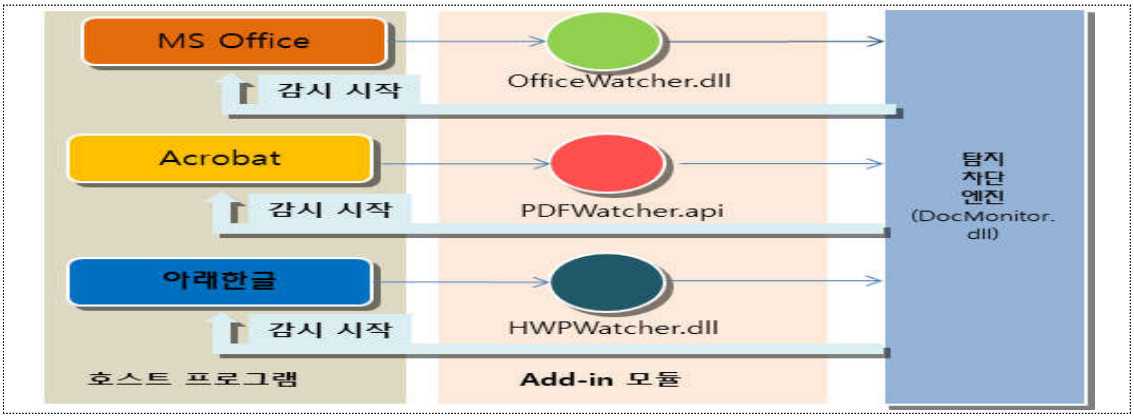
악성문서 행위 탐지 및 차단 기술

기술키워드	APT 공격, 이메일, 첨부문서,								
지식재산권	등록 1건(미국) / 등록 1건(대한민국)								
기술완성도 (TRL)	기초 실험	개념 정립	기능 및 개념검증	연구실환경 테스트	시제품 제작	시제품 성능평가	시제품 신뢰성평가	**시제품 인증**	상용품

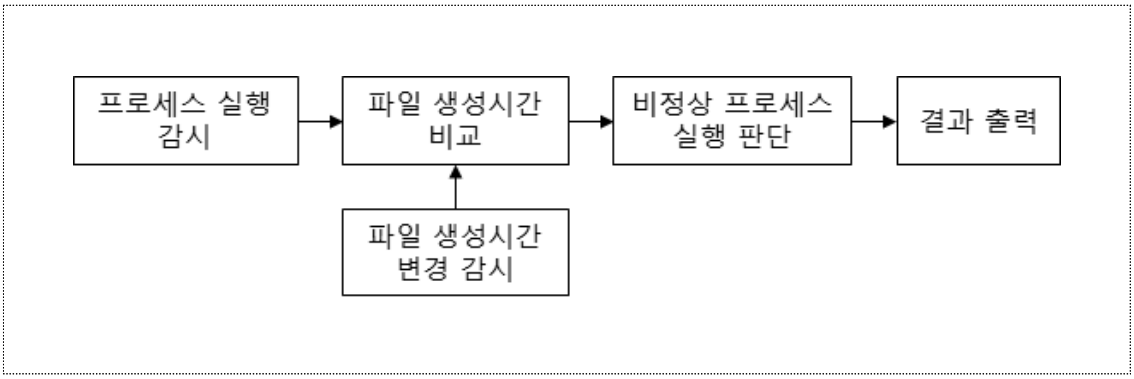
기술개요

- 악성문서 행위 탐지 및 차단 기술
  - 윈도우 운영체제 환경 개인 단말(PC)의 문서 응용프로그램 보안 취약점을 악용한 APT 공격이 끊이지 않고 있어, 문서 기반의 악성 행위를 사전에 탐지, 차단하는 기술을 이전하고자 함
  - 본 기술은 문서를 오픈하는 응용프로그램 내의 행위를 모니터링하여 악성 행위를 식별하기 때문에 알려지지 않은 공격까지도 탐지하여 차단할 수 있는 기술임
  - 본 기술은 문서 응용 프로그램에 플러그-인 방식으로 탐지 모듈을 탑재하는 기술과 문서 내에 숨겨진 실행 코드의 실행을 탐지, 차단하는 기술로 구성됨

- 기술 구성도(탐지모듈 탑재기술)



- 기술 구성도(문서 악성행위 탐지차단기술)



기술성

- 독창성
  · 문서 응용 프로그램 내에서 실행하는 프로그램들의 생성 시간을 비교하여 악성 여부를 판별하는 독창적 기술임
- 범용성
  · 문서 응용 프로그램은 대부분 PC 전산 환경의 일상적 활용 대상으로, 본 기술의 적용 범위는 매우 넓으며, 기술 이전 대상은 정보보호제품 뿐만 아니라, 문서 응용프로그램 개발사도 포함함
- 보안성
  · 문서 응용 프로그램 내 실행되는 프로그램의 생성시간을 활용하여 악성 여부를 탐지하는 특허를 활용한 기술에 대한 이전으로 국가보안 기술 및 핵심 기술 유출과 관련이 없음

시장성

- 국내외 다수의 Anti-virus 프로그램 개발사가 존재하나, 제로-데이 공격의 사이버위협에 대한 완벽한 솔루션을 제시 못하는 상황에서, 본 기술의 이전 활용은 해당 솔루션의 경쟁력 강화에 기여
- 문서 편집 기능의 응용프로그램과 보안 기능의 융합을 통해 새로운 시장 창출이 가능할 것으로 기대

기술 응용 분야

- 백신 프로그램의 제로데이 공격에 대한 실시간 위협 탐지 분야
- 문서 편집 프로그램 내 취약점을 악용한 Exploit 공격에 대한 탐지 분야

기술개발 완료시기

- 2010년 12월 완료

관련 특허 등 지식재산권

- (등록) 0897849(2009. 5. 8. 대한민국) "비정상 프로세스 탐지 방법 및 장치"
- (등록) 8091133(2012. 1. 3. 미국) "비정상 프로세스 탐지 방법 및 장치"