연구개발계획요구서(RFP)

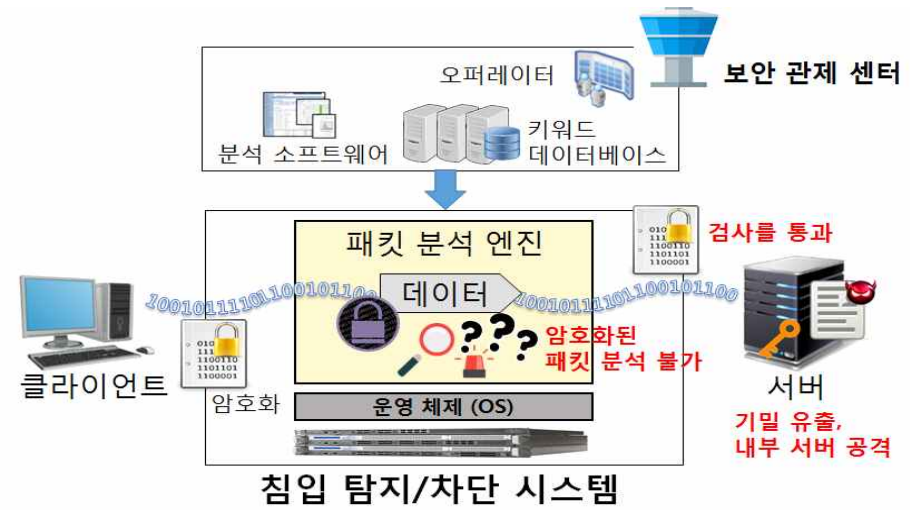
과제명 : 암호화된 트래픽 처리를 위한 보안성을 갖춘 침입 탐지 및 차단 기술 연구

1. 개요

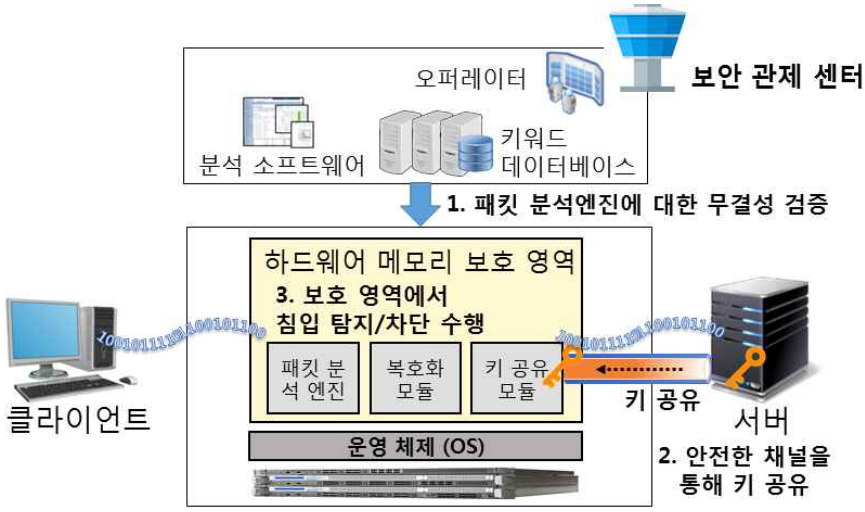
가. 기술의 개념 및 정의

◆ 네트워크상의 양 단말간(서버-클라이언트) 암호화된 트래픽이 송수신되는 망의 중간에 위치한 침입 탐지/차단 시스템에서, **보안성을 갖고** 공격 패턴을 탐지하는 기술 개발

◆ 최근 군 뿐만 아니라 민수 분야에서도 정보 보호와 보안에 대한 인식이 강조되면서, 트래픽을 암호화하여 전송하는 비율이 증가하여, 네트워크상에서 신뢰성 있게 다양한 공격패턴을 탐지/차단하는 기술 개발



[그림1] 키 공유가 없는 경우 암호화된 트래픽 운영개념



[그림2] 키를 공유한 경우 암호화된 트래픽 운영개념

나. 기술의 중요성/필요성 및 시급성

◆ 기술의 중요성 / 필요성

○ 현재의 침입탐지 관제시스템 보안성 강화 기술개발

- 보안성을 갖춘 암호화 트래픽 복호화/암호화
- 현재의 침입 탐지 시스템은 종단 간 암호화한 트래픽에는 무용지물

※ 유해한 공격 트래픽을 전혀 탐지할 수 없어 심각한 보안 위협을 초래한다.

○ 관제시스템의 암호키와 복호화된 트래픽을 제3자가 접근하는 것을 근본적으로 차단하는 기술

◆ 기술개발의 시급성

○ 최근 트래픽을 암호화하여 전송하는 비율이 증가하여, 네트워크상에서 신뢰성 있게 다양한 공격패턴을 탐지/차단하는 기술을 시급히 개발할 필요성 대두

다. 연구개발 최종 목표

연구개발 항목	목표성능	비고
암호 키 및 복호화 된 트래픽에 대한 메모리 보호 기능	운영체제 권한을 가진 공격자의 메모리 염탐 공격 방어 검증	
코드 무결성 보장	변종코드 실행차단 기능보유	
패턴 기반 침입 탐지기능 처리 속도	ET-Pro 룰셋 1000개 패턴 기준 700Mbps 이상	
정규식 매칭 지원 기능	패턴 매칭 / 정규식 매칭 지원	
범용 암호화 프로토콜 지원	2종 이상 프로토콜 과 호환 (SSL, VPN)	
	다중 암호화된 트래픽 처리 지원	
보안성을 갖춘 제어 평면	10개 취약점 대응 기술 확보 (제어 메시지 플로딩, 장비 정보 스푸핑 등)	
연결 초기화 지연 시간 (Connection setup time delay)	LAN 환경에서 10msec 이내	
암호 키 교환 지연 오버헤드	하나의 연결 당 지연 시간 0.1msec 이내	
범용 TLS 대비 복호화 성능 오버헤드	TLS 대비 복호화 성능 감소폭 2.5배 이하	

2. 국내외 기술현황 및 전망

가. 국내 기술동향 및 전망

◆ 침임 탐지시스템 성능 향상을 위한 연구들이 활발히 진행되고 있으나, 암호화된 트래픽 처리를 위한 침입탐지 시스템 연구는 초보단계 임.

나. 국외 기술동향 및 전망

◆ 세계적으로 암호화된 트래픽을 처리하기 위한 침임 탐지 시스템 연구는 초창기이며, 활발히 진행되고 있는 실정 임.

※ 상세한 국내외 기술현황 및 전망 제안가능 (인용 근거 제시필요)

3. 연구개발계획

가. 단계별 연구개발 목표

구분	연구 개발 목표	연구개발 내용	주요 결과물
시험 개발	1. 개요 다.항 참조	○ 하드웨어와 소프트웨어 보안 기술을 융합하여 보안성을 갖춘 복호화 및 침입 탐지 기술 • 하드웨어 보안 기술의 활용을 통한 보안성 향상 기술 • 소프트웨어 보안 기술의 활용을 통한 보안성 향상 기술 ○ 공격패턴 룰셋 및 침입 탐지 시스템 무결성 검증 기술 ○ 침입 탐지 시스템 고도화를 통한 범용 암호화 프로토콜들과의 호환 기술 ○ 관제 시스템의 보안성 향상 • 망 컨트롤러의 취약점을 보완한 보안성을 갖춘 컨트롤러 개발 ○ 보안성을 갖춘 Key 전송 알고리즘 개발	5. 연구 결과 제시물 가.항 참조

※ 연구개발목표를 달성하기 위한 연구개발 내용 제안가능

* 최종평가시 모든 평가 항목들은 공인인증기관의 성적서 첨부/제출
* 단계별 목표의 달성을 위한 연차별 목표를 연구개발계획서에서 제시하고, 연차별 목표에 대한 평가항목 및 달성목표치를 정량적으로 제시(상세한 작성방법은 계획서 양식 참조)
* 연차 구분은 회계연도를 기준으로 설정 및 예산 배분
  예시) 응용연구 2년, 시험개발 2년인 과제의 경우

연구단계	응용연구			시험개발		
연차	1차년도	2차년도	3차년도	1차년도	2차년도	3차년도
연차별 기간	7개월 ('18.6~12)	12개월 ('19.1~12)	5개월 ('20.1~5)	7개월 ('20.6~12)	12개월 ('21.1~12)	5개월 ('22.1~5)
평가	▲ 진도평가	▲ 진도평가	▲ 단계평가	▲ 진도평가	▲ 진도평가	▲ 최종평가
예산 지급	▲	▲	▲	▲	▲	▲

* 개발단계(응용연구/시험개발)간 예산 이동 불가
* 재료비, 장비비 등은 사업 초기에 집행하여 활용도 제고

* 응용연구에서 개발된 시제품의 시험개발단계 재활용계획 제출

※ 연도별 연구개발 목표 작성양식은 아래와 같음. (예시이며, 계획서 양식 참조)

평가항목 (주요성능 Spec[1])	단위	전체항목에서 차지하는 비중[2] (%)	세계최고 수준 보유국/ 보유기업 (/) 성능수준	연구개발 전 국내 수준 성능 수준	개발 목표치[4] 응용연구 1차 년도	응용연구 2차 년도	응용연구 3차년도	시험개발 1차 년도	시험개발 2차 년도	평가방법[3]
탑재중량	Kg	5	30	23	≥30	≥30	≥30		≥30	
탐지거리	Km	15	20	15	≥20	≥20	≥20		≥20	
....										
....										

* 연구개발 최종 목표(1. 라항)를 달성하기 위한, 년도별 개발 목표치를 기술함.
(추후 진도 및 최종평가시 정량적 목표달성 기준으로 활용됨)

* 1차년도에서 정량적 목표 설정이 불가능한 경우, 설계 문서/자료, 분석자료 또는 기술현황 분석 등으로 기입하고, 계획서 뒤 부분 년차별 개발 목표/내용 및 평가에 상세히 기술

다. 사업기간 및 연구개발비

◆ 사업기간 : 3.5년(시험개발)

◆ 총 연구개발비 중 정부출연금 : 20억 이내

4. 적용 및 파급효과

가. 적용분야

◆ 민수

- **서버 보호에 적용**

⇒ 서버를 공격하기 위해 트래픽도 암호화되어 유입되는 경우, 보호하려는 다수의 서버가 아닌, 관제 시스템에서만 탐지기능을 수행하여 다수의 서버를 보호

- **VPN 환경에서의 적용**

⇒ 지사와 본사가 나눠져 있는 형태 혹은 한 지사 내에서의 기업 인트라넷을 보호하기 위하여 VPN을 활용 암호화하여 트래픽을 전송하는 경우, 암호화된 트래픽에 대한 심층 패킷 분석을 통해 침입탐지 기능을 수행

◆ 군수

- 국방 분야에서는 군 자체 내부망의 보안성을 강화시킬 수 있고 사이버 공격에 대한 침입 탐지 및 내부 기밀 유출 워터마킹 등을 효과적으로 관리할 수 있다.
- 암호화된 기밀자료 트래픽에 대한 패턴 매칭 기반의 워터마킹 탐지를 통해 내부 기밀 유출 탐지 및 차단을 수행할 수 있다.
- TICN과 같은 전술 네트워크의 경우 매우 유동적이기 때문에 고정된 평시 네트워크에 비해 더 강력한 관제 시스템이 필요하다. 따라서 전체 네트워크 트래픽을 효과적으로 제어할 수 있는 관제 시스템을 구축이 필요한 분야에 적용

※ 관련 적용분야를 제안 가능 (인용 근거 제시필요)

나. 파급효과

◆ 기술적 측면 :

- 상용화 가능한 수준의 실효성과 보안성을 갖춘 침임 탐지 기술 획득
- 하드웨어와 소프트웨어 보안 기술을 융합하여 보안성을 강화한 침입 탐지/차단 및 관제 기술 획득
- 국내 네트워크 기능 가상화 및 보안 솔루션을 보유한 기업과의 협약을 통해 기술이전 추진
- 기술 이전한 기업과의 협력을 통해 암호화된 트래픽을 처리할 수 있는 기술을 NFV 솔루션에 탑재

◆ 경제·산업적 측면 :

- 외부 트래픽으로부터 보호되어야 할 기간 시설에 대한 (발전소 및 수도 시설 등) 보안 강화
- 전문 인력 양성 및 국내 정보보호 기술 수준 제고

◆ 군사적 측면

- 외산 장비 및 민수에 의존하지 않고 군용 자체의 네트워크 보안 시스템 구축 가능
- 군별, 계층별 다양하게 분리된 군 내부망간 유통되는 트래픽 정보 유출

탐지 및 침입 탐지를 통한 보안 강화

- 적의 침입으로부터 방어할 수 있는 사이버 정보전 방어 기술 획득

※ 관련 분야별 파급효과 제안 가능 (인용 근거 제시필요)

5. 연구개발 결과 제시물 및 평가항목

가. 연구개발 결과 최종 제시물

◆ H/W기반 암호화된 트래픽 처리를 위한 보안성을 갖춘 침입 탐지 및 차단 시스템 1식

- 강건한 Key 전달 protocol / 소프트웨어 등

◆ 기술자료 1식

- H/W, S/W 설계 보고서
- 설계도면 등

※ ① 시제 개념도(형상), 시제 수량 및 필요수량 근거 제시
② 시제 검증을 위해 제작되는 장비,모듈 또는 Zig 제시
③ 상세 기술자료 및 설계문서 등 제시

나. 연구개발 결과 평가항목

◆ **(년도별) 개발 목표/내용 및 평가**

1) 개발목표

- 개조식으로 구체적으로 서술
- 개발하고자 하는 기술(또는 공정)의 수준, 성능 품질을 가능한 한 정량적으로 기술

2) 개발범위 및 내용

- 목표달성을 위해 수행할 세부내용 및 이에 대한 구체적 설명을 서술
- 시제품이 제작되는 경우 제작할 시제품의 목표, 사양, 성능, 용도, 기능 등을 명시 (총 개발기간에 해당되는 연차별 사항 기입)

3) 평가 항목 및 방법 / 조건

- 평가항목에 대하여 년차별 평가 절차/방법 및 측정 방법을 구체적으로 기술
- 단계종료 및 최종종료 시는 평가항목 및 방법 등에 대하여 종합적으로 기술 가능

※ ① 최종평가시 모든 평가 항목들은 공인인증기관의 성적서 첨부/제출
② 평가시 **평가 방법 및 조건**을 명확히 기술
③ 추후 진도 및 최종평가시 **목표달성 기준**으로 활용됨
④ 최종 계획서 양식 적용

6. 참여 요건

가. 추진 체계 요건

◆ **주관연구기관 및 참여기관 : 민군기술협력사업 촉진법 제7조 2항 및 동법 시행령 제14조 2항 각 호에 해당하는 기관 또는 단체**

* 응용연구 및 시험개발의 경우에는 주관연구기관 또는 참여기관에 1개 이상의 기업 참여 필수(민·군기술협력사업 공동시행규정 제27조 4항)

◆ **기업분담율** : 민·군기술협력사업 공동시행규정 제27조(별표4)

나. 연구책임자의 자격 및 과제 신청요건

◆ **연구책임자의 자격**

관련분야의 연구 경험이 풍부한 중견 연구자를 책임자로 선임하여 연구의 최종 목표를 달성할 수 있도록 계획, 업무프로세스 정립, 원활한 추진 및 조정과 과제 관리를 수행할 수 있어야 한다.

◆ **과제 신청요건**

주관연구기관은 제안한 연구개발 목표를 충분히 달성할 수 있는 연구팀을 구성하여야 하며, 필요시 컨소시엄을 구성할 수 있다.

다. 기타

◆ 연구개발계획서는 민·군기술협력사업 공동시행규정 별지 서식 제4-1C호 (연구개발계획서)를 준용하여 작성

◆ 그림, 표 등 인용자료는 반드시 인용처 표기

◆ 필요시설 및 장비는 자체보유 또는 타 기관 시설 활용계획 명시 요망

7. 참고문헌

[1] C. Yoon et al., “Flow Wars: Systemizing the Attack Surface and Defenses in Software-Defined Networks”, In Proc. IEEE/ACM Transaction on Networking, 2017.

8. 과제 문의사항 연락처

소 속	성 명	연락처
민군협력진흥원	김도선	042-607-6040