

명세서

발명의 명칭: 위협 사용자의 접속차단방법 및 프로그램 보안 적용방법

기술분야

- [1] 본 발명은 위협 사용자의 접속차단방법 및 프로그램 보안 적용방법에 관한 것으로, 보다 상세하게는 위협 사용자의 접근을 원천적으로 차단하고 관리자가 차단 설정이 가능한 위협 사용자의 접속차단방법 및 프로그램의 디컴파일 및 컴파일 과정 없이 클래스를 추출하여 처리속도를 향상시키는 프로그램 보안 적용방법에 관한 것이다.

[2]

배경기술

- [3] 최근 전자분야의 발전으로 인해 다양한 하드웨어 기기들이 전자화, 디지털화되고 있고, 이에 따라 소프트웨어 프로그램에 의해 동작되는 하드웨어 기기들이 점차 늘어나고 있다.
- [4] 그중 대표적인 것이 컴퓨터로, 컴퓨터에는 운영체제가 설치되어 있고, 각종 어플리케이션이 별도의 프로그램으로 컴퓨터에 설치되어 동작된다. 이러한 컴퓨터는 비단 데스크톱과 같은 개인용 컴퓨터뿐만 아니라 스마트폰과 같은 통신 단말기도 해당된다.
- [5] 그러나, 이처럼 소프트웨어에 의해 프로그래밍된 어플리케이션들이 널리 이용됨에 따라 가장 크게 문제가 되는 것이 바로 프로그램 해킹이다.
- [6] 일반적으로 해킹은 컴퓨터 네트워크의 취약한 보안망에 불법적으로 접근하여, 정보 시스템 또는 특정 단말기 상의 동작에 유해한 영향을 끼치는 제반 행위를 일컫는 것으로서, 결국 시스템 상에서 구동되고 있는 어플리케이션의 프로그램 코드를 임의로 조작하여, 어플리케이션이 개발자가 의도하지 않은 형태로 동작하도록 만드는 것을 말한다.
- [7] 이런 프로그램 해킹의 일례로는, 인증되지 않은 다수의 사용자에게 어플리케이션을 배포하기 위하여 프로그램 코드를 무단 복사하거나, 어플리케이션해커가 원하는 기능을 수행하도록 프로그램 코드를 조작하는 것이 있다.
- [8] 이와 같은 프로그램 해킹은 개발자의 저작권을 해치거나 어플리케이션이 실행되는 시스템 전반에 큰 악영향을 미치는 것으로서 결코 무시하거나 간과할 수 없는 중요한 문제로 부각되고 있다.
- [9] 이에 따라 보안 전문가들은 프로그램 해킹을 방어할 수 있는 보안 솔루션을 개발하고 있다. 보안 솔루션의 일례로, 인증 서버에 접속하여 사용자 인증 절차를 수행하거나, 프로그램 코드의 무결성을 검증하는 등의 다양한 보안 솔루션이 개발되고 있다.

- [10] 그리고, 프로그램 개발자들은 이런 보안 솔루션을 프로그램에 추가하여, 어플리케이션의 프로그램 코드를 해킹으로부터 보호하도록 하고 있다.
- [11] 그러나, 상기한 보안 솔루션 프로그램의 기술이 발전함에 따라 상기한 보안을 뚫고 접속을 시도하는 해킹기술도 함께 지능화되어 발전하고 있어 해킹하는 위협 사용자를 효과적으로 차단하기 위한 기술이 필요한 실정이다.
- [12] 또한, 상기한 종래기술의 보안 솔루션 프로그램은 보안 솔루션 프로그램을 제공하는 기업에서 위협 사용자(=해커) 리스트의 정보도 함께 제공하는 것이 일반적이므로 보안 솔루션 프로그램을 제공받는 관리자가 자체적으로 저장하고 있는 위협 사용자 리스트를 맞춤형으로 적용하기 어려운 문제점이 있었다.
- [13] 또한, 이를 위한 프로그램에 보안 솔루션 적용하는 기존 방법은, 개발자가 프로그램 개발 단계에서 프로그램 코드 중간 중간에 보안 솔루션 코드를 직접 추가하는 것이었다.
- [14] 그러나, 이런 기존 방법에서는 프로그램 코드와 보안 솔루션 코드의 호환성 문제가 발생하였고, 프로그램 코드에 보안 솔루션 코드를 추가하는 과정에서 다양한 오류들이 발생하게 되었다. 그리고, 프로그램을 업데이트 하는 경우에 업데이트된 프로그램 코드와 보안 솔루션 코드 모두를 재확인해야하는 번거로움이 존재하였다.
- [15] <선행특허문헌>
- [16] (특허문헌 1) 등록특허공보 제10-1583545호(2016.01.04)
- [17] (특허문헌 2) 등록특허공보 제10-1420383호(2014.07.10.)
- [18]

발명의 상세한 설명

기술적 과제

- [19] 상기와 같은 문제를 해결하기 위한 본 발명의 목적은 사용자 단말기로부터 수집한 접속정보를 기반으로 서버부가 접속차단대상 여부를 판단하여 정상 실행코드 또는 차단 메시지를 사용자 단말기로 전송하는 위협 사용자의 접속차단방법을 제공하는 것이다.
- [20] 또한, 상기와 같은 문제를 해결하기 위한 본 발명의 목적은 관리자가 서버부에서 카운팅한 위협탐지수를 고려하여 탐지 횟수로 설정하는 위협 사용자의 접속차단방법을 제공하는 것이다.
- [21] 또한, 상기와 같은 문제를 해결하기 위한 본 발명의 목적은 서버부가 사용자 단말기로부터 업로드된 파일에서 앱정보를 추출하고 추출된 앱정보로부터 추출한 구동코드에 보안실행코드를 합하여 실행시킨 후 검사하여 원소스코드를 실행시키는 프로그램 보안 적용방법을 제공하는 것이다.
- [22] 본 발명이 이루고자 하는 기술적 과제는 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수

있을 것이다.

[23]

과제 해결 수단

- [24] 상기와 같은 목적을 달성하기 위한 본 발명의 구성은 (a) 사용자 단말기에서 어플리케이션이 실행되는 단계; (b) 상기 사용자 단말기가 접속정보를 수집하여 서버부로 전송하는 단계; (c) 상기 서버부가 상기 접속정보를 기반으로 접속차단대상 여부를 판단하는 단계; (d) 상기 서버부가 상기 접속차단대상 결과에 따라 정상 실행코드 또는 차단 메시지를 사용자 단말기로 전달하는 단계; 및 (e) 상기 사용자 단말기가 상기 정상 실행코드 또는 상기 차단 메시지에 따라 실행되는 단계;를 포함하는 것을 특징으로 하는 위협 사용자의 접속차단방법을 제공한다.
- [25] 본 발명의 실시예에 있어서, 상기 (b) 단계는, (b1) 상기 사용자 단말기의 정보 또는 상기 사용자 단말기를 소지한 사용자의 정보를 포함하는 접속정보를 수집하는 단계; 및 (b2) 상기 접속정보를 상기 서버부로 전송하는 단계;를 포함하는 것을 특징으로 할 수 있다.
- [26] 본 발명의 실시예에 있어서, 상기 (c) 단계는, (c1) 상기 서버부가 상기 사용자 단말기로부터 전송되는 상기 접속정보를 저장하는 단계; 및 (c2) 상기 서버부가 상기 접속정보를 기반으로 상기 접속차단대상 여부를 판단하는 단계를 포함하는 것을 특징으로 할 수 있다.
- [27] 본 발명의 실시예에 있어서, 상기 (c2) 단계에서, 상기 사용자가 상기 접속차단대상인 경우, 상기 (d) 단계를 수행하여 상기 차단 메시지를 전달하는 것을 특징으로 할 수 있다.
- [28] 본 발명의 실시예에 있어서, 상기 (c2) 단계에서, 상기 사용자가 상기 접속차단대상이 아닌 경우, 상기 (c) 단계는, (c3) 상기 서버부가 해킹에 대한 위협을 탐지하는 단계; (c4) 상기 해킹에 대한 위협탐지를 카운팅하는 단계; 및 (c5) 상기 카운팅한 위협탐지수가 기설정된 접속차단값에 포함되는지 판단하는 단계;를 더 포함하고, 관리자는 상기 카운팅한 위협탐지수에 따라 상기 기설정된 접속차단값을 설정하는 것을 특징으로 할 수 있다.
- [29] 본 발명의 실시예에 있어서, 상기 (c5) 단계에서, 상기 서버부가 해킹에 대한 위협을 미탐지하는 경우, 상기 (d) 단계를 수행하여 상기 정상 실행코드를 전달하는 것을 특징으로 할 수 있다.
- [30] 본 발명의 실시예에 있어서, 상기 (c5) 단계에서, 상기 카운팅한 위협탐지수가 상기 기설정된 접속차단값에 포함되는 것으로 판단되면, 상기 (d) 단계를 수행하여 상기 차단 메시지를 전달하는 것을 특징으로 할 수 있다.
- [31] 본 발명의 실시예에 있어서, 상기 (c5) 단계에서, 상기 카운팅한 위협탐지수가 상기 기설정된 접속차단값에 미포함되는 것으로 판단되면, 상기 (d) 단계를 수행하여 상기 차단 메시지를 전달하는 것을 특징으로 할 수 있다.

- [32] 본 발명의 실시예에 있어서, 상기 (d) 단계는, (d1) 상기 서버부가 상기 사용자 단말기로 상기 차단 메시지를 전달하는 단계; 및 (d2) 상기 서버부가 상기 사용자 단말기로 상기 정상 실행코드를 전달하는 단계;를 포함하는 것을 특징으로 할 수 있다.
- [33] 본 발명의 실시예에 있어서, 상기 (e) 단계는, (e1) 상기 사용자 단말기가 상기 서버부로부터 상기 차단 메시지 또는 상기 정상 실행코드를 수신하는 단계; 및 (e2) 상기 사용자 단말기가 상기 정상 실행코드를 수신하였는지 여부를 판단하는 단계;를 포함하는 것을 특징으로 할 수 있다.
- [34] 본 발명의 실시예에 있어서, 상기 (e2) 단계에서, 상기 사용자 단말기가 상기 정상 실행코드를 수신한 경우, 상기 (e) 단계는, (e3) 상기 사용자 단말기의 접속을 허용하도록 실행시키는 단계;를 더 포함하는 것을 특징으로 할 수 있다.
- [35] 본 발명의 실시예에 있어서, 상기 (e2) 단계에서, 상기 사용자 단말기가 상기 정상 실행코드를 미수신한 경우, 상기 (e) 단계는, (e4) 위협 탐지 메시지를 노출시키는 단계;를 더 포함하는 것을 특징으로 할 수 있다.
- [36] 한편, 상기와 같은 목적을 달성하기 위한 본 발명인 프로그램 보안 적용방법의 구성은 (A) 사용자 단말기가 파일을 서버부로 업로드하는 단계; (B) 상기 서버부가 상기 파일을 기반으로 앱정보를 추출하는 단계; (C) 상기 앱정보에서 코드를 분석하여 원소스코드와 구동코드로 분리하는 단계; (D) 상기 서버부가 상기 원소스코드와 교체한 보안실행코드를 상기 구동코드에 합치는 단계; (E) 사용자 클라이언트가 상기 보안실행코드를 실행시키는 단계; 및 (F) 상기 사용자 클라이언트가 상기 원소스코드를 실행시키는 단계;를 포함하는 것을 특징으로 하는 프로그램 보안 적용방법을 제공한다.
- [37] 본 발명의 일실시예에 있어서, 상기 (C) 단계는, (C1) 상기 서버부가 상기 앱정보에서 상기 코드를 추출하는 단계; (C2) 상기 서버부가 상기 코드를 분석하는 단계; (C3) 상기 서버부가 상기 원소스코드와 상기 구동코드로 분리하는 단계;를 포함하는 것을 특징으로 할 수 있다.
- [38] 본 발명의 일실시예에 있어서, 상기 (D) 단계는, (D1) 상기 서버부가 상기 원소스코드와 상기 보안실행코드를 교체하는 단계; 및 (D2) 상기 서버부가 상기 원소스코드와 상기 보안실행코드를 합치는 단계;를 포함하는 것을 특징으로 할 수 있다.
- [39] 본 발명의 일실시예에 있어서, 상기 (D) 단계에서, 상기 보안실행코드와 교체된 상기 원소스코드는 난독화 및 암호화를 거쳐 보안처리되는 것을 특징으로 할 수 있다.
- [40] 본 발명의 일실시예에 있어서, 상기 (E) 단계와 상기 (F) 단계 사이에, 상기 보안실행코드가 실행된 이후, 상기 사용자 단말기를 검사하는 단계; 및 상기 원소스코드 또는 보안실행코드를 복호화시키는 단계를 포함하는 것을 특징으로 할 수 있다.
- [41] 본 발명의 일실시예에 있어서, 상기 (C) 단계에서, 상기 원소스코드는 사용자가

개발한 코드이고, 상기 구동코드는 상기 사용자가 개발하지 않은 코드인 것을 특징으로 할 수 있다.

- [42] 본 발명의 일실시예에 있어서, 상기 (B) 단계에서, 상기 앱정보는 앱의 패키지명 정보, 어플리케이션 정보, 액티비티 정보, 서비스 정보 및 리스너 정보 중 적어도 어느 하나를 포함하는 것을 특징으로 할 수 있다.

[43]

발명의 효과

- [44] 상기와 같은 구성에 따르는 본 발명의 효과는, 사용자 단말기로부터 수집한 접속정보를 기반으로 서버부가 접속차단대상 여부를 판단하여 정상 실행코드 또는 차단 메시지를 사용자 단말기로 전송함에 따라 위협 사용자의 접속을 원천적으로 차단할 수 있다.
- [45] 또한, 상기와 같은 구성에 따르는 본 발명의 효과는, 관리자가 서버부에서 카운팅한 위협탐지수를 고려하여 탐지 횟수로 설정함에 따라 관리자가 위협 사용자에게 대한 차단을 주도적으로 참여할 수 있다.
- [46] 상기와 같은 구성에 따르는 본 발명의 효과는, 서버부가 앱정보로부터 원소스코드와 구동코드를 분리시킨 후 구동코드에 보안실행코드를 합쳐 실행시킴에 따라 종래기술보다 처리속도를 향상시킬 수 있다.
- [47] 본 발명의 효과는 상기한 효과로 한정되는 것은 아니며, 본 발명의 상세한 설명 또는 특허청구범위에 기재된 발명의 구성으로부터 추론 가능한 모든 효과를 포함하는 것으로 이해되어야 한다.

[48]

도면의 간단한 설명

- [49] 도 1은 본 발명의 일실시예에 따른 위협 사용자의 접속차단방법을 나타낸 순서도이다.
- [50] 도 2는 본 발명의 일실시예에 따른 위협 사용자의 접속차단방법의 세부단계를 나타낸 순서도이다.
- [51] 도 3은 본 발명의 일실시예에 따른 위협 사용자의 접속차단방법에서 오토 블록을 위한 설정창을 예시적으로 나타낸 도면이다.
- [52] 도 4는 본 발명의 일실시예에 따른 위협 사용자의 접속차단방법에서 매뉴얼 블록을 위한 설정창을 예시적으로 나타낸 도면이다.
- [53] 도 5는 본 발명의 일실시예에 따른 일 실시예에 따른 프로그램 보안 적용방법을 나타낸 순서도이다.
- [54] 도 6은 본 발명의 일실시예에 따른 일 실시예에 따른 프로그램 보안 적용방법에서 사용자 단말기 상에 앱이 실행되는 것을 나타낸 도면이다.
- [55] 도 7은 본 발명의 일실시예에 따른 일 실시예에 따른 프로그램 보안 적용방법에서 사용자 단말기가 서버부로 파일을 업로드하는 것을 예시적으로 나타낸 도면이다.

- [56] 도 8은 본 발명의 일실시예에 따른 일 실시예에 따른 프로그램 보안 적용방법에서 코드 및 앱을 보호하기 위한 과정을 나타낸 도면이다.
- [57] 도 9는 본 발명의 일실시예에 따른 일 실시예에 따른 프로그램 보안 적용방법에서 코드 및 앱을 보호하기 위해 적용된 결과를 나타낸 도면이다.

[58]

발명의 실시를 위한 최선의 형태

- [59] 본 발명은 (a) 사용자 단말기에서 어플리케이션이 실행되는 단계, (b) 사용자 단말기가 접속정보를 수집하여 서버부로 전송하는 단계, (c) 서버부가 접속정보를 기반으로 접속차단대상 여부를 판단하는 단계, (d) 서버부가 접속차단대상 결과에 따라 정상 실행코드 또는 차단 메시지를 사용자 단말기로 전달하는 단계 및 (e) 사용자 단말기가 정상 실행코드 또는 차단 메시지에 따라 실행되는 단계를 포함하는 것을 특징으로 하는 위협 사용자의 접속차단방법을 제공한다.

[60]

발명의 실시를 위한 형태

- [61] 이하에서는 첨부한 도면을 참조하여 본 발명을 설명하기로 한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 따라서 여기에서 설명하는 실시예로 한정되는 것은 아니다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.
- [62] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결(접속, 접촉, 결합)"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 부재를 사이에 두고 "간접적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 구비할 수 있다는 것을 의미한다.
- [63] 본 명세서에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.
- [64] 이하 첨부된 도면을 참고하여 본 발명의 실시예를 상세히 설명하기로 한다.
- [65] 도 1은 본 발명의 일실시예에 따른 위협 사용자의 접속차단방법을 나타낸 순서도이다. 도 2는 본 발명의 일실시예에 따른 위협 사용자의 접속차단방법의 세부단계를 나타낸 순서도이다.

- [66] 본 발명의 일 실시예에 따른 위협 사용자의 접속차단방법은 (a) 사용자 단말기에서 어플리케이션이 실행되는 단계(S100), (b) 사용자 단말기가 접속정보를 수집하여 서버부로 전송하는 단계(S200), (c) 서버부가 접속정보를 기반으로 접속차단대상 여부를 판단하는 단계(S300), (d) 서버부가 접속차단대상 결과에 따라 정상 실행코드 또는 차단 메시지를 사용자 단말기로 전달하는 단계(S400) 및 (e) 사용자 단말기가 정상 실행코드 또는 차단 메시지에 따라 실행되는 단계(S500)를 포함한다.
- [67] 여기서, 접속정보는 각 디바이스 또는 서비스를 사용하는 사용자의 고유한 식별을 위해 부여되는 고유의 값으로서, 사용자 단말기의 정보 및 사용자 단말기를 소지한 사용자의 정보 중 적어도 어느 하나를 포함할 수 있다.
- [68] 각 디바이스를 식별하기 위해 사용되는 식별값을 포함하는 접속정보는 디바이스 내 또는 사용자의 서비스 아이디(ID) 등의 맥(MAC), 하드웨어 아이디(Hardware ID), 디바이스 아이디(device ID), 광고 아이디(ID), 체인(Chain), 앱 시스템에서 사용하는 사용자 식별 코드(예를 들어, 게임 아이디)와 같은 정보 중 하나를 이용하거나 다수의 조합을 이용하여 도출한다.
- [69]
- [70] 다음, 상기 (b) 단계는, (b1) 사용자 단말기의 정보 또는 사용자 단말기를 소지한 사용자의 정보를 포함하는 접속정보를 수집하는 단계 및 (b2) 접속정보를 서버부로 전송하는 단계를 포함한다.
- [71] 다음, 상기 (c) 단계는, (c1) 서버부가 사용자 단말기로부터 전송되는 접속정보를 저장하는 단계 및 (c2) 서버부가 접속정보를 기반으로 접속차단대상 여부를 판단하는 단계를 포함한다.
- [72] 만약, 상기 (c2) 단계에서, 사용자가 접속차단대상인 경우, 상기 (d) 단계를 수행하여 차단 메시지를 전달함에 따라 사용자 단말기가 해당 사이트에 접속하지 못하도록 한다.
- [73] 도 3은 본 발명의 일 실시예에 따른 위협 사용자의 접속차단방법에서 오토 블록을 위한 설정창을 예시적으로 나타낸 도면이다.
- [74] 본 발명의 위협 사용자의 접속차단방법을 위해 제공되는 프로그램은 관리자(예를 들어, 네이버, 다음, 구글 등과 같은 웹사이트)에 기설치되어 상기한 접속차단대상이 접속을 시도할 경우, 차단할 수 있다.
- [75] 반면, 상기 (c2) 단계에서, 사용자가 접속차단대상이 아닌 경우, 상기 (c) 단계는, (c3) 서버부가 해킹에 대한 위협을 탐지하는 단계, (c4) 해킹에 대한 위협탐지를 카운팅하는 단계 및 (c5) 카운팅한 위협탐지수가 기설정된 접속차단값에 포함되는지 판단하는 단계를 더 포함하여 수행한다.
- [76] 이때, 관리자는 카운팅한 위협탐지수에 따라 기설정된 접속차단값을 설정할 수 있다. 구체적으로 관리자는 내부적으로 위협 사용자 리스트를 데이터베이스로 구축해 놓은 상태에서 서버부로부터 제공되는 위협감지수를 고려하여 기설정된 접속차단값을 설정할 수 있다.

- [77] 예를 들어, 관리자는 카운팅한 위협감지수를 서버부로부터 전송 받은 후 이를 검토하여 3회 이상 접근 시 차단하도록 설정할 수 있다. 기설정된 접속차단값은 탐지 횟수로 설정하거나 탐지 횟수의 범위로도 설정이 가능하다.
- [78] 즉, 본 발명은 보안 프로그램을 제공함에 있어서 서버부가 위협 대상자 정보를 제공하는 것이 아닌 위협감지수에 대한 정보를 수신한 후 관리자의 내부에서 관리하는 위협 대상자 정보를 고려하여 기설정된 접속차단값을 임의로 설정하여 서버부로 전송한다.
- [79] 상기한 위협 사용자의 접근을 차단하거나 블록하기 위해 관리자는 오토 블록을 이용할 수 있다. 구체적으로 관리자는 오토 블록창을 통하여 임의의 위협탐지 시 임의의 기간 동안 접근하지 못하도록 블록을 설정할 수 있고, 이에 따라 위협 사용자의 접속 차단 일수가 정해진다.
- [80] 도 4는 본 발명의 일실시예에 따른 위협 사용자의 접속차단방법에서 매뉴얼 블록을 위한 설정창을 예시적으로 나타낸 도면이다.
- [81] 이어서, 도 4에 도시된 매뉴얼 블록은 사용자 단말기의 고유 식별값을 시스템에 입력하고 블록하고 싶은 기간을 관리자가 입력할 수 있도록 지원한다.
- [82] 만약, 상기 (c5) 단계에서, 서버부가 해킹에 대한 위협을 미탐지하는 경우, 상기 (d) 단계를 수행하여 정상 실행코드를 전달한다.
- [83] 반면, 상기 (c5) 단계에서, 카운팅한 위협탐지수가 기설정된 접속차단값에 포함되는 것으로 판단되면, 상기 (d) 단계를 수행하여 차단 메시지를 전달한다.
- [84] 한편, 상기 (c5) 단계에서, 카운팅한 위협탐지수가 기설정된 접속차단값에 미포함되는 것으로 판단되면, 상기 (d) 단계를 수행하여 차단 메시지를 전달한다.
- [85] 다음, 상기 (d) 단계는, (d1) 서버부가 사용자 단말기로 차단 메시지를 전달하는 단계 및 (d2) 서버부가 사용자 단말기로 정상 실행코드를 전달하는 단계를 포함한다.
- [86] 다음, 상기 (e) 단계는, (e1) 사용자 단말기가 서버부로부터 차단 메시지 또는 정상 실행코드를 수신하는 단계 및 (e2) 사용자 단말기가 정상 실행코드를 수신하였는지 여부를 판단하는 단계를 포함한다.
- [87] 만약, 상기 (e2) 단계에서, 사용자 단말기가 정상 실행코드를 수신한 경우, 상기 (e) 단계는, (e3) 사용자 단말기의 접속을 허용하도록 실행시키는 단계를 더 포함하여 수행할 수 있다.
- [88] 만약, 상기 (e2) 단계에서, 사용자 단말기가 정상 실행코드를 미수신한 경우, 상기 (e) 단계는, (e4) 위협 탐지 메시지를 노출시키는 단계를 더 포함하여 수행할 수 있다. 이에 따라 사용자는 관리자로서의 접속이 차단되게 된다.
- [89]
- [90] 도 5는 본 발명의 일실시예에 따른 일 실시예에 따른 프로그램 보안 적용방법을 나타낸 순서도이다.
- [91] 본 발명의 일 실시예에 따른 프로그램 보안 적용방법은 (A) 사용자 단말기가 파일을 서버부로 업로드하는 단계(S1000), (B) 서버부가 파일을 기반으로

앱정보를 추출하는 단계(S2000), (C) 앱정보에서 코드를 분석하여 원소스코드 및 구동코드를 분리하는 단계(S3000), (D) 상기 서버부가 원소스코드와 교체한 보안실행코드를 구동코드에 합치는 단계(S4000), (E) 사용자 클라이언트가 보안실행코드를 실행시키는 단계(S5000) 및 (F) 사용자 클라이언트가 원소스코드를 실행시키는 단계(S6000)를 포함한다.

- [92] 이때, 원소스코드는 클래스일 수 있으며, 본 발명에서는 하나의 구동코드를 예시적으로 설명하였으나, 구동코드 이외에 각기 다른 기능을 수행하는 다수의 코드를 포함할 수 있다.
- [93] 종래기술에서는 원소스코드, 구동코드 및 다수의 코드 전체를 디컴파일링한 후 보안코드를 각각의 코드에 적용한 후 다시 컴파일링하므로 처리속도가 현저하게 느린 반면, 본 발명은 원소스코드 및 구동코드로 분리시킨 후 구동코드에만 보안실행코드를 적용하고, 별도의 디컴파일링을 수행하지 않으므로 종래기술보다 처리속도가 현저히 빠른 장점이 있다.
- [94] 또한, 보안실행코드는 모바일 디바이스를 식별할 수 있는 식별정보를 추출할 수 있는 기능을 포함함에 따라 위협 대상자의 접속을 차단할 수도 있다.
- [95] 아울러, 사용자 클라이언트는 모바일앱 시스템일 수 있다.
- [96] 도 6은 본 발명의 일실시예에 따른 일 실시예에 따른 프로그램 보안 적용방법에서 사용자 단말기 상에 앱이 실행되는 것을 나타낸 도면이다. 도 7은 본 발명의 일실시예에 따른 일 실시예에 따른 프로그램 보안 적용방법에서 사용자 단말기가 서버부로 파일을 업로드하는 것을 예시적으로 나타낸 도면이다.
- [97] 상기 (A) 단계는 서버부로 파일이 업로드되는 단계이다. 여기서, 파일은 접속정보를 포함할 수 있고, 접속정보는 사용자 단말기의 정보 및 사용자 단말기를 소지한 사용자의 정보 중 적어도 어느 하나를 포함할 수 있다.
- [98] 도 6과 같이 사용자 단말기에서 보안을 적용하기 위한 앱을 실행시키고 도 7에 도시된 서버부의 화면에서 파일을 업로드한다.
- [99] 각 디바이스를 식별하기 위해 사용되는 식별값을 포함하는 접속정보는 디바이스 내 또는 사용자의 서비스 아이디(ID) 등의 맥(MAC), 하드웨어 아이디(Hardware ID), 디바이스 아이디(device ID), 광고 아이디(ID), 체인(Chain), 앱 시스템에서 사용하는 사용자 식별 코드(예를 들어, 게임 아이디)와 같은 정보 중 하나를 이용하거나 다수의 조합을 이용하여 도출한다.
- [100] 상기 (B) 단계에서, 앱정보는 앱의 패키지명 정보, 어플리케이션 정보, 액티비티 정보, 서비스 정보 및 리스너 정보 중 적어도 어느 하나를 포함한다.
- [101] 액티비티 정보는 프로그램을 구성하는 컴포넌트이며, 프로그램이 제공되는 단위 서비스가 구현된 소스 코드이다.
- [102] 구체적으로, 액티비티는 사용자에게 출력되는 화면을 생성 및 제어하도록 구성된 소스 코드로이며, 예시적으로 사용자 입력 화면, 게임 정보 출력 화면 등을 생성 및 제어하도록 작성된 소스 코드이다.

- [103] 리스너는 네트워크를 이용하여 클라이언트에서 서버부로 연결하기 위한 네트워크 관리자로서, 이러한 리스너를 실행시켜야 클라이언트들이 접속할 수 있다.
- [104] 구체적으로 리스너는 필요에 따라 여러 개가 동시에 구성되고 실행될 수 있으며, 각각의 리스너는 서비스 목록을 동적 또는 수동으로 등록할 수 있다.
- [105] 기본 포트를 사용하는 리스너는 PMON으로부터 실행 중인 디스패처의 정보도 함께 등록하고 있다. 다만, 기본 포트를 사용하지 않는 리스너(로컬 리스너 설정을 변경한 다른 리스너)는 동적으로 서비스의 등록을 받을 수 없다.
- [106] 서비스 정보는 컴퓨터 내에서, 특히 하드웨어에 가까운 낮은 레벨에서 다른 프로그램을 지원하는 프로그램 또는 루틴에 대한 정보이다.
- [107] 도 8은 본 발명의 일 실시예에 따른 일 실시예에 따른 프로그램 보안 적용방법에서 코드 및 앱을 보호하기 위한 과정을 나타낸 도면이다.
- [108] 상기 (C) 단계는, (C1) 서버부가 앱정보에서 코드를 추출하는 단계, (C2) 서버부가 코드를 분석하는 단계 및 (C3) 서버부가 원소스코드와 구동코드로 분리하는 단계를 포함한다.
- [109] 이때, 상기 (C) 단계에서, 상기한 원소스코드는 사용자가 개발한 코드이고, 상기한 구동코드는 사용자가 개발하지 않은 코드이다.
- [110] 도 8에 도시된 바와 같이 (C1) 단계에서는 코드 및 앱 보호를 위한 프로세스가 구동될 수 있으며, 상기한 과정에 의해 원소스코드, 구동코드 및 그 외의 다양한 코드를 추출할 수 있다.
- [111] 상기 (C1) 단계에서, 코드는 전술한 원소스코드 및 구동코드를 포함할 수 있다. 추가적으로 상기 (C1) 단계에서는 앱정보인 앱의 패키지명 정보, 어플리케이션 정보, 액티비티 정보, 서비스 정보 및 리스너 정보 중 어느 하나로부터 코드를 추출한다. 이때, 코드는 기능별로 다양한 코드가 존재할 수 있다.
- [112] 상기 (C2) 단계에서는 서버부가 상기 (C1) 단계에서 추출한 코드를 기반으로 분석한다.
- [113] 상기 (C3) 단계에서는 서버부가 상기 (C2) 단계에서 원소스코드와 구동코드를 분리하게 된다.
- [114] 본 발명은 상기 (C) 단계를 통해 종래기술에서 프로그램을 디컴파일하여 프로그램 코드를 생성한 후 보안코드를 입혀서 다시 프로그램 코드를 컴파일함에 따라 처리속도가 지연되는 문제점을 해소할 수 있다.
- [115] 즉, 본 발명은 프로그램을 디컴파일 및 컴파일하는 과정 없이 클래스를 분리시킴에 따라 종래기술보다 획기적으로 빠른 처리속도를 가지는 장점이 있다.
- [116] 다음, 상기 (D) 단계는, (D1) 서버부가 원소스코드와 보안실행코드를 교체하는 단계 및 (D2) 서버부가 원소스코드와 보안실행코드를 합치는 단계를 포함한다.
- [117] 구체적으로 보안실행코드는 원소스코드가 위치했던 자리로 교체되고, 보안실행코드와 교체된 원소스코드는 난독화 및 암호화를 거쳐 보안처리되어

특정위치에 저장될 수 있다.

- [118] 도 9는 본 발명의 일실시예에 따른 일 실시예에 따른 프로그램 보안 적용방법에서 코드 및 앱을 보호하기 위해 적용된 결과를 나타낸 도면이다.
- [119] 상기 (E) 단계(S5000)에서는 서버부가 보안실행코드를 실행시키는 단계로서, 원소스코드를 실행시키기 전에 사용자 단말기의 안전성을 먼저 검사한다.
- [120] 상기한 (E) 단계를 거친 결과 화면이 도 9에 도시되어 있다.
- [121] 이를 위한 본 발명은 상기 (E) 단계와 상기 (F) 단계 사이에, 보안실행코드가 실행된 이후, 사용자 단말기를 검사하는 단계 및 원소스코드 또는 보안실행코드를 복호화시키는 단계를 포함할 수 있다.
- [122] 이때, 보안소스코드가 실행된 이후, 사용자 단말기를 검사하여 검사결과가 안전하다고 판단되면, 보안소스코드를 복호화 및 기타 작업을 거쳐 원소스코드화시킨다.
- [123] 한편, 보안소스코드가 실행된 이후, 사용자 단말기를 검사하여 검사결과가 미안전하다고 판단되면, 종료하거나 상기 단계(S2000)로 복귀할 수 있다.
- [124] 마지막으로 상기 (F) 단계에서는, 사용자 단말기가 안전하다고 확인된 상태에서 서버부가 원소스코드를 실행시킨다.
- [125]
- [126] 상기한 바에 따른 본 발명은 기업의 핵심 기술 유출 방지와 해킹 및 불법 변조로부터 안전하게 지식재산권을 보호하는 어플리케이션 프로텍터로서, 모바일 디바이스(안드로이드/iOS)에서 구동되는 모든 어플리케이션에 적용 가능하며 이를 통해 모바일 어플리케이션을 위협하는 모든 해킹과 금전적 피해를 입을 수 있는 상황을 모두 차단하고 어플리케이션의 주요 자산을 보호한다.
- [127] 본 발명은 어플리케이션 위협 탐지(application threat detection) 기술, 어플리케이션 보호(application protector) 기술, 안티 해킹 솔루션(anti hacking solution) 기술이 융합된 것으로서, 이러한 기술들은 단순히 더해진 것이 아닌 유기적 결합을 통해 기술의 중복과 충돌이 없이 각 기능들이 서로 간의 취약점을 보완해 효율적인 동작을 수행하며, SaaS방식을 이용하여 결제부터 보안 적용까지 한 번에 사용이 가능하다.
- [128] 또한, 적용방식에 있어서 개발자의 별도의 작업이 필요 없이 SaaS 방식을 통하여 사용자의 편의성을 극대화 하였으며, 파일을 업로드하는 것만으로 소스코드 보호, 메모리 변조, 실시간 디버깅 등 해킹이 가능한 모든 행위를 차단하고 게임 엔진 보호, 가상머신 탐지, 리패키징 차단, 위/변조 방지 기능 등 모바일 어플리케이션에 필요한 모든 보안 기능을 제공한다.
- [129]
- [130] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을

것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

[131] 본 발명의 범위는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

[132]