정 보 보 호 학 회 지
제28권 제5호, 2018. 10

IoT 보안을 위한 디바이스 DNA 개념

최 두 호*, 강 유 성*, 오 미 경*, 이 상 재*, 김 태 성*

요 약

사물인터넷 기술은 기본적으로 다양한 대규모의 IoT 디바이스가 인터넷에 연결되어 디바이스로부터 수집되는 데이터을 통해 스마트한 서비슬 제공하는 기술이다. 그러나, 이런한 환경은 역으로 다양한 사양의 다비이스가 네트워크에 연결되기 때문에 가장 취약한 지점으로 통해 IoT 네트워크를 공격할 수 있게 된다. 따라서, 저사양 IoT 디바이스일지라도 전제 연결 네트워크의 보안 수준에 걸맞는 보안강도를 보장해야 하는 다소 역설적인 상황에 봉착하게 된다. 이러한 상황을 해결하기 위해 저사양 IoT 디바이스의 보안을 강화할 수 있는 기술이 시급하다고 할 수 있다. 본 논문에서는 이를 위해 PUF 개념을 일반화하여 디바이스 DNA라는 새로운 개념을 정의하고 기본적인 디바이스 DNA의 성질을 바이오인식 기술에서 차용하여 설명하고자 한다.

Ⅰ. 서 론

사물인터넷 기술는 기본적으로 다양한 대규모의 IoT(Internet of Things) 디바이스가 인터넷에 연결되어 이러한 IoT 디바이스로부터 수집되고 분석된 데이터들을 수집·연결·분석하여 스마트한 서비스를 제공하는 기술이다. 그러나, 이러한 환경은 역으로 저사양에서 고사양까지 다양한 디바이스가 네트워크에 연결되기 때문에 공격자의 입장에서는 가장 취약한 디바이스를 통해 네트워크에 침투하거나 공격할 수 있는 공격 접점 또한 폭발적으로 늘어나는 것으로 볼 수 있다. 따라서, 저사양의 IoT 디바이스일지라도 전체 연결 네트워크의 보안 수준에 걸맞는 보안강도를 보장해야 하는 다소 역설적인 상황에 봉착하게 된다.

이러한 상황을 해결하기 위해 저사양 IoT 디바이스의 보안성을 높이기 위한 방안들이 고민되고 있다. 그중 PUF(Physically Unclonable Function) 기술은 저사양 IoT 디바이스 보안을 위해 적용 가능한 기술로 주목을 받고 있다[1,2,3,4,5,6]. 그러나, 대부분의 PUF 기술은 PUF 기능을 하는 전용칩을 디바이스에 장착해야 하기 때문에 그 한계를 가진다고 할 수 있다. 그래서, 본 논문에서는 IoT 서비스에서 사용하는 디바이스 자체에서부터 PUF와 유사하게 신뢰원천(Root of Trust) 구성의 근간을 제공할 수 있는 “디바이스 DNA“라는 새로운 개념을 제시하고자 한다. 사람을 인식하고 인증하기 위해 다양한 개인의 신체적 특징을 가지고 있는 바이오정보를 이용하는 것처럼 디바이스에서도 개별 디바이스마다 하드웨어적 특징을 반영하는 어떤 정보를 추출할 수 있고, 그 정보가 바이오인식에서 사용하는 바이오정보나 PUF값처럼 불변성(Reliability)과 유일성(Uniqueness)을 가진다면 이를 디바이스 DNA라 부를 수 있을 것이다. 본 논문에서는 인간에 대한 바이오인식 기술의 정의를 차용하여 디바이스에 대한 디바이스 DNA 개념을 정의하고(Ⅱ장), 제 Ⅲ장에서는 디바이스 DNA 개념의 근간이 되는 PUF 기술에 대해 살펴보고, 디바이스 DNA 기술로 사용 가능한 PUF 기술을 구분해 본다. 제 Ⅳ장에서는 바이오인식 기술에서 사용하는 바이오정보 선택의 7가지 요소를 디바이스 DNA 기술 몇가지 예에 적용하여 표현해 봄으로서 디바이스 DNA 기술 개념을 좀 더 명확히 하고자 한다. 마지막으로 제 Ⅴ장에서 디바이스 DNA의 저사양 IoT 디바이스에서이 실현 및 적용 가능성에 대해 논의하고 본 논문의 결론을 맺고자 한다.

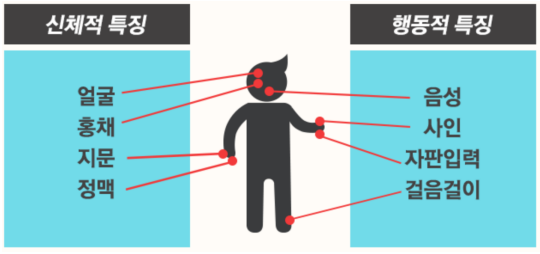
이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2018-0-00230, (IoT 총괄+1세부) IoT 디바이스 자율 신뢰보장 기술 및 글로벌 표준기반IoT 통합보안 오픈 플랫폼 기술개발 [TrusThingz 프로젝트])
* 한국전자통신연구원 지능보안연구그룹 (dhchoi, youskang, ohmik, leestrike, taesung@etri.re.kr)

Ⅱ. 디바이스 DNA

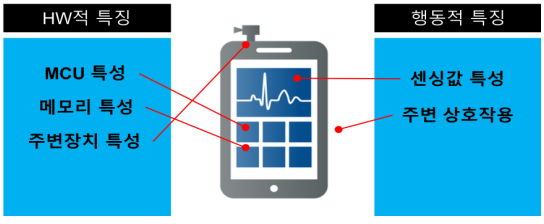
바이오인식 기술은, ”개개인의 신체적·행동적 특징을 자동화된 장치로 추출·저장하여 정확하고 편리하게 개인의 신원을 확인하는 기술“로 정의된다. 이와 유사하게 디바이스 DNA 기술은 아래와 같이 바이오인식 기술 정의에서 인간에 대한 부분을 기계, 즉, 디바이스로 대체한 개념으로 정의할 수 있다.

⊙ 디바이스 DNA: 디바이스의 하드웨어적·행동적 특징을 자동화된 장치로 추출·저장하여 정확하고 편리하게 디바이스 신원을 확인하는 기술

[그림 2]에서 예시되어 있듯이, 디바이스 하드웨어적 특징을 통해 디바이스 DNA를 추출할 수 있는 부분은 기본적으로 MCU나 CPU 자체의 특성이나, SRAM이나 DRAM 등 메모리장치의 특성(예를 들어, 메모리기반 PUF) 및 디바이스에 부착되어 있는 장치들의 특성(예를 들어, 전용 PUF칩 장착된 경우)을 통해 디바이스 DNA가 추출될 수도 있을 것이다. 그리고, 디바이스의 각종 센싱장치들에 의해 센싱되는 값들에서 어떤 특성을 찾을 수 있다면, 디바이스의 행동적 특징에 의한 디바이스 DNA의 예가 될 수 있을 것이다. 우리는 다음 장에서 디바이스 DNA의 전형적인 예시가 될 수 있는 PUF 기술에 대해 살펴보고자 한다.



〔그림 1〕 바이오인식 기술(출처: SK브로드밴드 블로그, http://http://blog.skbroadband.com/867



〔그림 2〕 디바이스 DNA

Ⅲ. PUF 기술

물리적 복제 방지 기술인 PUF는 반도체 칩의 제조공정 특성에 따라 자연스럽게 나타나는 각 반도체 칩의 물리적인 특성 차이에 기반하여 디바이스의 유일성을 확인할 수 있다는 아이디어에서 출발한 것으로 알려져 있다[7]. 초기 PUF 구현물은 반도체 칩 구현 시 각 소자의 특성에 기반한 아이디어를 FPGA 또는 ASIC으로 구현하여 성능을 확인하는 것이 일반적이었다. 이러한 PUF들은 각 구현 방법 및 대상에 따라 Arbiter-PUF [8], RO (Ring Oscillator)-PUF [9], LoopPUF [10], VIA PUF [11] 등으로 불린다. 이러한 PUF 기술은 전용 PUF 칩을 제작하여 디바이스에 부착하여 사용하는 방식을 취한다. II 장의 정의에 따르면 이러한 디바이스에 부착된 전용 PUF칩은 하드웨어적 특징 중 주변장치 특성으로부터의 디바이스 DNA 기술이라고 볼 수 있다.

이러한 반도체 칩의 물리적 특성을 이용하는 방법 외에 최근에는 상용 디바이스로부터 직접 PUF 출력을 유도하는 기술이 등장하였다. 대표적인 기법은 메모리 기반 PUF 출력 생성 기법으로 SRAM을 사용하는 기법 [12]과 DRAM을 사용하는 기법 [13,14] 등이 있다. 이렇게 디바이스 자체의 메모리로부터 PUF를 구현하는 기술은 II장에서 정의한 디바이스 DNA 중 메모리 특성에 따른 디바이스 DNA 기술이라 할 수 있을 것이다.

Ⅳ. 디바이스 DNA 기술 선택 고려 요소

통상적으로 바이오인식 정보의 선택은 다음과 같은 7가지 요소를 참고하여 선택할 수 있다[15].

- 보편성: 모든 사람들이 인증에 사용되는 바이오정보를 지니고 있어야 함
- 유일성: 바이오정보가 사람들마다 각각 달라야 함
- 영구성: 시간이 지남에 따라 변하는 정도. 높은 영구성을 가지는 바이오정보는 시간이 지나도 거의 변하지 않음
- 측정성: 바이오정보가 얼마나 간단히 획득되고 측정되는지와 관련된 요소
- 성능성: 사용되는 기술의 정확도, 속도, 견고함과 관련된 요소
- 수용성: 개인들이 자신들의 바이오정보 획득과 수집

을 허용하도록 얼마나 거부감 없이 수용하는와 관련된 요소

- 우회성: 바이오정보가 인공물 따위의 것으로 얼마나 모방 및 복제될 수 있는지와 관련된 요소

상기 바이오인식 정보 선택을 위한 7가지 고려 요소 중, 개인들의 거부감 여부와 관련된 요소인 수용성을 제외한 6가지 요소를 다음과 같이 표현함으로서 디바이스 DNA 기술 선택시 고려 요소를 정의할 수 있다,

- 보편성: 특정 서비스에서 사용하고자 하는 모든 디바이스 디바이스DNA 정보를 지니고 있어야 함
- 유일성: 디바이스DNA 정보가 디바이스마다 각각 달라야 함
- 영구성: 시간이 지남에 따라 변하는 정도. 높은 여구성을 가지는 디바이스DNA 정보는 시간이 지나도 거의 변하지 않음
- 측정성: 디바이스DNA 정보가 얼마나 간단히 획득되고 측정되는지와 관련된 요소
- 성능성: 사용되는 기술의 정확도, 속도, 견고함과 관련된 요소
- 우회성: 디바이스DNA 정보의 복제 가능성 및 어려움 정도와 관련된 요소

DRAM-PUF, SRAM-PUF, Serial No. 에 대해 [표 1]과 같은 기술별 특성을 정리해 보면 [표 2]와 같이 정리될 수 있을 것이다.

[표 2]에서 보면 디바이스 Serial No.가 우회성을 제외한 나머지 요소에 대해서는 모두 상위의 값으로 고려될 수 있다. 그러나, Serial No.와 같은 값은 그 쉬운 복제성, 즉, 현저히 낮은 우회성으로 인해, 디바이스 DNA 기술로 사용이 가능하지 않다고 볼 수 있다. 따라서, 바이오인식 기술과는 달리, 디바이스 DNA 기술에서는

〔표 1〕 바이오인식 기술별 특성

	보편성	유일성	영구성	측정성	성능성	수용성	우회성
얼굴	상	하	중	상	하	상	하
지문	중	상	상	중	상	중	상
홍채	상	상	상	중	상	하	상
걸음걸이	중	하	하	상	하	상	중

〔표 2〕 디바이스DNA 기술별 특성

	보편성	유일성	영구성	측정성	성능성	우회성
DRAM-PUF	상	상	중	중	상	상
SRAM-PUF	상	상	상	중	상	상
Serial No.	상	상	상	상	상	하

다른 고려요소보다 우선적으로 우회성을 고려해야 하며, 우회 불가능성인 높은, 즉, 복제불가능성이 높은 디바이스 DNA 기술에 대해 나머지 5가지의 요소를 고려해야 한다.

Ⅴ. 결 론

본 논문에서는 인간의 다양한 바이오정보를 이용하여 개인을 식별·인증하는 것처럼 디바이스 자체의 유일한 특성을 이용하여 디바이스 식별할 수 있는 신개념을 ”디바이스 DNA“라는 용어로 정의하고 이러한 디바이스 DNA 개념의 근간이 되는 PUF 기술에 대해 간단히 살펴보았으며, 기존의 바이오인식 기술의 특성을 구분짓는 요소들을 디바이스 DNA 기술에도 차용하여 디바이스 DNA 기술에 대한 기본적인 특성을 살펴볼 수 있음을 살펴보았다. 특히, 디바이스 DNA에서는 우회성(복제 불가능성)이 다른 요소보다 우선적으로 고려해야 하는 요소이어야 함을 살펴보았다. 향후, 이러한 디바이스 DNA 개념이 IoT 서비스에서 저사양 IoT 디바이스의 보안을 높이는 기술로서 많은 역할을 할 수 있을 것으로 예상된다.

참 고 문 헌

[1] J. R. Wallrabenstein, “Practical and Secure IoT Device Authentication Using Physical Unclonable Funtions”, In IEEE 4th International Conference on Future Internet of Things and Cloud, 2016

[2] C. Javli et.al. “Demo abstract; Location fingerprint evidence and authorisation using WiFi channel characteristics”, In IEEE PerCom Workshops, 2016

[3] J. Huang and T. Jiang, “Secret key generation exploiting Ultra-wideband indoor wireless channel characteristics”, In Security and Communication N

etworks, vol.8, no.13, pp 2329-2337, Sept. 2015
[4] W. Xiong et.al. “Run-time Accessible DRAM PUFs in Commodity Devices”, In CHES 2016, LNCS 9813, pp 432-453, 2016
[5] Y. Cao et.al. “CMOS Image Sensor Based Physical Unclonable Function for Coherent Sensor-Level Authentication”, In IEEE Transactions on Cricuits and Systems I, vol.62, no.11, pp. 262902640, 2015
[6] C, Huth et.al. “Securing Systems With Indispensable Entropy: LWE-Based Lossless Computational Fuzzy Extractor for the Internet of Things”, In IEEE Access, vo.5, pp. 11909-11926, Jun. 2017
[7] G. Simmons, “A system for verifying user identity and authorization at the point of sale or access”, Cryptologia, vol. 8, no. 1, pp. 1–21, 1984.
[8] D. Lim, J. Lee, B. Gassend, G. Suh, M. van Dijk, and S. Devadas, “Extracting secret keys from integrated circuits”, IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 13, no. 10, pp. 1200–1205, 2005.
[9] A Maiti, J. Casarona, L. McHale, and P. Schaumont, “A large scale characterization of RO-PUF”, In HOST 2010, Proceedings of IEEE International Symposium on Hardware-Oriented Security and Trust, pp. 94-99, June 2010.
[10] Z. Cherif, J. Danger, S. Guilley, and L. Bossuet, “An Easy-to-Design PUF based on a single oscillator: the Loop PUF”, In DSD 2012, Proceedings of Euromicro Conference on Digital System Design, September 2012.
[11] T.W. Kim, B.D. Choi, and D.K. Kim, “Zero bit error rate ID generation circuit using via formation probability in 0.18 μm CMOS process”, In Electronics Letters, vol. 50, no. 12, pp. 876-877, 2014.
[12] D. Holcomb, W. Burleson, and K. Fu, “Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers”, IEEE Trans. Computers, vol. 58, no. 9, pp. 1198-1210, September 2009.
[13] W. Xiong, A. Schaller, N. Anagnostopoulos, M. Saleem, S. Gabmeyer. S. Katzenbeisser, and J. Szefer, “Run-time Accessible DRAM PUFs in Commodity Devices”, In CHES 2016, Proceedings of Conference on Cryptographic Hardware and Embedded Systems, pp. 432-453, Santa Barbara, August 2016.
[14] I, Kumari, M. Oh, and D. Choi, “Rapid Run-time DRAM PUF based on Bit-Flip Position for Secure IoT Devices”, To appear Proceeding of IEEE Sensors 2018
[15] A.K. Jain, R. Bolle, and S. Pankanti, “Biometrics: Personal Identification in Networked Society”, Kluwer Academic Publications, ISBN 978-0-7923-8345-1, 1999

〈저자소개〉

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/PL
관심분야 : 암호엔지니어링, 부채널 분석, IoT보안 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/PL
2011년 1월~2012년 4월 : 영국 북아일랜드 QUB 방문연구원
관심분야 : 암호엔지니어링, 키은닉, IoT보안, 드론보안, 부채널 분석 등

오 미 경 (Mi-Kyung Oh)

2000년 2월 : 중앙대학교 전기전자제어공학부 졸업
2002년 2월 : KAIST 전기및전자공학과 석사
2006년 2월 : KAIST 전기및전자공학과 박사
2006년 3월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원
관심분야 : IoT보안, 키은닉, 물리계층 보안, 통신공학 등

이 상 재 (Sangjae Lee)

1999년 2월 : 전북대학교 전자공학과 졸업
2001년 2월 : 전북대학교 전자공학과 석사
2013년 8월 : 충북대학교 정보통신공학부 박사
2000년 12월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원
관심분야 : 전자공학, 무선통신 칩, PUF 설계, IoT보안 등

김 태 성 (Taesung Kim)

종신회원

1999년 2월 : 동국대학교 컴퓨터공학과 졸업
2001년 2월 : 동국대학교 컴퓨터공학과 석사
2017년 2월 : KAIST 전산학부 박사
2001년 3월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원
관심분야 : 부채널 분석, 머신러닝, IoT 보안 등