산업 제어시스템 보호를 위한 Whitelist 기반 네트워크 침입대응 기술

기술키워드	제어시스템, 보안스위치, 네트워크 스위치, Whitelist, 감시 및 차단								
지식재산권	출원 1건(일본) / 등록 9건(대한민국 5건, 미국 3건, 일본 1건)								
기술완성도 (TRL)	기초 실험	개념 정립	기능 및 개념검증	연구실환경 테스트	**시제품 제작**	시제품 성능평가	시제품 신뢰성평가	시제품 인증	상용품

기술개요

- (필요성) USB메모리, 유지보수 노트북 등 외부반입장비 또는 내부자에 의해 내부 네트워크의 사이버 사고가 증가하는 추세이나 기존 보안솔루션의 한계가 존재
  - · NAC 등 기존 보안솔루션은 보호대상 시스템에 별도의 SW에이전트를 설치해야 하여 제어시스템 뿐 아니라 BYOD, IoT환경에 적용/운영하기 어려운 경우가 많음
  - · 미러링, 태핑 등 기존 네트워크 모니터링 기술은 미러링 네트워크 스위치 성능의 한계, 모니터링 장비(네트워크 탭, aggregator 등)의 설치가 복잡하고 도입비용이 많이 필요함
  - · 기존 네트워크 스위치의 ACL(Access control list)을 활용할 경우 사용자가 모든 ACL을 직접 작성해야 하므로 모든 보안대상 시스템에 대한 정확한 ACL 작성이 어렵고 현장 변화에 대응이 느림
  - · NetFlow와 같은 기술은 샘플링 기반의 모니터링으로 모든 트래픽을 감시할 수 없음
- (기술요약) 네트워크 전영역을 감시하고 Whitelist[1] 위배트래픽을 차단할 수 있는 네트워크 스위치(이하 F.Switch)와 현장의 변화에 맞게 Whitelist를 쉽고 효과적으로 관리할 수 있는 시스템(이하 F.Manager)
  - · 모든 트래픽에 대해 Whitelist 기반으로 모니터링하여 이상트래픽을 차단하는 네트워크 스위치
  - · 네트워크 내 모든 시스템들의 통신관계를 파악할 수 있는 Whitelist 자동생성 및 관리기능
  - · 악성코드 등에 의한 비정상 통신 탐지/차단을 위해 신속히 대응할 수 있는 사용자 인터페이스 제공
- 기술 구성도

1) 네트워크 내 장비(IP, MAC) 간에 어떤 서비스(프로토콜, port)를 이용해 통신하는지에 대한 접근관계를 나타내는 것으로 기존 ACL과 동일 수준의 표현력을 가짐

기술성

- 별도의 모니터링 장비 없이 F.Switch를 통과하는 모든 트래픽에 대한 보안감시 및 선별적 차단 가능
- 네트워크 트래픽을 분석하여 Whitelist를 자동생성하고 환경 변화에 따른 Whitelist 변경사항 추천
  - 사용자가 보안대상 네트워크에 적용할 ACL을 직접 작성할 필요 없음
  - F.Manager가 시스템 및 서비스의 추가/삭제를 감지하여 사용자에게 알려 줌
- 상황마다 사용자의 역할과 권한에 맞게 해야 할 일을 명확히 해주는 사용자 인터페이스 설계
  - 사고대응 및 예방을 위해 해야 할 일을 확인할 수 있는 대쉬보드
  - 담당자에게 보고완료된 알람을 제거하여 신규 알람을 신속히 확인하는 것을 돕는 Blindlist

시장성

- 국가기반시설 제어시스템 및 민간 산업제어시스템 등에 보안장비로 활용 가능
  - 대한민국(제어시스템 관련 보안가이드)과 미국(NIST SP800-82)에서 시스템 간 접근제어, 정보흐름제어, 중요 시스템의 통신로그 저장을 권고하고 있음
  - 제어시스템(원자력 발전소, 조선, 전력 등) 수출을 위해 보안기능 확보가 필수적
- 산업 제어시스템 사이버보안 강화로 보안솔루션을 탑재한 시스템의 수요가 늘어날 것으로 예상
  - 2017년까지 120억 달러 규모의 제어시스템 사이버보안 시장이 창출
- 금융, 산업제어시스템 등 다양한 민간영역에서 활용 가능

기술 응용 분야

- 네트워크 통합보안관제
  - F.Switch를 내부 네트워크 보안센서로 활용
  - 보안통제 수행을 위한 기존 보안장비(방화벽, IDS 등)와의 협업
  - Whitelist 자동생성/관리 기술 및 F.Manager의 인터페이스를 이용하여 모니터링 인터페이스를 개선
- 일부 주요구간에 대한 보안통제
  - 외부반입장비 및 내·외부인이 접근하는 시스템들에 대한 보안통제
  - 보안기능을 탑재할 수 없는 시스템들을 위한 접근제어, 정보흐름제어 및 통신활동 로깅 수행
- 방화벽 규칙관리를 위한 Whitelist 자동생성 및 관리기능 활용
- 기업 내 자산관리를 위해 Whitelist 자동생성 및 관리기능 활용
- 제어시스템 테스트베드 및 교육시스템 구축
  - 사용자 실수에 의한 사고 방지 및 테스트/교육 수행과정 모니터링 가능

관련 특허 등 지식재산권

- (출원) 2014-115611(2014. 6. 4. 일본) "네트워크 장치 및 이를 이용한 선별적 정보 모니터링 방법"
- (등록) 10-1455167(2014. 10. 21. 대한민국), 9369434(2016. 6. 14. 미국) "화이트리스트 기반의 네트워크 스위치"
- (등록) 10-1564643(2015. 10. 26. 대한민국), 9742699(2017. 8. 22. 미국) "네트워크 장치 및 이를 이용한 선별적 정보 모니터링 방법"
- (등록) 1564644(2015. 10. 26. 대한민국), 5942013(2016. 5. 27. 일본) 9894074(2018. 2. 13. 미국) "접근제어 리스트 추출 방법 및 시스템"
- (등록) 10-1626293(2016. 5. 26. 대한민국) "접근제어리스트 생성 및 검증 장치 및 방법"
- (등록) 10-1823421(2018. 1. 24. 대한민국) "화이트리스트 기반의 네트워크 보안 장치 및 방법"