# 사물인터넷 노린 사이버 공격, 복제 불가능한 정보로 막는다!
# 지스트 연구진, IoT 보안 신뢰성 높일 기술 '美 특허' 출원

- 물리적 복제 방지기능과 채널 정보 결합, 재전송 공격에 강한 보안키 생성 및 인증기법 개발
- 황의석 교수 연구팀, 과기정통부 장관상 이어 **IEEE** 빅데이터 학술대회서 성과 발표

▲ 지스트 황의석 교수

지스트(광주과학기술원, 총장 김기선) 연구진이 보편화 되고 있는 **사물인터넷(Internet of Things, IoT)을 타깃으로 한 재전송 공격*을 방어할 수 있는 새로운 인증 기법을 개발**했다.

* **재전송 공격**: 공격자가 무선 통신 인증 체계를 교란하고자 할 때 취할 수 있는 전략 중 하나. 적법한 사용자들이 주고받는 인증 신호를 도청해 그대로 재전송하는 기법으로, 일반적으로 방어하기 어려운 공격으로 알려져 있다.

IoT를 적용한 시스템의 보안이 뚫릴 경우 발생할 수 있는 **심각한 사회문제들을 예방**하고 IoT 관련 보안의 신뢰성을 제고해 **IoT 산업의 활성화를 촉진**할 수 있을 것으로 예상된다.

지스트 **전기전자컴퓨터공학부 황의석 교수와 한승남·이해원 학생(전기전자컴퓨터공학부), 윤승욱 학생(기계공학부)**은 이번 연구 성과로 지난 11월 과학기술정보통신부가 개최한 <**2022년도 대학ICT연구센터 연구책임자 워크숍**>**에서 과기정통부 장관상**을 수상했으며, 관련 기술을 **미국에 특허로 출원**했다. (특허명: 채널상태정보를 이용하는 PUF 기반 사물인터넷 디바이스 및 그 인증 방법)


▲ <대학ICT연구센터 연구책임자 워크숍 2022>에서 학생창의자율과제 부문 과학기술정보통신부 장관상을 수상하는 황의석 교수(오른쪽)

또한, 오는 12월 17~20일에 일본 오사카에서 열리는 **'빅 데이터' 관련 국제학술대회인 「IEEE International Conference on Big Data 2022」에서 관련 연구 성과를 발표**할 예정이다.

연구팀은 IoT 장치에서 측정한 **PUF와 무선 통신 채널에서 수집한 채널 상태정보(Channel State Information, CSI)를 결합하는 인증기법**을 고안했다.

모든 장치는 공정 과정에서 발생하는 오차로 인해 서로 다른 응답 특성을 갖게 되는데, 이를 **'물리적 복제 방지기능'(Physically Unclonable Function, PUF)**'이라 한다. **이 특성만을 사용해 보안키를 생성하고 사용자 인증을 진행할 경우, 신호 도청을 기반으로 하는 재전송 공격에 취약**하다고 알려져 있다.

사람마다 지문이 다른 것처럼 **채널 상태 정보(CSI)**는 물리적 환경의 공간적 특성이 반영돼 측정되므로 **측정하는 환경에 따라 그 값이 다르다.** 따라서 공격자가 적법한 인증 신호를 도청해 재전송하더라도 적법한 사용자와 물리적으로 같은 위치에 존재하는 것은 불가능하므로 **공격자의 인증 시도는 무력화**된다.

연구팀이 **32bits 길이의 보안키를 사용해 재전송 공격에 대한 신원 인증 성능을 평가**한 결과, 기존 PUF를 활용한 인증기법은 50만 번의 공격 중 약 0.5% 확률로 공격자의 인증 시도가 허용됐지만, **연구팀의 새로운 인증기법은 공격자의 인증 시도를 모두 차단**할 수 있었다.

황의석 교수는 "IoT는 가전 장치부터 사회 중요시설까지 광범위하게 설치되고 있으며, IoT 장치에 대한 사이버 공격은 심각한 사회문제로 이어질 수 있다"며 "**CSI와 PUF를 결합한 보안키 생성기법은 공격자의 도청으로부터 IoT 장치를 보호할 수 있는 솔루션**이 될 수 있을 것"이라고 밝혔다.

한승남 학생은 "연구 과정에서 발생한 어려움을 극복할 수 있었던 건 팀원들 사이의 끊임없는 의견 교환과 교수님의 지도가 있었기 때문"이라며 "앞으로도 PUF와 CSI를 이용해서 다양한 연구를 진행하고 싶다"고 말했다.

▲ 2022년도 ICT혁신인재양성사업의 학생창의자율과제에 참여한
(왼쪽부터) 전기전자컴퓨터공학부 한승남, 이해원, 기계공학부 윤승욱 학생

이번 연구는 **과학기술정보통신부 정보통신방송혁신인재양성사업**(과제명: 영지식 센싱, 암호인증, 블록체인 기반 클라우드 서비스 융합 기술 개발, 연구책임자: 지스트 이흥노 교수)의 지원을 받아 수행됐다.