(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
G06F 12/16 (2006.01)
G06F 12/14 (2006.01)
G06F 12/00 (2006.01)

(45) 공고일자 2007년08월07일
(11) 등록번호 10-0746944
(24) 등록일자 2007년08월01일

(21) 출원번호 10-2006-0033914
(22) 출원일자 2006년04월14일
심사청구일자 2006년04월14일

(65) 공개번호
(43) 공개일자

(73) 특허권자 고려대학교 산학협력단

(72) 발명자 이희조

한제헌

(74) 대리인 유미특허법인

(56) 선행기술조사문헌
JP09185502 A
KR1020040066237 A
KR1020030043900 A
KR1020040086235 A

심사관 : 이종익

전체 청구항 수 : 총 11 항

(54) 정보 유출 방지 방법 및 정보 유출 방지를 수행하는프로그램이 저장된 기록 매체

(57) 요약

다양한 형태의 키로거 및 알려지지 않은 키로거를 탐지하여 정보 유출을 방지할 수 있는 방법 및 프로그램이 저장된 기록 매체가 개시된다.

정보 유출을 방지하는 프로그램은 가상의 식별 정보를 생성하고, 생성한 가상의 식별 식별 정보로 키이벤트를 발생시킨다. 그리고, 프로그램은 메모리에서 가상의 식별 정보를 검색하여 가상의 식별 정보를 발견하는 경우에 사용자에게 경고하거나 가상의 식별 정보가 발견된 메모리 영역을 사용하는 프로세스를 종료한다.

대표도

도 1

특허청구의 범위

청구항 1.

가상의 식별 정보를 생성하는 기능;

상기 가상의 식별 정보로 키이벤트를 발생시키는 기능;

메모리에서 상기 가상의 식별 정보를 검색하는 메모리 검색 기능;

상기 메모리에서 상기 가상의 식별 정보를 발견하는 경우 사용자에게 경고하는 기능을 포함하는 프로그램이 저장된 기록 매체.

청구항 2.

제1항에 있어서,

상기 메모리 검색 기능은,

상기 메모리를 사용하는 프로세스의 리스트를 획득하여 상기 리스트에 포함된 프로세스가 사용하는 메모리 영역에서 상기 가상의 식별 정보를 검색하는 프로그램이 저장된 기록 매체.

청구항 3.

제1항에 있어서,

상기 메모리 검색 기능은,

상기 메모리를 사용하는 프로세스의 리스트를 획득하고 상기 리스트에서 알려진 프로세스를 제외한 후 상기 리스트에 포함된 프로세스가 사용하는 메모리 영역에서 상기 가상의 식별 정보를 검색하는 프로그램이 저장된 기록 매체.

청구항 4.

제2항 또는 제3항에 있어서,

상기 메모리 검색 기능은,

상기 메모리 영역에서 읽고 쓰기가 모두 가능한 메모리 영역을 추출하여 추출한 메모리 영역에서 상기 가상의 식별 정보를 검색하는 프로그램이 저장된 기록 매체.

청구항 5.

가상의 식별 정보를 생성하는 가상 정보 생성 기능;

상기 가상의 식별 정보로 키이벤트를 발생시키는 키이벤트 발생 기능;

메모리를 사용하는 프로세스의 리스트를 획득하여 상기 리스트에 포함된 프로세스가 사용하는 메모리 영역에서 상기 가상의 식별 정보를 검색하는 기능;

상기 메모리 영역에서 상기 가상의 식별 정보가 검색되는 경우 상기 가상의 식별 정보가 저장된 메모리 영역을 사용하는 프로세스를 종료하는 기능을 포함하는 프로그램이 저장된 기록 매체.

청구항 6.

가상의 식별 정보를 생성하는 단계;

상기 가상의 식별 정보로 키이벤트를 발생시키는 단계;

메모리에서 상기 가상의 식별 정보를 검색하는 단계;

상기 메모리에서 상기 가상의 식별 정보를 발견하는 경우 사용자에게 경고하는 단계를 포함하는 정보 유출 방지 방법.

청구항 7.

제6항에 있어서,

상기 메모리에서 상기 가상의 식별 정보를 검색하는 단계는,

상기 메모리를 사용하는 프로세스의 리스트를 획득하는 단계;

상기 리스트에 포함된 프로세스가 사용하는 메모리 영역에서 상기 가상의 식별 정보를 검색하는 단계를 포함하는 정보 유출 방지 방법.

청구항 8.

제7항에 있어서,

상기 메모리에서 상기 가상의 식별 정보를 검색하는 단계는,

상기 리스트에서 알려진 프로세스를 제외하는 단계를 더 포함하는 정보 유출 방지 방법.

청구항 9.

제8항에 있어서,

상기 메모리에서 상기 가상의 식별 정보를 검색하는 단계는,

상기 리스트에 포함된 프로세스가 사용하는 API 함수의 분석을 통해 상기 API 함수가 메시지 후킹, 함수 후킹, 드라이버 로딩 또는 동적 연결 라이브러리 로딩을 수행하는 함수가 아닌 경우 상기 API 함수를 사용하는 프로세스를 상기 리스트에서 제외하는 단계를 더 포함하는 정보 유출 방지 방법.

청구항 10.

제7항 내지 제9항 중 어느 한에 있어서,

상기 메모리 영역에서 상기 가상의 식별 정보를 검색하는 단계는,

상기 메모리 영역에서 읽고 쓰기가 모두 가능한 메모리 영역을 추출하여 추출한 메모리 영역에서 상기 가상의 식별 정보를 검색하는 정보 유출 방지 방법.

청구항 11.

제6항 내지 제9항 중 어느 한 항에 있어서,

상기 메모리에서 상기 가상의 식별 정보가 검색되는 경우 상기 가상의 식별 정보가 저장된 메모리 영역을 사용하는 프로세스를 종료하는 단계를 더 포함하는 정보 유출 방지 방법.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 정보 유출 방지 방법 및 정보 유출 방지를 수행하는 프로그램이 저장된 기록 매체에 관한 것이다. 특히 본 발명은 다양한 형태의 키로거 및 알려지지 않은 키로거를 탐지하여 정보 유출을 방지할 수 있는 방법 및 프로그램에 관한 것이다.

전자 상거래의 확산으로 개인 정보와 관련한 보안의 중요성이 커지게 되었다. 특히, 금융 거래와 관련한 정보의 유출은 곧바로 금전적 피해로 연결되고, 여러 사람이 공용으로 사용하는 컴퓨터가 증가함에 따라 개인 정보 유출 가능성이 증가하여, 개인 정보와 관련한 보안은 큰 관심의 대상이 되었다.

개인 정보의 유출은 주로 키로거(Keylogger)라고 불리우는 프로그램에 의해 이루어진다. 키로거는 사용자의 키보드 입력 정보를 가로채 파일로 저장하거나 네트워크를 통해 원격으로 전송하는 등의 역할을 수행하는 프로그램이다. 키로거는 운영체제 레벨, 드라이버 레벨, 응용 어플리케이션 레벨 등 다양한 계층에서 존재하여 자신의 존재를 사용자에게 드러내지 않고 개인 정보를 수집한다.

개인 정보의 유출은 심각한 피해를 유발할 수 있으므로 이러한 키로거에 대응하기 위한 여러 방식이 제시되었다.

키로거에 대응하기 위해 제시된 한 방법은 인터럽트 선점에 따른 정보 유출 방지 방법이다. 이 방법을 따르는 키로거 대응 프로그램은 키로거보다 먼저 키보드 입력에 따른 인터럽트를 가로채 응용 프로그램에 전달하여 키로거에 의한 정보 유출을 방지한다. 그러나 키로거가 키보드 입력에 따른 인터럽트를 키로거 대응 프로그램보다 먼저 가로챌 수 있으므로 이 인터럽트 선점 방식은 충분한 보안을 제공하지 못한다.

키로거에 대응하기 위해 제시된 다른 방법은 키로거의 정보를 모아 패턴화하여(signature) 이 정보와 일치하는 것을 탐지하는 방법이다. 여기에서 키로거의 정보는 "프로세스 정보", "파일 정보", "저장 방식 정보", 네트워크 자원 사용 정보" 등을 포함한다. 이 방법에 따르는 키로거 탐지 프로그램은 다양한 키로거의 정보를 미리 패턴화하고 데이터베이스에 저장하여, 이 정보와 일치하는 패턴이 검색되면 사용자에게 키로거의 존재를 알린다. 그러나 이러한 키로거 정보를 이용하는 키로거 탐지 프로그램은 새로이 출현한 키로거의 패턴에 대한 데이터베이스를 획득하기 전까지는 키로거를 탐지할 수 없는 한계가 있다.

키로거에 대응하기 위해 제시된 또 다른 방법은 특정 API(application program interface)를 Hooking하려고 하는 프로세스를 찾아내는 방법이다. 일부 키로거는 특정 API 함수를 가로채 조작을 가하여(hooking) 사용자의 정보를 가로채는 방식을 이용하기 때문에 특정 API를 Hooking하는 프로세스를 찾으면 키로거를 찾을 수 있다. 하지만, 이 방식을 따르는 키로거 대응 프로그램은 API를 Hooking하지 않는 키로거를 탐지할 수 없다는 한계가 있으며, 정상적인 프로그램 중에서도 API를 Hooking하는 프로그램이 존재하기 때문에 오판의 가능성이 높다.

발명이 이루고자 하는 기술적 과제

본 발명이 이루고자 하는 기술적 과제는 다양한 형태의 키로거 및 알려지지 않은 키로거를 탐지할 수 있는 키로거 탐지를 수행하는 프로그램이 저장된 기록매체를 제공하는 것이다.

발명의 구성

본 발명의 한 특징에 따른 프로그램은 기록 매체에 저장되어 있으며, 가상의 식별 정보를 생성하는 기능과, 상기 가상의 식별 정보로 키이벤트를 발생시키는 기능과, 메모리에서 상기 가상의 식별 정보를 검색하는 메모리 검색 기능과, 상기 메모리에서 상기 가상의 식별 정보를 발견하는 경우 사용자에게 경고하는 기능을 포함한다.

이때 상기 메모리 검색 기능은 상기 메모리를 사용하는 프로세스의 리스트를 획득하여 상기 리스트에 포함된 프로세스가 사용하는 메모리 영역에서 상기 가상의 식별 정보를 검색할 수 있다.

본 발명의 다른 특징에 따른 프로그램은 기록 매체에 저장되어 있으며, 가상의 식별 정보를 생성하는 가상 정보 생성 기능과, 상기 가상의 식별 정보로 키이벤트를 발생시키는 키이벤트 발생 기능과, 메모리를 사용하는 프로세스의 리스트를 획득하여 상기 리스트에 포함된 프로세스가 사용하는 메모리 영역에서 상기 가상의 식별 정보를 검색하는 기능과, 상기 메모리 영역에서 상기 가상의 식별 정보가 검색되는 경우 상기 가상의 식별 정보가 저장된 메모리 영역을 사용하는 프로세스를 종료하는 기능을 포함한다.

본 발명의 한 특징에 따른 정보 유출 방지 방법은 가상의 식별 정보를 생성하는 단계와, 상기 가상의 식별 정보로 키이벤트를 발생시키는 단계와, 메모리에서 상기 가상의 식별 정보를 검색하는 단계와, 상기 메모리에서 상기 가상의 식별 정보를 발견하는 경우 사용자에게 경고하는 단계를 포함한다.

이때 상기 메모리에서 상기 가상의 식별 정보를 검색하는 단계는, 상기 메모리를 사용하는 프로세스의 리스트를 획득하는 단계와, 상기 리스트에 포함된 프로세스가 사용하는 메모리 영역에서 상기 가상의 식별 정보를 검색하는 단계를 포함할 수 있다.

아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

또한, 본 명세서에서 기재한 모듈(module)이란 용어는 특정한 기능이나 동작을 처리하는 하나의 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현할 수 있다.

다음은 본 발명의 실시예에 따른 키로거 탐지 프로그램(100)을 도 1을 참고하여 설명한다.

도 1은 본 발명의 실시예에 따른 키로거 탐지 프로그램(100)을 도시한 블록도이다.

도 1에 도시된 바와 같이 키로거 탐지 프로그램(100)은 메모리(1)를 검색하여 키로거를 탐지하며, 가상 식별 정보 생성 모듈(110), 키이벤트 발생 모듈(120), 메모리 검색 모듈(130), 경고 모듈(140), 키로거 강제 종료 모듈(150)을 포함한다. 메모리(1)에는 5개의 프로세스(11, 12, 13, 14, 15)와 각 프로세스가 사용하는 5개의 메모리 영역(21, 22, 23, 24, 25)이 존재한다고 가정한다. 그리고 제5 프로세스(15)는 키로거라고 가정한다. 키로거 탐지 프로그램(100) 또한 메모리(1)에 존재하지만, 설명의 편의를 위하여 별도로 도시하였다.

가상 식별 정보 생성 모듈(110)은 가상의 식별 정보를 생성한다. 특히 가상 식별 정보 생성 모듈(110)은 랜덤한 방식으로 일정한 길이의 문자열을 생성하고 이 문자열을 가상의 식별 정보로 할 수도 있다. 한편, 키로거가 이 가상의 식별 정보를 가로채지 않더라도 메모리에 이 가상의 식별 정보와 동일한 정보가 존재할 가능성을 줄이기 위하여 가상의 식별 정보는 일정 이상의 길이를 가질 필요가 있다.

키이벤트 발생 모듈(120)은 가상 식별 정보 생성 모듈(110)이 생성한 가상 식별 정보로 키이벤트를 발생시킨다. 즉, 키이벤트 발생 모듈(120)은 사용자가 가상 식별 정보를 키보드로 직접 입력할 때 발생하는 이벤트와 동일한 이벤트를 발생시켜 키로거(15)가 가상 식별 정보를 가로채도록 한다. 키로거(15)는 가상 식별 정보를 가로채는 경우 키로거(15)가 사용하는 메모리 영역인 제5 메모리 영역(25)에 이를 저장한다.

메모리 검색 모듈(130)은 메모리(1)에서 가상 식별 정보를 검색한다. 메모리 검색 모듈(130)은 메모리(1)의 전 영역을 검색할 수도 있으나, 이 경우 검색 시간이 길다. 따라서 메모리 검색 모듈(130)은 검색할 메모리 영역의 범위에 대한 축소를 수행할 수도 있다.

경고 모듈(140)은 메모리 검색 모듈(130)이 메모리(1)에서 가상 식별 정보를 발견한 경우 사용자에게 개인 정보가 유출될 수 있음을 알리거나 키로거가 존재함을 알린다.

키로거 강제 종료 모듈(150)은 메모리 검색 모듈(130)이 메모리(1)에서 가상 식별 정보를 발견한 경우 가상 식별 정보가 저장된 메모리 영역을 사용하는 프로세스를 강제로 종료한다. 키로거 강제 종료 모듈(150)은 사용자로부터 프로세스 강제 종료에 대한 확인을 받아 해당 프로세스를 종료할 수도 있다.

다음은 도 2를 참고하여 프로세스가 사용하는 메모리 영역에 대하여 설명한다.

도 2는 프로세스가 사용하는 메모리 영역을 도시한 도면이다.

도 2에 도시된 바와 같이 메모리 영역(30)은 읽기만 가능한 영역으로 사용중인 메모리 영역(31), 사용 예약된 메모리 영역(33), 사용 해제된 메모리 영역(35)를 포함하고, 읽고 쓰기가 모두 가능한 영역으로 사용중인 메모리 영역(32), 사용 예약된 메모리 영역(34), 사용 해제된 메모리 영역(36)을 포함한다.

도 2에 도시된 바와 같은 메모리 영역(30)에 대한 정보는 운영 체제(Operating System, OS)로부터 얻어질 수 있다. 운영 체제가 Windows 계열이라면, 각 프로세스가 사용하는 메모리 영역에 대한 정보는 메모리 기초 정보(Memory Basic Information, MBI)라 불리운다.

한편, 도 2에 도시된 바와 같은 메모리 영역(30)을 사용하는 프로세스가 키로거인 경우, 키로거는 메모리 영역(32)에 수집한 정보를 저장하게 된다. 즉 키이벤트 발생 모듈(120)이 가상 식별 정보로 키이벤트를 발생시키면, 키로거는 가상 식별 정보를 수집하여 메모리 영역(32)에 저장한다. 따라서 메모리 검색 모듈(130)은 메모리 영역(30) 중에서 메모리 영역(32)에 대한 검색만 수행하면 된다.

다음은 도 3을 참고하여 키로거 탐지 프로그램(100)의 동작에 대하여 설명한다.

도 3은 본 발명의 실시예에 따른 키로거 탐지 프로그램(100)의 동작을 도시한 흐름도이다.

도 3에 도시된 바와 같이 키로거 탐지 프로그램(100)의 가상 식별 정보 생성 모듈(110)은 가상의 식별 정보를 생성한다(S101).

다음, 키로거 탐지 프로그램(100)의 키이벤트 발생 모듈(120)은 가상 식별 정보 생성 모듈(110)이 생성한 가상의 식별 정보로 키이벤트를 발생시킨다(S102).

메모리 검색 모듈(130)은 메모리(1)를 사용하는 프로세스의 리스트를 운영 체제로부터 제공받는다(S103). 이때, 메모리 검색 모듈(130)이 제공받은 프로세스 리스트는 현재 실행 중인 프로세스들의 리스트이며, 이하에서는 실행중인 프로세스 리스트라 하기로 한다. 도 1을 참조하면, 실행중인 프로세스 리스트는 제1 프로세스(11), 제2 프로세스(12), 제3 프로세스(13), 제4 프로세스(14) 및 제5 프로세스(15)를 포함한다.

그리고 메모리 검색 모듈(130)은 실행중인 프로세스 리스트에서 알려진 프로세스(known process)를 제외한다(S104). 이때 알려진 프로세스는 키로거가 아닌 프로세스로서 운영 체제와 관련된 프로세스나 범용적으로 사용되는 프로세스 등에 해당한다. 또한 메모리 검색 모듈(130)은 키로거가 아닌 프로세스에 대한 정보를 미리 가지고 있어서 특정 프로세스를 키로거가 아니라고 판단할 수 있다. 알려진 프로세스가 제외된 프로세스의 리스트를 이하에서는 알려지지 않은 프로세스 리스트(unknown process list)라 하기로 하고, 알려지지 않은 프로세스 리스트에 포함된 프로세스를 알려지지 않은 프로세

스(unknown process)라고 하도록 한다. 즉, 알려지지 않은 프로세스는 키로거 탐지 프로그램(100)이 정보를 가지고 있지 않은 프로세스이다. 예를 들어 도 1에서 제1 프로세스(11)와 제3 프로세스(13)이 알려진 프로세스라고 한다면, 알려지지 않은 프로세스 리스트는 제2 프로세스(12), 제4 프로세스(14), 및 제5 프로세스(15)를 포함한다. 메모리 검색 모듈(130)은 실행중인 프로세스 리스트에 포함되어 있는 프로세스가 알려진 프로세스인지 판단할 때 프로세스의 이름으로 판단할 수도 있다. 하지만, 키로거가 알려진 프로세스와 동일한 이름을 사용할 수도 있으므로 메모리 검색 모듈(130)은 프로세스의 실행 파일의 체크섬을 검사하여 해당 프로세스가 알려진 프로세스인 지를 판단할 수도 있다.

한편, 메모리 검색 모듈(130)은 검색 대상의 프로세스의 범위를 더 축소할 수도 있다. 메모리 검색 모듈(130)은 알려지지 않은 프로세스 리스트에 포함되어 있는 프로세스의 실행 파일을 분석하여 해당 프로세스가 사용하는 API 함수를 추출한다. 그리고 메모리 검색 모듈(130)은 추출한 API 함수가 메시지 후킹, 함수 후킹, 드라이버 로딩, 동적 연결 라이브러리(dynamic linking library, DLL) 로딩을 수행하는 함수인 경우에 해당 API 함수를 사용하는 프로세스를 검색 대상의 프로세스로 하여 검색 시간을 단축할 수도 있다. 즉, 메모리 검색 모듈(130)은 알려지지 않은 프로세스 리스트에 포함된 프로세스가 사용하는 API 함수를 분석하여 해당 API 함수가 메시지 후킹, 함수 후킹, 드라이버 로딩 또는 동적 연결 라이브러리 로딩을 수행하는 함수가 아니라면 해당 API 함수를 사용하는 프로세스를 알려지지 않은 프로세스 리스트에서 제외한다.

다음, 메모리 검색 모듈(130)은 알려지지 않은 프로세스 리스트에 포함된 프로세스가 사용하는 메모리 영역을 추출한다(S105). 그리고 메모리 검색 모듈(130)은 메모리 영역에서 알려지지 않은 프로세스들이 현재 사용 중이며 읽고 쓰기가 가능한 메모리 영역(32)만을 MBI를 참고하여 더 추출한다(S106).

메모리 검색 모듈(130)은 단계 S105 및 단계 S106을 통해 추출된 메모리 영역(32)에서 가상 식별 정보의 검색을 수행한다(S107).

메모리 검색 모듈(130)이 가상 식별 정보을 발견하지 못하는 경우(S108), 키로거 탐지 프로그램(100)은 키로거가 존재하지 않는다고 판단한다(S109).

한편, 메모리 검색 모듈(130)이 가상 식별 정보을 발견하는 경우(S108), 경고 모듈(140)은 사용자에게 개인 정보가 유출될 수 있음을 알리거나 키로거가 존재함을 알린다(S110). 또한, 메모리 검색 모듈(130)이 가상 식별 정보을 발견하는 경우(S108), 키로거 강제 종료 모듈(150)은 가상 식별 정보가 발견된 메모리 영역을 사용하는 프로세스를 강제로 종료한다(S111).

이상에서 설명한 본 발명의 실시예는 장치 및 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시예의 구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 기록 매체를 통해 구현될 수도 있으며, 이러한 구현은 앞서 설명한 실시예의 기재로부터 본 발명이 속하는 기술분야의 전문가라면 쉽게 구현할 수 있는 것이다.

이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

발명의 효과

본 발명에 따르면, 키로거 탐지 프로그램은 가상 식별 정보를 키로거가 탈취하도록 하여 메모리 검사를 통해 키로거의 존재를 파악함으로써, 드라이버 레벨의 키로거를 포함한 다양한 형태 키로거에 의한 정보 유출을 방지할 수 있다.

또한, 본 발명에 따르면 알려지지 않은 키로거에 의한 정보 유출을 방지할 수 있으므로, 사용자는 새로운 키로거가 나타날 때마다 프로그램을 업데이트하지 않아도 된다.

뿐만 아니라, 본 발명에 따르면 키로거 탐지 프로그램은 검색하는 메모리의 범위를 축소함으로써 고속으로 가상 식별 정보를 검색할 수 있다.

도면의 간단한 설명

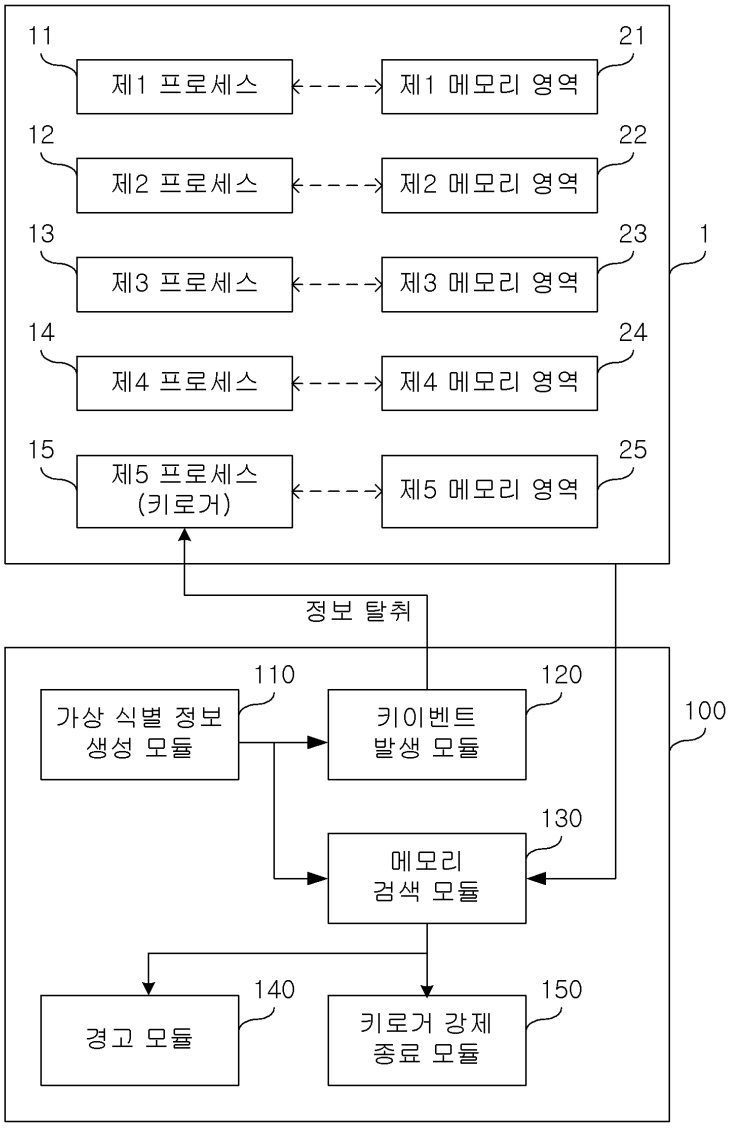
도 1은 본 발명의 실시예에 따른 키로거 탐지 프로그램을 도시한 블록도이다.

도 2는 프로세스가 사용하는 메모리 영역을 도시한 도면이다.

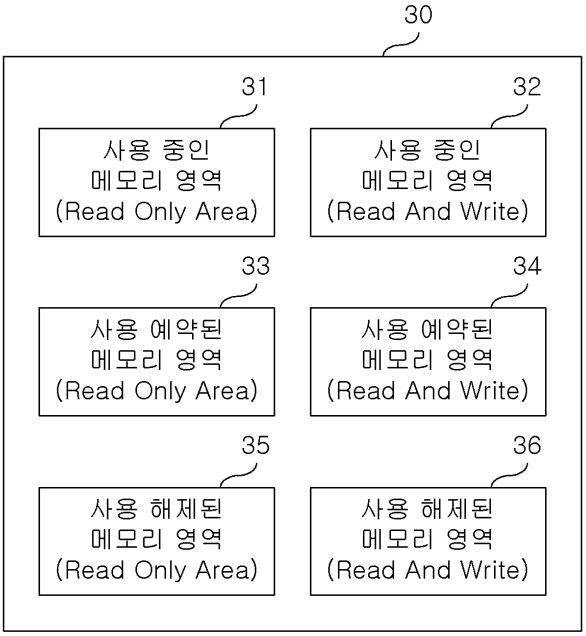
도 3은 본 발명의 실시예에 따른 키로거 탐지 프로그램의 동작을 도시한 흐름도이다.

도면

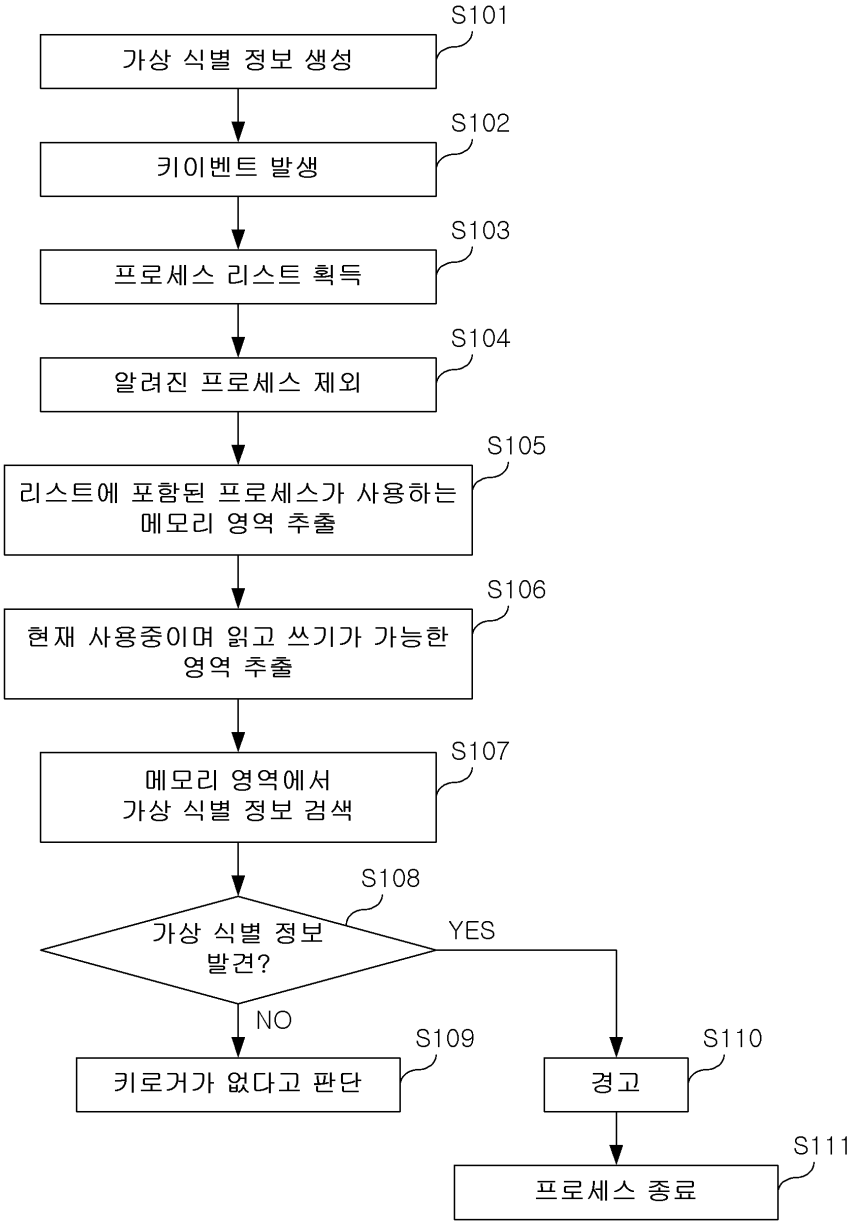
도면1



도면2


30
31
사용 중인
메모리 영역
(Read Only Area)
32
사용 중인
메모리 영역
(Read And Write)
33
사용 예약된
메모리 영역
(Read Only Area)
34
사용 예약된
메모리 영역
(Read And Write)
35
사용 해제된
메모리 영역
(Read Only Area)
36
사용 해제된
메모리 영역
(Read And Write)

도면3


S101
가상 식별 정보 생성
S102
키이벤트 발생
S103
프로세스 리스트 획득
S104
알려진 프로세스 제외
S105
리스트에 포함된 프로세스가 사용하는 메모리 영역 추출
S106
현재 사용중이며 읽고 쓰기가 가능한 영역 추출
S107
메모리 영역에서 가상 식별 정보 검색
S108
가상 식별 정보 발견?
YES
NO
S109
키로거가 없다고 판단
S110
경고
S111
프로세스 종료