과학기술정보통신부 공고 제2024-0328호

붙임2. 2024년도 정보보호핵심원천기술개발사업 2차 신규지원 연장 대상과제 목록

※ 범부처통합연구지원시스템(IRIS) 內 신청·접수 과제 확인 방법

① 부문별 공고명 확인

ex. **2024년도 정보보호핵심원천기술개발사업 2차 신규지원 대상과제 공고**

② 세부사업명 및 내역사업명(공모방식) 확인

ex. 정보보호핵심원천기술개발 → 데이터 및 네트워크 보호기술개발(품목공모)

③ 과제명 확인 후 해당 RFP에 접수

ex. **(RFP명) 데이터 프라이버시 전주기적 보호 컴퓨팅 기술 개발**

(단위 : 억원)

부문	번호	세부 사업명	내역 사업명	과제명	총 수행 기간	'24년 정부지원 (총 정부지원)	공모 방식	연구 단계 (TRL)	주관 기관	과제특징
보안·블록체인	1	정보보호핵심 원천기술개발	데이터 및 네트워크 보호기술개발	데이터 프라이버시 전주기적 보호 컴퓨팅 기술 개발	4년	12 (57.3)	품목 공모	응용 (3~6)	제한 없음	▸ 임무지향형 ▸ 혁신도약형
	3	정보보호핵심 원천기술개발	데이터 및 네트워크 보호기술개발	AI 모델 취약성 분석, 평가 기술 및 생성정보 비밀성 판단 도구 개발	3년	12 (41.3)	품목 공모	개발 (4~7)	제한 없음	▸ 임무지향형 ▸ 혁신도약형
	6	정보보호핵심 원천기술개발	데이터 및 네트워크 보호기술개발	이동통신 및 AirGap 환경에서 스니핑 방지 기술 개발	3년	12 (41.3)	지정 공모	응용 (4~6)	제한 없음	▸ 임무지향형 ▸ 혁신도약형
	14	정보보호핵심 원천기술개발	취약점대응 및신산업융합 보호기술개발	메모리 안전 언어의 적용 확대 및 안전 적용을 위한 통합 플랫폼 기술 개발	4년	10.5 (50.17)	지정 공모	응용 (3~6)	제한 없음	▸ 임무지향형 ▸ 혁신도약형

[참고] 과제목록 용어 및 공모방식 설명

※ 과제목록 용어 설명

용어		내용설명
예산		○ 정부지원연구개발비를 의미 ○ 하나의 과제번호에 여러 과제를 선정하는 경우, 과제당 최대 예산은 정부지원연구개발비를 과제명에 표기된 과제 개수로 정률 배분한 예산임 * 예: <'24년 4개과제x9억원, 총예산 84억원 과제>의 경우, 과제당 예산은 '24년 9억원, 총 21억원 이내임
기술료	징수	○ 과제특징에 '기술료비징수'라고 표기되지 않은 모든 과제는 기술료 징수 대상과제임
	비징수	○ '기술료비징수' 과제는 연구개발성과의 활용 촉진을 위해 연구개발성과를 공개 활용하는 과제로 기술료를 비징수함 *「국가연구개발혁신법」 제18조 3항 및 동법 시행령 제40조
혁신도약형 R&D (=고위험도전형)		○ 패러다임의 전환, 새로운 시장 창출 등 기술 혁신으로 연결될 수 있는 도전적·창의적 연구개발 과제 ○ 연구자의 몰입연구가 가능하도록 단계평가 부담을 완화시키고, 연구개발 결과를 중점적으로 평가하여 평가등급 부여 *「국가연구개발 과제평가 표준지침」
보안과제		○ 방위력개선사업 관련 과제, 외국에서 기술이전을 거부하여 국산화를 추진 중인 과제, 미래핵심기술, 국가핵심기술, 수출허가 등 제한이 필요한 기술에 대해 보안과제 지정 *「국가연구개발혁신법」 제 21조 2항 및 동법 시행령 45조 2항
수요기업		○ 참여기업 중 연구개발 과정에서 제품·장치·서비스의 성능평가·검증 등을 수행하고 해당 연구개발과제에서 개발하는 제품·장치·서비스의 구매를 희망하는 기업을 말함 * 과제에 수요기업으로 참여하는 기업은 기업 유형에 상관없이 중소기업 기준의 정부지원연구개발비 지원기준 및 기관부담연구개발비 현금부담 기준을 적용받을 수 있으며, 주관연구개발기관 또는 공동연구개발기관의 개발제품을 구매할 경우 기술료 감면 가능 ** 수요기업은 정부지원연구개발비 지원없이 과제 참여 가능하며, 이 경우 기관부담연구개발비 현금부담을 면제 가능함
임무지향·문제해결형		o R&D 성과의 산업적 파급효과 극대화를 위해 시장 수요를 사전에 발굴하고, 해결할 문제(또는 임무)를 제시하는 과제

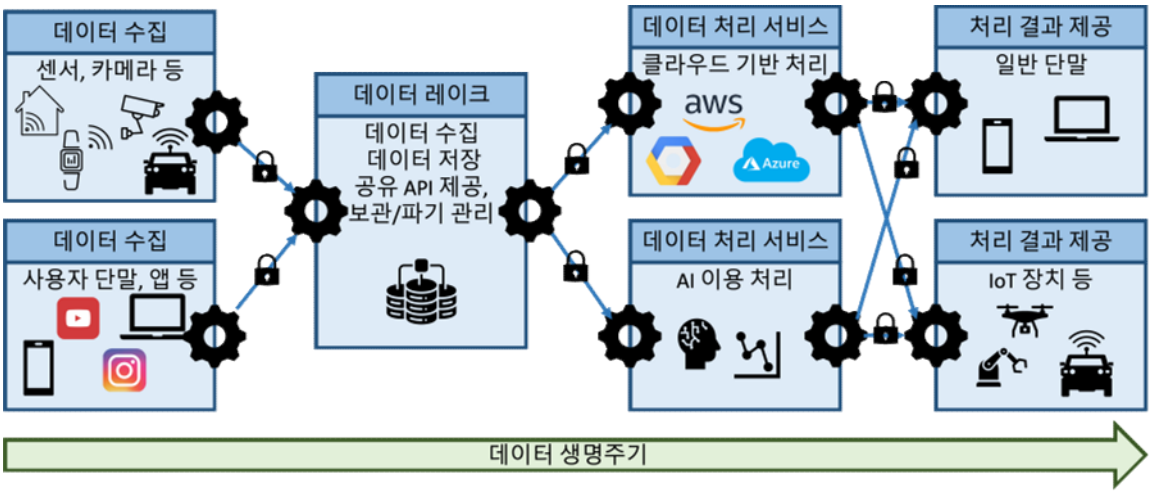
※ 공모방식에 대한 설명

공모방식	내용 설명
지정공모	해당 연구개발과제가 정책적으로 필요하다고 인정되어 장관이 지정하되 그 연구개발기관은 공모에 따라 선정하는 방식으로서 개발이 필요한 대상기술과 기술목표를 과제제안요구서(RFP)에 제시
품목(문제)공모	품목(문제)를 정의·제시하면, 연구개발기관이 제시된 품목 지원 범위 안에서 개발내용을 자유롭게 제안 (해결 문제가 정의된 경우 문제해결에 필요한 연구목표, 연구내용 및 최종 결과물 등을 자유롭게 제안)

관리번호	2024-정보보호-01	(품목공모형)
기술분류	대분류(차세대보안)-중분류(데이터 및 응용 서비스보안)-소분류(데이터 보안)-세분류(프라이버시 보호)	
중점분야	AI( ), AI반도체( ), 5G·6G( ), 양자( ), 메타버스( ), 사이버보안(√)	
기획유형	임무지향형R&D(√), 문제해결형R&D( ), 기술축적형R&D( )	
품목(문제)명	데이터 프라이버시 전주기적 보호 컴퓨팅 기술 개발	

1. 품목(문제) 정의

○ **(개념)** 데이터 프라이버시에 대한 정보주체의 통제권을 강화하기 위해, 데이터의 전체 생명주기 (생성/수집, 전달, 사용/처리, 보관, 파기)에 걸친 잠재적 침해에 대응하기 위한 유연하며 표준화된 데이터 프라이버시 보호 및 처리 기술 개발



<개발 기술 개념도>

* 데이터 레이크 : 대량의 데이터를 수집, 저장하며 처리될 수 있도록 제공해주는 서비스 계층

○ **(목표)** 데이터의 전체 생명주기에 걸친 유연하며* 통합적*인 통제권 강화에 필요한 기반 기술, 라이브러리 (미들웨어) 및 프로토콜 등을 개발 및 공개.

* 유연성 : 기밀성, 무결성, 보관, 처리 등 다양한 공격모델 및 활용 시나리오 지원

* 통합성 : 시스템 구조 및 구성 노드 등에 무관한 데이터 공유 범위 정의 모델 제공

As is	To Be
○ **[장치 및 채널 수준 보안]** 기존 기법들은 장치간의 상호인증 및 보안 채널 (secure channel) 생성에 주로 집중. ○ **[채널 수준 기밀성]** 기존 기법은 전송단계에서의 데이터 기밀성 보호에 집중. 타 단계에서의 기밀성 보호기술과 연계될 수 없어 데이터 활용주기에 관여하는 모든 장치에 데이터 노출. ○ **[장치별 접근 제어]** 기존 기법은 접근제어	○ **[데이터 및 사용자 수준 보안]** 생성, 저장 및 활용되는 데이터의 기밀성을 사용자 중심으로 실제 처리되는 장치들 및 하위 프로토콜과 독립적으로 보호해 주는 기법 개발 필요. ○ **[전주기 기밀성]** 생성, 전송, 저장, 처리 등 단계를 통합적으로 고려한 기밀성 보호 프레임워크 개발을 통해 데이터 노출 대상 최소화 필요.

방법을 장치 수준에서 접근제어리스트(Access Control List, ACL) 형태로 정의 및 활용. 데이터 유형별 분류 및 전체 시스템 수준에서의 접근제어 정책 설정 불가. o **[개별 노드의 자의적 데이터 보호 및 공유]**개인정보 생명주기상에 존재하는 각 노드가 개발사의 의도에 따라 개별적으로 데이터에 대한 보호기술 및 공유 권한 정의 및 구현 o **[CNN 등 전통적인 연산 대한 특화]** 기밀컴퓨팅, 암호컴퓨팅 등 프라이버시 강화 기술 기반의 침해탐지기술이 비교적 전통적으로 사용되는 연산유형들에만 특화 됨	o **[데이터별 접근제어]** 데이터 유형별 접근제어 권한 설정 및 적용 방법 필요. 데이터가 현재 존재하는 장치 또는 전달중인 보안 채널 등과 독립적인 사용자 중심의 접근 제어 기법 개발 및 활용 필요. o **[통합적 보호수준 및 정책 정의 및 구현]** 각 개인정보 및 파생정보에 요구 보호수준 및 공유 권한 정의를 연동하고, 공통된 라이브러리를 이용해 통합적 정책 적용 및 보호 구현 o **[Transformer 등 새롭게 도입 및 활용되고있는 연산에 대한 특화]** 프라이버시 강화 기술을 Transformer 등 새롭게 연구 및 활용되고 있는 유형의 연산에 특화

o (연구내용)

(1) 데이터 유출 및 변조 등 보안 문제 발생 시나리오 및 보호 기술 요구사항 분석
- 데이터의 생명주기 각 단계에서 발생할 수 있는 보안 사고 시나리오 수집 및 분석
- 각 보안 사고 시나리오에 맞는 보호기술 요구사항 분석
- 분석된 보안 사고 시나리오 대응 기법 평가를 위한 테스트베드 구축 및 지표 도출

(2) 일원화된 데이터 보안 정책 인터페이스 개발
- 다양한 유형의 연산 및 기밀 컴퓨팅 환경을 고려한 일원화된 보호 정책 적용 인터페이스 계층 개발
- 데이터의 생명주기를 고려해 보안 정책이 적용된 안전한 데이터 송수신을 위한 동적 전송 채널 토폴로지 구성 및 관리 기술 개발
- 세 가지 이상의 환경에 대해 보안 정책 적용 라이브러리 개발 및 성능 최적화
  * 세 가지 환경은 자유 선정 (예 : 센서 노드, 외부 클라우드, 사용자 단말 등)

(3) 데이터별 접근제어 정책 명세 기법 및 일원화된 적용 기법 개발
- 데이터별 접근제어 정책 명세 기법 및 일원화된 적용 기법 개발
- 데이터 생명주기 중 접근제어 정책 기밀성, 무결성 및 가용성 보장 기술 개발
- 정의된 보호 정책 기반의 데이터 생명주기 및 실행환경별 파생 보안 정책 자동 도출 기법 개발 및 적용

(4) Transformer 등 최근 활발히 연구되는 AI연산에 특화된 침해 탐지 및 보호 기술
- Transformer 등 널리 쓰이는 AI연산에 대한 지원을 인터페이스 계층에 추가
- 개발된 인터페이스가 지원하는 AI연산의 성능 극대화를 위한 연산 라이브러리 개발
- 개발된 인터페이스 지원 AI연산의 워크로드의 특성을 고려한 최적화 기술 개발

2. 현황 및 필요성

ㅇ **(기존 기술현황)**

- **(개인정보 활용 환경의 복잡성)** 우리의 개인 정보는 점점 다양하고 인지하기 힘든 경로로 우리 주변 장치의 입력이 되고 여러 주체에 의해 활용되고 있음. 우리가 사용하는 스마트폰, PC등의 단말 뿐 아니라, 점점 더 많은 센서들이 네트워크에 직접 연결되어 개인정보의 수집 수단이 되고 있으며, 이는 다양한 주체로 전달되어 여러 서비스 구현을 위해 사용/처리 및 보관되며, 여러 제반 규정에 의해 파기되어야 함.
- **(정보주체의 통제 어려움)** 이와같이 전례없이 다양한 장치 (노드)로 구성된 클라우드 활용이 일반화되면서, 정보주체들이 개인정보의 생성, 흐름 등을 인지하기가 점점 어려워지고 있으며, 이는 정보주체의 통제 능력 상실로 이어지고 있음.

ㅇ **(필요성)**

- **(보호·처리 기술 개발의 필요성)** 이와같이 복잡한 개인정보 활용 환경 하에서 정보주체가 개인정보에 대한 강한 통제권을 가질 수 있도록 하기 위서는, 개인정보의 전체 생명주기 (생성/수집, 전달, 사용/처리, 보관, 파기)에 걸쳐 침해 요소 및 경로를 탐지하고 이에 대응할 수 있는 유연하며 표준화된 개인정보 보호 및 처리 기술 개발이 필요함

3. 수요분석

ㅇ **(주요 수요처)** 프라이버시를 보장하며 개인정보를 생성, 배포, 활용하는 기업 및 기관, 개인정보 생명주기에 따라 개인정보에 대한 통제권을 가지고자 하는 기관 및 개인

ㅇ **(협력방안)** 개인정보의 생명주기에 따른 관련 사업자 및 기관들과 협력하여 개인정보 보호 요구사항 파악 및 개발기술의 활용 방안 제시

4. 기대 효과

ㅇ 다양한 개인정보 기반 서비스 기업들이 개인정보 관리 형태에 대한 정보를 더욱 명료하게 사용자에게 제공하여, 개인정보 유출에 대한 사용자의 우려를 불식시키고 시장을 확대해갈 수 있음.

ㅇ 빠르게 성장하는 프라이버시 보안 기술 시장에서 국내 보안 기업들의 기술 및 시장 경쟁력 제고 (Privacy Management Software 시장은 2023년 27억 달러에서 2028년 152억달러까지 성장할 것으로 예상, marketsandmarkets.com)

5. 개발기간/예산/추진체계

ㅇ **연구개발기간** : 4년 이내

ㅇ **정부지원연구개발비** : ‘24년 12억원 이내(총 정부지원연구개발비 57.3억원 이내)

구분	기간	개월수	정부지원연구개발비
1년차	'24.6월~'25.2월	9개월	1,200 백만원 이내
2년차	'25.3월~'25.12월	10개월	1,330 백만원 이내
3년차	'26.1월~'26.12월	12개월	1,600 백만원 이내
4년차	'27.1월~'27.12월	12개월	1,600 백만원 이내
합계	-	43개월	5,730 백만원 이내

* 연차별 정부지원연구개발비는 당해연도 예산심의결과에 따라 변동될 수 있음

ㅇ **주관기관** : 제한없음

연구유형	기초연구 ( ), 응용연구 (√), 개발연구 ( )	TRL (3)~(6)단계
과제특징	경쟁형( ), 경쟁형(챌린지)( ), SW자산뱅크등록( ), 공개SW( ), 기술료비징수( ) 국제협력R&D( ), 정책지정( ), 혁신도약형(√), 표준화연계( ), 사회문제해결형( ), 일자리연계( ), 소재부품장비( ), 규제샌드박스( ), 연구데이터공개( ), 사업화연계( ), IP-R&D연계( )	

구분	기술분야명/팀명	성명
책임PM(과제기획위원장)	보안·블록체인	정현철
담당 팀장	사이버보안팀	김남훈

관리번호	2024-정보보호-03	(품목공모형)
기술분류	대분류(차세대보안)-중분류(융합보안)-소분류(기타ICT보안)-세분류(인공지능 및 로봇 보안)	
중점분야	AI( ), AI반도체( ), 5G·6G( ), 양자( ), 메타버스( ), 사이버보안(√)	
기획유형	임무지향형R&D(√), 문제해결형R&D( ), 기술축적형R&D( )	
품목(문제)명	AI 모델 취약성 분석, 평가 기술 및 생성정보 비밀성 판단 도구 개발	

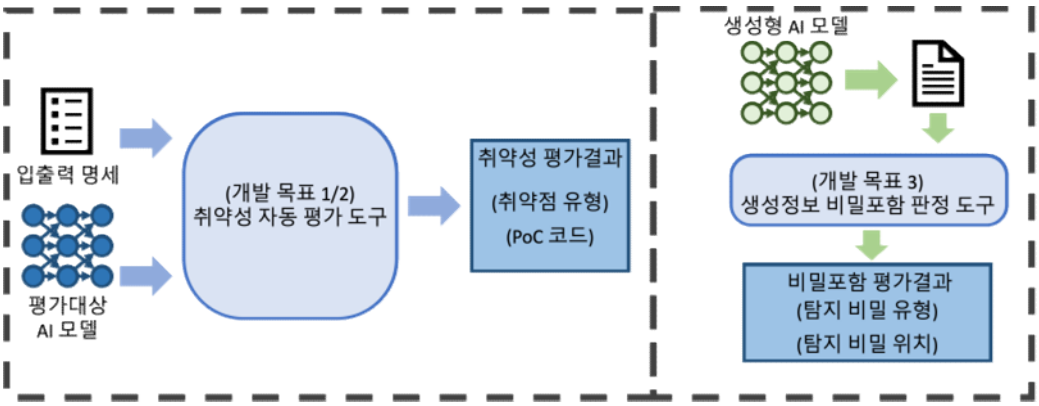
1. 품목(문제) 정의

○ **(배경)**

- 軍은 정부의 'AI 과학기술 강군' 육성을 위해 조직 · 법규 정비, 전문가 양성, 신규사업 활성화 등 각고의 노력 중
- 반면, AI모델과 관련된 다양한 보안취약점(탈취, 중동, 회피, 전도, 추출 공격 등)이 공개되고 있으나, AI모델 내 취약점 내재 여부를 검증 가능한 범용기술 부재
- 또한, 일반 데이터를 학습하여 개발된 생성형 AI에 의해 비밀 · 개인정보가 생성될 수 있으나, 개인정보를 식별 가능한 기술은 존재하는 반면, 군사자료(비밀) 생성여부 및 민감도를 판단 가능한 기술 부재

○ **(개념)** 인공신경망 기반의 AI 모델들은 잠재적으로 여러 종류의 취약성을 가질 수 있음이 알려져있음 [Papernot18]. 그럼에도 불구하고 이런 AI 모델들을 기반으로 자율주행, 데이터 분석, 문서 생성 등 여러 기술은 향후 높은 수준의 비밀들을 다루는 군 관련 분야에서도 AI 모델의 활용을 피하기 어렵게 할 것으로 생각됨.

* [Papernot18] N. Papernot, P. McDaniel, A. Sinha and M. P. Wellman, "SoK: Security and Privacy in Machine Learning,"2018 IEEE European Symposium on Security and Privacy (EuroS&P), London, UK, 2018, pp. 399-414, doi: 10.1109/EuroSP.2018.00035.



<개발 기술 개념도>

○ **(목표**)** 주어진 AI 모델이 비밀 정보 생성, 학습 데이터 역추출 · 탈취, 연산 과정

무결성 등 측면에서 일반적으로 알려진 유형의 AI 모델 수준 취약성을 갖는지 여부를 자동으로 평가하는 기술 개발

As is	To Be
o **[AI 모델 기밀성 공격 평가기술 범용성 부족]** 학습 데이터 탈취 공격 등 기밀성 공격 저항성 평가기술이 AI 모델의 개발목적 및 대상 데이터 유형 등에 따라 별도 개발됨	o **[AI 모델 기밀성 공격 평가기술 범용화]** 다양한 데이터 유형 및 목적을 위해 개발된 AI 모델에 대한 기밀성 공격 (학습데이터 역추출·탈취 공격 등) 저항성 범용 평가 기술 개발
o **[AI 모델 무결성 공격 평가 기술 범용성 부족]** AI 모델의 생성, 추론 결과 및 과정 등의 무결성에 영향을 주는 여러 공격에 대한 평가 기법이 AI 모델의 개발목적 및 대상 데이터 유형 등에 따라 별도 개발됨	o **[AI 모델 무결성 공격 평가 기술 범용화]** Data poisoning, 백도어 삽입 등의 무결성 공격에 대한 저항성 평가기술을 대상 데이터 유형 및 목적에 무관하게 활용할 수 있도록 범용화
o **[AI 모델 생성정보의 기밀 누출 가능성 평가 기술 부재]** AI 모델의 정보 생성 과정에서 발생할 수 있는 군 기밀 누출 가능성 평가 기술 부재	o **[군 기밀 정의 기반 판정 기술]** 자연어 등 비정형 데이터로 생성될 수 있는 AI 모델 생성 결과물에 대한 비밀성 판정 기술 개발. 비밀성의 정의로는 이미 공개되어 있는 군 기밀 정의 문서 (자연어 작성) 이용
o **[AI 모델 평가 지표 및 방법론 부재]** AI 모델의 안전성 수준에 대한 일반화 가능한 평가 지표 및 방법론 부재	o **[AI 모델 평가 지표 및 방법론 개발]** AI 모델의 안전성 수준에 대한 평가 지표 제시 및 평가 방법론 개발

o **(연구내용)**

- **목표 1 : AI 모델의 자동 평가를 위한 평가 지표 및 방법론 개발**
  . 학계의 최신 자동 평가 기술 동향 파악
  . 세계 각국의 기관들에서 사용하고있는 AI 모델 취약성 평가 지표 및 방법론 조사 및 비교분석

- **목표 2 : 예제 또는 입출력 명세 기반 AI 모델 학습 데이터 역추출·탈취 공격 자동화 및 결과 자동 평가 기술 개발**
  . 주어진 AI 모델의 사용환경 정보를 예시 입출력 또는 입출력 명세 등으로 획득
  . 사용환경 정보를 기반으로 학습 데이터 역추출·탈취 공격 자동 수행
  . 공격 수행 결과 기반 AI 모델의 역추출·탈취 공격 대상 취약성 수준 자동 평가
  . 평가 결과를 취약여부, 취약성에대한 PoC (Proof-of-Concept) 공격 등의 형태로 생성
  . 성능 목표
  > 3종 이상 유형의 데이터에 대한 적용
  ※ 유형은 텍스트, 이미지, 비디오 포함, 관련 사이트(https://paperswithcode.com/datasets) Modality 항목 기준

https://paperswithcode.com/datasets

> 정탐률 (Sensitivity) : 98%

> 정확도 (Accuracy) : 90%

> 신규 (zero-day) 취약점 식별 : 1건 이상

※ 정탐률 : 전체 취약성 positive 중 실제로 탐지된 positive 수

$$\frac{True\ Positive}{True\ Positive + False\ Negative}$$

※ 정확도 : 전체 시도 중 true positive와 false negative의 수

$$\frac{True\ Positive\ +\ True\ Negative}{True\ Positive\ +\ False\ Positive\ +\ True\ Negative\ +\ False\ Negative}$$

※ 성능 목표 달성 여부 검증용 데이터 셋은 수요기관과 협의하여 결정

※ 신규 (zero-day) 취약점이란, 새로운 유형의 취약점을 의미하는 것이 아닌, 특정 AI 모델이 가진 별도로 보고된 바 없는 취약점을 의미함

- 목표 3 : 예제 또는 입출력 명세 기반 연산과정 무결성 측면의 취약성 자동 평가 기술 개발

. 무결성 측면에서의 공격 기법 및 경로 분석

. Data poisoning, 백도어 등 포함한 무결성 측면 취약성 자동 평가 기술 개발

. 무결성 측면 공격을 활용해 AI모델에 적대적 교란을 발생시킬 수 있는 적대적 AI 모델 또는 소프트웨어, 알고리즘 등 개발

> 3종 이상 유형의 데이터에 대한 적용

> 정탐률 (Sensitivity) : 98%

> 정확도 (Accuracy) : 90%

> 신규 (zero-day) 취약점 식별 : 1건 이상

※ 데이터 유형, 검증용 데이터 셋 조건, 정탐률, 정확도, 신규 취약점 정의는 목표 2 참조

- 목표 4 : AI 모델 생성 정보의 비밀(민감)성 판정 기술 개발

. 군사비밀 분류기준 등 *자연어로 문서화된 비밀의 정의를 기반으로 주어진 생성형 AI 모델의 생성 결과가 비밀정보를 포함하는지 여부를 판정하는 기술 개발

. 군사비밀을 이용한 AI 모델 학습 시 추후 민감 데이터 유출 대응을 위한 특정 정보 (Tag) 삽입 및 활용 기술 개발

> 목표 탐지 정확도 (accuracy) : 90%

※ 자연어로 문서화된 비밀의 정의란 군사기밀 보호법 시행령의 [별표 1]을 의미함.

2. 현황 및 필요성

o (필요성)

- 한정된 목적(안면인식, 자율주행 등)으로 개발된 AI모델의 특정 보안취약점은 학술적 수준으로 지속 연구 · 발표 中
- 반면, 다양한 AI 학습데이터 및 모델 유형을 고려하여 개발된 AI 모델의 보안

취약점을 범용적으로 분석 가능한 검증기술은 개발된 바 없어 개발 절실
- 국가적으로 보안취약점이 내재된 AI가 확산된 이후 '사후약방문 식'으로 보완조치가 진행되지 않도록 선제면역 필요

3. 수요분석

ㅇ **(주요 수요처)**
- 국방AI체계에 대한 보안평가(측정) 및 보안적합성검증 등에 활용
- 민간 시장에서도 AI모델 외부 도입 시 적용 및 활용될 수 있음

ㅇ **(협력 방안)**
- 부처 수요기관과의 협력을 위한 회의체/협의체 등을 구성하고 수요기관과 실증(실증에 필요한 결과물을 수요기관에 제공)
- 부처 수요기관에서 제시하는 보안대책 준수

4. 기대 효과

ㅇ 국방 분야에 도입되어 주요 기밀 처리용 장비 및 군 무기체계 등에 대한 취약 AI 모델 적용 가능성 차단

ㅇ 자동화된 기밀정보 생성 여부 확인 및 차단 기능 도입으로, 기밀 정보 처리 과정에 대한 생성형 AI 모델 도입 및 이를 통한 생산성 증대 가능

ㅇ 군 수준의 높은 동화된 기밀정보 생성 여부 확인 및 차단 기능 도입으로, 기밀 정보 처리 과정에 대한 생성형 AI 모델 도입 및 이를 통한 생산성 증대 가능

ㅇ 이러한 기술은 군 뿐 아니라 기업 등 특정 단체 수준의 비밀 정보 관리가필요한 AI 모델 수요처들에서 필요로 하며 활용 가능

5. 개발기간/예산/추진체계

ㅇ **연구개발기간** : 3년 이내

ㅇ **정부지원연구개발비** : '24년 12억원 이내(총 정부지원연구개발비 41.3억원 이내)

구분	기간	개월수	정부지원연구개발비
1년차	'24.6월~'25.2월	9개월	1,200 백만원 이내
2년차	'25.3월~'25.12월	10개월	1,330 백만원 이내
3년차	'26.1월~'26.12월	12개월	1,600 백만원 이내
합계	-	31개월	4,130 백만원 이내

* 연차별 정부지원연구개발비는 당해연도 예산심의결과에 따라 변동될 수 있음

ㅇ **주관기관** : 제한없음

연구유형	기초연구 ( ), 응용연구 ( ), 개발연구 (√)	TRL (4)~(7)단계
과제특징	경쟁형( ), 경쟁형(챌린지)( ), SW자산뱅크등록( ), 공개SW( ), 기술료비징수( ) 국제협력R&D( ), 정책지정( ), 혁신도약형(√), 표준화연계( ), 사회문제해결형( ), 일자리연계( ), 소재부품장비( ), 규제샌드박스( ), 연구데이터공개( ), 사업화연계( ), IP-R&D연계( )	

구분	기술분야명/팀명	성명
책임PM(과제기획위원장)	보안·블록체인	정현철

담당 팀장	사이버보안팀	김남훈

관리번호	2024-정보보호-06	(지정공모형)
기술분류	대분류(차세대보안)-중분류(네트워크보안)-소분류(무선네트워크 보안)-세분류(이동 통신망 보안)	
중점분야	AI( ), AI반도체( ), 5G·6G( ), 양자( ), 메타버스( ), 사이버보안(√)	
기획유형	임무지향형R&D(√), 문제해결형R&D( ), 기술축적형R&D( )	
과제명	이동통신 및 AirGap 환경에서 스니핑 방지 기술 개발	

1. 개요

○ **(배경)** 정보획득을 위한 각 국의 시도는 수단과 방법을 가리지 않고 있으며, 각 국의 정보기관이나 국가 배후세력의 공격 기술은 새로운 IT 기술 출현과 결합해서 국가, 경제, 안보 분야에서 가장 심각한 위협으로 대두

※ 미국 중앙정보국(CIA) 등이 한국을 포함한 우방과 적을 감시한 정황을 담은 기밀문서가 공개되어 파문('23.4.)

※ 나라장터 발주품목 조사결과 정부기관의 '상시형 도청방지장비' 도입 수준은 15.4%로 확인('23.4, 한국경제)

구분	사례	기법
국가 정보전	(2023년) 미국이 한국, 이스라엘, 프랑스 등을 감청한 정황이 담긴 기밀 문건이 유출	스파이앱, 템페스트, 레이저도청, 초소형도청 등
	(2021년) 이스라엘이 개발한 스마트폰 스파이앱(페가수스)을 이용, 프랑스 주요 인사를 대상으로 무차별 도감청 및 정보유출 수행	
	(2021년) 미국 정보기관(NSA)와 덴마크 정보기관(FE)가 협력, 2012년부터 2014년까지 덴마크 해저케이블을 통해 유럽 정/관계인사 도청을 수행	
	(2020년) 미국 워싱턴포스트(WP), 미국 CIA가 1970년부터 2018년까지 40여 년 전 세계 120여 개국을 상대로 첩보 활동 폭로	
AirGap 환경 정보유출	(2020년) 벤구리온대학 연구팀(이스라엘)은 분리망 환경에서 컴퓨터의 하드 드라이브 LED를 조작하여 데이터를 비트 단위로 전송하는 기술을 시연	
	(2019년) 러트거즈대(미국)은 스마트폰 모션 센서가 기록한 정보에 무제한으로 접근할 수 있다는 사실을 공개(안드로이드, 삼성 갤럭시 등)	
사이버범죄	(2023년) 경찰 애플리케이션(앱)을 사칭한 악성 도청앱을 피해자 휴대전화에 깔아 60억 원대 사기를 벌인 보이스피싱 범죄 적발	악성앱 설치
	(2021년) 미국 FBI, 피해자 스마트폰의 유심을 복제해 피해자의 개인정보 또는 은행계좌, 가상화폐 계좌를 확보한 후 금융자산 탈취 ※ FBI 발표 : '21년 1,611건(6,800만달러) 피해접수, 년간 5배이상 증가	심스와핑 (USIM 복제)

○ **(문제점)** 디지털 정보유출 기법이 소형녹음기, 전자파, 레이저를 이용하는 전통적인 방법에서 보다 대중적인 환경에서 대규모 정보유출이 가능한 스마트폰, IoT 기기 등으로 해킹 대상 환경이 빠르게 변화하고 있음

- 스마트폰 및 이동통신분야 도청방지 기술은 이동통신 모뎀칩/통신프로토콜 취약점 분석, 하드웨어 보안 모듈, 어플리케이션 연구가 국내외적으로 연구되고 있으나, 복잡성, 호환성, 우회기법 출현 이슈 등으로 기초 연구 단계에 있으며 종합적인 분석 연구는 아직 초기 단계
- 이스라엘 및 국내 일부 대학에서 AirGap 분리망 환경에서 네트워크 취약점, 분리망간

정보유출 시도, IoT 기기 프로토콜 취약점 및 스마트폰 센서의 발생 정보 분석 연구를 통해 그 가능성을 진행 중이나 개념증명(PoC) 수준의 기초 연구 단계

○ **(중요성)** 주요 국가들은 사이버공간에서 고도화된 정보유출 기술과 이를 탐지하고 방어하는 기술을 바탕으로 국가 안보를 강화하고 있는 가운데, 우리나라도 이에 상응하는 관련 기술을 개발하고 확보함으로써 국가, 기업, 국민이 안심하는 환경 마련이 중요

2. 현황 및 필요성

○ **(기존 기술현황)** 정보유출(도청)수단에 따라 대응기술은 상이하며, 전자파 차단, 교란, 등 도청방해기술, 초소형 도청장비 탐지기술 등을 중심으로 연구와 관련 제품 존재

○ **(기술 고도화)** 다양한 멀티모달 형태로 정보의 유출이 이루어지고 있으며 이동통신망과 스마트폰 환경은 물론 상대적으로 안전한 분리망 환경에서도 취약점 기반의 정보유출 위협이 만연

* 멀티모달 : 사람과 기기(컴퓨터)간 통신하기 위한 인터페이스로 텍스트, 음성, 영상, RF 신호, 키보드 등의 다양한 사용자 입출력 방식을 통칭

- (이동통신 취약요소) 스마트폰과 이동통신망의 취약요소를 악용한 도감청 및 정보유출 시도가 국가간 첨예한 정보 획득 수단으로 진행
- (AirGap 우회) 안전성 강화를 위해 구축한 분리망 환경에서도 스마트기기, 펌웨어, 네트워크 프로토콜의 취약점을 이용한 정보 유출 및 침투가 가능

구분	설명	정보유출 기법	방지 기술
녹음기 도청	특정한 위치에 설치해놓고, 소리를 실시간으로 녹음기기	초소형 기기	신호 탐지
전자파 도청 (템페스트)	PC 등 전자기기 전자파 수신 후 복원하는 기술	전자파 안테나	전자파 분석
유선전화 도청	유선전화기 선로를 Tapping 하여 통화내용을 도청	유선전화 도청장비	도청장비 탐지
레이저 도청	레이저를 쏴서 벽면/창문의 소리(진동)을 분석 후 음성으로 복원 기술	음파/진동 탐지	음성, 진동 주파수 분석 기술
AirGap 도청	외부와 단절된 네트워크 차단 환경에서 도청할 수 있는 기술	PC, 스피커 등 부채널 정보	PC 센서 부채널 정보 분석
스마트폰 도청	해킹, 무선구간(LTE, Wifi, 블루투스 등), 중계기 해킹, 가짜 기지국, 스피어폰(가속기), 이어스파이, USIM 탈취 등	스파이앱, 가짜 중계기, 무선이어폰, 스마트폰 센서 등	스파이앱탐지, 취약점분석, 무선통신분석, 복제방지 등
인터넷 통신도청	컴퓨터에 악성코드 침투시켜 인터넷전화, 이메일 등을 통해 정보 수집 및 도청	스파이앱, 무선 중계기, 네트워크 장비	DPI 기술
IoT 기기 도청	PC 스피커, IoT 가전제품(스피커) 비마이크 정보 이용한 도청 ※ 라이더폰(라이더센서), 램폰(전구) 등	IoT 기기(가속기 등 센서) 등으로 음성 복원	비아크 특징 및 부채널 분석, 비마이크 특징 분석

○ **(정부지원 필요성,** 국가안보강화**)** 국경이나 동맹이 무의미한 사이버공간에서 무차별적 정보수집을 시도하는 각 국의 최첨단 공격에 대한 방어 체계 수립은 국가안보 유지, 경제적 손실 방지, 사회적 신뢰 구축 및 사이버위협에 대한 지속적 대응이란 측면에서 매우 중요

- 정보 유출의 근본 원인인 보안 취약점을 빠르게 식별, 분석하고 점검 기술을 통해

원인을 제거할 수 있는 원천기술역량 확보가 중요

- 관련 기술의 독자적 확보가 어려워 해외에 의존할 경우, 공급망 보안 이슈와 백도어 이슈에 대해 적극적 대응의 어려움은 물론 사이버공간 자주권 확보에 지장
- 본 연구의 결과물은 원천기술 국가안보측면에서 우선적으로 사용하고, 기업에 기술이전을 통해 국내기술로 내재화 하는 방식이 추진을 위해 국가 R&D 예산을 투입하는 것이 적절하다고 판단

○ **(기술성)** 신호처리방식이 아날로그에서 디지털방식(이동통신 등)으로 진화, 스마트폰 고주파수 대역 사용, AirGap/비마이크 등 첨단기술 사용, 다양한 스텔스(은닉) 기법에 대한 대응 기술 연구는 기초 연구(논문, 개념증명) 단계 수준임

〔이동통신 환경 취약점 대응 및 스마트폰 음성 정보유출 방지 기술〕

- LTE, 5G 보안 관련된 연구가 출연연, 학계 중심으로 활발히 진행 중이나, 도청방지 등 정보유출 대응 기술에 집중된 연구는 아직 초기 단계
- 이동통신 단말 베이스밴드와 무선통신 프로토콜 취약점 연구는 카이스트(모뎀, 프로토콜 취약점), 고려대(펌웨어 보안) 등 진행
- LTE 및 5G 보안 관련된 암호 및 인증, 보안 아키텍처 등 전반적인 연구가 진행 중이나, 일부 제품과 버전에 제한한 연구 수준
- 스파이앱 관련 연구는 악성코드 분석의 일환으로 일부 다루고 있으나, 다양한 응용/부가기능 특화된 확장 연구는 미흡
- 허위기지국 관련 연구는 KAIST, ETRI, 국민대 등에서 기지국의 신호 및 트래픽 분석, 소형기지국 보안 취약점 등 기초연구를 수행
- KAIST(펨토셀 취약성 분석), ETRI(5G MEC 환경 탐지기술), 국민대(5G 허위기지국 탐지기술) 연구가 추진 중이나 실험실 수준으로 진행

〔AirGap 및 IoT 환경 정보유출 대응 기술〕

- 물리적 망분리 환경에 보안 의존, 다양한 IoT 기기의 취약점 연구 부족 및 새로운 공격 기술에 대한 대응 준비가 미흡한 상태
- 보안업체 펜테라(Pentera)는 민감한 데이터를 별도로 분리된 망에서 보관하고 있더라도 DNS 서버에 연결되어 있다면 데이터 침해 공격을 허용할 수 있다는 연구 결과를 발표
- 조선대(부채널 기반의 정보 유출 보호기술 연구), 충남대(IoT 기기 프로토콜 취약점 연구) 등의 기초 연구 진행
- ETRI(무선은닉채널 위험성 검증)는 약속된 송수신 디바이스간에 무선통신내 비정상 채널(WiFi 비콘 인터벌, 자기장 진폭변조, 발열 변화 등)을 형성하여 디지털 및 아날로그 신호의 전달 가능성을 검증하기 위한 기초 연구 진행

○ **(경제성)** 초고속으로 성장하는 5G 특화망 보안 시장에서 국내 보안기업의 기술 및 시장 경쟁력 제고

- 무선 및 사물인터넷 기술의 보급 확산으로 주요 정보의 도청위험이 증가하여, 세계적으로 관련 감시대책(TSCM)* 시장규모(2020년)가 지속해서 확대**

* Technical Surveillance Countermeasures

** 1억5천만 달러('20년, USD) 연평균 4.9% 성장률 예측(EMERGEN RESEARCH)

ㅇ **(사회성)**

- 現, 국내 주요 국가기관 85% 도청에 무방비 노출되어 있어, 해당 기술개발을 통해 정보 유출 방지 및 국가 공공기관의 ' 국가정보보안기본지침 ' 93조 준수 가능

※ "주요 국가기관 85%, 도청에 무방비 노출", 한국경제, 2023.4.18.

※ 국가정보보안기본지침: 국가정보원에서 배포한 지침으로 93조는 '대도청 측정'에 관한 지침, 2023.1.31. 개정

- (국민 피해 예방) 스마트폰 심스와핑을 통한 가상자산 탈취 및 보이스 피싱을 위해 악성앱 설치를 통한 금융사기 피해 지속 발생에 따른 피해가 속출하고 있어 디지털 기기를 이용한 도청 탐지/대응기술 개발, 고도화 필요

3. 수요분석

ㅇ **(주요 수요처) 정부부처 및 해외공관, 공공기관, 산업기밀 보호 기업, 개인**

- (정부) 국가주요시설, 외교부 재외 공관, 정부부처 등 정부기관의 정보유출방지 솔루션의 선제적 도입으로 국가안보 확보
- (기업) 산업스파이 실시간 검출/대응에 활용, 기업 핵심기술 유출방지 기술로 활용
- (개인) 스마트폰 유심복제, 통화탈취 등을 방지하는 대응기술을 통해 금융피해, 사생활 침해방지에 활용

ㅇ **(협력방안)** 정부부처, 수사기관, 국가중요시설 등에 선 적용하여 보안성 향상 및 국가 경쟁력 강화

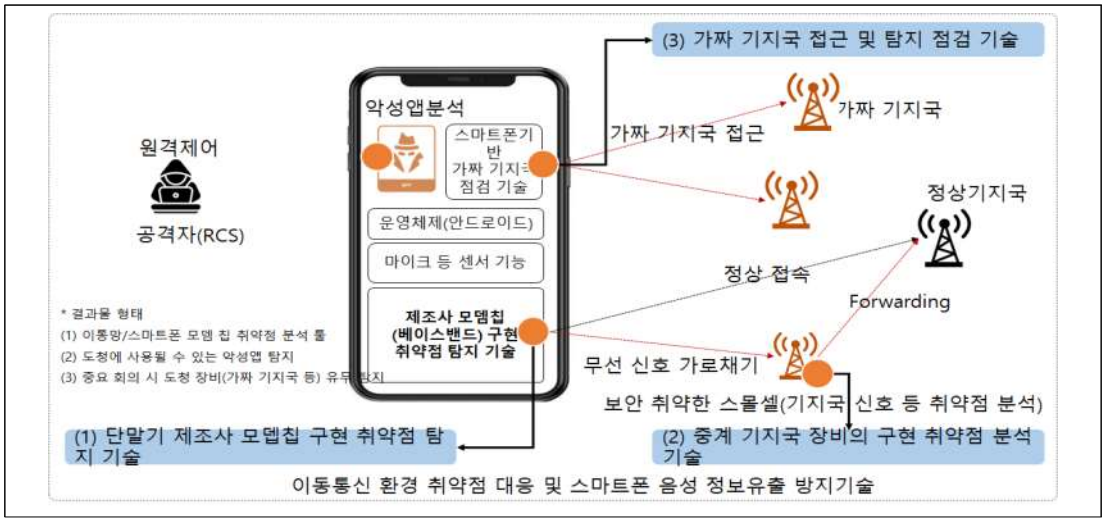
4. 연구목표

ㅇ **최종목표** : 이동통신 보안 취약점 악용 및 스마트폰 해킹으로 발생하는 도감청 기술과 네트워크 연결이 제한적인 AirGap* 및 IoT 기기 환경에서도 가능한 정보유출 기술 분석을 통해 정보유출 탐지와 대응에 대한 원천기술 확보와 고도화된 시그인트(SigINT)에 대응하기 위한 기술 확보

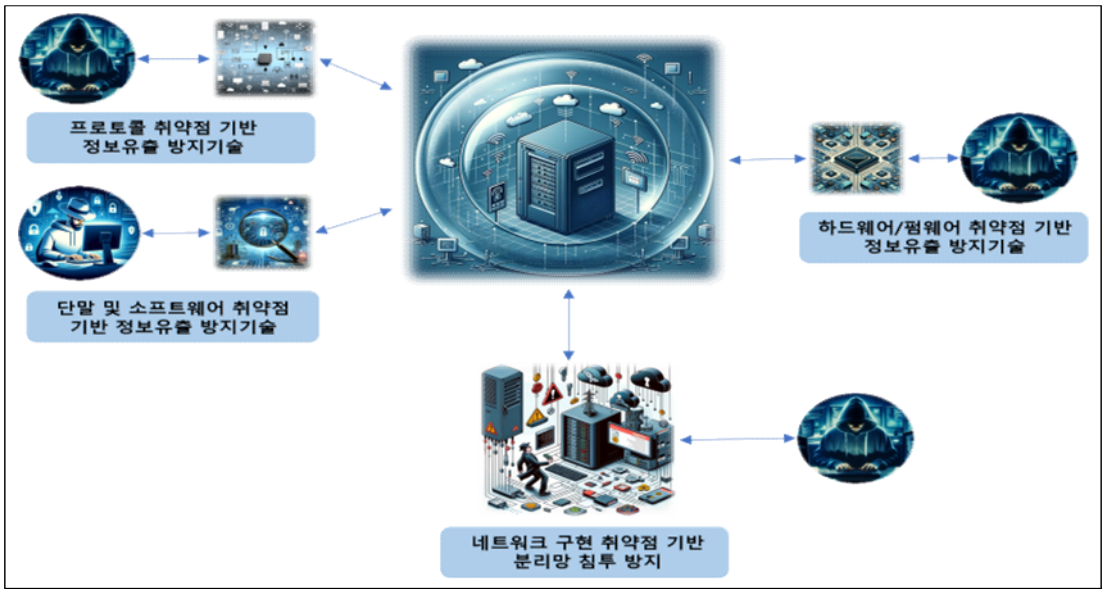
* 에어갭(Air Gap): 기기가 유선(이더넷, 전원 등) 및 무선(와이파이, 이동통신, 블루투스 등) 네트워크와 상호 연결되지 않은 상태로, 해당 기기는 에어갭 상태로 판단

- 스마트폰 및 이동통신 환경의 정보 유출 방지기술 개발
- 에어갭(AirGap) 환경에서 중요 정보 유출 능동 대응 기술개발

<개념도 : 이동통신 환경 취약점 대응 및 스마트폰 정보유출 방지기술>



<개념도 : AirGap 및 IoT 환경 도청 방지기술>



ㅇ 연구개발 목표

연도별	연구목표
2024.6. ~ 2027.12.	▪ 3GPP 표준 및 공개 구현 취약점 기반 단말 프로토콜 보안 위협 데이터베이스 구축 ▪ 이동통신 모뎀칩 프로토콜 구현 취약점 검증 및 진단 도구 개발 ▪ AirGap 환경 네트워크 구성/구현 취약점 기반 정보유출 시나리오 및 PoC 개발 ▪ IoT 허브 및 연동 기기의 HW/펌웨어 취약점 분석 도구 개발

ㅇ 정량적 연구개발 목표

성능지표		단위	연구개발 목표치 2024~2026	연구개발 전 국내 수준	세계 최고수준 (보유국/보유기관)
1	AirGap 환경 보안취약성 검증 및 증명 코드[1]	개	2	60%	미국 (MITRE)
2	AirGap 환경 네트워크간 침투 대응 방지 기술[2]	종	1	70%	미국(NSA의 TURBINE program) 미국(MITRE)
3	하향링크(베이스밴드 모뎀) 신규 취약점 CVE 등록[3]	건	4	3건	3건 (미국/플로리다 대학)
4	상향링크(기지국/코어망) 신규 취약점 발견[3]	건	4	17건 (LTE 대상)	4건 (LTE대상) (독일/루어대학)
5	스마트폰 기반 허위기지국 탐지율[4]	%	92%	80%	92% (미국/퍼듀대학)

1) 해당 결과물은 일반적으로 비공개 영역으로 다루어지고 있는 바, MITRE의 ATT&CK 자료를 기반으로 추정
2) 미국과 영국의 정보기관이 수행한 정보수집 행위에 대한 외부 공개된 자료와 장기간 망분리 환경에서 정보유통을 위한 기술을 개발한 국내 정보보안 시장의 기술력을 바탕으로 추정
3) 이동통신 상향링크 보안 취약점은 LTE 대상 보안취약점 발견건수, 하향링크는 CVE 취약점 등록 건수를 목표치로 설정함
4) 허위기지국 탐지율: 미국 퍼듀대(2024), 모바일앱기반 "Fake Base Station and Multi Step Attack Detection inCellular Networks using Machine Learning" 연구결과를 근거하여 목표치를 산출함

5. 연구내용

① 이동통신 환경 취약점 대응 및 스마트폰 음성 정보유출 방지기술 개발

- (모뎀칩) 단말기 제조사 모뎀칩 구현 취약점 탐지 기술
  - 이동통신 기반 단말기에 대한 무선상 보안 위협 분석
  - 3GPP 표준 및 공개 구현 취약점 기반 단말 프로토콜 보안 위협 데이터베이스 구축
  - 이동통신 모뎀칩의 제어평면 프로토콜 구현 취약점 검증 및 진단 도구 개발
  - 공개코드 기반 이동통신 라이브러리 및 SDR을 활용하여 상용 단말기에 연동해 취약점을 자동으로 탐지하는 기술 개발
- (기지국) 스마트폰 연결 중계 기지국 장비의 구현 취약점 분석 기술
  - 이동통신 네트워크 기지국/코어망 장비에 대한 보안 위협 분석
  - 3GPP 표준 및 공개된 구현 취약점 기반 기지국/코어망 프로토콜상 보안 위협 데이터베이스 구축
  - 이동통신망 기지국/코어망 장비의 제어평면 프로토콜 구현 취약점 검증 및 진단 도구 개발
  - 공개코드 기반 이동통신 라이브러리 및 SDR을 활용하여 상용 기지국/코어망에 연동해 취약점을 자동으로 탐지하는 기술 개발
- (스마트폰) 스마트폰 탑재 에이전트 기반 가짜 기지국 접근 및 탐지 점검 기술
  - 허위 기지국 기반 도청 시나리오 분석 및 대응 기술 분석
  - 안드로이드 탑재 에이전트 기반의 허위 기지국 탐지 기술 개발
  - 에이전트 기반의 허위 기지국 탐지를 위한 연합 학습 모델 고도화

② AirGap 및 IoT 환경에서 네트워크 스니핑(Sniffing) 능동 대응 기술개발

- (네트워크) AirGap 환경 네트워크 취약성 기반 스니핑 위협 대응 기술개발
  - 무선 네트워크(Wifi, Bluetooth, NFC 등) 스니핑 기법 분석 연구
  - AirGap 환경 네트워크 구성/구현 취약점 기반 스니핑 대응 연구
- (IoT) AirGap 환경 내 IoT 기기*의 취약점 기반 스니핑 대응 연구
  * 표준 및 비표준 프로토콜이 탑재된 IoT 기기
  - AirGap 내외부 단말 장치(IoT 기기 등)를 활용한 스니핑 기법 분석 및 방지 기술 연구
  - IoT 기기의 프로토콜 스푸핑 기법 분석 및 방지 기술 연구
- (HW 및 펌웨어) AirGap 환경 내 IoT 기기 HW/펌웨어 취약점 기반 정보유출 대응 연구
  - IoT 허브 및 연동 기기의 HW/펌웨어 취약점* 기반 능동 대응 기법 분석
  - IoT 기기 취약점 기반 스니핑 대응 기술 개발

  * 펌웨어 재프로그래밍을 통한 백도어 설치 기술은 공격자가 장치에 무단으로 접근할 수 있어 이는 네트워크 연결 없이도 내부 데이터에 접근이 가능

※ 스니핑(sniffing): 네트워크 중간에서 취약점 등을 활용하여 불법적으로 정보를 획득하는 해킹 기법

6. 기대 효과

○ (기술적 효과) 디지털 첨단기술 기반한 다층적 도청방지 핵심기술의 국산화

- 국내 비표준 통신신호 분석기술은 선진국에 높은 비중으로 의존하고 있는 상황에서, 독자적인 정보생산 능력 확보 가능
- 스마트폰 도청방지 기술 확보를 통해 최근 이슈가 되고 글로벌 기업 IT 제품(스파이칩 등)의 백도어 이슈를 해결
- 스마트폰 복제, 스파이앱 등 도청방지기술 확보로 스마트폰이 범죄에 악용되어 국민의 사생활 침해 방지에 기여
- AirGap환경에서 비표준 프로토콜, 신규 IoT 장비의 취약점으로 발생할 수 있는 도감청 및 정보 유출 등 보안위협 선제 대응
- 스마트기기의 도청 공격에 대한 방지기술로 민감한 데이터에 대한 무단 접근을 방지하고 도난으로부터 보호하는데 기여

○ (안보적 효과) 외교, 안보, 국방 환경 등에 적용하여 새로운 해킹 공격에 대한 예방을 강화하여 국가 중요 정보유출 방지에 기여

- 국가 간 경계 없는 정보전에서 기술적 우위 선점과 선제적 방어체계 구축을 통한 글로벌 국가 경쟁력 확보
- 대내외적인 정보유출 대응 수준 고도화를 통해 국가 주요시설과 민간의 안정 지향적인 생활환경 조성

7. 지원기간/예산/추진체계

○ 연구개발기간 : 3년

○ 정부지원연구개발비 : ‘24년 12억원 이내(총 정부지원연구개발비 41.3억원 이내)

구분	기간	개월수	정부지원연구개발비
1년차	'24.6월~'25.2월	9개월	1,200 백만원 이내
2년차	'25.3월~'25.12월	10개월	1,330 백만원 이내
3년차	'26.1월~'26.12월	12개월	1,600 백만원 이내
합계	-	31개월	4,130 백만원 이내

* 연차별 정부지원연구개발비는 당해연도 예산심의결과에 따라 변동될 수 있음

ㅇ **주관기관** : 제한없음

연구유형	기초연구 ( ), 응용연구 (√), 개발연구 ( )	TRL (4)~(6)단계
과제특징	경쟁형( ), 경쟁형(챌린지)( ), SW자산뱅크등록( ), 공개SW( ), 기술료비징수( ) 국제협력R&D( ), 정책지정( ), 혁신도약형(√), 표준화연계( ), 사회문제해결형( ), 일자리 연계( ), 소재부품장비( ), 규제샌드박스( ), 연구데이터공개( ), 사업화연계( ), IP-R&D연계( )	

구분	기술분야명/팀명	성명
책임PM(과제기획위원장)	보안・블록체인	정현철
담당 팀장	사이버보안팀	김남훈

관리번호	2024-정보보호-14	**(지정공모형)**
기술분류	대분류(차세대보안)-중분류(시스템및암호보안)-소분류(보안취약성)-세분류(SW취약성분석)	
중점분야	AI( ), AI반도체( ), 5G·6G( ), 양자( ), 메타버스( ), 사이버보안(√)	
기획유형	임무지향형R&D(√), 문제해결형R&D( ), 기술축적형R&D( )	
품목(문제)명	메모리 안전 언어의 적용 확대 및 안전 적용을 위한 통합 플랫폼 기술 개발	

1. 개요

ㅇ 메모리 안전 언어는 강력한 메모리 취약점 대응기법으로 알려져 있으나, 메모리 안전 언어의 비 안전 (Unsafe) 영역에 대한 부적절한 사용 등 지속해서 다양한 보안 문제점이 보고되고 있음. 따라서, 최근 광범위하게 활용되는 메모리 안전 언어의 안전하고 정확한 적용을 돕고 강력한 메모리 안전 언어의 적용 확대를 위한 통합 플랫폼 기술 개발이 필요

2. 현황 및 필요성

ㅇ 메모리 안전 언어 (Memory Safety Language)는 높은 안정성 때문에 다양한 영역에 적용되어 활용되고 있음

- RUST의 경우 비 메모리 안전 언어인 (Memory Unsafety Language) C/C++ 와 유사한 속도를 보여주면서 높은 안정성을 보장하여 안드로이드[1], 리눅스 커널[2], Windows[3]가 RUST로 구현되고 있음. 모질라 사의 파이어폭스의 경우 시스템 언어로 구현되어야 영역 중 15%[4] 이상이 RUST로 구현되어 있음

1) Google now supports Rust for underlying Android OS development, 9to5 Google, 2021.4.

2) Linus Torvalds: Rust will go into Linux 6.1, ZDNET, 2022.10

3) Microsoft is Rewriting Parts of the Windows Kernel in Rust, Thrrott 2023.4.

4) https://openhub.net/p/firefox/analyses/latest/languages_summary, Mozilla Firefox, 2024.2.

- Go 언어는 클라우드 환경과 API/RPC (Remote Procedure Call) 서비스 개발에 많이 사용되는 언어로 API/RPC 서비스 개발의 경우 72%[5]가 Go 언어로 개발되고 있음

5) Go Developer Survey 2021 Results, GO, 2022.4.

o 하지만, 메모리 안전 언어는 메모리 안전성을 보장할 수 없는 비 안전 (Unsafe) 영역을 사용하고 있으며 이 영역에서는 메모리 취약점이 발생할 수 있음

- RUST의 경우 강력한 메모리 안전 정책이 적용되지 않는 비 안전 (Unsafe) RUST 영역이 존재. 이러한 RUST의 비 안전 영역과 유사하게 Go는 unsafe.go, Dlang는 @safe 어노테이션 (annotation) 삭제, NIM은 .noalias 어노테이션을 이용해 메모리 안전성을 보장할 수 없는 비 안전 영역을 사용하고 있음

o 실제로 메모리 안전 언어의 비 안전 영역의 부적절한 사용으로 지속적인 메모리 취약점이 보고 되고 있음

- RUST의 경우 2016년부터 2023년까지 RustSec Advisory Database에 보고된 581개의 RUST 취약점 중 22%[6]가 메모리 취약점 버그임

※ 6) 출처: RustSec Advisory Database에 보고된 581개의 취약점을 전수 조사하여 Buffer Overflow, Double Free, Use After free에 해당하는 버그 개수를 측정한 결과임

- Go[7], Dlang[8]의 경우도 비 안전 영역을 사용하기 때문에 지속적으로 메모리 취약점이 발견되고 있음

7) Go vulnerability report Issue (https://pkg.go.dev/vuln/list), Go

8) Dlang's Issue Tracking System (https://issues.dlang.org/), Bugzilla

o 메모리 안전 언어는 메모리 취약점이 발생할 수 있는 공격표면을 크게 줄였지만, 부적절한 비 안전 영역의 부적절한 사용으로 메모리 취약점이 지속해서 발견되고 있으므로, 이러한 문제점을 해결하여 강력한 메모리 안전 언어의 올바른 사용과 보급을 도울 수 있는 기술이 필요

o 또한, 2024년 2월에 발표된 대한민국 국가 사이버안보 전략[9] 및 2023년 12월에 발표된 미국 연방 사이버보안 R&D 전략 계획[10]에서 언급한 핵심기술인 사이버 복원력 강화를 위해 공격표면을 최소화하여 공격 피해를 줄여 빠른 복원을 돕는 메모리 안전 언어의 안전하고 정확한 적용을 위한 기술 개발이 필요

9) 국가 사이버 안보 전략 (https://www.president.go.kr/), 대한민국 대통령실

10) 연방 사이버보안 R&D 전략 계획 (https://www.whitehouse.gov/), 미국 백악관

3. 수요분석

o (주요 수요처)

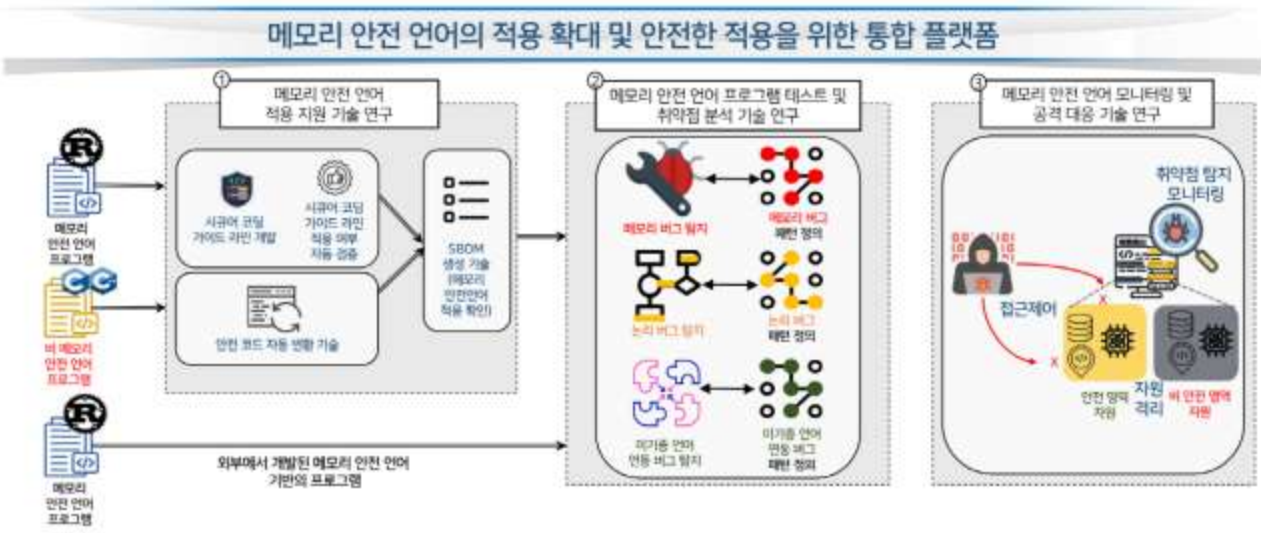
- 기존 비 안전 언어로 개발되어 메모리 취약점에 노출된 소프트웨어를 사용하는 교통, 국방, 사회 안전, 에너지, 스마트 공장 등 모든 영역
- 안전 언어를 통해 개발을 수행하고 있지만 체계적인 체계나 적용이 이루어지고 있지 않은 교통, 국방, 사회 안전, 에너지, 스마트 공장 등 모든 영역

o (적용 제품군)

- 운영체제, 클라우드, 군용 장비, 기업 및 정부 서비스, 일반 소프트웨어 등 기존 메모리 비 안전 언어를 사용하여 개발된 모든 제품
- 메모리 안전 언어를 이용해 구현하였지만, 체계적인 개발 및 검증 과정을 거치지 않고 개발된 운영체제, 클라우드, 군용 장비, 기업 및 정부 서비스, 일반 소프트웨어 등의 모든 제품

4. 연구목표

o 최종목표 : 강력한 메모리 취약점 대응기법인 메모리 안전 언어의 적용 확대 및 안전 적용을 위한 통합 플랫폼 기술 개발



- (메모리 안전 언어 적용 지원 기술) 메모리 안전 언어의 개발단계에 적용되어 메모리 안전 언어의 부적절한 사용을 탐지하고 수정할 수 있는 기술 및 메모리 비 안전 언어의 메모리 안전 언어 자동 변환 기술 개발
- (메모리 안전 언어 프로그램 테스트 기술) 개발된 메모리 안전 언어의 테스트 단계에 사용되며 메모리 안전 언어의 안전성 보장 영역, 취약점 발생 가능 패턴 등을 고려한 메모리 안전 언어에 최적화된 취약점 탐지 기술 개발
- (메모리 안전 언어 모니터링 및 공격 대응 기술) 개발된 메모리 안전 언어의 적용단계에 사용되며 낮은 오버헤드 및 높은 정확성을 가지는 모니터링 및 공격 대응 기술 개발

○ 단계별 목표

구분	단계별 연구목표
1단계	개발단계에 메모리 안전 언어의 올바른 적용을 도울 수 있는 가이드 라인을 개발하고 메모리 안전 언어가 적용된 기존 프로그램에 대한 올바른 적용 여부를 테스트할 수 있는 기술 개발
2단계	실제 제품에 적용된 메모리 안전 언어 코드에 제거되지 못한 취약점을 실시간으로 탐지하고 대응할 수 있는 낮은 오버헤드와 높은 정확성을 가지는 기술 개발. 개발된 전체 기술에 대한 연동, 테스트 및 최적화 작업 수행

○ 정량적 연구개발목표

성능지표		단위	연구개발 목표치	연구개발 전 국내 수준	세계 최고수준 (보유국/보유기관)
1	메모리 안전 언어 자동 변환 패치의 정확도	%	75[1)]	-	-
2	메모리 안전 언어의 취약점 탐지 오버헤드	%	≤ 25[2)]	-	52% (미국/Stevens Institute of Technology)
3	메모리 안전 언어의 취약점 탐지 정확도	%	95[3)]		

1) 개발된 (1) 시큐어 코딩 위반 코드 탐지 및 고품질 패치, (2) 메모리 비 안전 프로그램 코드의 안전 언어

자동 변환 패치 기술의 정확도를 평가하기 위해 실제 존재는 사례를 공정하게 선택하여 올바를 패치를 생성하는지 정확도를 측정함.

- 연구개발 목표치 75%는 C언어의 메모리 오류 최신 패치 기술인 SAVER (ICSE 2020) 도구의 정확도와 유사한 수준으로, RUST의 경우 C와 달리 Ownership 등 다양하게 고려해야 할 사항 등을 고려하여 C언어 최신 패치 기술 성능과 유사한 수준으로 설정

2) 개발된 취약점 탐지 기술의 평균 오버헤드를 평가하기 위해서 동일한 충분한 워크로드를 생성할 수 있는 벤치마크 등을 이용해 성능을 측정함

- 연구개발 목표치 25% 이하는, C/C++를 대상으로 하지만 가장 범용적으로 사용되는 Address Sanitizer를 최적화한 세계 최고 기술인 Debloating Address Sanitizer (Usenix Security 2022)의 성능인 52%의 오버헤드를 2배 이상 개선하는 것을 목표로 설정함

3) 개발된 (1) 비 안전 영역 파생 메모리 취약점, (2) 메모리 안전 언어의 논리적 버그, (3) 다 언어 프로그램과 연동 시 발생하는 취약점, (4) 바이너리만 제공되는 프로그램에 대한 취약점 탐지 기술의 정확도를 평가하기 위해서 공정하게 선택된 실제 버그를 정확하게 탐지하는지 측정함

- 연구개발 목표치 95%는, 실제 다양한 버그를 극히 작은 긍정 오류의 경우를 제외하고 버그를 모두 정확히 찾을 수 있는 수준의 도구를 개발하는 것을 목표로 설정함

5. 연구내용

ㅇ 메모리 안전 언어 적용 지원 기술 연구

– 메모리 안전 언어 시큐어 코딩 (Secure Coding) 가이드라인 개발

• 개발단계에서부터 비 안전 (Unsafe) 영역의 적절한 사용 예제 등 메모리 안전 언어의 잘못된 사용으로 인해 발생하는 보안상 취약점을 방지할 수 있는 메모리 안전 언어 개발 보안 가이드라인 개발

– 시큐어 코딩 가이드라인 위반 검증 기술 개발

• 지속해서 변하는 언어에 대한 시큐어 코딩 가이드라인을 자동 인식하고 기존에 작성된 코드의 가이드라인 위반 여부를 자동으로 검증하는 기술 개발

• 시큐어 코딩 위반 코드에 대한 오류 리포트 및 자동 패치 기술 (정적 분석 및 LLM 등의 기술 기반) 개발

– 메모리 비 안전 프로그램 코드의 메모리 안전 언어 코드 자동 변환 기술

• 비 메모리 안전 언어 (예: C/C++) 프로그램 코드에 대응되는 메모리 안전 언어 생성 기술 개발

• 다양한 메모리 안전 언어 (예: RUST/GO/Dlang/NIM)의 특성을 고려한 최적 언어 선택 기술 개발

– 메모리 안전 기술 적용 여부를 측정할 수 있는 SBOM (Software Bill of Materials) 생성 기술 개발

• 전달되는 패키지에 대한 메모리 안전 언어 적용 여부 검증을 가능하게 하는 최적 메타데이터 및 이를 반영하는 SBOM 기술 개발

ㅇ 메모리 안전 언어 프로그램 테스트 및 취약점 분석 연구

– 비 안전 영역 관련 메모리 안전 위반 취약점 분석 기술 개발

• 메모리 안전 언어의 비 안전 (예: Rust unsafe) 영역의 사용으로부터 파생되는 메모리 안전 위반 취약점 유형 식별

• 잘못된 비 안전 영역의 사용으로부터 파생되는 메모리 취약점 탐지 도구 개발, 취약점 유형에 따라서 센이타이저 (Sanitizer), 퍼징, 정적 분석, 정형 검증 등의 기술에 기반한 도구 개발

– 메모리 안전 언어의 논리적 취약점 분석 기술 개발

• 메모리 안전 언어에서 발생할 수 있는 논리적 취약점 유형 (예: 명세서와 다른 구현 및 동작, 누락된 보안 체크 코드) 식별

• 논리적 버그 탐지 기술 (센이타이저, 퍼징, 정적 분석 등의 기술 기반) 개발

- 메모리 안전 언어의 다언어 프로그램과 연동 시 발생 취약점 분석 기술 개발
• 타 메모리 안전 언어 및 메모리 비 안전 언어와의 통신 시 발생할 수 있는 공격 유형 (예: 타입 안전 위반 오류) 식별
• 다양한 이기종 언어를 하나의 통합된 형태의 IR 코드를 이용하는 정적 분석 기술과 센이타이저, 퍼징 등의 기술과 상호 보완하여 높은 정확도를 보장하는 취약점 분석 기술 개발

- 바이너리만 제공되는 메모리 안전 프로그램에 대한 취약점 분석 기술 개발
• 바이너리만 제공되는 메모리 안전 언어 프로그램의 취약점을 분석하기 위한 바이너리 리프팅 (Binary Lifting) 및 동적 분석 등의 기반 기술을 통한 취약점 분석 기술 개발

- 개발 기술은 실제 운영체제 (예: 리눅스) 개발 환경에 적용하여 개발 도구의 효율성 측정 및 안정화 작업 수행

ㅇ 메모리 안전 언어 모니터링 및 공격 대응 기술 연구

- 실시간 메모리 안전 언어 취약점 탐지 모니터링 기술 개발
• 낮은 오버헤드와 적은 오탐율로 실제 메모리 안전 프로그램 제품에 적용할 수 있는 취약점 탐지 모니터링 기술 개발

- 메모리 언어의 안전 영역과 비 안전 영역의 사용 자원 분리 및 접근제어 기술 개발
• 안전 영역 및 비 안전 영역이 사용하는 자원 (예: 메모리) 자체를 근본적으로 분리해 주는 기술 (예: 새로운 메모리 안전 할당기) 개발
• 분리된 자원을 메모리 안전 영역 또는 비 안전 영역 등으로 구분된 환경에서 유효하지 않은 접근 제어할 수 있는 정책 생성 및 접근제어 기술 개발

6. 기대효과

ㅇ 메모리 안전 언어의 안전하고 정확한 적용을 통해 공격표면을 크게 감소시켜 사이버 공격 시 공격 피해를 최소화할 수 있는 사이버 복원력의 핵심기술로 국가 기반 시설물의 보안성 향상

ㅇ 메모리 안전 언어 기술의 안전하고 정확한 활용을 통해 가장 많이 발생하고 악용되는 취약점 중 하나인 메모리 취약점에 대해 효과적으로 대응하여 사이버 공격으로 인한 서비스 불능 등의 피해를 최소화하여 기업 서비스의 신뢰성 향상

ㅇ 전 세계적으로 도입이 시작되고 있는 메모리 안전 언어의 안전하고 정확한 적용을 위한 기술의 선제적 확보를 통한 안전한 적용 기술을 선점하여 해외 기술의 수입을 막고 차세대 보안 기술을 선도

7. 지원기간/예산/추진체계

ㅇ 연구개발기간 : 4년 이내 (1단계 2년→2단계 2년)

ㅇ 정부지원연구개발비 : ‘24년 10.5억원(총 정부지원연구개발비 50.17억원)

구분		기간	개월수	정부지원연구개발비
1단계	1년차	’24.6월~’25.2월	9개월	1,050 백만원 이내
	2년차	’25.3월~’25.12월	10개월	1,167 백만원 이내
2단계	3년차	’26.1월~’26.12월	12개월	1,400 백만원 이내
	4년차	’27.1월~’27.12월	12개월	1,400 백만원 이내
합계		-	43개월	5,017 백만원 이내

* 연차별 정부지원연구개발비는 당해연도 예산심의결과에 따라 변동될 수 있음

ㅇ 주관기관 : 제한없음

연구유형	기초연구 ( ), 응용연구 (√), 개발연구 ( )	TRL (3)~(6)단계
과제특징	경쟁형( ), 경쟁형(챌린지)( ), SW자산뱅크등록( ), 공개SW( ), 기술료비징수( ) 국제협력R&D( ), 정책지정( ), 혁신도약형(√), 표준화연계( ), 사회문제해결형( ), 일자리연계( ), 소재부품장비( ), 규제샌드박스( ), 연구데이터공개( ), 사업화연계( ), IP-R&D연계( )	

구분	기술분야명/팀명	성명
책임PM(과제기획위원장)	보안·블록체인	정현철
담당 팀장	사이버보안팀	김남훈