한밭대학교
우수기술

04

노이즈가 삽입된 물리적 복제 불가 함수 시스템

물리적 복제 불가 함수의 출력에 의도적으로 가공 노이즈를 삽입하여 챌린지(challenge)/응답(response) 분석 난이도를 높이도록 한 노이즈가 삽입된 물리적 복제 불가 함수 시스템 기술

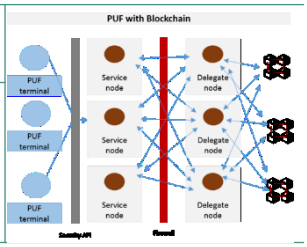
연구책임자
한밭대학교
컴퓨터공학과
이현빈 교수

기술 개요

- 다수의 CRP(Challenge and Response Pair)들을 사용하고 신호 전파의 지연을 이용하는 대표적인 PUF(Physical Unclonable Function)를 대상으로 외부에 노출되는 CRP들 중 2차 응답 신호(RP'') 비트열에 가공 노이즈를 삽입하여 모델링 공격의 데이터 분석을 어렵게 하는 기술

기술의 적용처

응용분야	적용제품
IoT, 암호화폐, RFID, 정품인증시스템 등	사물인터넷용 보안 반도체(G3), 블록체인(퓨어체인), RFID 칩(VERA X1)



기존 기술의 문제점

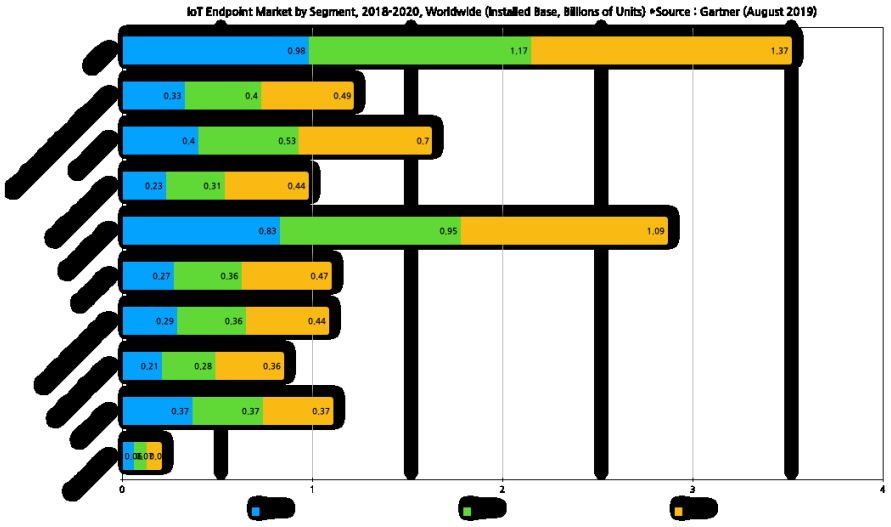
- 디바이스의 인증에 이용되는 PUF에는 약한-PUF(weak-PUF)와 강한-PUF(strong-PUF)로 나누어짐
- 강한-PUF는 많은 CRP를 저장하고 있으며 각 CRP가 디바이스의 인증 또는 식별하는데 직접적으로 사용되며, 인증에 사용되는 CRP들은 일반적으로 외부로 공개됨
- 최근에는 기계학습과 같이 많은 데이터들을 바탕으로 분석하는 기술이 발전하면서 노출된 CRP들을 수집하여 해당 PUF의 특성을 모델링하는 공격이 가능해지고 있음

기술의 특장점

- PUF를 이용한 디바이스의 인증 수행 과정에서 노출되는 응답신호(RP)에 가공 노이즈를 삽입하여 외부 공격자의 CRP 분석을 어렵게 함
- 인증에 사용되는 2차 응답신호(RP")와 노출되는 응답신호(RP)의 차이를 증가시켜 아직 사용되지 않은 CRP들의 예측이 어려움
- 디바이스 부분에 별도의 보안 모듈을 사용하지 않고 ECC 디코더 모듈을 인증기에 배치하여 하드웨어 오버헤드를 줄일 수 있음

기술의 시장성

- 가트너에 따르면 2020년 엔터프라이즈 및 자동차 관련 IoT 시장이 2019년과 비교할 때 21% 증가한 58억 개의 엔드포인트로 성장할 것으로 전망함
- 특히, 유틸리티와 물리 보안 분야에서 IoT 엔드포인트가 많이 사용될 것으로 예측함



기술 성숙도

1	2	3	**4**	5	6	7	8	9

TRL 4 단계
실험실 규모의 소재/부품/시스템 핵심성능 평가

지식재산권 현황

발명의 명칭	노이즈가 삽입된 물리적 복제 불가 함수 시스템		
등록번호	10-1974465	등록일자	2019.04.25

문의

한밭대학교
산학협력단

TEL

042-821-1947

E-mail

sskim@hanbat.ac.kr