화이트리스트 기반 전사적 IT자원 보안 관제 시스템

박성식*, 고미은**, 박용범***
*단국대학교 컴퓨터과학과
**단국대학교 컴퓨터학과
***단국대학교 소프트웨어학과
e-mail:chocolateaz@dankook.ac.kr

WhiteList-based Enterprise IT Resource Security Control System

Sung-Sik Park*, Mi-eun Ko**, Young B. Park***
*Dept of Computer Science, Dan-kook University
**Dept of Computer Engineering, Dan-kook University
***Dept of Computer Science & Engineering, Dan-kook University

요 약

기업 사용자의 PC를 노리는 알려지지 않은 지능형 위협으로 전사적 IT자원 보안 문제가 대두하고 있다. 지정된 프로그램만 동작하게 하는 화이트리스트 보안 기술로 알려지지 않은 지능형 위협에 대응이 가능하다. 따라서 화이트리스트 기반 전사적 IT자원 보안 관제가 필요하다. 본 논문에서는 WhiteList 기반의 실시간 프로세스 분석을 통해 기업 사용자 PC 내에 허가되지 않은 프로그램을 관제할 수 있는 방법을 제시 하였고, 화이트리스트 기반 전사적 IT자원 보안 관제 시스템을 구현하였다.

1. 서론

카스퍼스키랩이 발표한 2016년 4분기 DDoS(Distributed Denial of Service) 인텔리전스 보고서에 따르면, 전 세계적으로 공격 범위는 축소됐지만 정교함은 증가하였고, 공격 대상 국가 69개국 중 대한민국이 23.2%로 중국에 이어 두 번째로 높은 비율을 차지하였다. APT(Advanced Persistent Threat) 공격, DDoS 공격같이 다양한 해킹 공격이 급격히 증가하고 있어 인터넷 환경이 발달하고 사용자가 많아질수록 그 피해 또한 급증하고 있다[1].

개인정보보호위원회의 2013년 개인정보의 가치와 개인정보 침해에 따른 사회적 비용 분석 연구보고서에 따르면, SK컴즈, 넥슨 등 거대 규모의 개인정보 유출이 일어난 2011년의 경우 약 2,400억 원, KT와 EBS의 개인정보 유출이 일어난 2012년의 경우 약 1,780억 원 정도의 피해가 일어난 것으로 추정하였다[2]. 안티바이러스처럼 위험요소를 식별하고 필터링하는 보안 시스템은 블랙리스트 기반 보안 솔루션들이 주류를 이루고 있어, 기업은 보안 문제가 발생할 때마다 보안 시스템을 강화하지만, 다양화되고 정교한 악성코드의 증가로 완전한 방어는 힘들다[3].

이러한 이유로 최근 기업 사용자 PC를 노리는 악성코드 침입 문제를 해결하는 화이트리스트(WhiteList) 보안 기술이 새롭게 부상하고 있다[4]. 또한, 급격하게 증가하고 변종하는 악성코드로 인해 발생하는 피해를 최소화하기 위해 최대한 빠르게 대응하는 것이 중요하다. 실시간 프로세스 모니터링을 이용해 악성코드를 탐지한다면 조기 대응이 가능할 것이다.

본 논문에서는 전사적 IT자원 보안 문제를 사전에 예방하고 알려지지 않은 지능형 위협에 대응하기 위해 화이트리스트 기반의 실시간 프로세스 분석을 통해 기업 사용자 PC 내에 허가되지 않은 프로그램을 모니터링 할 수 있는 시스템을 구현하였다. 이 시스템을 이용해 비 허가된 프로그램이 실행되지 않도록 관리할 수 있다.

2. 관련 연구

2.1. 화이트리스트

안티바이러스처럼 위험요소를 식별하고 필터링하는 보안 시스템은 블랙리스트 기반 보안 솔루션들이 주류를 이루고 있다. 그러나 시스템의 안정적인 운용과 정해진 프로그램만 사용하는 산업용 보안 시스템 개발 업체들은 별도의 화이트리스트 기반의 솔루션을 출시하거나, 기존의 제품에 화이트리스트 방식을 통합하는 추세이다.

화이트리스트는 정해진 프로그램의 사용만 허용되기 때문에 허용되지 않은 프로그램이 컴퓨터에서 실행되는 것을 막아 안정성을 유지할 수 있다. 하지만 특정 프로그램의 사용만 허용하기 때문에 애플리케이션의 수가 적고 변동이 크지 않은 제한적인 환경에 적합하다[3].

그리고 화이트리스트를 이용하면 사양이 낮은 단말에서 갖는 자원(Resource)의 부담을 줄이면서 허용되지 않은 프로그램의 실행을 효율적으로 제어할 수 있다. 또한, 알려지지 않은 지능형 보안 위협이 지속하는 시점에서 네트워크

통신 트래픽이 규칙적인 시스템의 경우 화이트리스트 기법이 효과적이다[4].

2.2. McAfee Application Control

McAfee사의 McAfee Complete Endpoint Protection-Enterprise 제품은 엔드포인트 보호 솔루션으로 제공하는 기능은 데스크톱과 노트북을 위한 핵심 안티바이러스, 안티스팸, 웹 보호, 방화벽 및 침입 방지 이외에 동작 안티멀웨어, 스마트 검색, 동적 화이트리스트 등이다. McAfee Complete Endpoint Protection-Enterprise의 단일 제품군으로 포함된 McAfee Application Control은 서버, 회사 데스크톱 및 고정 기능 장치에서 허가되지 않은 실행파일을 차단한다[5].

<표 1> McAfee Application Control의 주요기능[6]

기능	설명
소프트웨어배포	중앙에서 McAfee ePO를 통하여 컨트롤 에이전트 소프트웨어 자동 배포
화이트리스팅	에이전트 소프트웨어가 배포되면 해당 머신에 대하여 현재 운영 중인 애플리케이션들의 실행을 허용하도록 자동 화이트리스팅 수행
애플리케이션 차단	화이트리스팅 작업 이후에 발생하는 모든 애플리케이션 실행, 언인스톨, 삭제, 설치, ActiveX 실행시도를 차단
블랙리스트 기능	화이트리스트에 등록된 애플리케이션이라도 실행을 차단할 수 있도록 블랙리스트 정의 제공
신뢰된 디렉터리 기능	잠금 상태에서 신뢰된 디렉터리에 저장된 애플리케이션의 설치 및 실행을 허용
신뢰된 퍼블리셔	설치 파일의 인증서를 추가하여 신뢰된 퍼블리셔인 경우에 설치를 허용
신뢰된 설치파일	중앙에서 관리자가 지정한 신뢰된 설치 파일일 경우에 설치를 허용
신뢰된 사용자	지정된 사용자일 경우에 모든 설치 및 실행 작업을 허용
신뢰된 타임 윈도우	임의의 혹은 계획된 지정된 시간 동안에 소프트웨어 설치 및 실행을 허용
이벤트 취합	클라이언트 상에서 발생하는 모든 이벤트들에 ePO를 통하여 감시 및 증적로그 관리

2.3. AhnLab TrusLine

AhnLab의 AhnLab TrusLine은 산업용 제어 시스템 전용 보안 솔루션으로 허용된 프로그램만 실행할 수 있게 함으로써 악성코드의 침입을 방지하고 악성코드를 이용한 정보유출을 방지한다. 제공하는 기능은 애플리케이션 제어, 비 허가 실행 코드 차단, USB 등 매체 제어, IP/Port 차단, 멀웨어 분석 Agent Lock/unlock 설정 등이다[7].

<표 2> AhnLab TrusLine의 주요기능[7]

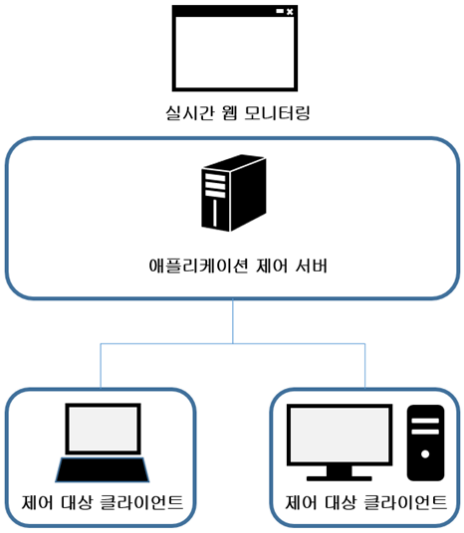
기능	설명
화이트리스트 기반 애플리케이션 제어	TrusLine 에이전트를 통하여 화이트리스트 방식의 애플리케이션 제어 기능을 수행
Agent/Server 분리구성	화이트리스트 방식의 애플리케이션 제어 기능을 수행하는 에이전트와 블랙리스트 방식의 악성코드 분석 엔진을 탑재한 서버를 분리 구성
악성코드 분석 엔진	악성코드 분석 엔진을 TrusLine Server에 탑재해 제어 시스템에 생성되는 모든 파일에 대한 실시간 검사 수행
중앙 집중 관리 시스템	웹 기반의 관리 시스템을 제공하여 제어 시스템의 정책 설정, 로그 관리 등 통합 관리 기능 제공

3. 화이트리스트 기반 전사적 IT자원 보안 관제 시스템

제안하는 시스템은 화이트리스트 기반으로 정해진 프로그램만 사용할 수 있어 IT자원 보안 관제를 위해 기업 및 개인의 사용자 PC에서 허용되지 않은 프로그램의 실행을 모니터링하고 차단하는 시스템이다.

화이트리스트 방식을 기반으로 한 실시간 모니터링을 통해 악성행위를 실시간으로 탐지해 시스템 프로세스에 DLL을 삽입시키는 시도나 지속적으로 데이터를 읽으려는 시도를 실시간으로 대응할 수 있다.

기존의 HTTP 실시간 통신 방식인 COMET은 자원 소비 면에서 상당한 오버헤드와 구현의 복잡성을 초래하지만, 웹 소켓 방식은 요청을 위해 최초 서버와 연결 후 연결이 그대로 유지되므로 새로운 연결을 만들 필요가 없어 HTTP 헤더 트래픽을 감소되고, 클라이언트가 재요청을 보낼 필요가 없어 추가적인 대기시간이 발생하지 않는 장점이 있다[8]. 이러한 웹 소켓 통신을 사용하여 실시간 양방향 통신을 제공해 전체 제어 시스템을 실시간으로 통합 관리한다.



(그림 1) 제안 시스템 구성

3.1. 제안 시스템 구성

(그림 1)은 제안 시스템의 전체 구성을 보여준다. 제어 대상 클라이언트, 애플리케이션 제어 서버, 실시간 웹 모니터링으로 구성된다. 애플리케이션 제어 서버는 각 클라이언트가 등록된 프로그램만을 실행할 수 있도록 화이트리스트를 전달하고, 실시간 모니터링 결과 화면을 웹 브라우저 화면으로 보여주는 역할을 한다. 제어 대상 클라이언트는 전송받은 화이트리스트만을 실행할 수 있고 만일 전달받은 리스트 이외의 프로그램이 실행된다면 프로그램의 실행을 종료시킨다. 실시간 웹 모니터링은 각 클라이언트로부터 받은 결과를 보여주는 역할을 한다.

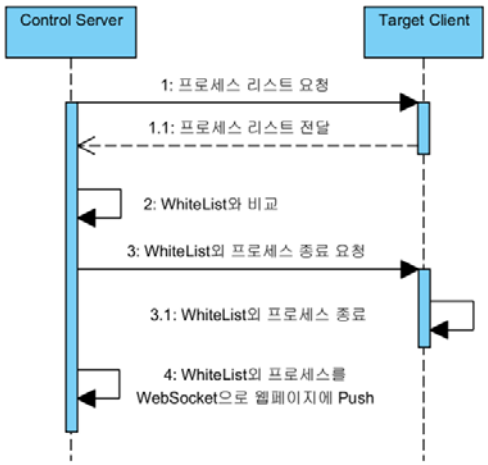
```
while(true){
    WhiteList = get_WhiteList();
    Client_Process_List = get_ClientProcessList();
    new_exe = Client_Process_List - WhiteList;

    if(new_exe != null){
        Client_Process_Kill(new_exe);
        WebSocket.push(new_exe);
    }
}
```

(그림 2) 제안 시스템 코드

(그림 2)의 제안 시스템 코드를 보면 제어 대상 클라이언트로부터 전송받은 리스트에서 화이트리스트에 등록된 프로그램이 아닌 것을 실행 종료하고 각 클라이언트로부터 받은 결과를 실시간 웹 모니터링 하는 것을 알 수 있다.

3.2. 제안 시스템 시나리오

우선 제어 대상 클라이언트에 자원 관리 프로그램을 실행시키고, 각 클라이언트는 실시간으로 프로세스를 모니터링하고 그 결과를 리스트 형태로 애플리케이션 제어 서버에 전달한다. 애플리케이션 제어 서버는 전달받은 리스트 중 정의된 프로세스는 실행을 허용하고, 정의되지 않은 프로세스는 각 PC에 정의되지 않은 프로세스 종료 메시지를 전달한다. 메시지를 전달받은 PC는 해당 프로세스를 종료시킨다.

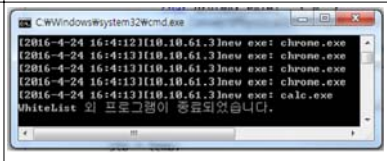
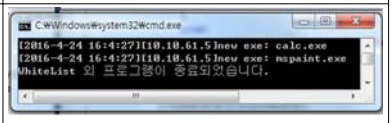
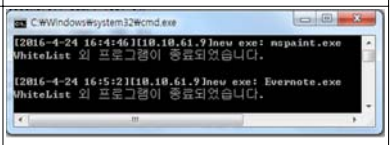
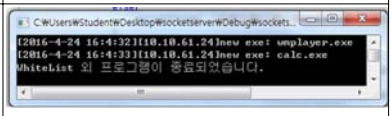
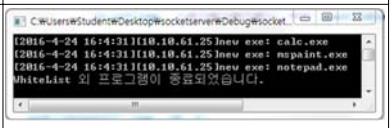
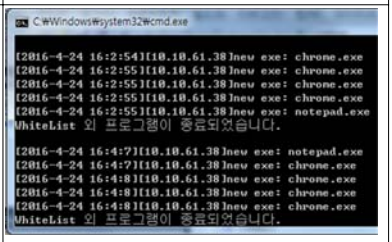
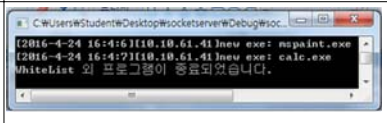


(그림 3) 제안 시스템 시퀀스 다이어그램

3.3. 제안 시스템 테스트 결과

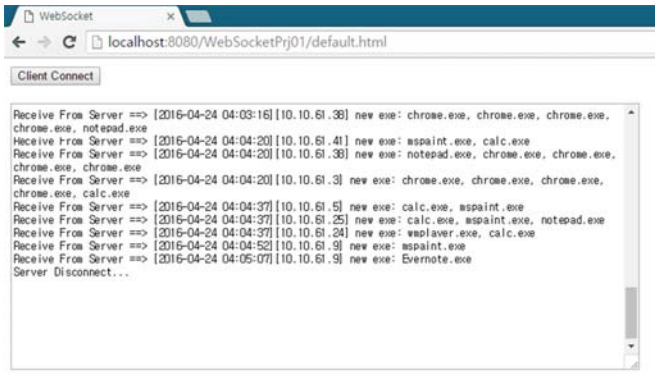
제안 시스템의 테스트 환경은 일반적인 데스크톱 PC로 화이트리스트 구성을 제어 대상 클라이언트의 프로그램이 실행되는 시점의 프로세스들을 애플리케이션 제어 서버에 화이트리스트로 등록하였다. 등록된 화이트리스트를 서버에서 관리하게 되고 클라이언트 PC에서 새로운 프로그램이 실행되면 새로운 프로그램을 종료시킨다. 제안 시스템의 테스트를 위한 제어 대상 클라이언트 리스트는 다음과 같다.

<표 3> 제어 대상 클라이언트 콘솔 화면

IP	클라이언트 화면
10.10.61.3	
10.10.61.5	
10.10.61.9	
10.10.61.24	
10.10.61.25	
10.10.61.38	
10.10.61.41	

서버는 클라이언트로부터 받은 새롭게 실행된 프로그램의 리스트와 등록된 화이트리스트를 비교하여 그 결과를 클라이언트에 전달하고 클라이언트는 허가되지 않은 프로그램의 실행을 차단한다. <표 3>은 클라이언트 상의 화면으로, 화이트리스트 외의 프로그램이 실행되면 실행된 프로그램명과 화이트리스트 외의 프로그램이 종료되었음을

보여주며, (그림 4)는 서버의 실시간 웹 모니터링 화면으로 모니터링 결과를 보여준다.



(그림 4) 실시간 웹 모니터링 화면

4. 결론

기업 사용자 PC 내에 허가되지 않은 프로그램의 실행은 안정성과 신뢰성이 중요한 전사적 IT자원 보안에 심각한 위협이 되고 있다. 다양화되고 복잡화된 공격으로 인해 일일이 대응하는 기존의 방식으로 해결하려는 시도는 쉽지 않다. 따라서 본 논문에서는 이러한 공격을 사전에 예방하고 알려지지 않은 지능형 위협에 대응하기 악성코드를 화이트리스트 방식을 기반으로 리스트 화하여 프로세스를 관리해 지정된 프로그램만 작동하게 하였다. 또한, 이를 웹소켓 통신을 통해 실시간으로 모니터링하여 지능화되고 있는 공격방식에 대응해 감염을 조기에 대응함으로써 피해를 최소화하는 데 사용될 수 있도록 하였다.

감사의 글

“이 논문은 2016년도 정부(미래창조과학부)의 재원으로 한국연구재단-차세대정보 · 컴퓨팅기술개발사업의 지원을 받아 수행된 연구임(No.2012M3C4A7033348).”

참고문헌

[1] Kaspersky Lab, “Kaspersky Lab DDoS 인텔리전스 보고서: 전세계적으로 공격 범위는 축소된 반면 정교함은 증가”, 새소식, 1.2016.

[2] 정상호, 유진호, 유병준, 한창희, 유승동, “개인정보의 가치와 개인정보 침해에 따른 사회적 비용 분석”, 개인정보보호협회, pp.58, 11.2013.

[3] 이대성, “소프트웨어 업데이트 유형별 위협요소와 안전성 강화를 위한 화이트리스트 구성방안”, 한국정보통신학회논문지, 제18권, 제6호, pp.4, 6.2014.

[4] 유형욱, 윤정한, 손태식, “제어시스템 보안을 위한 whitelist 기반 이상징후 탐지 기법”, 한국통신학회논문지, 8.2013.

[5] Intel Security, “McAfee Complete Endpoint Protection Enterprise”, 제품 및 솔루션, 2014-2016.

[6] STARBITSYSTEMS, “McAfee Embedded Security 솔루션 소개”, 자료실, pp.8, 5.2013.

[7] Softwarecatalog, “AhnLab TrusLine 2.0 표준제안서”, 기술자료/정보, pp.14-22, 6.2015.

[8] 바네사 왕, 프랭크 살림, 피터 모스코비츠,“모던웹을 위한 웹소켓 프로그래밍”, 한빛미디어, 7.2013