화이트리스트 기반 프로그램 실행 통제 방안 연구

김창홍* · 최대영** · 이정현*** · 김종배****

*,**,***,****숭실대학교

A Study of Program Execution Control based on Whitelist

Chang-hong Kim* · Dae-young Choi** · Jeong-hyun Yi*** · Jong-bae Kim****

*,**,***,****Soong-sil University

E-mail : *chkim@nextup.kr, **choidy219@naver.com, ***jhyi@ssu.ac.kr, ****kjb123@ssu.ac.kr

요 약

현재 사이버 위협은 계속적으로 증대되고 있으며, 진화하는 악성코드에 의한 보안 사고의 피해도 점점 더 커져가고 있다. 또한 기존의 보안체계를 회피한 은밀한 악성코드 기반의 공격으로 기밀 데이터 및 개인정보 유출이 지속적으로 증가하는 추세이다. 그러나 기존의 블랙리스트 기반의 시그니처 탐지 기법으로는 진화된 “알려지지 않은 악성코드”의 대응에 한계가 있다. 본 연구에서는 인가된 프로그램의 위변조 여부, 인가된 프로그램의 실행여부, 운영체제 주요 파일에 대한 변경 여부 등 복합적인 분석을 통한 탐지 및 식별로 악성코드 행위를 차단하는 화이트리스트 기반 프로그램 실행 통제 방안을 제시하고자 한다.

ABSTRACT

Currently, the growing cyber threat continues, the damage caused by the evolution of malicious code incidents become more bigger. Such advanced attacks as APT using 'zero-day vulnerability' bring easy way to steal sensitive data or personal information. However it has a lot of limitation that the traditional ways of defense like 'access control' with blocking of application ports or signature base detection mechanism. This study is suggesting a way of controlling application activities focusing on keeping integrity of applications, authorization to running programs and changes of files of operating system by hardening of legitimate resources and programs based on 'white-listing' technology which analysis applications' behavior and its usage.

키워드

화이트리스트, 블랙리스트, 악성코드, 개인정보 유출, 시그니처 탐지기법, 프로그램 실행 통제

Ⅰ. 서 론

최근 5년간 국가기관, 금융기관, 통신사, 쇼핑몰 등에 대한 DDoS공격, 대규모 개인정보 유출 등의 사고가 빈번히 발생하고 있다. 이러한 대형 해킹사고의 공통점은 보안체계가 상대적으로 견고한 공공/금융기관에서 발생했으며, 사용자인증, 내부통제, 백신, 접근통제 등의 정보보호시스템이 있음에도 불구하고, 주요정보 유출 및 단말 PC의 파괴를 막지 못했다.

특히 공격의 대상이 상대적으로 해킹 및 악성코드의 유포가 쉬운 단말 PC를 공격하여 권한 상승을 통해 서버를 해킹하는 방식으로 진화하고 있고, 네트워크 침해 대비 단말 PC의 악성코드 공격에 대한 원인분석 및 해결에 많은 시간이 소요되고 있어, 단말 PC에 대해서도 통합관제와 같은 관리 필요성이 요구되고 있다.

본 연구에서는 이러한 문제점들을 해결하기 위해 화이트리스트 기반으로 프로그램의 실행 흐름을 통제하는 방안을 제시하여 알려지지 않은 악성코드 공격에 대한 대응방안으로의 선험적 모델을 제시하는데 목적을 두고 있다.

Ⅱ. 본 론

본 연구에서는 화이트리스트 기반 실행파일 무결성 검증 프로토타입을 설계 및 구현하여 핵심 기술을 도출하고 기존 기술과의 차별성을 검증한다.

2.1 화이트리스트 기반 무결성검증 프로토타입

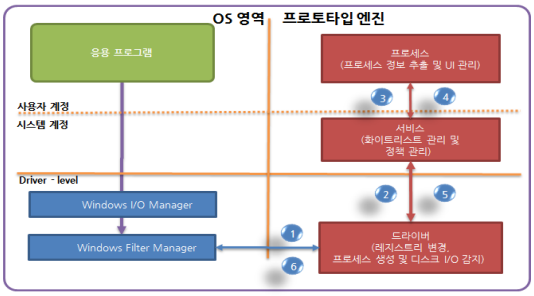

그림 1. 프로토타입 기술구조도

① 검증대상 응용 프로그램이 사용자 계정에서 실행되면, 윈도우 I/O Manager를 통해서 Driver에서 윈도우 OS 커널로 CreateProcess 이벤트를 전달한다. 선행 연구를 통해 Driver-Level에서 CreateProcess 이벤트를 윈도우 OS 커널로 전달 전 감지하여 프로세스의 Full Path와 PID 정보를 필터드라이버에 전달한다.
② 필터드라이버는 이벤트가 감지된 프로세스의 Full Path와 PID 정보를 서비스로 전달한다.
③ 서비스는 필터드라이버에서 넘어온 프로세스 정보에 정책을 적용, 사용자가 실행하려는 계정과 동일한 권한 및 정책으로 검증프로세스 생성 및 검증대상 프로세스의 Full Path와 PID를 전달한다.
④ 검증프로세스는 전달된 대상 프로세스 정보를 이용하여 프로세스에 속한 종속 프로세스 및 실행파일에 대한 해시 값 및 속성정보를 추출한다.
⑤ 로컬DB(이벤트 서버로부터 전송된 화이트리스트 해시 값과 정책정보)와 검증프로세스로부터 추출된 해시 값 및 속성정보를 비교하여 필터드라이버에 실행제어 결과를 전달한다.
⑥ 필터드라이버는 실행제어 결과에 따라 실행 및 차단을 수행한다.

2.2 핵심기술 내용 및 기존기술과의 차별성

2.2.1 화이트리스트 기반의 단말 PC 실행제어

화이트리스트 기반의 단말 PC 프로그램 실행 제어는 비업무 응용 프로그램 및 악성코드로 위·변조된 응용 프로그램에 대한 무결성 검증을 수행한다.

주요기능은 다음과 같다.

- PE 정보로 실행파일 여부 확인, 파일 해시 값, 파일속성, 디지털서명정보를 통한 유효성 검증
- 이벤트 서버로부터 전송받은 화이트리스트 파일 로컬 DB 저장
- 응용 프로그램 검증 후 검증 결과 로그 기록 및 이벤트 서버로 전송

기술구조도는 다음과 같다.

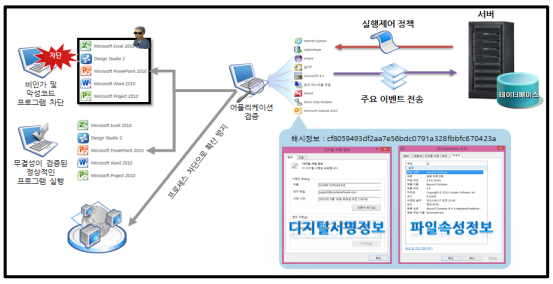

그림 2. 화이트리스트 기반 실행제어

기존기술과의 차별성은 다음과 같다.

① 파일 전체 해시 추출, 속성정보 및 디지털 서명정보 검증을 통한 무결성 검증으로 기존기술대비 무결성 검증 강화
② 드라이버 레벨에서 윈도우 메시지 감지를 통한 파일의 실행 이전 검증으로 기존 기술의 단점인 보안제품 접근 차단 및 보안제품 검증 회피 취약점 제거
③ PE정보, 해시정보, 속성정보, 경로정보, 프로세스 정보 등 다양한 정보를 통한 분석으로 위변조 식별 및 분석 강화

2.2.2 레지스트리 보호를 통한 위변조 방지

레지스트리 보호를 통해 트로이목마, WORM, 루트킷 해킹에 의한 레지스트리 위변조를 방지한다.

주요기능은 다음과 같다.

- 비인가 응용프로그램에 의한 시스템 자동시작 레지스트리 등록 방지
- 악성코드에 의한 윈도우 재시작 및 작업관리자 무력화 방지
- 악성코드에 의한 레지스트리 변조 시도 차단
- 레지스트리 백업 및 복구 기능

기술구조도는 다음과 같다.

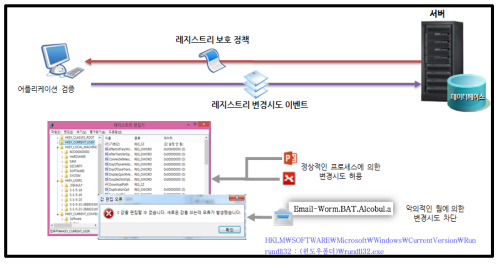

그림 3. 악의적 레지스트리 편집 차단

기존기술과의 차별성은 다음과 같다.

① 기존 기술은 레지스트리 보호를 하나의 옵션 기능으로서 제공하였고 사용자 선택에 따라 시작페이지에 자동 등록 차단의 일부 기능만 제공
② 중요한 레지스트리 키 값을 정책에 등록하여, 레지스트리 키 변경 모니터링 및 단말 PC와 동기화 관리
③ 키 값에 대한 보호뿐만 아니라 키 값의 변조를 유발한 원인의 식별 및 추적으로 근원적 원인 탐지 및 제거
④ 레지스트리의 시작프로그램 등록 및 보안프로그램에 대한 키 변조를 방지하고, 레지스트리 변조를 시도하는 프로세스를 강제로 종료시키고, 해당 프로세스에 대한 정보를 사용자가 식별, 관리자가 분석하여 초치토록 일련의 프로세스화

2.2.3 디스크 I/O 체크를 통한 주요파일보호

디스크 I/O체크를 통한 주요파일보호로 악성코드에 의한 운영체제 주요 시스템 파일에 대한 위변조를 차단한다.
주요기능은 다음과 같다.

- 위변조시 악의적 행위를 유발하는 윈도우 운영체제의 주요파일에 대한 디스크 I/O 체크로 변경여부 감지
- 윈도우 시스템의 API를 이용하여 추출된 정보를 기반으로 시스템파일에 악의적 위변조 시도 차단
- 주요 시스템파일(비실행 파일) 보호로 PC 파괴 방어
- MBR(Master Boot Recode) 백업 및 복구 기능

기술구조도는 다음과 같다.

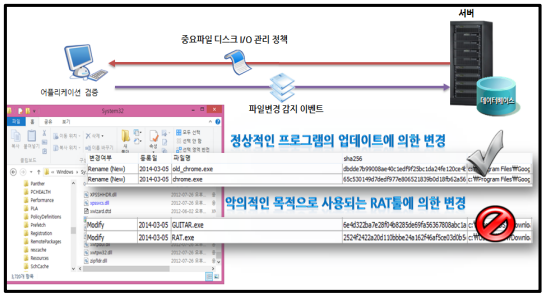

그림 4. 디스크 I/O 체크를 통한 파일보호

기존기술과의 차별성은 다음과 같다.

① 기존 기술은 문서, 동영상, 음악파일 등 콘텐츠 파일에 대한 DRM 기술을 적용한 위변조 방지 및 사용자가 지정한 파일에 대해서 무결성 정보를 추출하여, 지정된 파일에 대해서 무결성 체크
② 윈도우 운영체제의 주요 파일에 대한 디스크 I/O 체크를 통해 생성, 변경, 삭제 시도에 대해서 감지하여 어떠한 프로세스로부터 변조가 유발되었는지 원인의 식별 및 추적으로 근원적 원인 제거
③ 단말 PC의 기관 고유 업무프로그램의 로컬파일DB와 중요업무 프로그램에 사용되는 환경설정 파일 보호

2.2.4 매체제어 및 비정상적 역접속 탐지

악의적인 하드웨어 접근시도 차단을 위한 매체제어 및 해킹서버 접속여부 확인을 위한 비정상적 역접속을 탐지한다.
주요기능은 다음과 같다.

- 단말 PC에서 외부저장장치를 사용하기 위한 프로세스(보안USB)에 대한 우회접근시도 또는 비인가된 프로세스의 접근 시도에 대한 차단
- 보안 USB를 우회하기 위한 방법 중 외장디스크를 다른 드라이브 폴더로 탑재시 실행되는 diskmgmt.msc를 분석하여 통제
- 외부페이지로 접속하여 현재 시스템 정보 송출 또는 파일 다운로드를 시도하는 프로세스를 Remote Address 및 Port로 식별 및 해당 프로세스차단

기술구조도는 다음과 같다.

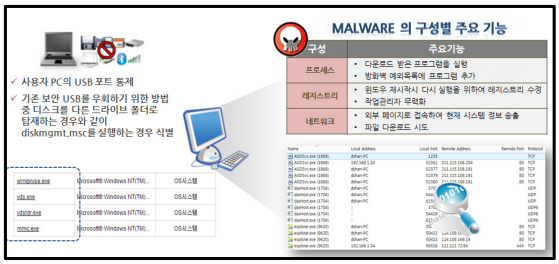

그림 5. 매체제어 및 비정상적 역접속 탐지

기존기술과의 차별성은 다음과 같다.

① 기존기술은 프로세스의 실행 패킷을 분석하여 차단하여, 외부 정보유출은 차단 가능하나, PC 파괴에는 한계점이 있고, 보안 USB의 경우에는 해당 프로세스 우회를 통해 외부 저장장치 유출 등 한계점을 보유
② 블랙리스트에 의한 비정상적인 외부 첩속 시도를 식별하여, 해당 프로세스를 강제 종료
③ 매체제어의 경우는 보안 USB 등을 우회하여, 특정 폴더로 Mount되는 등의 우회 시도를 차단 및 우회 접근시도를 수행하는 프로세스 식별로 악성코드 감염 파일 추적

Ⅲ. 결 론

사이버 위협은 계속적으로 증대되고 있으며, 진화하는 악성코드에 의한 보안 사고의 피해도 점점 더 커져가고 있다. 또한 기존의 보안체계를 회피한 은밀한 악성코드 기반의 공격으로 기밀 데이터 및 개인정보 유출이 지속적으로 증가하는 추세이다. 그러나 기존의 블랙리스트 기반의 시그니처 탐지 기법으로는 진화된 “알려지지 않은 악성코드”의 대응에 한계가 있다.

본 연구에서는 인가된 프로그램의 위변조 여부, 인가된 프로그램의 실행여부, 운영체제 주요 파일에 대한 변경 여부 등 복합적인 분석을 통한 탐지 및 식별로 악성코드 행위를 차단하는 화이트리스트 기반 프로그램 실행 통제 방안에 대한 선험적 모델을 제시하였고 핵심 기술을 도출하였다.

향후 연구에서는 선험적 모델을 프로토타입 형태로 개발하여 실 환경에서 통합테스트를 하여 공공기관, 금융기관, 통신사 등 실제 환경에 적합한 기술 및 기능을 검토해야 할 것으로 보인다.

참고문헌

[1] 블룸필터를 사용한 화이트리스트 기반의 SIP 서비스 거부 공격 대응 기법, 김주완, 류제택,한국통신학회 논문지, 2011.11

[2] 제어망에서 화이트리스트 기법을 이용한 이상징후 탐지에 관한 연구, 이동휘, 최경호, 융합보안논문지 2012.09

[3] 제어시스템 보안을 위한 화이트리스트 기반 이상징후 탐지 기법, 유형욱, 윤정한, 한국통신학회 논문지 2013.08

[4] 종합침해사고대응시스템 에서의 블랙리스트 추출방법과 관리 방안 연구, 박광철, 윤덕상, 정보보호학회지, 2005.02

[5] Whitelists Based Multiple Filtering Techniques in SCADA Sensor Networks, DongHo Kang, AyoungKoo Kim, Journal of Applied Mathematics, 2014

[6] IDC STAP(Specialized Threat and Analysis Protection) 분류 예측, 2013.08

[7] 한국인터넷진흥원(KISA) 침해사고 분석 현황, 2013.

[8] 국가보안연구 제6권 1호 국가 사이버보안 피해금액 분석과 대안, 2013

[9] 미래창조과학부 정보보안 기본지침, 2013.06

[10] 의료기관 개인정보보호 가이드라인, 2013.12

[11] 금융전산 망분리 가이드라인, 2013.09

[12] 금융위원회 금융전산 보안강화 종합대책, 2013.03

[13] 전자금융감독 규정 및 금융회사 정보기술부문 보호업무 모범규준, 2011