정 보 보 호 학 회 지
제27권 제6호, 2017. 12

IoT 장비에 대한 악성 프로세스 실행 제어 제품 시험방법 연구

박 명 서*, 김 종 성**

요 약

현대 사회에서 주요 사회적 이슈가 되는 CCTV, 네트워크 프린터, 스마트 가전기기 등 IoT 장비 해킹 사고의 발생 횟수 및 피해 규모는 지속적으로 증가하고 있다. 최근 침해사고 사례를 살펴보면, 엔드포인트에 해당하는 IoT 장비의 허술한 보안대책으로 인하여 악성코드 설치 및 실행을 탐지하지 못한 피해가 대부분이다. 이로 인해 IoT 장비에 대한 악성 프로세스 실행 제어 제품이 개발되어 도입되는 추세이지만, 아직까지 안전성 평가에 대한 연구가 부족한 실정이다. 따라서 본 논문에서는 IoT 장비에 대한 악성 프로세스 실행 제어 제품의 기본 보안요구사항을 식별하고, 필요한 시험항목과 시험 시 유의사항에 대해 제안한다.

Ⅰ. 서 론

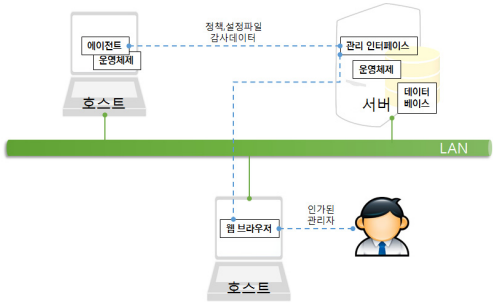
스마트 TV, 냉장고 등의 스마트 가전기기와 CCTV, 네트워크 프린터의 해킹 사고는 다양한 기법으로 진화된 악성코드로 인하여 지속적으로 발생 횟수 및 피해 규모가 증가하고 있다. 특히 새로운 변종 악성코드와 제로데이 공격은 기존 등록된 패턴만으로 탐지하는 백신만의 보호체계로는 한계가 있다. 이에 따라 최근 백신의 한계를 보완할 수 있는 악성 프로세스 실행 제어 제품의 수요가 증가하는 추세이지만, 아직까지 안전성 평가를 위한 연구가 부족한 실정이다. 따라서 IoT 장비에 대한 악성 프로세스 실행 제어 제품의 보안 취약성 및 위협 등을 분석하여 안전하게 운용할 수 있도록 기본 보안요구사항 및 이를 시험할 수 있는 시험 방법에 대한 연구가 필요하다. 본 논문에서는 악성 프로세스 실행 제어 제품에 대해 필요한 기본 보안요구사항을 식별하고, 이에 대한 만족 여부를 확인하기 위해 필요한 시험항목과 시험 시 유의사항에 대해 제안한다.

Ⅱ. 보안요구사항

본 장에서는 IoT 장비에 대한 악성 프로세스 실행 제어 제품에 대한 기능 및 구성에 대해 설명하고, 제공하는 보안기능에 대한 보안요구사항을 식별한다.

2.1. 악성 프로세스 실행 제어 제품

IoT 장비에 대한 악성 프로세스 실행 제어 제품은 네트워크 보안 제품 및 백신 등에서 방지하지 못한 악성코드 등의 위협 요인이 엔드포인트(스마트 가전기기, CCTV, PC 등) 단에서 실행될 수 없도록 보호하는 기능을 제공하며, 대부분 [그림 1]과 같이 에이전트/서버 방식으로 구성된다. 악성 프로세스 실행 제어 기능을 제



〔그림 1〕 IoT 장비에 대한 악성 프로세스 실행 제어 제품 구성

이 논문은 2016년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2016R1D1A1A09919726).
* 국민대학교 금융정보보안학과 DF&C Lab. (pms91@kookmin.ac.kr)
** 국민대학교 정보보안암호수학과, 금융정보보안학과 DF&C Lab. (jskim.kookmin.ac.kr)

공하기 위해 서버에서 설정한 정책 및 설정파일을 에이전트로 전송하며, 엔드포인트에 설치된 에이전트는 설정 정책에 따라 프로세스 실행을 제어한다.

2.2. 악성 프로세스 실행 제어 제품 보안요구사항

악성 프로세스 실행 제어 제품의 보안기능에 대한 시험항목을 도출하기 위해 먼저, 악성 프로세스 실행 제어 제품이 제공해야 할 보안요구사항에 대한 식별이 필요하다. 다음 SR(Security Requirement)1~SR8은 식별된 보안요구사항을 나타낸다.

SR1. 악성 프로세스 실행 제어 제품은 비인가 프로그램(위/변조된 인가 프로그램 포함)의 실행을 제어해야 한다.
SR2. 악성 프로세스 실행 제어 제품은 악성코드 프로세스의 실행을 제어해야 한다.
SR3. 악성 프로세스 실행 제어 제품은 에이전트와 서버 간 안전한 보안 통신을 제공해야 한다.
SR4. 악성 프로세스 실행 제어 제품은 외부 위협으로부터 에이전트를 보호해야 한다.
SR5. 악성 프로세스 실행 제어 제품은 에이전트/서버 내 주요 비밀데이터를 안전하게 보호해야 한다.
SR6. 악성 프로세스 실행 제어 제품은 정당한 사용자/관리자 인가를 위해 식별 및 인증 기능을 제공해야 한다.
SR7. 악성 프로세스 실행 제어 제품은 인가된 관리자가 모든 감사데이터를 열람할 수 있는 기능을 제공해야 한다.
SR8. 악성 프로세스 실행 제어 제품은 안전성 확보를 위해 적합한 보안 강도의 암호체계를 제공해야 한다.

Ⅲ. 보안요구사항에 대한 시험항목

본 장에서는 2장에서 식별한 보안요구사항의 시험항목 및 절차에 대해 설명하고, 시험 시 유의할 사항에 대해 제시한다.

3.1. 보안요구사항의 시험항목 및 절차

SR1 시험항목: 비인가 프로그램 실행 제어
1) 비인가 프로그램, 위/변조한 인가 프로그램을 실행시킨다.
2) 프로그램에 대한 실행 제어 수행 여부를 확인한다.

SR2 시험항목: 악성코드 실행 제어
1) 악성코드를 실행시킨다.
2) 해당 악성코드에 대한 실행 제어 수행 여부를 확인한다.

SR3 시험항목: 에이전트 서버 간 암호화 통신
1) 에이전트와 서버 간 전송되는 패킷을 수집한다.
2) 수집된 패킷을 분석한다.

SR4-1 시험항목: 에이전트 비인가 실행 종료 방지
1) 동작 중인 에이전트를 종료한다.
2) 종료 방지기능 제공 여부를 확인한다.

SR4-2 시험항목: 에이전트 비인가 위변조, 삭제 방지
1) 운영체제 내 설치된 에이전트를 위변조, 삭제한다.
2) 위변조, 삭제 방지기능 제공 여부를 확인한다.

SR5 시험항목: 비밀정보 보호
1) 에이전트/서버 내 비밀정보(암호화 키, 비밀번호, 에이전트 삭제키(제공시) 등)를 찾는다.
2) 비밀정보 암호화 저장 기능 제공 여부를 확인한다.

SR6-1 시험항목: 사용자 인증
1) 인가된 사용자를 식별 및 인증하기 위해 인증 기능 제공 여부를 확인한다.

SR6-2 시험항목: 사용자 인증 실패 대응
1) 의도적으로 사용자 인증 실패를 유도한다.
2) 설정된 인증 실패 대응 기능 동작 여부를 확인한다.

SR7 시험항목: 인가된 관리자 감사데이터 열람 확인
1) 인가된 관리자가 아닌 계정으로 로그인을 시도한다.
2) 감사데이터 열람 기능 동작 여부를 확인한다.
3) 사용자(인가된 관리자가 아닌)으로 로그인하여 감사데이터 열람 가능 여부를 확인한다.

SR8 시험항목: 적합한 보안강도의 암호 사용
1) 사용되는 암호 알고리즘을 점검한다.
2) 암호 알고리즘이 적합한 보안강도를 제공하는지 확인한다.

3.2. 시험 시 유의사항

본 절에서는 보안요구사항 시험 수행 시 유의할 사항에 대해 설명한다.

SR3 시험 시 유의사항

1) SSL 프로토콜을 통해 암호화 통신을 수행할 경우 최신 버전(TLS v1.2 이상)을 적용해야 한다.
2) 또한 오픈소스인 OpenSSL를 이용할 경우 알려진 취약성에 대해 보안패치가 완료된 최신버전을 적용해야 한다.

SR4 시험 시 유의사항

1) 악의적인 사용자가 안전모드와 같은 비정상 부팅환경에서 에이전트 보호 기능(비인가 위변조, 삭제, 실행종료 방지)을 무력화시키고, 정상 부팅하여 악성행위를 시도할 수 있다. 따라서 비정상 부팅환경에서도 에이전트 보호 기능 활성화 여부를 확인해야 한다.
2) 에이전트 실행파일, 설정파일, 정책파일 등의 무결성을 확인해야 한다. 이때 주기적으로 변경되는 감사데이터는 제외될 수 있다.

SR5 시험 시 유의사항

1) 저장된 비밀정보가 하드코딩 되거나 평문(단순 인코딩 포함)으로 저장 여부를 확인해야 한다.
2) 에이전트의 삭제를 위한 삭제키를 제공 시 각 에이전트 간의 삭제키는 상이해야 한다.
   - 삭제키가 동일하면 삭제키 노출 시 동일 배포 기관의 모든 에이전트 삭제를 유도할 수 있는 위험이 존재한다.

SR8 시험 시 유의사항

1) 보안 강도는 112비트 이상을 만족하는 암호 알고리즘을 사용해야 한다.
   - 대칭키 암호: 키 길이 128비트 이상
   - 해쉬 함수: 출력 값 224비트 이상
   - 공개키 암호: 키 길이 2048비트 이상

해당 보안 강도를 만족하는 알고리즘은 [1]에서 확인할 수 있다.

Ⅳ. 결 론

본 논문에서는 IoT 장비에 대한 악성 프로세스 실행 제어 제품의 보안요구사항을 식별하고, 시험항목 및 절차, 시험 시 유의사항에 대해 제안하였다. 악성 프로세스 실행 제어 제품은 비인가 프로세스 제어를 통해 백신을 보완할 수 있으므로 향후 다양한 악성코드 및 제로데이 공격 보호를 위해 수요가 증가할 것으로 예상된다. 따라서 안전성 평가뿐 아니라 보안취약성 및 예상 위협 등을 정의하여 보다 상세한 보안요구사항 식별 및 시험방법에 대한 연구가 필요하다. 이를 위해 향후 연구 내용으로는 악성 프로세스 실행 제어 제품에 대한 보안 위협 식별과 이에 대응되는 세부 보안요구사항 도출 및 분석, 또한 적합한 시험도구 사용 방법, 추가적인 유의사항 등의 시험 방법에 대해 연구를 수행할 예정이다.

참 고 문 헌

[1] KISA, *암호 알고리즘 및 키길이 이용안내서*, 2013
[2] Keunwoo Rhee, Hawon Kim, Hac Yun Na, “Security Test Methodology for an Agent of a Mobile Device Management System”, IJSIA, 6(2), pp137-142, April, 2012.

〈저 자 소 개〉

박 명 서 (Park Myungseo)
2015년 2월 : 국민대학교 금융정보보안학과 석사
2014년 12월~2017년 2월 : 국가보안기술연구소 연구원
2017년 3월~현재 : 국민대학교 박사과정
관심분야 : 정보보호, 암호 알고리즘

김 종 성 (Kim Jongsung)

2006년 11월 : K. U. Leuven, ESAT /SCD-COSIC 정보보호 공학박사
2007년 2월 : 고려대학교 정보보호 대학원 공학박사
2007년 3월~2009 8월 : 고려대학교 정보보호기술연구센터 연구교수
2009년 9월~2013년 2월 : 경남대학교 e-비즈니스학과 조교수
2013년 3월~현재 : 국민대학교 정보보안암호수학과 부교수
2013년 3월~현재 : 국민대학교 금융정보보안학과 부교수
관심분야 : 정보보호, 암호 알고리즘, 디지털 포렌식