내부망 안전한 패치 전달 및 관리 시스템

기술키워드	패치 파일 검증, 파일 무결성 검증, RDS 기반 무결성 검증, 문서 내 매크로 탐지								
지식재산권	출원 3건(대한민국 2건, 미국 1건)								
기술완성도 (TRL)	기초 실험	개념 정립	기능 및 개념검증	연구실 환경 테스트	**시제품 제작**	시제품 성능 평가	시제품 신뢰성 평가	시제품 인증	상용품

기술개요

- 시스템 소개
  - 제어시스템 패치 검증 및 관리 시스템은 휴대용 저장매체 내 존재하는 파일들에 대해 각종 검증, 통제, 이력관리 그리고 신규 운영체제 패치 알람을 관리자에게 제공함으로써 사전에 발생할 위협을 예방하고 기관 보안성 향상을 목적으로 함
  - 제어시스템 패치 검증 및 관리 시스템은 외부 출입자 또는 제어망으로 파일 이동을 원하는 내부 직원이 직접 휴대용 저장매체(USB, CD)를 키오스크에 꽂고, 파일 검증을 수행하는 키오스크 시스템과 키오스크 시스템을 관리하기 위한 정책 설정과 파일 이력 확인을 수행하는 관리자 프로그램으로 구성
- 필요성
  - 2011년 4월, 외주업체 직원 노트북에서 감염된 악성코드로 인해 시스템이 마비되고 각종 정보가 유출된 농협 사태에서 알 수 있듯, 외부로부터 유입되는 파일에 대해 검증 수행이 중요함
  - 2016년 국가기반시설의 보안위협 3위는 보안패치의 미설치로 인한 위협이며, 보안패치 설치율이 낮은 이유 중 하나는 보안패치 파일의 무결성 확인이 어렵고 내부망으로 이동하는 방식의 불편함이 한 원인
- 기술 구성도

기술성

- 독창성
  - · 시그니처 분석을 통한 파일 필터링, RDS를 기반한 제조사 펌웨어 패치 파일에 대한 위·변조 검증
  - · 문서 파일의 경우 백신 검사 수행할 뿐만 아니라 숨겨진 매크로 존재 여부 탐지
  - · 제어망 내부 자산에 대한 보안 업데이트 알림 및 패치 현황 이력 관리
- 범용성
  - · 키오스크 형태의 터치스크린을 통해 누구나 쉽게 사용가능 하도록 제작 되었으며, 제어망 뿐만 아니라 내/외부 분리망을 운영하는 모든 기관에 즉시 사용가능
  - · 국내외 다종의 백신을 선택적으로 설치가능 하며 및 행위기반 악성코드 탐지 제품과의 연동가능
- 보안성
  - · 내/외부 분리된 망에서 USB를 통한 파일 유통 시 악성코드 탐지 차단 및 펌웨어 무결성 검증
  - · Windows 보안패치 파일에 대한 신규 업데이트 알림 및 코드 사인 검증
  - · 내부망에 유통되는 모든 파일을 백업 추후 사고발생시 원인 분석
  - · 키오스크 내부 데이터 및 시스템 보안성 강화를 위한 자체 보안 방안 확보

시장성

- 정부차원에서 보안성을 위해 물리적 망분리를 구현을 권장하여 네트워크로부터 단절된 제어망으로 휴대용 저장매체로 패치 파일을 옮기는 기관이 운영기관, 공공기관, 대기업 대부분에 해당함
- 내부 또는 외부 직원으로부터 휴대용 저장매체에 담긴 파일을 검증하고자 하는 수요는 높으나, 이를 제공하는 국내 제품이 별도로 존재하지 않고, 특히 현장제어기기 펌웨어 패치 파일의 경우에는 백신으로 검증이 되지 않아 향후 시장성이 높다고 판단됨

기술 응용 분야

- 국가기반시설 운영기관, 공공기관, 대기업과 같이 물리적 망 분리를 구축한 시설
- 휴대용 저장매체를 통해 외부로부터 유입되는 파일들을 대상으로 아래 기능을 수행하고 싶은 시설
  - · 백신 검사를 비롯한 다양한 방법으로 악성코드 감염여부 검사 또는 제조사가 배포한 패치 파일과 일치 여부를 시스템을 통해 확인하여 보안성을 향상하고자 하는 시설
  - · 미리 관리자가 지정한 형태의 파일의 유입만을 허용하여 사전 위협을 차단하고자 하는 시설
  - · 이력 관리를 지속적으로 수행하여 관리자의 이력 관리 부담을 줄이고, 사고 발생 시 사고 경위 조사에 이력 내역을 활용하고자 하는 시설

기술개발 완료시기

- 2017년 12월 완료

관련 특허 등 지식재산권

- (출원) 2016-0141984(2016. 10. 28. 대한민국) 15/791786(2017. 10. 24. 미국) "제어 시스템의 업데이트 관리 장치, 업데이트 검증 장치 및 그 방법"
- (출원) 2017-0093741(2017. 7. 24. 대한민국) "내부망 전달용 파일 검증 장치 및 방법"