ETRI

45

능동적 사이버공격 사전대응을 위한 네트워크 주소변이 기술

기술개요

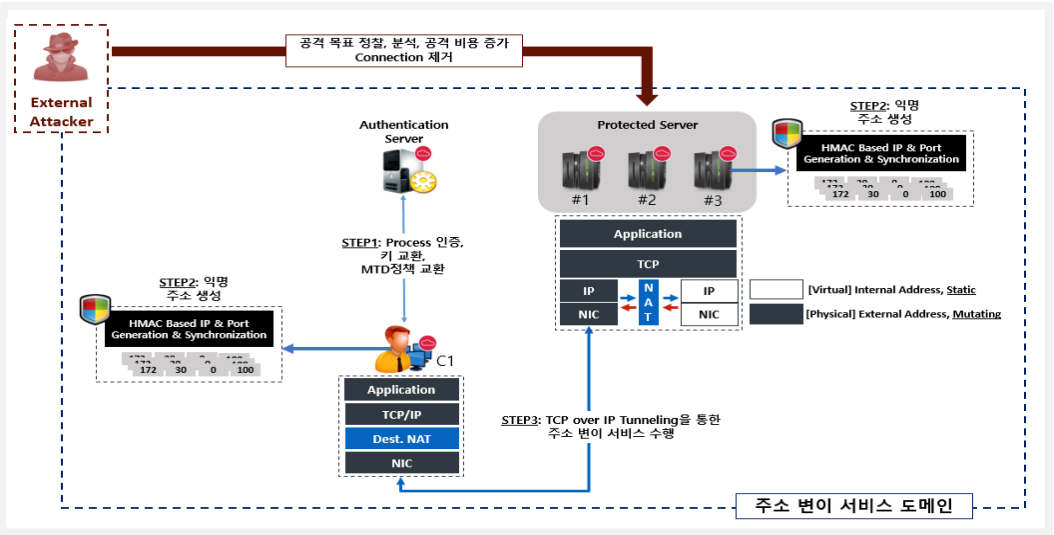
▪ 능동적 사이버공격 사전대응을 위한 네트워크 주소변이 기술

– 보호대상 서버의 주소와 오픈 포트번호 노출을 막기 위하여, 서비스의 Transparency를 보장하면서 주기적으로 보호대상 서버의 주소와 포트번호를 변이하는 기술로, 사이버 공격시 공격대상 목표물 탐색을 어렵게 하여 사이버 공격 복잡도를 높이는 기술

기술의 특장점

▪ 익명 IP 주소생성과 터널 은닉 및 의심스러운 연결 제거 기술 제공

- 내부 공격자의 스캐닝 및 패킷 스니핑에 대한 서버 노출 대응이 가능
- 네트워크에서 발생하는 다양한 예외 상황에 대한 고려 및 구현 방법을 상세히 제공
- 기존 기술과는 달리, 내부 위협에 대응함과 동시에 실제 적용 가능한 수준까지 기술개발과 검증이 완료된 세계 최초의 MTD 네트워킹 기술



적용분야

▪ 네트워크 보안/빅데이터 기반 보안관제 서비스/EDR 솔루션 개발 등

네트워크 보안	빅데이터	네트워크 보안성 평가	보안 컨설팅
			
• EDR 솔루션 개발 • 데이터손실방지 제품 개발 • 백신 개발 • 침입탐지 시스템 개발 • 네트워크 보안 시스템 개발 • 빅데이터 기반 보안관제 시스템 개발	• 빅데이터 기반 보안관제 서비스 • EDR 솔루션 개발 • 백신 개발	• 침입탐지 예측 서비스 • 네트워크 보안 평가 서비스 • 사이버 보험 평가 기준 제공	• 사이버 보안 컨설팅 서비스 • 사이버 보험 솔루션 • 보안 담당자 교육 서비스 • 보안 전문가 양성 서비스

기술완성도 (TRL)

▪ TRL 5단계 : 확정된 소재/부품/시스템시작품 제작 및 성능 평가 단계

기술이전 내용 및 범위

▪ Outside Anonymity 보장을 위한 익명 주소 생성 기술

- 네트워크 주소 변이 서비스 참여 Entity간의 인증 및 키 분배
- 충돌회피를 통한 분산 익명 주소 생성 및 동기화

▪ Hidden Tunnel Networking 기술

- 네트워크 서버 주소 변이/추적 기술
  - a. 익명 주소를 기반으로 서버의 주기적인 주소 변이를 위한 Local NAT
  - b. 익명 주소를 기반으로 클라이언트의 Moving 서버 추적을 위한 Local NAT
- 인증된 사용자의 연결 유지 기술
  - a. TCP 계층의 연결을 IP 계층과 분리
  - b. TCP 계층과 IP 계층의 Transparency를 보장
  - c. Compacted ARP Table Partitioning
- 의심스러운 연결 감지 및 제거 기술
  - a. 주소 변이 주기마다 시행되는 연결 정보 분석
  - b. 연결 정보 분석 결과에 따른 의심스러운 연결 제거

관련 지재권 현황

No.	출원번호	특허 명	상태
1	2017-0098153	HMAC 기반의 동적 CAN ID 생성 및 운용장치, 및 그 방법	출원
2	2019-0056476	서버 장치, 클라이언트 장치 및 네트워크 주소 변이 기반 통신 방법	출원
3	2017-0109698	TFO 쿠키 값을 이용하는 보안방법 및 장치, 그리고 이를 이용한 통신방법 및 장치	등록

기술이전 문의

▪ 연구성과확산실 (042-860-4946 / hjchoi2@etri.re.kr)