들에 로드된 데이터를 획득하는 방식으로 데이터를 추출할 수 있을 것이다. 물론, 상기의 방법 이외에 메모리

주소가 변하지 않는 데이터를 획득할 수 있는 방법이 있다면, 이 또한 다양하게 적용될 수 있을 것이다.

[0055] 단계 S12를 통해 추출된 데이터를 함수별로 구분하고(S13), 함수별로 구분된 데이터 각각에 대해 CRC 알고리즘을 적용하여 다수의 함수 각각에 대응되는 CRC 값을 생성하도록 한다(S14).

[0056] 그리고 서로 대응되는 CRC 값과 메모리 주소를 함수별로 매핑하여, 보호대상 파일에 대응되는 다수의 파일 시그니처를 생성하고 저장하도록 한다(S15).

[0057] 도4는 본 발명의 일 실시예에 따른 파일 위변조 확인 단계를 보다 상세히 설명하기 위한 도면이다.

[0058] 도4에서는, 설명의 편이를 위해 클라이언트 단말(200)이 파일 실행을 요청하여 파일 위변조 감시 이벤트가 발생하고, 이에 따른 파일 위변조 확인 동작이 수행되는 경우에 한해 설명하기로 한다.

[0059] 만약, 클라이언트 단말(200)이 서버(100)로부터 제공받은 파일을 선택한 후 실행 요청하면(S31), 서버(100)는 이에 응답하여 파일 위변조 확인 이벤트를 발생한다(S32).

[0060] 그러면 서버(100)는 클라이언트 단말(200)이 실행 요청한 파일에 관련된 다수의 파일 시그니처들 중 하나를 랜덤 선택하고(S33), 랜덤 선택된 파일 시그니처에 포함된 메모리 주소를 클라이언트 단말(200)에 통보하여, 클라이언트 단말(200)이 해당 메모리 주소에 대응되는 CRC 값을 생성 및 피드백하도록 한다(S34).

[0061] 한편, 클라이언트 단말(200)는 해당 파일을 자신의 메모리에 로드한 후(S35), 서버(100)로부터 특정 메모리 주소를 통보받으면, 해당 메모리 주소에 접근, 이에 저장된 데이터를 기반으로 CRC 값을 생성하여 서버(100)에 전송한다(S36, S37).

[0062] 그러면, 서버(100)는 랜덤 선택된 파일 시그니처에 포함된 CRC 값과 클라이언트 단말(200)이 전송한 CRC 값을 비교한 후(S38), 두 값이 불일치하는 경우에는 클라이언트 단말(200)에 제공된 파일이 위변조되었다고 판단하고 해당 파일의 실행을 불허하고(S39), 그렇지 않으면 클라이언트 단말(200)에 제공된 파일이 위변조되지 않다고 판단한 후 해당 파일의 실행을 허용하도록 하도록 한다(S310).

[0063] 그러면, 클라이언트 단말(200)은 해당 파일이 위변조되지 않았음이 확인된 경우에만 파일을 실행하기 시작하고(S311), 이에 따라 해킹에 의한 메모리 조작 동작에 의한 각종 피해 상황의 발생을 사전에 방지할 수 있게 된다.

[0064] 이와 같이, 본 발명에서는 ASLR와 같은 메모리 보호 기술이 적용된 파일에 대해서도 항상 일정한 CRC 값이 생성될 수 있도록 함으로써, CRC 체크 기술을 이용한 파일 위변조 검출 동작이 수행될 수 있도록 해준다.

[0065] 또한, 파일 위변조 검출 동작을 파일 함수 단위로 수행할 수 있도록 함으로써, CRC 값 생성에 소용되는 부하를 최소화하고, 최종적으로는 파일 위변조 검출 동작에 소용되는 처리 부하가 전체적으로 감소될 수 있도록 한다.

[0066] 다만, 필요한 경우, 도5의 방법을 통해 파일 위변조 검출 동작을 파일 함수 단위 뿐 만 아니라 파일 단위로도 파일 위변조 상황을 검출할 수도 있도록 한다.

[0067] 도5는 본 발명의 다른 실시예에 따른 CRC를 이용한 메모리 보호 파일의 위변조 검출 방법을 설명하기 위한 도면이다.

[0068] 도5를 참고하면, 본 발명의 방법은 크게 보호대상 파일에 대응되는 하나의 파일 시그니처를 생성하는 단계(S40), 보호대상 파일을 클라이언트 단말(200)에 제공하는 단계(S50), 및 파일 시그니처 하나를 통해 파일 위변조 여부를 확인하는 단계(S60) 등을 포함할 수 있다.

[0069] 이하, 각 단계별 동작을 보다 상세히 살펴보면 다음과 같다.

[0070] 먼저, 보호대상 파일을 메모리 로드하고(S41), 앞서 설명된 바와 같이 메모리 로드된 데이터 중에서 메모리 주소가 변하지 않는 데이터를 추출하도록 한다(S42). 그리고 추출된 데이터 모두를 기반으로 CRC 값을 생성하고(S43), 추출된 데이터가 저장된 적어도 하나의 메모리 주소를 매핑하여 하나의 파일 시그니처를 생성 및 저장하

도록 한다(S44).

[0071] 이러한 상태에서 특정 클라이언트 단말(200)이 파일 제공을 요청하면, 서버(100)는 해당 클라이언트 단말(200)이 요청한 파일을 선택 및 제공하도록 한다(S50).

[0072] 그러고 나서, 파일 위변조 감시 이벤트가 발생하면(S61), 서버(100)는 클라이언트 단말(200)에 파일 시그니처에 포함된 메모리 주소들을 통보하여, 클라이언트 단말(200)이 해당 메모리 주소들에 대응되는 CRC 값을 생성 및 피드백하도록 한다(S62).

[0073] 클라이언트 단말(200)이 이에 응답하여 파일을 메모리 로드한 후 해당 메모리 주소들에 저장된 데이터들을 기반으로 CRC 값을 생성 및 제공하고 서버(100)가 이를 수신하면(S63), 서버(100)는 파일 시그니처에 포함된 CRC 값과 수신한 CRC 값을 비교 분석하여 파일 위변조 여부를 확인하도록 한다. 즉, 저장된 CRC 값과 수신한 CRC 값이 일치하는 경우에는 파일이 위변조되지 않았음을, 그렇지 않은 경우에는 해당 파일이 위변조되었음을 확인하도록 한다(S64).

[0074] 이상에서 전술한 바와 같은 이를 구현하기 위한 프로그램 명령어로서 구현될 수 있으며, 이러한 프로그램 명령어를 기록한 컴퓨터로 읽힐 수 있는 기록매체는, 일예로, ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 미디어 저장장치 등이 있다.

[0075] 또한 전술한 바와 같은 프로그램을 기록한 컴퓨터로 읽힐 수 있는 기록매체는 네트워크로 커넥션된 컴퓨터 장치에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 이 경우, 다수의 분산된 컴퓨터 중 어느 하나 이상의 컴퓨터는 상기에 제시된 기능들 중 일부를 실행하고, 그 결과를 다른 분산된 컴퓨터들 중 하나 이상에 그 실행 결과를 전송할 수 있으며, 그 결과를 전송받은 컴퓨터 역시 상기에 제시된 기능들 중 일부를 실행하여, 그 결과를 역시 다른 분산된 컴퓨터들에 제공할 수 있다.

[0076] 본 발명의 각 실시예에 따른 CRC 알고리즘을 이용한 메모리 보호 파일의 위변조 검출 방법 및 서버를 구동시키기 위한 프로그램인 애플리케이션을 기록한 기록매체를 읽을 수 있는 컴퓨터는, 일반적인 데스크 탑이나 노트북 등의 일반 PC뿐 만 아니라, 스마트 폰, 태블릿 PC, 스마트 TV 및 이동통신 단말 등의 각종 통신 장치를 포함할 수 있으며, 이뿐만 아니라, 컴퓨팅(Computing) 가능한 모든 기기로 해석되어야 할 것이다.

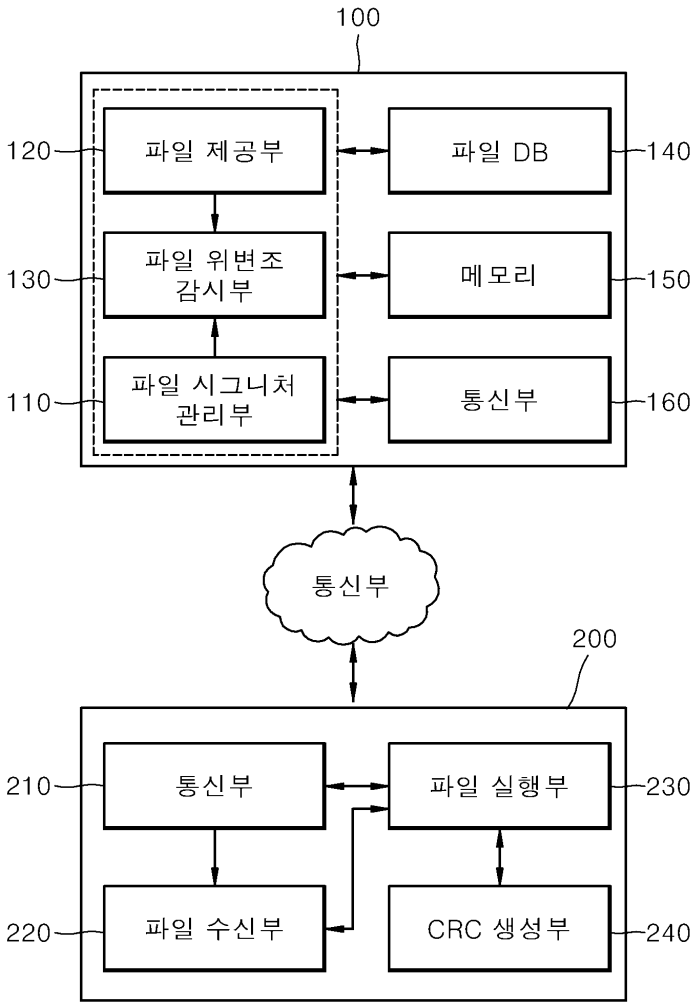
[0077] 이상에서, 본 발명의 실시예를 구성하는 모든 구성 요소들이 하나로 결합되거나 결합되어 동작하는 것으로 설명되었다고 해서, 본 발명이 반드시 이러한 실시예에 한정되는 것은 아니다. 즉, 본 발명의 목적 범위 안에서라면, 그 모든 구성 요소들이 하나 이상으로 선택적으로 결합하여 동작할 수도 있다. 또한, 그 모든 구성 요소들이 각각 하나의 독립적인 하드웨어로 구현될 수 있지만, 각 구성 요소들의 그 일부 또는 전부가 선택적으로 조합되어 하나 또는 복수 개의 하드웨어에서 조합된 일부 또는 전부의 기능을 수행하는 프로그램 모듈을 갖는 컴퓨터 프로그램으로서 구현될 수도 있다. 그 컴퓨터 프로그램을 구성하는 코드들 및 코드 세그먼트들은 본 발명의 기술분야의 당업자에 의해 용이하게 추론될 수 있을 것이다. 이러한 컴퓨터 프로그램은 컴퓨터가 읽을 수 있는 저장매체(Computer Readable Media)에 저장되어 컴퓨터에 의하여 읽혀지고 실행됨으로써, 본 발명의 실시예를 구현할 수 있다. 컴퓨터 프로그램의 저장매체로서는 자기 기록매체, 광 기록매체, 등이 포함될 수 있다.

[0078] 또한, 이상에서 기재된 "포함하다", "구성하다" 또는 "가지다" 등의 용어는, 특별히 반대되는 기재가 없는 한, 해당 구성 요소가 내재될 수 있음을 의미하는 것이므로, 다른 구성 요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있는 것으로 해석되어야 한다. 기술적이거나 과학적인 용어를 포함한 모든 용어들은, 다르게 정의되지 않는 한, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 사전에 정의된 용어와 같이 일반적으로 사용되는 용어들은 관련 기술의 문맥상의 의미와 일치하는 것으로 해석되어야 하며, 본 발명에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

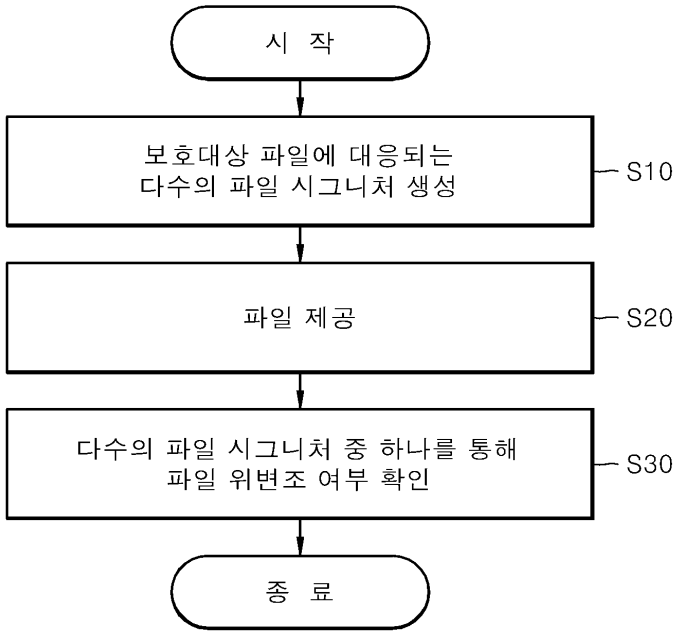
[0079] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

도면

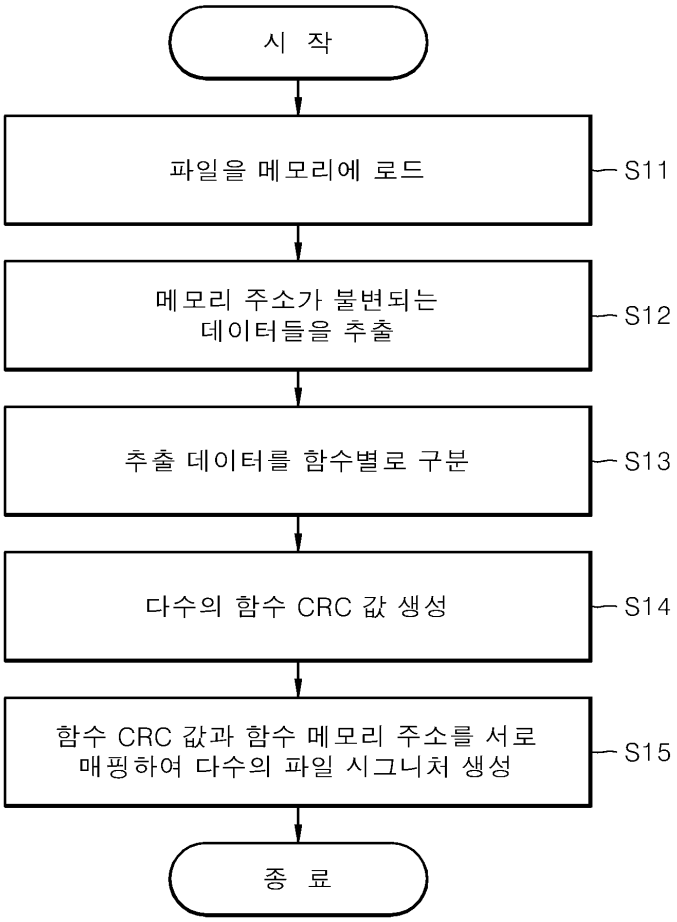
도면1


100
120
파일 제공부
파일 DB
140
130
파일 위변조 감시부
메모리
150
110
파일 시그니처 관리부
통신부
160
통신부
200
210
통신부
파일 실행부
230
220
파일 수신부
CRC 생성부
240

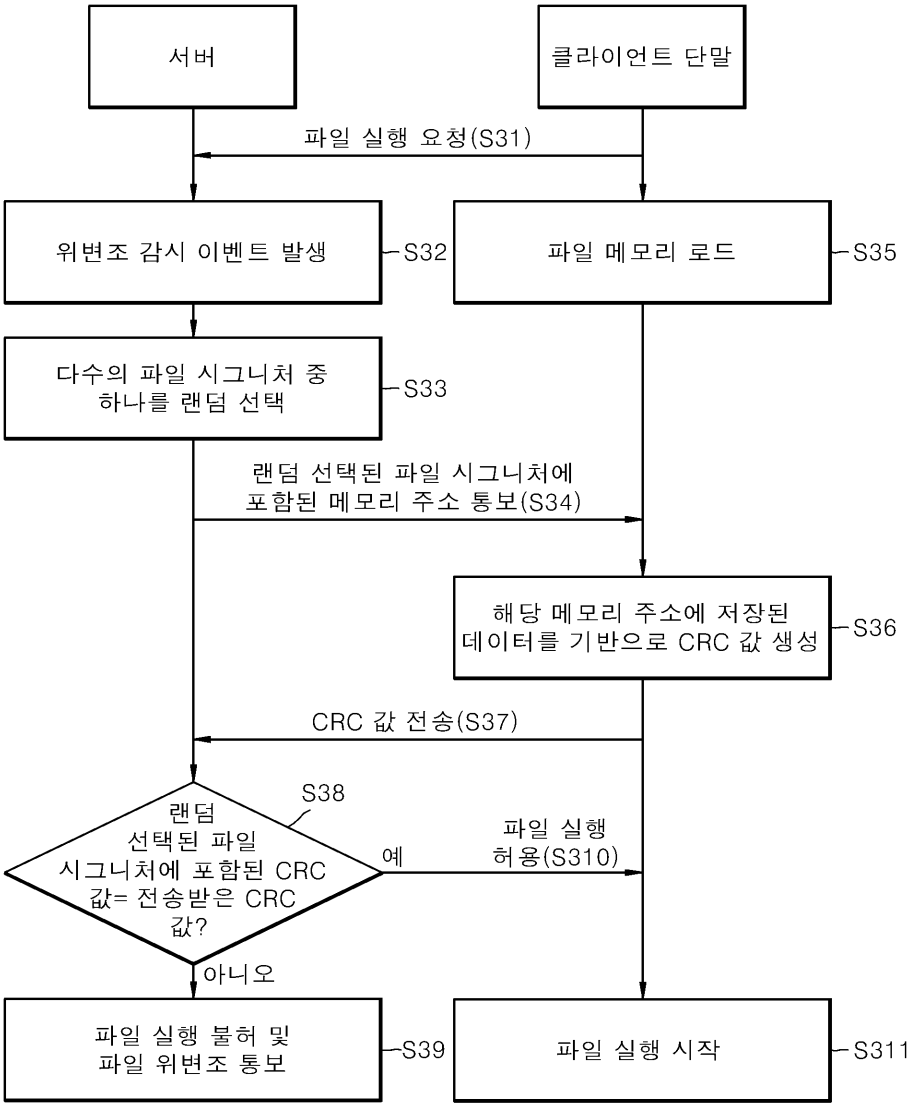
도면2


시 작
보호대상 파일에 대응되는 다수의 파일 시그니처 생성
S10
파일 제공
S20
다수의 파일 시그니처 중 하나를 통해 파일 위변조 여부 확인
S30
종 료

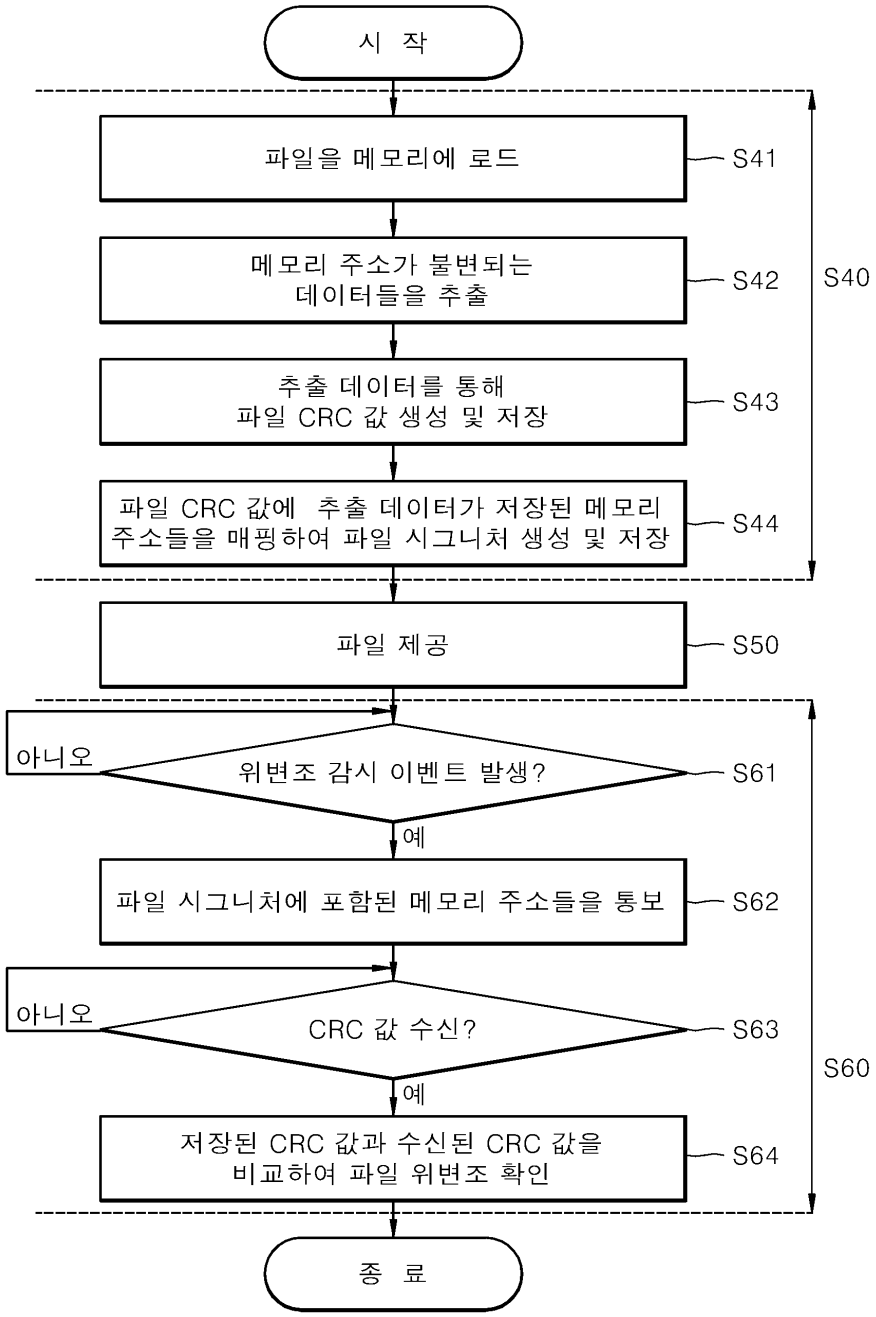
도면3


시 작
파일을 메모리에 로드
S11
메모리 주소가 불변되는
데이터들을 추출
S12
추출 데이터를 함수별로 구분
S13
다수의 함수 CRC 값 생성
S14
함수 CRC 값과 함수 메모리 주소를 서로
매핑하여 다수의 파일 시그니처 생성
S15
종 료

도면4


서버
클라이언트 단말
파일 실행 요청(S31)
위변조 감시 이벤트 발생
S32
파일 메모리 로드
S35
다수의 파일 시그니처 중 하나를 랜덤 선택
S33
랜덤 선택된 파일 시그니처에 포함된 메모리 주소 통보(S34)
해당 메모리 주소에 저장된 데이터를 기반으로 CRC 값 생성
S36
CRC 값 전송(S37)
S38
랜덤 선택된 파일 시그니처에 포함된 CRC 값= 전송받은 CRC 값?
예
파일 실행 허용(S310)
아니오
파일 실행 불허 및 파일 위변조 통보
S39
파일 실행 시작
S311

도면5


시 작
파일을 메모리에 로드
S41
메모리 주소가 불변되는
데이터들을 추출
S42
S40
추출 데이터를 통해
파일 CRC 값 생성 및 저장
S43
파일 CRC 값에 추출 데이터가 저장된 메모리
주소들을 매핑하여 파일 시그니처 생성 및 저장
S44
파일 제공
S50
아니오
위변조 감시 이벤트 발생?
S61
예
파일 시그니처에 포함된 메모리 주소들을 통보
S62
아니오
CRC 값 수신?
S63
S60
예
저장된 CRC 값과 수신된 CRC 값을
비교하여 파일 위변조 확인
S64
종 료