붙임 3 대표성과 후보 추천서 양식

① 요약본 ※ 분량 : 1페이지 이내

2021년도 ETRI 10대 대표성과 후보 추천서(요약)

<table>
<tr><td rowspan="2">성과Track</td><td colspan="2">기초·미래선도</td><td>산업육성</td><td>국가·사회문제해결</td></tr>
<tr><td colspan="2"></td><td></td><td>17.사이버 범죄</td></tr>
<tr><td>협약(세부)과제명</td><td colspan="4">(총괄+1세부) IoT 디바이스 자율 신뢰보장 기술 및 글로벌 표준기반 IoT 통합보안 오픈 플랫폼 기술개발
(2세부) IoT 인프라 공격 확산 방어를 위한 상황 적응형 보안 자율제어 기술개발</td></tr>
<tr><td rowspan="2">과제번호</td><td colspan="2">협약(세부) 과제번호</td><td colspan="2">NTIS 과제번호</td></tr>
<tr><td colspan="2">21HR2200, 21HR2500</td><td colspan="2">1711082859, 1711082684</td></tr>
<tr><td>성과목표</td><td colspan="4">[5-5] 잠재적 사이버 위협을 원천 차단하는 지능형 사이버 보안 및 신뢰 인프라 기술 연구</td></tr>
<tr><td>총 연구기간</td><td colspan="4">2018년 04월 01일~ 2021년 12월 31일</td></tr>
<tr><td>총 연구비</td><td colspan="2">총 15,136백만원</td><td colspan="2">정부: 14,419백만원, 민간: 717백만원</td></tr>
<tr><td rowspan="2">연구책임자</td><td>연구자 성명</td><td>직할부서</td><td>연구본부/연구실</td><td>직위/직급</td></tr>
<tr><td>강유성</td><td>지능화융합연구소</td><td>정보보호연구본부</td><td>책임(실장)/책임</td></tr>
<tr><td colspan="5">성과 정보</td></tr>
<tr><td>성과 내용</td><td colspan="4">- (IoT 기기 공격 사이버 범죄 예방) 대규모 IoT 환경에서 관리자 개입없이 디바이스 스스로 디바이스 DNA를 생성·활용하는 자율적 ID/PW 및 IoT 키관리 핵심기술 개발
• (세계 최고 수준) 7종 프리미티브(사람의 지문, 홍채, 정맥처럼 디바이스에서 저항/커패시터, 메모리, 센서 등 다양성 확보) 검증 완료 (다양한 기기에 적용가능)
• (적용기기) 지능형 CCTV, IP 카메라, 스마트 가로등, Wi-Fi AP 등 모든 IoT 기기
- (IoT 기기 공격 확산 방지) 대규모 IoT 환경에서 빠른 사물봇 공격 확산, 서비스 거부 공격(DDoS) 등 보안 위협을 방어하는 IoT 인프라 보호 자율제어 핵심기술 개발
• (국내 최초) 글로벌 표준(CSA SDP Ver 1.0) 기반 IoT 인프라용 DDoS 방어를 위한 C-ITS 서비스 환경 적용 (유성JC와 북대전IC 사이 7.5km 리빙랩 시뮬레이션 완료)
• (적용환경) 지능형 교통정보시스템(C-ITS), 지능형 원격검침 인프라(AMI) 등
- (경량 보안기술 국산화로 외산 종속성 감소) IoT 기기 보안 위협(예, 데이터 유출, 암호화폐 채굴기로 악용, 디도스 공격용 좀비로 악용)을 원천차단하는 국산기술 개발로 수입대체 효과로, 로얄티를 절감하고 국내기업 기술 경쟁력 확보
• (로열티 및 라이센싱 수익) 1,200억 매출, '21.12 누적 2.08억 로열티 수입
- (홍보) 세계보안엑스포('21.5, 킨텍스), AIoT국제전시회('21.10, 코엑스), 대한민국과학대전('21.12 예정, 킨텍스) VIP 코어존 출품
- 후속 R&D 과제창출 기여 (과기부 2건, 국방부 1건 등 총 정부출연금 500억 규모)</td></tr>
<tr><td>대표성과 1</td><td colspan="4">- (기술이전) 6건, 98.1백만원 (VAT 포함)
• IoT 디바이스 인증 기술 : 66백만원 (3건), 경량형 DTLS 기술 : 32.1백만원 (3건)
- (사업화) 도로공사의 판교 C-ITC 리빙랩 시뮬레이션 환경에서 실증 및 기술검증
• 대전 유성JC와 북대전 IC 사이 7.5Km 상황에 대한 리빙랩 실증, '21년 01월</td></tr>
<tr><td>대표성과 2</td><td colspan="4">- (특허) 총 14건 (국내출원 5건, 국내등록 3건, 미국출원 5건, 미국등록 1건)
• 대규모 환경에서 원격 검증을 위한 장치 및 방법, 대한민국, 2021.07.01. 출원
- (논문) SCI 논문 총 8편 (평균 IF 3.24, 최고 IF 5.577)
• Two-Factor Device DNA-based Fuzzy Vault for Industrial IoT Device Security (IEEE Access, '21.07.07.)</td></tr>
</table>

② 상세본 ※ 분량 : 7페이지 이내

2021년도 ETRI 10대 대표성과 후보 추천 요약서(상세)

1. 성과명

무인관리 IoT 기기가 공격자에 의해 설정권한을 장악당해 꼭두각시가 되어 DDoS 공격의 시작점으로 악용되는 것을 방어하는 IoT 기기 접근제어 보호 및 인프라 보호 기술

2. 성과내용

기술개발 목표달성도

□ 기술적 선점이 필요한 분야

○ IoT 기기(예를 들면, 인터넷 연결된 지능형 CCTV, IP 카메라, Wi-Fi AP 등)의 설정권한을 공격자로부터 보호하기 위한 IoT 보안 기술

- 2021년 상반기에 약 15억건 이상의 IoT 공격이 감지됨 (글로벌 백신업체 카스퍼스키 분석자료, 2021)
- 감염된 IoT 기기는 원격 접속 프로토콜의 일종인 텔넷을 통해 개인 또는 기업 **데이터를 훔치는 데 쓰이는 것**은 물론, **암호화폐 모네로를 채굴하는 사례**도 발견됐으며, **디도스 공격을 위한 봇넷 구축** 등 다양한 형태로 악용될 수 있음
- 따라서, IoT 기기의 감염을 방어하기 위하여 **공격자의 접근 시도를 원천적으로 차단할 수 있는 관리효율적* 접근제어 기술** 및 **1대가 감염되더라도 감염확산을 방어할 수 있는 인프라 보호 기술** 선점이 필요함

* 대규모 IT 환경에서는 키관리 편의성 때문에 공장 출하시 설정한 디폴트 ID/PW를 동일하게 사용하는 경향이 있기 때문에 관리자의 관리효율성과 IoT 보안성을 모두 고려한 IoT 보안 기술 개발이 요구됨

□ 기술개발 목표

○ 대규모 IoT 디바이스가 사용되는 환경에서 관리자 개입없이 디바이스 스스로 디지털 지문정보(디바이스 DNA)를 생성하고 활용하는 자율적 ID/PW 및 IoT 키관리 핵심기술

(목표 ①) IoT 기기의 유일무이한 디지털 지문정보(디바이스 DNA) 생성 기술 개발

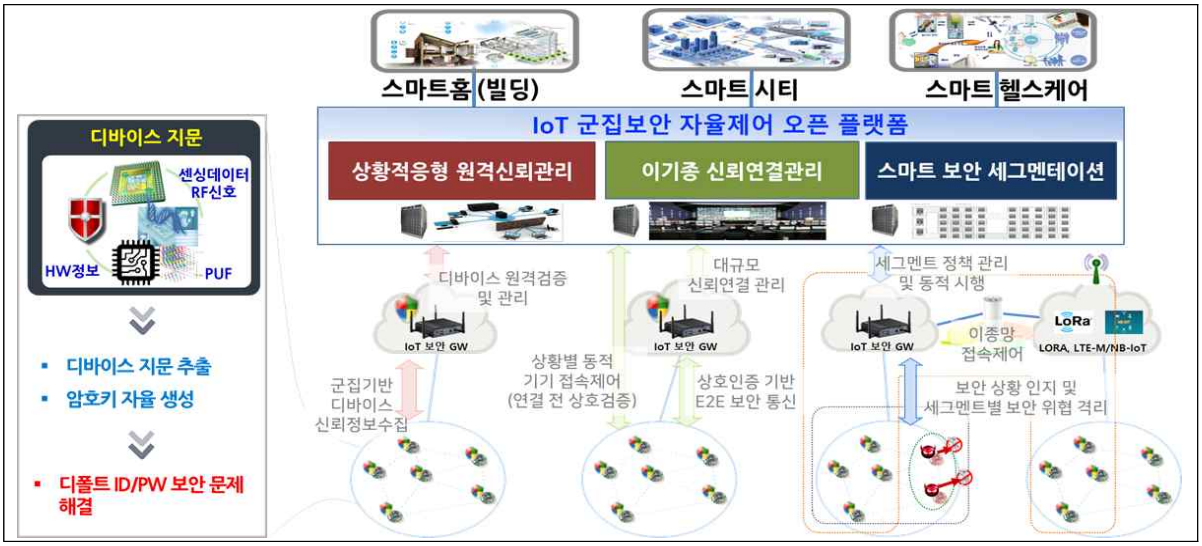
(목표 ②) 글로벌 IoT 오픈 플랫폼 연동 디바이스 자율인증 기술 개발

○ 대규모 IoT 인프라 환경에서 빠른 사물봇 공격 확산, 서비스 거부 공격(DDoS) 등 보안 위협을 방어하는 IoT 인프라 보호용 보안 자율제어 핵심기술

(목표 ③) 빠른 공격 확산 방지를 위한 스마트 세그멘테이션 기술 개발

(목표 ④) 서비스 거부 공격(DDoS) 방어를 위한 동적경계망 기술 개발

<기술개발 개념도>



□ 기술개발 목표의 달성성과 및 핵심기술 확보

[개발목표 ①] IoT 기기의 유일무이한 디바이스 DNA 생성 기술 개발

➡ **(달성성과) IoT 디바이스 DNA 생성 기술 확보: 총 7종 프리미티브 발굴**

➡ **(핵심기술 확보)**

- IoT 기기의 하드웨어 고유특성 기반 디바이스 DNA 생성 기술 확보
  - 7종 프리미티브: RC/PHY/Flash/DRAM/PDRO/이미지PRNU/가속도센서 기반
  - 칩, 보드, 상용제품 등 개발사 요구에 따라 최적화된 프리미티브 제공 가능
- IoT 기기별 유일성, 난수성, 엔트로피를 보장하는 암호키(또는 ID/PW) 생성
- 대규모 자원 제약적인 IoT 기기의 암호키 생성 및 보호를 위한 핵심 기술

[개발목표 ②] 글로벌 IoT 오픈 플랫폼 연동 디바이스 자율인증 기술 개발

➡ **(달성성과) OCF IoTivity 기반 디바이스 자율인증 검증 및 글로벌 표준 확보**

➡ **(핵심기술 확보)**

- 사용자 개입이 없는 OCF IoTivity-Lite 기반의 경량 디바이스 인증 기술
- 디바이스 DNA를 활용한 PSK-TLS 및 인증서 기반 자율인증 검증
- 디바이스 자율인증 핵심 특허 및 글로벌 사실 표준(OCF) 2건 확보

[개발목표 ③] 빠른 공격 확산 방지를 위한 스마트 세그멘테이션 기술 개발

➡ **(달성성과) 세계최초 IoT 인프라 환경에 최적화된 계층적 위협 전파방지 기술 핵심원천기술 확보**

➡ **(핵심기술 확보)**

- 사물봇 공격/자동 전파 등 빠른 공격 확산 방지를 위한 스마트 세그멘테이션 핵심기술 확보
- IoT 인프라 환경에 최적화된 계층적 위협 전파방지 기술

- 감염 기기/GW/서비스 세그먼트 단위 보안 위협 자동격리 및 자율 보안통제
- NIST 위험평가 가이드(SP 800-30)와 위험관리 가이드(ISO 31000:2018) 기반 보안 위협 분석 기술

[개발목표 ④] 서비스 거부 공격(DDoS) 방어를 위한 동적경계망 기술 개발

➡ **(달성성과) 국내 최초 글로벌 표준 기반 IoT 인프라 소프트웨어 정의 경계망(SDP) 핵심 원천기술 확보 및 적용**

➡ **(핵심기술 확보)**

- 사물봇넷 기반의 대규모 서비스거부공격(DDoS) 방어를 위한 동적경계망 기술
- 선기기검증 기반 이종망연동 신뢰연결관리 기술(CSA SDP Ver.1.0 표준 준수)
- 대규모 DDoS방어/메시지 위변조·도감청 방지 기술
- 스마트홈 IoT 보안 서비스 인프라 구축 및 C-ITS 보안 인프라 (K-City) 테스트베드 실증을 위한 기술 검증

3. 우수성 및 차별성

기술수준 향상 성과

○ 고품질 IoT 디바이스 DNA 생성 기술 개발

- 별도의 보안 하드웨어 모듈이 없는 자원 제약적인 IoT 디바이스에서 관리자의 직접 개입없이 고품질의 암호키 생성으로 접근제어 보안성 보장

  * **NIST SP 800-90B 기반 엔트로피** 측정을 통해 자율생성 암호키(또는 ID/PW) 키 비도(보안 레벨) **256비트 달성**

- IoT 기기 스스로 필요시 생성 및 사용하는 디바이스 DNA 성능 검증

  * 유일성 49.2%(이상적인 값 50%), 재생성시 오차율 1.9%(이상적인 값 0%)

  * 환경변화(온도/전압 등)에 대한 신뢰성 검증 완료

○ OCF IoTivity 오픈 플랫폼상에 디바이스 DNA를 활용한 자율인증 기술 개발

- 표준 스펙을 준용한 Mediator/OTGC, IoT 디바이스, 클라우드 서버 기반 원격 서비스 실증 완료
- OCF IoTivity-Lite 2.0.5 기반의 경량 인증체계 구축

  * 자원 제약이 심한 클래스 **1~2등급의 경량 IoT 디바이스**(>256KB 플래시, >64KB RAM)에서 **동작 가능한 자율인증 소프트웨어 검증** 완료

○ 글로벌 표준 기반 사물봇 빠른 확산 방지, 비인가 접속 방어용 보안 자율제어 플랫폼 개발 및 스마트 IoT 보안 서비스 적용

- **150대 이상 대규모 기기 IoT 인프라 환경에 최적화**된 계층적 위협 전파방지 기술 및 IoT 보안 GW 시제품 개발
- **글로벌 표준(CSA SDP Ver. 1.0 표준 만족) 기반 IoT 인프라 DDoS 방어용 소프트웨어 정의 경계망(SDP)** 핵심 원천기술 확보

○ 국제표준 준수 국내최초 IoT 인프라용 DDoS 방어 보안 자율제어 핵심기술 검증

- 차세대 지능형 교통정보시스템(C-ITS) 인프라 서비스 보안 실증 및 위협상황경

고서비스 등 14개 서비스 적용 확보(CSA SDP Ver. 1.0 표준 만족)

* 국내 최초 글로벌 표준 기반 IoT 인프라용 DDoS 방어를 위한 C-ITS 서비스 환경 적용

세계 최고 수준 대비 연구개발 수준

○ 고품질 IoT 디바이스 DNA 생성 기술 개발

- 단일기관 세계 최다(7종) 디바이스 DNA 프리미티브 확보 (100% 수준)
- 서비스 개발사의 요구에 따라 칩 제작형, 보드 탑재형, 상용제품의 메모리 사용방식 등 개발사 상황에 따른 최적화된 프리미티브 제공 가능

<IoT 디바이스 DNA 프리미티브 요약 - 7종>

Primitive 명칭	(1) RC PUF	(2) PHY PUF	(3) Flash PUF	(4) DRAM PUF	(5) PDRO PUF	(6) Image Sensor PRNU	(7) External Sensing Data
대상 하드웨어	Resistor-Capacitor (저항-커패시터)	통신 칩셋 SRAM 메모리 (Wi-Fi, SUN)	Flash 메모리	DRAM 메모리	링 오실레이터 (Phase detection ring oscillator)	Camera module (이미지 센서)	주변 센서류 (가속도, 자이로스코프 등)
출력 타입	Dynamic (32bits challenge)	Fixed or Restricted Dynamic	Fixed or Restricted Dynamic	Fixed or Restricted Dynamic	Dynamic	Dynamic	Dynamic
출력 사이즈	128 bits ~ 2048 bits	통신모듈 버퍼 사이즈 (256 bits 이상 가능)	Flash 메모리 사이즈 (256 bits 이상 가능)	DRAM 사이즈 (256 bits 이상 가능)	128 bits ~ 2048 bits	학습 네트워크 모델(오토인코더의 잠재공간 노드 수에 비례)	학습 네트워크 모델(오토인코더의 잠재공간 노드 수에 비례)
개발 보드 (시험 제품)	- Kidden-Ruby 보드 (STM32F4) + RC회로	- Kidden-Ruby 보드 (STM32F4) + Pmod WiFi module	- Kidden-Ruby 보드 (STM32F4) + S25FL128S (16MB) Flash Memory	- Kidden-Topaz 보드 (STM32F7) + IS42S32800G (32MB) DRAM	Zybo Z7-20 보드(Xilinx)의 Zynq FPGA	삼성, 로지텍, 샤오미 IP 카메라, 아이폰	스마트폰 (안드로이드), 아두이노
특징	• 반복성, 유일성, 난수성 등 우수 • 3V~3.6V 범위에서 1%이하 error 특성 • 챔버 테스트 (-20 ~ 70 ℃ stability 유지) • 다양한 MCU에 적용	• 반복성, 유일성, 난수성 등 우수 • 챔버 테스트 (-20 ~ 70 ℃ stability 유지) • Voltage variance에 강인 • 하드웨어수정 불필요	• 반복성, 유일성, 난수성 등 우수 • 하드웨어 수정 불필요 • 온도, 전압 등 환경변화에 강인한 추출 방법 적용	• 반복성, 유일성, 난수성 등 우수 • 하드웨어 수정 불필요 • 온도, 전압 등 환경변화에 강인한 추출 방법 적용 • 추출 시간 축소	• 칩 또는 FPGA 구현을 위한 PUF IP 확보 • 반복성, 유일성, 난수성 등 우수	• 상용제품(판매중인 IP 카메라)에서 디바이스 DNA 확보 • 카메라 모듈 고유 노이즈(PRNU)를 학습시켜 활용	• 상용제품(판매중인 안드로이드/아두이노 기반 스마트폰)에서 디바이스 확보 • 주변 센서류의 센싱 데이터를 추출하여 활용
							

○ 세계 최초 디바이스 DNA를 활용한 인증서 기반 자율인증 기술 개발 (100% 수준)

- ECC 공개키 암호(secp256r1) 기반의 디바이스 DNA 활용 인증서 생성 및 적용

○ 세계 최초 IoT 인프라 환경에 최적화된 계층적 위협 전파방지 기술 개발 (100% 수준)

- 150대 이상 대규모 기기통제 가능, NIST 위험평가 및 ISO 위험관리 가이드 기반 보안 위험도 평가

○ 국내 최초 글로벌 표준 기반 IoT 인프라 동적경계망(DPS) 핵심기술 개발 (100% 수준)

- CSA(Cloud Security Alliance) SDP(Software Defined Perimeter) Ver. 1.0 표준규격 만족
- IETF 국제 표준규격 (HOTP, TLS) 만족, KCMVP 인증 대응 고성능 암호 구현

기술수준 공인 성과

○ 고품질 IoT 디바이스 DNA 생성 기술

- 디바이스 DNA 기반 자율생성 ID/PW **키비도 256비트 달성(TTA 인증 취득) ('21.7)**

○ 국제표준 규격(IETF PANA, EAP-TLS 등)을 준수한 IoT 보안 인프라 구현 및 **유럽 현지 대규모 기기 운영/유지보수 (유럽 현지 약 85만호 운영, ~ '21.8)**

○ 세계 최초 IoT 인프라 환경에 최적화된 계층적 위협 전파방지 기술 및 글로벌 표준 기반 IoT 인프라용 DDoS 방어 기술 확보
- CSA SDP Ver. 1.0, IETF HOTP, TLS 등, 동시 신뢰연결 처리 세션수 10,000개
- **기술이전 기업을 통해 K-City내 C-ITS 서비스 실증 및 기술검증 완료('21.10)**

○ 상용 암호 대비 고성능 암호 구현(ARM mbed 대비 서명생성 4.2배, 서명검증 3.9배)과 공공기관 적용 시 필요한 KCMVP 인증에 준하는 국정원 테스트 벡터 기반의 시험 완료로 업체의 **KCMVP 인증 과정 간소화 및 경쟁력 강화 기여**

4. 성과의 활용도 및 파급효과

경제 활성화 효과

기업 경쟁력 향상

○ 하드웨어 기반 'IoT 디바이스 DNA를 활용한 보안 솔루션' 개발로 기존 상용화되어 있는 순수 소프트웨어 기반 제품에 비해 높은 보안성과 활용 측면에서 유연성 제공

○ IoT 디바이스 DNA 기반 암호키 안전성 검증 기술을 통해 IoT 보안 취약성 검증에 경험이 부족한 **중소 임베디드 보안 디바이스 제조 업체의 보안성** 검증 기간 단축

○ **IoT 서비스를 위한 경량형 보안 기술 국산화를 통한 외산 종속성 감소**로 수입대체 효과에 의한 로얄티를 절감하고, 국내기업 기술 경쟁력 확보를 통한 신규 IoT 보안 서비스 시장 선점 가능
- 로열티 및 라이센싱 수익: **1,200억 매출, 2021년 12월 누적 2.08억 로열티 수입**

○ IoT 서비스 산업 활성화의 걸림돌인 사물봇 보안 위협의 조기 해소 및 이종망과 이종 서비스 간 연동 지점의 보안 기능 제공으로 새로운 서비스 모델 창출 기여가 기대됨

산업 경쟁력 향상

○ IoT 환경에서 큰 위협이 될 암호키 유출 등의 보안 문제를 해결함으로써 국내 IoT 시장의 확장을 촉진하고 국내 IoT 기술의 국제 경쟁력 강화에 기여

○ 4차 산업혁명이 가져올 직업 혁명에 대비하여 디바이스 DNA, 암호키 안전성 검증, 국제 표준 기반의 보안 등 하드웨어/소프트웨어 보안 전문가, **IoT 디바이스 보안 전문가 등 정보보안 분야에서 미래 신직업군 발굴**

○ 스마트 시티 환경에 보안 인프라를 구축하여 데이터 유출 및 검침 데이터 위·변조 위협에서 발생하는 **사이버 보안 문제 해결하는 제품 국산화를 통한 외산종속성 감소 및 2020년 기준 약 1.08조원 정도의 수입대체 효과**

* 세계 최초 글로벌 표준 기반 지능형 원격검침 인프라(AMI) 보안 서비스 유럽현지 운영/유지보수

○ 사물봇 해킹에도 안심하는 경량형 IoT 보안 기술로써 국내 IoT 보안 산업 및 서비스 활성화에 기여

○ 사물봇 공격/자동 전파 등 빠른 확산 방지, 대규모 서비스 거부 공격 방어, 사물

봇 악성코드 방지 핵심 기술 개발로 국내 기업의 기술 경쟁력을 확보하고 관련 장비의 국내·외 시장 진출에 기여

경제적 파급효과

○ **(파급효과 전망)**

- IoT 디바이스 DNA라는 새로운 분야의 보안 기술 적용을 통해 향후 IoT 디바이스가 갖춰야 할 보안 수준의 기준을 높여 기존에는 요구되지 않았던 기술 및 장치의 탑재를 유도하여 관련 산업 및 시장 확대 기대
- 스마트 시티, 스마트 팩토리, Connected Car, 드론 등 보안성이 필수인 IoT 기기의 수요가 급증할 것으로 예상되는 상황에서 IoT 디바이스 DNA 등의 기술을 적용한 보안성이 강화된 IoT 기기를 사용함으로써 IoT 시장 확대 및 신사업 활성화 기대

○ IoT 보안 핵심원천 기술을 통한 다양한 IoT 서비스에 대한 신시장 개척을 도모 및 이로 인한 인력고용 확대 기여(**'22년까지 14조 4000억달러 가치 창출**, CISCO)

○ **해외 사업화(노르웨이 85만호, 약 1,200억 규모) 운영/유지보수 사례**를 통해, 해외 IoT 보안 솔루션 시장을 선점하였고 관련 장비의 세계시장 진출 및 수출효과 증가에 기여

국가·사회적 파급효과

○ **해결해야 할 국가·사회문제**

- 통신 3사가 IoT 서비스 경쟁에 뛰어들며 앞다투어 IP 카메라, 스마트 홈 등의 서비스를 출시하고 있지만, 사회적으로는 스마트 밴드를 통해 의료정보가 노출되거나 IP 카메라 해킹을 통해 **사생활 정보가 노출되고 있어 IoT 기기의 침해 방지 기능을 강화하여 개인의 사생활을 보호해야 하는 국가·사회적 요구**가 있음. 이러한 요구에 대응할 수 있는 기술적 토대가 IoT 디바이스 DNA 생성 기술임.
- 빈번히 발생하는 가정용 CCTV 해킹 사건 등과 같이 보안 기술 설정과 관리를 어려워하는 사용자들이 겪는 잠재적 위협을 제거하고 **IoT 기기가 사용자 개입없이 스스로 기본적 보안 수준을 향상시켜 공격자의 설정권한 장악을 방어**함으로써 개인정보 유출 등으로 인한 사회적 비용을 감소시킬 것으로 기대
- 기존 **IoT 기기에서 데이터 유출, 프라이버시 침해 등의 문제가 지속적으로 제기되어 왔고** 사용자의 거부감이 존재하였지만 IoT 디바이스 DNA를 이용한 자율 보안 기술 적용을 통한 신뢰성 있는 스마트 시티 환경으로의 발전에 기여
- 스마트 시티 서비스 분석 및 보안 요구사항 도출, 플랫폼 및 서비스용 보안 아키텍쳐 설계 및 개발, 적용을 통해 교통, 물류, 환경 등 도시에서 유발할 수 있는 다양한 보안 문제 사전 해결을 통해 사회적 비용 절감 기대
- **복잡하고 다양한 IoT 서비스 환경에서 보안사고 발생 시 유발될 대규모 피해의 사전 대비**를 통한 국가 주요 산업 및 국내 기업 보호와 경쟁력 강화에 기여

* 보안사고로 인한 제품 수요 10% 감소 및 산업 1% 장애를 가정할 경우, 스마트 단말 16조, 스마트 카 24조, 금융산업 1조 7천억 등의 피해 예상(산업연구원)

- 자율협력주행을 위한 분산형 C-ITS 서비스 인프라에 알맞은 보안 자율제어 기술 적용을 통해 **도로교통 상황에서의 공격 위협에서 발생하는 사이버 보안 문제를 해결하고 편의성과 안전성을 제공하여 국민생활 개선에 기여**

* 국토부(도로공사) 본 사업을 위한 판교 C-ITS Living Lab에 구축된 시뮬레이션 환경에서 실증 및 기술 검증 완료 (대전유성JC와 북대전 IC 사이 7.5km 시범 적용, 21.1.)

* 국내 최초 글로벌 표준 기반 IoT 인프라용 DDoS 방어를 위한 C-ITS 서비스 환경 구축 및 K-City 실증 완료 ('21.10.)

○ 성과에서 개발된 기술적 솔루션

- IoT 디바이스 DNA 기술은 기존에 사용되고 있던 상용화된 하드웨어 소자(예, SRAM, DRAM, 센서 등)의 고유특성을 이용하거나 값싼 수동 소자(예, 저항, 커패시터)를 이용하여 간단히 디바이스 DNA를 추출하기 때문에 별도의 추가 비용이 거의 없어 IoT 디바이스 개발 업체에서 손쉽게 적용 가능
- 하드웨어 고유특성을 이용한 IoT 디바이스 DNA 추출 및 이를 활용하는 디바이스 인증 기술은 각종 센서들을 가지고 있는 스마트폰, 가전, IoT 서비스, 및 각종 센서들을 사용하는 산업 전반에 걸쳐 활용 가능
- 글로벌 표준 기반 사물봇 빠른 확산 방지, 비인가 접속 방어용 보안 자율제어 플랫폼 및 보안 GW 시제품 제작 완료

* 사물봇 공격 확산 방지를 위한 스마트 세그멘테이션(SSS) 기술 및 솔루션

* 대규모 DDoS 방어를 위한 신뢰 연결관리 기반 동적경계망(DPS) 기술 및 솔루션

- **DDoS 공격이 예방되는 C-ITS(지능형교통정보시스템) 서비스 플랫폼 실용 시제품 제작 완료**

* 국내 최초 글로벌 표준 기반 IoT 인프라용 DDoS 방어를 위한 C-ITS 서비스 환경 구축으로 실증 완료('21.1.~10.)

○ 국가·사회적 파급효과

- PC와 스마트폰 해킹만 걱정하는 현재와 달리, 4차 산업혁명 시대에는 네트워크에 연결된 모든 사물이 공격 대상이 되므로 보안과 안전을 요구하는 IoT 분야의 다양한 스마트 디바이스 시스템 보안에 적용 가능
- 지능형 CCTV/스마트 홈/스마트 에너지/스마트 의료 서비스 환경에서 안전성 보장을 위한 IoT 기기 보안에 활용
- 스마트 디바이스의 해킹으로부터 국가의 스마트 모바일 서비스를 보호하기 위한 보안 서비스 인프라 구축에 활용
- 향후 안전성이 요구되는 스마트 홈, 시티 및 스마트 팩토리, 스마트 교통 등 다양한 IoT 환경에 확장 구축하여 IoT 인프라 공격 위협에서 발생하는 사이버 보안 문제를 해결하고, 편의성과 안전성을 제공하여 국민생활 개선에 기여
- IoT 기반 보안 서비스 지원 일자리 창출을 통한 고용창출 효과 증진

붙임 1 정량적 성과 목록 ('21.01~ '21.11)

■ 기술이전: 6 건, 98.1백만원

1) DDNA를 활용한 인증서 기반 IoT 디바이스 인증 플랫폼 기술: ㈜루테스, 2021.07, 착수기본료: 22백만원,
2) DDNA를 활용한 인증서 기반 IoT 디바이스 인증 플랫폼 기술: ㈜스마트엠투엠, 2021.09, 착수기본료: 22백만원
3) DDNA를 활용한 인증서 기반 IoT 디바이스 인증 플랫폼 기술: ㈜아이씨티케이홀딩스, 2021.11, 착수기본료: 22백만원
4) 스마트 경량 IoT 기기용 네트워크 보안 프로토콜 기술: 누리플렉스, 2021.05, 경상기술료: 2.3백만원
5) 스마트 경량 IoT 기기용 암호 기술: 누리플렉스, 2021.05, 경상기술료: 2.3백만원
6) 스마트 IoT 기기용 경량형 DTLS 보안 프로토콜 기술: ㈜이더블유비엠, 2021.07, 착수기본료: 27.5백만원

■ 특허: 14 건

1) APPARATUS AND METHOD FOR AUTHENTICATING DEVICE BASED ON CERTIFICATE USING PHYSICAL UNCLONABLE FUNCTION, 미국, 2021.03 출원
2) 비밀 정보 생성 장치 및 그것의 동작 방법, 대한민국, 2021.06 등록
3) 비밀키 산출을 위한 신호처리 기법 결정 방법 및 장치, 대한민국, 2021.03 출원
4) 블록체인 환경의 사용자 중심 IoT 데이터 관리 방법 및 시스템, 대한민국, 2021.08 출원
5) 프라이빗 블록체인 기반 IoT 디바이스의 토큰 인증 및 인가 방법 및 시스템, 대한민국, 2021.08 등록
6) METHOD FOR COMMUNICATING IN MULTI-MAC-OPERATING ENVIRONMENT AND IoT APPARATUS, 미국, 2021.05.04. 등록
7) APPARATUS AND METHOD FOR PROVIDING SENSOR DATA BASED ON BLOCKCHAIN, 미국, 202104.13. 출원
8) DYNAMIC SEGMENTATION APPARATUS AND METHOD FOR PREVENTING SPREAD OF SECURITY THREAT, 미국, 2021.05.26. 출원
9) APPARATUS AND METHOD FOR MANAGING REMOTE ATTESTATION, 미국, 2021.05.28. 출원
10) APPARATUS AND METHOD FOR SECURITY OF INTERNET OF THINGS DEVICE, 미국, 2021.11.01. 출원
11) 보안 통제 장치 및 방법, 대한민국, 2021.07.02. 등록
12) 사물 인터넷 기기 보안 장치 및 방법, 대한민국, 2021.03.04. 출원
13) 대규모 환경에서 원격 검증을 위한 장치 및 방법, 대한민국, 2021.07.01. 출원
14) 디바이스 특징의 유사성을 이용한 격리 디바이스 그룹 결정 장치 및 이를 이용한 방법, 대한민국, 2021.08.30. 출원

■ 표준기고서: 6 건

1) OCF: CR3398 - Extension of Account Resource (r7)
2) OCF: CR2658 Push Proxy (r11)
3) TTA: BGP 운영 및 보안
4) TTA: 생산자 사용설명서 규격
5) TTA: 사물인터넷 보안 - 최신기술 및 과제
6) IoTF: 스마트시티 환경에서의 개방형 사물인터넷 플랫폼 보안 요구사항, IoTFS-0218, 2021.06.30. (NP 채택)

■ SCI논문: 8 건

1) A metadata-driven approach to efficiently detect code-reuse attacks on ARM multiprocessors (The Journal of Supercomputing, 2021.01.04.) (IF 2.474)
2) A Trusted Execution Environment for Remote Applications on FPGA (IEEE Access, 2021.03.29.) (IF 3.367)
3) Ambassy: A Runtime Framework to Delegate Trusted Applications in an ARM/FPGA Hybrid System (IEEE Transactions on Mobile Computing, 2021.06.03.) (IF 5.577)
4) Panop: Mimicry-Resistant ANN-Based Distributed NIDS for IoT Networks (IEEE Access, 2021.08.06.) (IF 3.367)
5) A Hardware Platform for Ensuring OS Kernel Integrity on RISC-V (Electronics, 2021.08.26.) (IF 2.397)
6) Two-Factor Device DNA-based Fuzzy Vault for Industrial IoT Device Security (IEEE Access, 2021.07.07.) (IF 3.367)
7) Scrutinizing the Vulnerability of Ephemeral Diffie–Hellman over COSE (EDHOC) for IoT Environment Using Formal Approaches (Mobile Information Systems, 2021.09.13.) (IF 1.802)
8) A malware distribution simulator for the verification of network threat prevention tools (Sensors, 2021.10.21.) (IF 3.576)

붙임 2 대외 인증 및 수상

■ [수상] Best Paper Award (2021 World Conference on Information Security Applications)
- 논문명: Echo-Guard: Acoustic-based Anomaly Detection System for Smart Manufacturing Environments (2021-08-12)

KIISC-2021-020

Best Paper Award

The KIISC award for WISA 2021 Best Paper is presented to

Chang-Bae Seo, Gyuseop Lee, Yeonjoon Lee
and Seung-Hyeon Seo (Hanyang University, Republic of Korea)

for the paper entitled

"Echo-Guard : Acoustic-based Anomaly Detection System for Smart Manufacturing Environments"

August 12, 2021

Jaecheol Ryou, President
General Chair

Korea Institute of Information Security and Cryptology

< WISA 2021 Best Paper Award >

■ [대외 인증] TTA 공인 시험성적서 획득 (TTA-21-0601, 2021-06-17)

- IoT 디바이스 자율 신뢰보장 기술
  * IoT 디바이스 DNA 자율생성 ID/PW 키 비도: 256비트 달성
  * 신뢰실행환경 TCB 크기 : 100K LoC 이하 달성
  * 디바이스 자율진단 정상상태 모델 정립 : 5종 이상 달성

시험 성적서

한국정보통신기술협회
주소: 경기도 성남시 분당구 분당로 47
전화: 031-780-9120, 팩스: 070-4705-0909

성적서 번호: TTA-21-0601

TTA

1. 의 뢰 자

o 기관명: 한국전자통신연구원

o 주 소: 대전광역시 유성구 가정로 218

2. 시 료: 'IoT 디바이스 자율 신뢰보장 기술 및 글로벌 표준기반 IoT 통합보안 오픈 플랫폼 기술개발' 과제 결과물

3. 시험기간: 2021.6.3. ~ 2021.6.9.

4. 시험장소: 대전광역시 유성구 가정로 218 한국전자통신연구원 7 연구동
서울특별시 금천구 가산디지털1로 165 가산비즈니스센터 ㈜아이오트러스트
서울특별시 관악구 관악로1 서울대학교 제2공학관

5. 시험방법: 시험결과 참조

이 성적서의 시험결과는 의뢰자에 의해 제공된 시료에 한하며 용도 이외의 사용을 금합니다.

확 인	작성자	승인자
	성 명: 정 희 진 (서명)	성 명: 이 종 민 (서명)

2021. 6. 17.

한국정보통신기술협회 회장 (인)

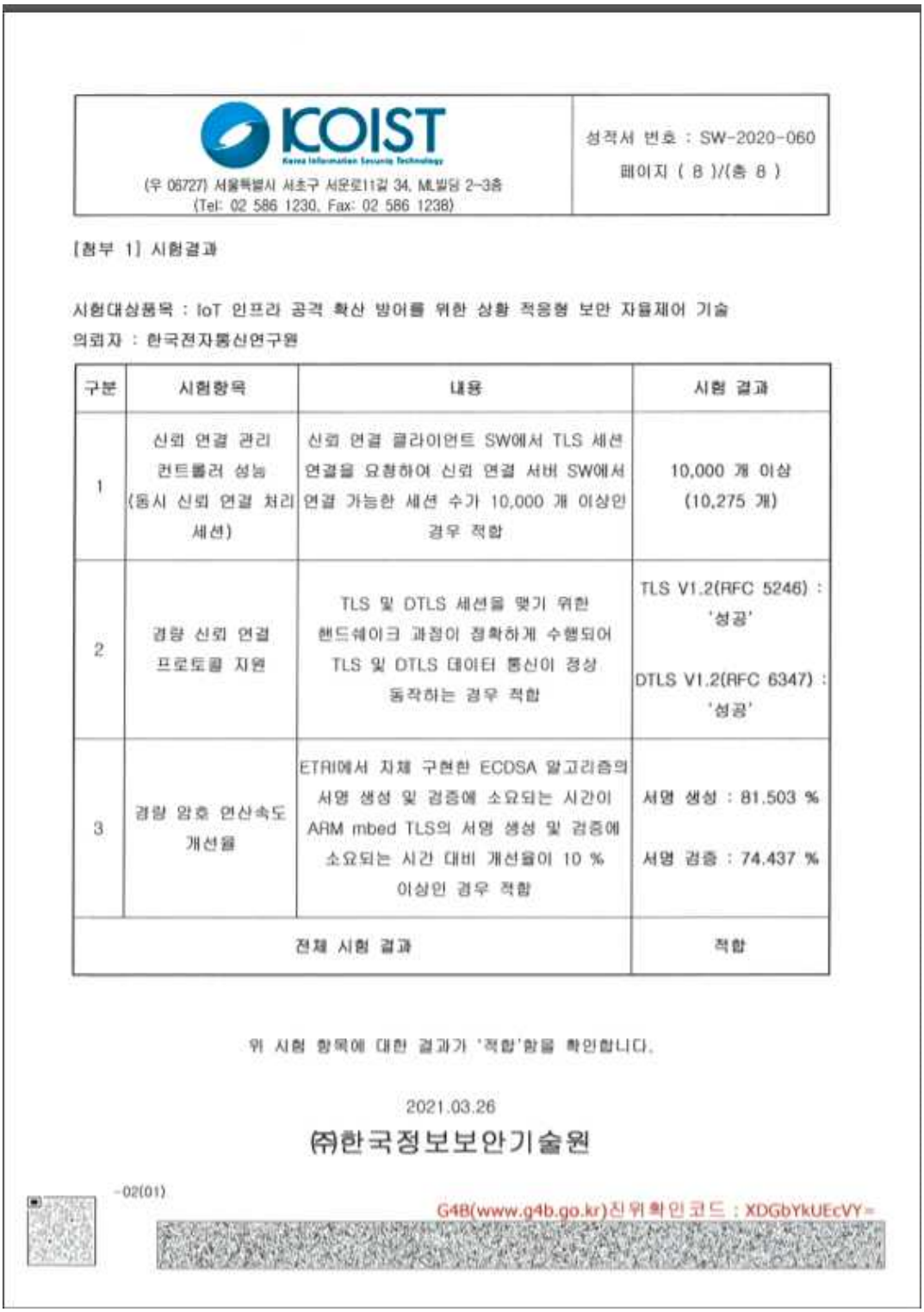
TPG-0024-1-A(01) 페이지 (1) / (총26)

※ You can verify the forgery and authenticity by the barcode at the end of this document.

<TTA 공인 시험성적서>

■ [대외 인증] KOIST 공인 시험성적서 획득 (2021-03-26)

- IoT 인프라 공격 확산 방어를 위한 상황 적응형 보안 자율제어 기술
  * 신뢰연결관리 컨트롤러 성능 : 동시 신뢰연결 처리 세션수 10,000세션 이상 달성
  * 경량 신뢰 연결 프로토콜 지원 : (TLS V1.2, DTLS V1.2) 적합여부 달성
  * 경량 암호 연산속도 개선율 : (서명생성 개선율 81.503%, 서명검증 74.437%) 10%이상 달성



KOIST
Korea Information Security Technology

(우 06727) 서울특별시 서초구 서운로11길 34, ML빌딩 2~3층
(Tel: 02 586 1230, Fax: 02 586 1238)

성적서 번호 : SW-2020-060
페이지 (8)/(총 8)

[첨부 1] 시험결과

시험대상품목 : IoT 인프라 공격 확산 방어를 위한 상황 적응형 보안 자율제어 기술
의뢰자 : 한국전자통신연구원

구분	시험항목	내용	시험 결과
1	신뢰 연결 관리 컨트롤러 성능 (동시 신뢰 연결 처리 세션)	신뢰 연결 클라이언트 SW에서 TLS 세션 연결을 요청하여 신뢰 연결 서버 SW에서 연결 가능한 세션 수가 10,000 개 이상인 경우 적합	10,000 개 이상 (10,275 개)
2	경량 신뢰 연결 프로토콜 지원	TLS 및 DTLS 세션을 맺기 위한 핸드쉐이크 과정이 정확하게 수행되어 TLS 및 DTLS 데이터 통신이 정상 동작하는 경우 적합	TLS V1.2(RFC 5246) : '성공' DTLS V1.2(RFC 6347) : '성공'
3	경량 암호 연산속도 개선율	ETRI에서 자체 구현한 ECDSA 알고리즘의 서명 생성 및 검증에 소요되는 시간이 ARM mbed TLS의 서명 생성 및 검증에 소요되는 시간 대비 개선율이 10 % 이상인 경우 적합	서명 생성 : 81.503 % 서명 검증 : 74.437 %
전체 시험 결과			적합

위 시험 항목에 대한 결과가 '적합'함을 확인합니다.

2021.03.26

㈜한국정보보안기술원

-02(01)

G4B(www.g4b.go.kr)진위확인코드 : XDGbYkUEcVY=

<KOIST 공인 시험성적서>