정 보 보 호 학 회 지
제 30 권 제1호, 2020. 2

키 은닉 기법을 활용한 안전하고 신뢰성 있는 사물인터넷 디바이스 인증 기술

김 병 구*, 윤 승 용*, 강 유 성*, 최 두 호*

요 약

사물인터넷 환경으로 연결되는 디바이스 종류가 점점 다양해지고, 이를 통해 유통되고 처리되는 정보의 양이 절대적으로 증가함에 따라 여러 보안 이슈들도 함께 부각 되고 있다. 무엇보다도, 사물인터넷 기술은 우리 실생활에 직접 접목되기 때문에, 기존 사이버공간의 위험이 현실 세계로 전이 및 확대될 수 있다는 우려가 점차 증대되고 있다. 특히, 사물인터넷 기기들의 인증 및 데이터 보호에 필요한 키의 누출은 불법 복제 및 데이터 유출을 통한 경제적, 산업적 손실을 유발하고 있는 실정이다. 따라서, 본 논문에서는 이러한 보안 위협에 대응하기 위한 하드웨어 기반의 키 은닉 기술 및 소프트웨어 기반의 키 은닉 기술의 연구 동향에 대해서 살펴보고, 이를 활용한 사물인터넷 디바이스 인증기법을 제시한다. 이는 하드웨어 및 소프트웨어 기반의 키 은닉 기술을 적절히 접목함으로써, 여러 보안 취약점으로 인한 인증키 노출 위협을 근본적으로 차단하여 효과적이고 안전한 인증키 관리를 가능하게 한다. 즉, 본 논문은 다양한 키 은닉 기술에 대해서 설명하고, 이를 토대로 보다 안전하고 신뢰성 있는 사물인터넷 디바이스 인증 기술을 제공하고자 한다.

Ⅰ. 서 론

사물인터넷 기술은 다양한 IoT(Internet of Things) 디바이스들을 유무선 네트워크로 연결해 정보를 공유하고 활용할 수 있는 서비스 환경을 제공해준다. 그러나, 이와 같은 IoT 디바이스에 적용된 보안 기술은 대부분 메모리 상에 키를 보관하기 때문에, 이의 유출로 인한 다양한 피해사례가 전해지고 있다. 게다가, 최근 IT 기술의 급격한 발전으로 IoT 디바이스들을 이용한 다양한 응용 서비스가 폭발적으로 증가함과 동시에, IoT 기기의 탈취, 도난, 해킹 등을 통한 불법 복제 및 데이터 유출로 인한 경제적, 산업적 손실이 날이 갈수록 커져가고 있는 실정이다.

이러한 문제를 해결하고자 다양한 형태의 키 은닉 기술이 등장하게 되었으며, 이를 통해서 IoT 디바이스의 보안 안정성을 증가시키고자 하였다. 즉, 이러한 키 은닉 기술을 이용하여 생성된 키는 유출 가능성이 있는 데이터를 암호화하거나, IoT 디바이스의 인증에 이용될 수 있다. 무엇보다도, 이와 같은 키 은닉 기술을 인증에 적절하게 활용한다면, 각 디바이스를 식별하기 위한 고유 식별자를 외부에서 주입하는 과정 없이, 디바이스 내부에서 고유의 식별자를 생성할 수 있다. 또한, 각 식별자를 저장하기 위한 내부의 비휘발성 메모리를 두지 않아도 되기 때문에, 비용절감도 기대할 수 있다. 따라서, IoT 디바이스의 인증을 위해서 키 은닉 기술을 적절히 활용할 수 있다면, 인증 키 노출로 인한 외부로부터의 보안 위협을 최소화함은 물론, 보다 안전하고 신뢰성 있는 IoT 디바이스 인증이 가능하다.

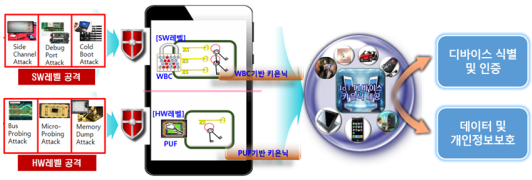
본 논문에서는 II장에서 IoT 디바이스의 인증에 활용될 수 있는 다양한 형태의 키 은닉 기술에 대한 현재의 연구 동향에 대해서 살펴보고, III장에서는 이와 같은 키 은닉 기법을 활용한 IoT 디바이스 인증기술을 제시해 보고자 한다. 마지막으로 IV장은 제시한 기법의 실현 및 적용 가능성에 대해 논의하고 결론을 맺고자 한다.

이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2018-0-00230, (IoT 총괄/1세부) IoT 디바이스 자율 신뢰보장 기술 및 글로벌 표준기반 IoT 통합보안 오픈 플랫폼 기술개발 [TrusThingz 프로젝트])
* 한국전자통신연구원 미래암호공학연구실(연구원, {bkkim05, syyoon, youskang, dhchoi}@etri.re.kr)

Ⅱ. 키 은닉 기술 동향

키 은닉 기술은 IoT 디바이스의 메모리에 키를 저장하지 않고 필요한 시점에 데이터 암복호화를 위해 키를 즉시 사용할 수 있는 기술로써, 기존의 메모리 공격, 디버그 포트 공격, 역공학 공격 등의 키 노출 보안 위협에 대응할 수 있다. 대표적인 기술로는 하드웨어 기반의 PUF(Physically Unclonable Function) 기술과 소프트웨어 기반의 WBC(White-Box Cryptography) 기술이 존재한다.

본 장에서는 이와 같은 키 은닉 기술 동향에 대해서 자세히 살펴본다.



〔그림 1〕 키 은닉 기술 개요

2.1. 하드웨어 기반 PUF 기술 동향

PUF 기술은 반도체 제조 공정상에서 미세한 차이로 발생하는 하드웨어 고유 특성을 이용하여, 물리적으로 복제가 불가능한 디바이스를 개발하는 기술이다. 따라서, 동일한 설계를 동일한 공정으로 구현하더라도 각 디바이스는 복제 불가능한 고유값을 가지며, 이를 디바이스 식별 및 인증, 비밀 키 생성 등에 활용할 수 있다. IoT 디바이스로부터의 안정성(Steadiness), 난수성(Randomness), 유일성(Uniqueness), 예측 불가능성(Unpredictability), 복제 불가능성(Physical unclonability) 등의 보안 요구사항을 만족하는 고유값 추출을 위한 PUF 기술 개발에 대한 연구는 지난 수년 동안 지속되었으며, 최근 IoT 디바이스의 보안이 강조됨에 따라 해당 연구가 더욱 활발히 진행되고 있다.

이에, 한국전자통신연구원에서는 부채널 공격 방지를 위한 암호 키 마스킹을 위한 난수 생성에 PUF를 활용하였고, FPGA 상에서 PUF 로직 구현 및 안정적인 출력값 생성을 위한 ECC(Error Correcting Code) 적용 모듈 테스트용 보드를 구현하였다. 최근에는 디바이스 DNA 기반 기술[1]로써 다양한 종류의 하드웨어 소스로부터 고유값을 추출하는 PUF 기술을 연구개발 중이며, Resistor-Capacitor(RC) 회로의 Variation, PCB Parasitic, Analog-to-Digital Converter(ADC)의 고유 특성을 이용하여 입력 비트 패턴에 따른 ADC 샘플링 값의 특정 비트를 출력으로 하는 RC PUF[2], 기존 Ring Oscillator(RO) PUF의 성능을 개선시키기 위한 위상검출(Phase-Detection) 방식의 PDRO PUF[3], Wireless Transceiver의 데이터 송수신용 버퍼를 이용한 PHY(Physical Layer) PUF[4] 기술 등이 대표적인 기술이다.

국내 대학을 중심으로는 이상적인 PUF 로직을 가정한 보안 프로토콜 및 응용, PUF 분석을 위한 전자계 모델링 기법, 전송선의 크로스 토크를 이용한 PUF, 듀얼 안티퓨즈 OTP(One Time Programmable) 메모리와 SRAM을 이용한 결정적 PUF 기술에 대한 연구가 진행되었으며, 특히 한양대에서는 반도체 제조 과정에서 인접한 두 메탈 레이어를 연결하는 공정인 VIA가 형성될 확률을 기반으로 랜덤값을 생성하는 VIA PUF 기술[5]을 개발하여 아이씨티케이홀딩스를 통해 상용화하였다. 삼성전자도 IoT 전용 프로세서에 자체 개발한 SAMPUF를 적용하여 칩의 복제를 원천적으로 차단하는 보안솔루션을 제공하고 있다.

국외에서도 PUF에 대한 연구가 활발히 진행되고 있는데, MIT에서는 RO-PUF[6]와 Arbiter PUF[7]를 제안하였다. RO-PUF는 인버터를 이용한 회로상의 루프를 이용하여 발진되는 진동주파수를 비교하여 출력이 결정되는 PUF이고, Arbiter PUF는 설계상으로 동일한 거리를 갖는 두 경로에 동일한 신호를 보내 어떤 신호가 먼저 Arbiter에 도착하는지에 따라 출력이 결정되는 PUF이다. 이 두 기술은 모두 딜레이 (Delay) 기반의 구현 기술로써 가장 많은 연구가 진행되고 있다. 또한, Arbiter와 RO 기술의 특징을 조합한 S-ArbRO-PUF, CMOS 공급전압에 따른 지연시간 영향을 추가한 멀티 전원 RO-PUF, 반도체 칩 제작 시 테스트를 위한 DFT(Design for Test) Scan-chain을 PUF 딜레이 로직으로 이용한 ScanPUF, 칩의 Clock 트리를 활용한 ClockPUF, LFSR 로직과 RO-PUF를 병합한 Pseudo-LFSR PUF, 마이크로 프로세서의 파이프라인 데이터 패스와 컨트롤 패스의 딜레이를 활용한 PUF 등 다양한 기술들이 제안되었다.

이외에도, 많이 연구되고 있는 또 다른 종류의 PUF

로 메모리 기반 PUF가 있다. 대표적인 것으로 SRAM PUF[8]를 들 수 있는데, 2개의 동일한 인버터로 구성되어 있는 셀 구조를 이용하여 전원을 인가할 때의 초기 값 변이에 기반을 둔 PUF이다. SRAM PUF 발표 이후 NAND나 NOR 게이트를 Butterfly 구조로 구현 후 불안정 상태에서의 초기 값을 이용하는 Latch PUF, Flash 메모리의 각 셀마다 프로그래밍 되는 시간 차를 이용하는 Flash 메모리 PUF, 전압 공급이 끊어져도 이전의 Current 양을 기억하여 전원이 다시 인가되면 기존 상태가 그대로 복원되는 특징이 있는 Memristor 비휘발성 메모리 소자를 이용하는 Memristor PUF 등 많은 메모리 기반의 PUF 기술들이 개발되었다. 그 외에도 PUF의 Challenge-Response 매핑을 확장할 수 있도록 재설정 동작을 추가한 Reconfigurable PUF[9], 보안 응용에서 PUF 모듈 삭제 필요성을 위하여 ALLIE 공정을 이용한 Erasable PUF[10] 등이 제안되었으며, EU는 2012년부터 2015년까지 4년간 독일 반도체 업체인 Infineon, 프랑스의 보안 업체인 Safran, Cassidian cybersecurity 등과 함께 PUF 기술을 반도체 위조 방지 및 물리 공격 방지에 적용하고자 하는 HINT 프로젝트[11]를 수행하였다,

PUF는 구현 기술과 상관없이 동일한 혹은 다른 challenge 입력에 대한 response 특성인 안전성, 유일성, 난수성 등으로 성능을 평가한다. 이러한 특성을 높이고자 환경 적응형 PUF 구현 기술을 찾거나 ECC와 같은 오류 수정 기술과 병합하는 연구 등이 진행되고 있으나, 아직 이상적인 성능의 PUF는 개발되지 못하고 있다. 현재 개발된 기술들은 불안정성으로 인하여 완전한 비밀 키 은닉에는 활용되지 못하고 부분적으로 사용되고 있는 실정이다. 또한, 머신 러닝을 활용한 모델링 공격[12], RO-PUF에 대한 EM 기반 모델링 공격, PUF 자체 로직이나 해시 또는 오류 정정 연산 로직에 대한 전력 부채널 공격[13], 메모리 기반의 PUF 복제 공격[14] 가능성 등이 발표되면서 다양한 분석 방지 및 복제 방지 기능에 대한 연구가 추가로 진행되고 있다.

〔표 1〕 PUF 종류에 따른 장단점 분석

PUF 종류	장점	단점
Arbiter PUF	(부분적으로) 머신러닝 공격에 강인함	딜레이 패스가 동일해야함
RO-PUF	구현이 용이함	환경요인에 민감함
SRAM PUF	통계적 성능치가 우수함	CRP 개수가 적음
VIA PUF	ECC 모듈이 필요없음	CRP 개수가 적음
RC PUF	저비용으로 구현 가능함	-
PDRO PUF	기존 RO-PUF 대비 CRPs 개수가 많음	환경요인에 민감함
PHY PUF	실시간으로 PUF값 획득이 가능함	CRP 개수가 적음

지금까지 살펴본 PUF 구현에 대한 원천 기술 연구뿐만 아니라, 현재는 개발된 PUF 기술을 기반으로 아이씨티케이홀딩스, Intrisic-ID, NXP, Verayo 등에서 PUF 성능 개선을 통한 보안 상용 제품 개발 및 보안 시스템 접목 기술 등을 제공하기 위해 노력하고 있다.

2.2. 소프트웨어 기반 WBC 기술 동향

소프트웨어 기반 키 은닉 기술은 다양한 난독화 및 패커 기술을 활용한 역공학 방어 기법이 개발되었는데, 가장 대표적인 것이 WBC 기술이다. WBC 기술은 암호 키와 연산을 한꺼번에 테이블화 시켜서 메모리 영역에 테이블로 저장하여 암호 키 노출을 방어하는 암호화 기법으로서, 암호화 테이블과 복호화 테이블을 별도로 저장하는 구조로 설계하면 키 은닉 효과를 기대할 수 있다.

한국전자통신연구원에서는 WBC와 응용기술, 이를 이용한 콘텐츠 보호 방법, 대수적 분석에 강인한 재인코딩 방법, 테이블 탈취 위협에 대응하기 위한 관련 연구를 진행하였다. 서울대에서도 WBC에 대한 공격으로 퍼터베이션을 이용한 WBC의 대수적 분석을 발표하였으며, 국내기업 중에는 삼성SDS에서 WBC 연구 및 상용화를 활발하게 추진하고 있는 것으로 알려져 있다.

국외에서는 Chow와 그 외 3명이 2002년에 WBC를 소개하고 White-Box 공격 상황을 정의하였다[15,16]. DES와 AES에 대한 WBC 구현 방법을 발표하였는데, WBC 구현 방식에 따라 AES-128 알고리즘을 구현할 경우 화이트박스 암호/복호 룩업 테이블의 크기는 각각 770KB이고 연산속도는 AES 알고리즘의 표준 구현 방식 대비 10배 정도 느려지는 것을 보였다. 이후, WBC에 대한 분석 및 공격과 대응에 관한 연구가 활발히 진행되었다. 2004년 Billet은 매우 효율적인 화이트박스 AES 분석 기법[17]을 발표하였는데, 특별히 내부 인코

딩의 비선형인 부분을 제거한 줄어든 버전에서 대수적인 분석이 가능함을 보였다. 또한, AES에 대한 공격을 일반화하여 다른 블록 암호 알고리즘에 대한 WBC 구현을 분석할 수 있음을 보인 연구[18]도 발표하였다.

WBC에 대한 공격 방법 중 충돌 공격은 다른 입력값으로 같은 출력값을 얻었을 경우를 예측해서 비밀 키를 찾아내는 공격 방법이다. 선형 시스템을 만들기 위해 첫 번째 라운드 출력값의 충돌을 이용하고 이 시스템을 풀어 입력값에 적용된 인코딩과 비밀 키를 추출한다. Billet 단독 공격이 불가능한 Karroumi[19]의 화이트박스 AES에 이 충돌 공격과 Billet 공격이 함께 적용되면 비밀 키를 찾을 수 있다. Biryukov는 DES와 AES 등 기존의 화이트박스로 구현된 블록 암호에 대한 키 추출 공격 및 테이블 분해 공격은 Affine-Substitution-Affine(ASA) 구조가 주된 원인이라고 분석하였다[20]. 이에 2014년 두 개의 비밀 Substitution 층과 세 개의 Affine 층이 교대로 나타나 5개 층으로 배치되는 ASASA의 구조를 제안하여 테이블 분해 공격을 방지함으로써 키 추출 공격에 대응하는 한편, 테이블 탈취 공격은 공격자가 추출해야 할 데이터 크기를 증가시키는 방법으로 대응하였다. ASASA 구조의 화이트박스 구현에 따른 메모리 요구량은 선택에 따라 2MB부터 20GB까지 다양하게 존재한다. 이러한 ASASA 구조에 대한 테이블 분해 공격 및 키 추출 공격은 각각 2015년 Dinur의 연구[21]와 Minaud의 연구[22]에 의해 발표되었다. 이 공격들에 대응하기 위하여 발표된 화이트박스 전용 암호가 SPACE[23] 알고리즘이다. ASASA 구조에 근거한 SPACE 알고리즘은 테이블 분해 및 키 추출 공격에 대응하는 동시에 테이블 탈취 공격에도 대응 가능하다.

소프트웨어 기반 키 은닉 기술의 선두 기업인 Irdeto는 WBC와 관련된 다수의 특허를 출원하고 미디어 접근 제한, 키 관리, 개인정보보호 및 사이버 범죄 관리 등 폭넓은 응용에 이를 이용하고 있다. 현재 Irdeto Research 팀에서는 제2, 3세대 WBC를 개발하여 기존의 차분분석 및 오류주입 공격 등을 방어하였고, 제4세대 WBC의 개발을 통해 테이블에 의존하지 않는 차세대 기법을 선보일 예정이라고 한다. 또한, Gemalto는 소프트웨어 라이센싱 솔루션에 WBC 기술을 최초로 제공했던 SafeNet을 인수하고, 지속적으로 취약점 대응 및 응용에 대한 연구개발을 진행하고 있다.

IoT 보안 위협이 증가함에 따라 소프트웨어 기반 키 은닉 기술은 사용자의 데이터 보호와 개인정보보호를 위하여 필수 불가결한 요소가 될 것으로 예상된다. 하지만, 기존의 소프트웨어 기반 키은닉 기술인 WBC 기술은 요구되는 하드웨어 리소스가 너무 방대하여 한계점을 가지고 있어 이를 극복하기 위한 대책을 찾으려 노력하고 있는 실정이다. 상용화 제품의 경우, WBC 기술을 위하여 사용된 알고리즘은 대부분 비공개로 되어 있는데, 이 배경에는 비공개로 인한 보안강도 강화뿐만 아니라 해당 기술이 가진 대수적 취약점을 완벽하게 극복하지 못했다는 불안감이 존재하는 것으로 해석이 가능하다. 키 은닉 기술의 대표 기업인 Irdeto가 차세대 WBC 기술로 '탈 룩업 테이블'을 선언한 것처럼, 메모리 크기에 구애받지 않는 보안성이 향상된 기법을 적용하여 키 은닉 안전성을 향상시킬 필요가 있다. 따라서, 소프트웨어 기반 키 은닉 기술인 WBC 기술을 구현함에 있어서, 공개된 암호 알고리즘을 이용해야 하며, 요구되는 리소스가 기존 기술보다 작아야 하고, 최근 알려진 부채널 분석에도 강인하게 구현될 수 있도록 연구개발이 진행되어야 할 것이다.

Ⅲ. 키 은닉 기술을 활용한 사물인터넷 디바이스 인증

하드웨어 기반의 대표적인 키 은닉 기술인 PUF는 키를 따로 보관할 필요 없이 필요할 때마다 생성할 수 있으므로 키 노출로 인한 보안 위협을 최소화할 수 있다. 이러한 PUF 기술의 특성을 활용한 IoT 디바이스의 인증기법은 보안 안정성을 크게 향상시킬 수 있다. 그러나, 일반적인 PUF 기반의 인증기법들은 인증키로 사용되는 상당히 많은 양의 CRP 정보들을 인증 서버 측면에서 저장 관리해야 하는 부담이 있으며, PUF 장치에 대한 부채널 공격이나 복제 공격, 통신 선로 상의 프로토콜 공격으로 인증키가 노출될 수 있는 다양한 보안 위협이 존재한다. 따라서, 인증 서버의 부하를 줄일 뿐만 아니라, 인증키 노출에 강인한 보다 효과적인 인증기법들이 요구되고 있다.

본 장에서는 상기의 PUF 기술에 소프트웨어 기반의 키 은닉 기술인 WBC 기술을 접목하는 방안을 제시한다. 이는 통신 선로 상의 CRP 정보 노출 및 인증 서버의 취약점으로 인한 키 노출 위협을 최소화함으로써,

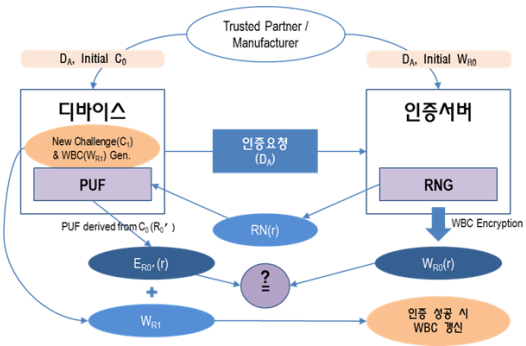
IoT 디바이스에 대한 보다 안전하고 신뢰성 있는 인증 기법을 제공할 수 있다. [그림 2]는 이와 같은 하드웨어 및 소프트웨어 기반의 키 은닉 기술을 활용한 IoT 디바이스 인증기법에 대한 간략한 수행 개념도를 나타낸다.

[그림 2]처럼, 제시된 PUF 장치를 갖는 디바이스에 대한 인증 방식은 기존의 PUF 기반 인증 방식과 달리, 제조 공정단계에서 도출된 하나의 CRP 정보만을 해당 디바이스 및 인증 서버 내에 가지고 수행된다. 이때, 해당 디바이스는 도출된 초기 CRP 정보 중 Challenge 값(C0)을 초기 정보로 가지며, 인증 서버는 해당 Challenge 값에 대응하는 Response 값(R0)을 토대로 생성한 WBC 로직인 WR0를 나누어 갖는다. 이와 같은 초기 설정을 바탕으로 수행되는 상기의 디바이스 인증 방식에 대한 대략적인 수행 시나리오는 다음과 같다.

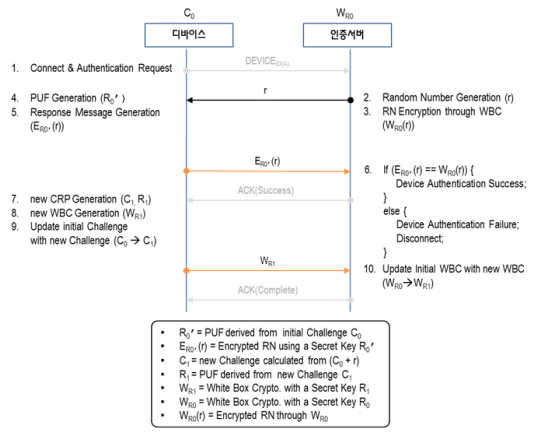
우선, 인증하고자 하는 디바이스의 인증 요청에 따라 인증 서버는 난수 발생기(Random Number Generator: RNG)를 통해서 임의의 난수 값 r을 생성하여 되돌려 줌은 물론, 해당 디바이스와 연관된 WBC 로직을 통해서 해당 값을 암호화(WR0(r))한다. 이어서, 해당 디바이스는 인증 서버로부터 임의의 난수 값 r을 수신하게 되면, 기 저장된 초기 Challenge 값 C0에 대응하는 Response 값 R0'을 자신의 PUF 장치로부터 도출하고, 이를 바탕으로 해당 난수 값을 암호화(ER0'(r))하여 인증 서버로 되돌려 준다. 인증 서버는 기생성해 놓은 암호문(WR0(r))과 해당 디바이스로부터 수신한 암호문(ER0'(r))의 일치 여부를 통해서 해당 디바이스를 인증한다. 이와 같이, 해당 디바이스에 대한 인증이 성공한다면, 해당 디바이스는 초기 Challenge 값 C0와 인증 서버로부터 수신한 난수 값 r을 바탕으로 새로운 Challenge 값인 C1을 생성하며, 이에 대응하는 Response 값(R1)을 PUF로부터 생성한다. 그리고, 해당 Response 값 R1을 토대로 새로운 WBC 로직(WR1)을 생성하여 인증 서버로 전달한다. 이를 통해서, 해당 디바이스 및 인증 서버는 기저장된 자신의 Challenge 값 및 WBC 로직을 계속적으로 갱신하면서 인증 기능을 수행하게 된다. [그림 3]은 이와 같은 IoT 디바이스 인증기법에 대한 순차적인 세부 수행 흐름도를 나타낸다.

제시된 키 은닉 기법을 활용한 IoT 디바이스 인증기법은 기존의 인증기법과 달리, 디바이스 인증을 위한 다수의 CRP 정보 관리가 불필요함으로써 인증 서버의 자원 및 수행 부하를 최소화할 수 있다. 또한, 인증 서버는 물론 통신로 상으로의 CRP 정보 노출이 필요하지 않기 때문에, 인증키 노출로 인한 보안 위협을 근본적으로 제거할 수 있다. 즉, 이와 같은 인증기법은 하나의 CRP 정보를 바탕으로 인증에 필요한 정보들을 계속적으로 갱신함으로써, 인증 서버의 부하를 최소화함은 물론, 보다 안전하고 신뢰성 있는 인증키 관리가 가능하다는 장점이 있다.

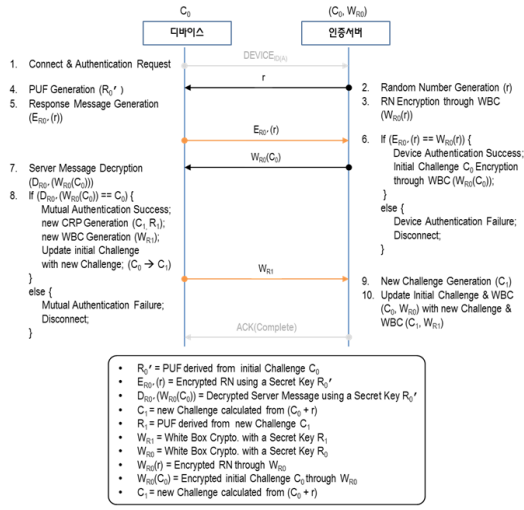
더 나아가, 상기의 IoT 디바이스 인증기법은 디바이스 자체의 인증뿐만 아니라, 디바이스와 인증 서버 간 상호인증에도 확장 적용될 수 있다. 이를 수행하기 위한 인증 대상 디바이스 및 인증 서버의 초기 설정은 인증 서버에 해당 디바이스에 등록되는 초기 Challenge 값을 추가로 할당해 줌으로써 가능하다. 즉, 인증 서버에서 생성된 임의의 난수 값은 기존 방식대로 디바이스 인증에 활용되며, 새로 인증 서버에 할당된 Challenge 값은 디바이스 입장에서 인증 서버를 인증하기 위해서 활용된다. [그림 4]는 이와 같은 디바이스와 인증 서버 간



〔그림 2〕 키 은닉 기술을 활용한 디바이스 인증 개념도



〔그림 3〕 디바이스 인증 세부 수행 흐름도



〔그림 4〕 디바이스 및 인증 서버 간 상호인증 세부 수행 흐름도

상호인증 기법에 대한 세부 수행 흐름도를 나타낸다.

상기와 같은 WBC 기술을 활용한 PUF 기반의 IoT 디바이스 인증기법은 대표적인 하드웨어 기반의 키 은닉 기술 및 소프트웨어 기반의 키 은닉 기술을 적절하게 접목한 방식으로써, 키 노출로 인한 보안 위협을 최소화할 수 있다. 무엇보다도, 이와 같은 방식은 직접적인 CRP 정보 노출에 의한 보안 취약점을 보완할 수 있으며, 기존의 인증기법과 달리 다수의 CRP 정보를 관리할 필요가 없으므로 인증 서버의 수행 부하를 최소화할 수 있다. 또한, 인증 서버 자체 및 통신로 상으로의 CRP 정보 노출이 근본적으로 차단되기 때문에 효과적이고 안전한 인증키 관리가 가능해진다. 더욱이, 인증 요구 시마다 PUF의 Challenge 값 및 이를 활용한 WBC 로직을 계속적으로 갱신함으로써, 혹시나 발생할 수 있는 스니핑이나 재사용 공격 등의 보안 위협을 직접적으로 방지할 수 있다. 이처럼, IoT 디바이스의 인증을 위해서 키 은닉 기술을 적절히 활용한다면, 키 노출 위협을 최소화하면서 보다 안전하고 신뢰성 있는 디바이스 인증이 가능하다.

Ⅳ. 결 론

본 논문에서는 사물인터넷 환경에서 IoT 디바이스의 키 누출 위협에 대응하기 위한 다양한 형태의 키 은닉 기술들 및 이의 연구 동향에 대해서 살펴보았다. 또한, 대표적인 하드웨어 기반의 키 은닉 기술인 PUF에 소프트웨어 기반의 키 은닉 기술인 WBC를 접목함으로써, 보다 안전하고 신뢰성 있는 IoT 디바이스 인증기법을 제시하고자 하였다. 물론, 각각의 키 은닉 기술들에 대한 한계점 및 기술적 이슈가 존재하고, 실제 적용에도 풀어야 할 숙제들이 많이 있을 것으로 판단되나, 이와 같은 다양한 시도들은 IoT 디바이스의 보안성 향상에 아주 많은 역할을 할 것으로 예상된다.

참 고 문 헌

[1] 최두호, “IoT 보안을 위한 디바이스 DNA 개념,” *정보보호학회지*, 28(5), 2018

[2] S. Lee et al., “RC PUF: A low-cost and easy-to-design PUF for Resource-Constrained IoT devices”, *WISA 2019*, pp. 326-337, Aug. 2019.

[3] S. Lee et al., “Implementing a phase detection ring oscillator PUF on FPGA,” *ICTC 2018*, pp. 845-847, Oct. 2018.

[4] M. Oh et al., “Secure key extraction for IoT devices integrating IEEE 802.15.4g/k transceiver,” *ICTC 2018*, pp. 833-835, Oct. 2018.

[5] 백종학, “PUF 기술을 활용한 보안칩 기술 개발과 그 응용 분야,” *전자공학회지,* 2016

[6] B. Gassend, D. Clarke, M. v. Dijk and S. Devadas, "Silicon Physical Random Functions," *ACM Conference on Computer and Communications Security*, pp. 148 - 160, 2002

[7] J. Lee, D. Lim, B. Gassend, G. Suh, M. v. Dijk and S. Devadas, "A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications," *Proceedings of the IEEE VLSI Circuits Symposium*, pp. 176 - 179, 2004

[8] J. Guajardo, S. S. Kumar, G.-J. Schrijen and P. Tuyls, "FPGA Intrinsic PUFs and Their Use for IP Protection," *in Cryptographic Hardware and Embedded Systems,* 2007

[9] K. Klaus, A.-R. Sadeghi, D. Schellekens, B. Škorić and P. Tulys, "Reconfigurable Physical

Unclonable Functions – Enabling Technology for Tamper-Resistant Storage," *In IEEE International Symposium on Hardware-Oriented Security and Trust*, pp. 53-54, 2009

[10] U. Rührmair, C. Jaeger and M.Algasinger, "An Attack on PUF-Based Session Key Exchange and a Hardware-Based Countermeasure: Erasable PUFs," *in Financial Cryptography and Data Security*, 2012

[11] http://www.hint-project.eu/

[12] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas and J. Schmidhuber, "Modeling Attacks on Physical Unclonable Functions," *in ACM*, 2010.

[13] D. Karakoyunlu and B. Sunar, "Differential Template Attacks on PUF Enabled Cryptographic Devices," *Information Forensics and Security (WIFS)*, pp. 1-6, 2010.

[14] C. Helfmeier, C. Boit, D. Nedospasov and J. Seifert, "Cloning Physically Unclonable Functions," i*n Hardware-Oriented Security and Trust (HOST)*, 2013.

[15] S. Chow et al., "White-Box Cryptography and an AES Implementation". *Selected Areas in Cryptography,* 2002

[16] S. Chow et al., "A White-Box DES implementation for DRM applications", DRM, 2002

[17] O. Billet et al., "Cryptanalysis of a White Box AES Implementation", *Selected Areas in Cryptography*, pp. 227-240, 2004

[18] W. Miciels et al., "Cryptanalysis of a Generic Class of White-Box Implementations", *Selected Areas in Cryptography*, pp. 414-428, 2008

[19] M. Karroumi, "Protecting White-Box AES With Dual Ciphers", *Information Security and Cryptology,* pp. 278-291, 2010

[20] A. Biryukov et al., "Cryptographic Schemes Based on the ASASA Structure: Black-Box, White-Box, and Public-Key", *Advances in Cryptology*, pp. 63-84, 2014

[21] I. Dinur et al., "Decomposing the ASASA Block Cipher Construction", *IACR Cryptology ePrint Archive*, 2015

[22] B. Minaud et al., "Key-Recovery Attacks on ASASA", *Advances in Cryptology*, pp. 3-27, 2015

[23] A. Bogdanov and T. Isobe, "White-box Cryptography Revisited: Space-Hard Ciphers", *In CCS 2016, Proceedings of Conference on Computer and Communications*, pp. 1058-1069, 2015

〈저자소개〉

김 병 구 (Byoungkoo Kim)

1999년 2월 : 성균관대학교 정보공학과 졸업
2001년 8월 : 성균관대학교 컴퓨터공학과 석사
2001년 2월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원
<관심분야> 네트워크 보안, IoT 보안, 키은닉, 단방향 데이터 송수신 등

윤 승 용 (Seungyong Yoon)

1999년 2월 : 충남대학교 컴퓨터공학과 졸업
2001년 2월 : 충남대학교 컴퓨터공학과 석사
2001년 2월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원
<관심분야> 네트워크 보안, 모바일 보안, 임베디드 시스템 보안, IoT 보안 등

강 유 성 (Yousung Kang)

종신회원

1997년 2월 : 전남대학교 전자공학과 졸업

1999년 8월 : 전남대학교 전자공학과 석사

2015년 8월 : KAIST 전기및전자공학부 박사

1999년 11월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원/기술총괄

2011년 1월~2012년 4월 : 영국 북아일랜드 QUB 방문연구원

<관심분야> 암호엔지니어링, 키은닉, IoT 보안, 드론 보안, 부채널 분석 등

최 두 호 (Dooho Choi)

종신회원

1994년 2월 : 성균관대학교 수학과 졸업

1996년 2월 : KAIST 수학과 석사

2002년 2월 : KAIST 수학과 박사

2002년 1월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원/실장

<관심분야> 암호엔지니어링, 부채널 분석, IoT 보안 등