

청구범위

- [청구항 1] (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 접속차단방법.
- [청구항 2] 제1 항에 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 하는 위협 사용자의 접속차단방법.
- [청구항 3] 제1 항에 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 하는 위협 사용자의 접속차단방법.
- [청구항 4] 제3 항에 있어서,
상기 (c2) 단계에서,
상기 사용자가 상기 접속차단대상인 경우, 상기 (d) 단계를 수행하여 상기 차단 메시지를 전달하는 것을 특징으로 하는 위협 사용자의 접속차단방법.
- [청구항 5] 제3 항에 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 하는 위협 사용자의 접속차단방법.
- [청구항 6] 제5 항에 있어서,
상기 (c5) 단계에서,
상기 서버부가 해킹에 대한 위협을 미탐지하는 경우, 상기 (d) 단계를 수행하여 상기 정상 실행코드를 전달하는 것을 특징으로 하는 위협 사용자의 접속차단방법.
- [청구항 7] 제5 항에 있어서,
상기 (c5) 단계에서,
상기 카운팅한 위협탐지수가 상기 기설정된 접속차단값에 포함되는 것으로 판단되면, 상기 (d) 단계를 수행하여 상기 차단 메시지를 전달하는 것을 특징으로 하는 위협 사용자의 접속차단방법.
- [청구항 8] 제5 항에 있어서,
상기 (c5) 단계에서,
상기 카운팅한 위협탐지수가 상기 기설정된 접속차단값에 미포함되는 것으로 판단되면, 상기 (d) 단계를 수행하여 상기 차단 메시지를 전달하는 것을 특징으로 하는 위협 사용자의 접속차단방법.
- [청구항 9] 제1 항에 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 하는 위협 사용자의 접속차단방법.
- [청구항 10] 제9 항에 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 하는 위협 사용자의 접속차단방법.
- [청구항 11] 제10 항에 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 하는 위협 사용자의 접속차단방법.
- [청구항 12] 제10 항에 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
 하는 위협 사용자의 접속차단방법.

- [청구항 13] (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 적용방법.

- [청구항 14] 제13 항에 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 하는 프로그램 보안 적용방법.

- [청구항 15] 제13 항에 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 하는 프로그램 보안 적용방법.

- [청구항 16] 제15 항에 있어서,
 상기 (D) 단계에서,
 상기 보안실행코드와 교체된 상기 원소스코드는 난독화 및 암호화를
 거쳐 보안처리되는 것을 특징으로 하는 프로그램 보안 적용방법.

- [청구항 17] 제13 항에 있어서,
 상기 (E) 단계와 상기 (F) 단계 사이에,
 상기 보안실행코드가 실행된 이후, 상기 사용자 단말기를 검사하는 단계;
 및
 상기 보안실행코드를 복호화시키는 단계를 포함하는 것을 특징으로 하는
 프로그램 보안 적용방법.

- [청구항 18] 제13 항에 있어서,
 상기 (C) 단계에서,
 상기 원소스코드는 사용자가 개발한 코드이고,

상기 구동코드는 상기 사용자가 개발하지 않은 코드인 것을 특징으로 하는 프로그램 보안 적용방법.

- [청구항 19] 제13 항에 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 하는 프로그램 보안 적용방법.