


[첨부 제4호]

스마트디바이스 키누출 검증 시스템 (KLA-SCARF)



김태성 (taesung@etri.re.kr)
디바이스보안분석연구실



목 차

1. 기술의 개요
2. 기술이전 내용 및 범위
3. 경쟁기술과 비교
4. 기술의 사업성
 - 활용분야 및 기대효과
5. 국내외 시장 동향

기술의 개요

키누출 공격 안전성 검증 시스템



· 기술미전 내용 및 범위

▣ 기술이전 내용 및 범위

- ❖ KLA-SCARF 시스템 기술
 - ❖ 부채널 공격 안전성 검증 소프트웨어
- ❖ 검증 보드 기술
 - ❖ IC 카드, 소프트웨어, 하드웨어 용도의 6종

▣ 기술 개발 현황

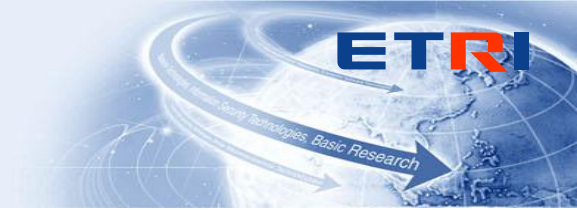


기술미전 내용 및 범위

기술 개발 현황

❖ 기술성숙도(TRL : Technology Readiness Level) 단계 : (6)단계

구분	단계	정의	세부설명
기초 연구 단계	1	기초 이론/실험	기초이론 정립 단계
	2	실용 목적의 아이디어/특허 등 개념정립	기술개발 개념 정립 및 아이디어에 대한 특허 출원 단계
실험 단계	3	실험실 규모의 기본성능 검증	실험실 환경에서 실험 또는 전산 시뮬레이션을 통해 기본성능이 검증될 수 있는 단계 개발하려는 부품/시스템의 기본 설계도면을 확보하는 단계
	4	실험실 규모의 소재/부품/시스템 핵심성능 평가	시험생품을 제작하여 핵심성능에 대한 평가가 완료된 단계 3단계에서 도출된 다양한 결과 중에서 최적의 결과를 선택하려는 단계 컴퓨터 모사가 가능한 경우 최적화를 완료하는 단계
시작품 단계	5	확정된 소재/부품/시스템 시작품 제작 및 성능 평가	확정된 소재/부품/시스템의 실험실 시작품 제작 및 성능 평가가 완료된 단계 개발 대상의 생산을 고려하여 설계하나 실제 제작한 시작품 샘플은 1~수개 미만인 단계 경제성을 고려하지 않고 기술의 핵심성능으로만 볼 때, 실제로 판매가 될 수 있는 정도로 목표 성능을 달성한 단계
	6	파일럿 규모 시작품 제작 및 성능 평가	파일럿 규모(복수 개~양산규모의 1/10정도)의 시작품 제작 및 평가가 완료된 단계 파일럿 규모 생산품에 대해 생산량, 생산용량 불량을 등 제시 파일럿 생산을 위한 대규모 투자가 동반되는 단계 생산기업이 수요기업 적용환경에 유사하게 자체 현장테스트를 실시하여 목표 성능을 만족시킨 단계 성능 평가 결과에 대해 가능하면 공인인증 기관의 성적서 확보
실용화 단계	7	신뢰성평가 및 수요기업 평가	실제 환경에서 성능 검증이 이루어지는 단계 부품 및 소재개발의 경우 수요업체에서 직접 파일럿 시작품을 현장 평가(성능 및 신뢰성 평가) 가능하면 인증기관의 신뢰성 평가 결과 제출
	8	시제품 인증 및 표준화	표준화 및 인허가 취득 단계
사업화	9	사업화	본격적인 양산 및 사업화 단계 6-시그마 등 품질관리가 중요한 단계



. 기술의 사업성

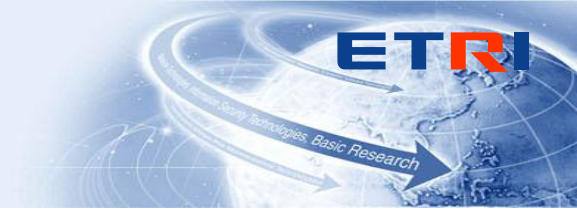
▣ 제품 서비스의 예상 수요자

- ❖ 보안 알고리즘, 보안 칩, 보안이 적용된 소형 디바이스 제작업체
- ❖ 제품 보안성 평가 기관

❖ 기존 기술과 비교하여 유리한 점

- 다양한 u-Device에 대한 부채널 공격에 대한 안전성 검증 가능
- 다양한 형태의 검증 보드 지원 가능
- 기술전수 교육 및 기술지원의 용이함

. 국내외 시장 동향



▣ 국외 관련 제품 및 서비스 동향

- Cryptography Research Inc. 사, RiScure 사, Brightsight 사 등에서 부채널 분석 장비 개발
- (유럽) 오스트리아, 독일, 벨기에 등이 참여한 SCARD(Side Channel Analysis Resistant Design) 프로젝트('03년~'06년)는 스마트카드 안전성 평가방법 및 대응법 가이드라인 등에 대한 연구 진행
- (일본) '07년부터 산업기술종합연구소(AIST) 산하 정보보호연구센터(RCIS) 주관으로 부채널 분석보드(SASEBO보드)를 개발/배포하고 그 결과를 반영한 JCMVP 및 NIST FIPS 140-3 표준 작성 중

감사합니다.



www.etri.re.kr

※ 하단의 문의처 소개후, 발표후 개별기술 상담이 가능함을 다시 한 번 안내함

♣ 연락처 : 소프트웨어연구부, 김태성 선·연 (042-860-1612, taesung@etri.re.kr)