정 보 보 호 학 회 지
제25권 제3호, 2015. 6

HCI 기반 스마트그리드 제어시스템의 인증 기술 동향

이 석 철*, 권 성 문*, 김 성 진*, 손 태 식**

요 약

스마트그리드(Smartgrid) 시대의 도래 및 제어시스템으로의 IIoT(Industrial Internet of Things) 기술 도입으로 외부 인터넷망과의 접점이 증가하면서 스마트그리드 제어시스템을 대상으로 하는 사이버위협이 증가하고 있는 추세이며, 그에 대한 피해 사례가 지속적으로 보고되고 있다. 또한 스마트그리드 제어시스템에 HCI(Human-Computer Interaction) 기술이 악의적인 내부 공격자는 전문적인 지식이 없더라도 비교적 쉽게 제어시스템을 조작 및 오작동 시킬 수 있게 되었다. 본 논문에서는 HCI가 적용된 스마트그리드 제어시스템에서의 내부자 공격에 대응하기 위해 사용자 및 구성 장비에 대한 인증 기능을 강화하여 제어시스템 사용자와 구성 장비의 신뢰성을 보장할 수 있는 방법을 제시한다.

Ⅰ. 서 론

발전부터 송전, 배전, 그리고 저장 및 사용까지 전력 자원의 효율적인 관리를 위한 스마트그리드는 실증연구가 마무리되고 있고, 현재 실용화를 목전에 두고 있다. 스마트그리드 환경에서는 제어시스템의 첨단화 및 효율화를 위해 스마트그리드 구성 장비에 IIoT 기술 도입의 등 ICT(Information Communication Technology) 기술과의 융합으로 외부 인터넷과 접점이 증가하고 있다. 또한 최근에는 [1],[2],[3]에서 언급된 것과 같이 스마트그리드 제어시스템 및 구성 장비를 사용자가 보다 편리하게 사용할 수 있도록 직관적인 HCI를 구축하고 있는 추세이다. 이에 따라, 스마트그리드 제어시스템을 대상으로 하는 사이버공격 및 내부자공격이 급격히 세계적으로 증가하고 있는 추세이며, 최근 국내에서도 제어시스템 대상의 공격 사례가 발생했다.

스마트그리드 환경에서 발생하는 사이버보안 침해사고는 블랙아웃 등 전력공급에서 발생하는 경제적 손실뿐만 아니라, 사이버공격이 공공 인프라로 전이되어 기능이 마비되는 등 사회적 혼란을 야기할 수 있기 때문에 스마트그리드의 제어시스템을 위한 보안 기술의 중요성이 부각되고 있다.

IIoT 기술이 적용된 스마트그리드 환경에서 발생하는 일반적인 사이버공격은 스마트그리드의 구성 장비로 위장한 악성 AP(Access Point)를 이용하기 때문에, 스마트그리드 환경에 적용되는 보안 기술 중 구성 장비에 대한 인증 기술이 매우 중요하다. 또한 내부자 공격을 방지 및 탐지할 수 있도록 HCI가 적용된 제어시스템의 사용자 인증 기술이 요구된다. 따라서 본 논문에서는 HCI가 적용된 스마트그리드 제어시스템에서의 인증 기능을 강화하기 위한 방향을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 스마트그리드 환경과 HCI에 적용되고 있는 보안 기술에 대해 살펴보고, 3장에서는 각 보안 기술의 연구 동향을 소개한다. 4장에서는 스마트그리드 보안 기술과 HCI 보안 기술의 연계를 통해 HCI가 적용된 스마트그리드 제어시스템에서의 인증 기능을 강화하기 위한 방향을 제시한다. 마지막으로 5장에서는 본 논문에 대한 결론을 서술한다.

Ⅱ. 인증 기술

본 장에서는 스마트그리드의 제어시스템 및 HCI를 위한 보안 기술에 대해 알아본다. 스마트그리드 환경에서는 제어시스템을 구성하고 있는 장비를 인증 및 식별하기 위해 사용되는 기술은 공개키 및 개인키 기반의 PKI(Public Key Infrastructure)를 이용한 전자서명, 각 장비의 물리적 고유성을 이용한 PUF(Physically

* 아주대학교 컴퓨터공학과 (go467913@ajou.ac.kr, minter@ajou.ac.kr, ksjskyblue@ajou.ac.kr)
** 아주대학교 정보컴퓨터공학과 (tsshon@ajou.ac.kr)

Unclonable Function) 등이 있다. HCI을 보다 안전하게 사용하기 위해 사용되는 기술은 터치 인터페이스를 이용한 ID/ Password 기법, 마이크를 이용한 음성인식, 스캔장치를 이용한 지문인식 등이 있다.

2.1. 전자서명

PKI 기반의 전자서명은 ICT 환경에서 사용되고 있는 대표적인 인증 기술 중 하나이다. PKI 기반 장비들은 각각 공개키-개인키 쌍을 가지며, 공개키-개인키 쌍에 대한 정보는 CA(Certificate Authority)에서 저장 및 관리한다. 인증을 받고자하는 장비는 자신의 개인키로 전자서명을 생성하고, 그 반대편에서는 인증 대상의 공개키를 이용해 인증을 수행한다.

2.2. PUF

PUF 기술은 같은 역할을 수행하는 동일한 장비라도 반도체 또는 회로를 생산하는 공정단계에서 발생하는 공정편차를 이용하여 물리적으로 복제 불가능한 키를 생성한다. 각 장비의 PUF 키는 중앙 서버에 저장 및 관리되며, 각 장비의 키는 중앙 서버와 장비간의 인증 및 비밀통신에 사용된다.

2.3. IP/Password

ICT 환경이 구축된 이래 현재까지 가장 보편적으로 사용되고 있는 사용자인증 방법은 ID/Password 기반의 인증 기술이다. 시스템 구현이 매우 쉬운 장점이 있으나 사전 공격(Dictionary attack)이나 무차별 대입공격(Brute force) 등 기초적인 공격에 취약할 정도로 보안성이 낮아, 최근에는 OTP(One Time Password) 등과 같은 추가 인증방안을 함께 사용하는 이중인증(2-factor authentication)을 사용한다.

2.4. 목소리 인식

말할 때의 속도나 억양, 그리고 목소리의 주파수가 개인별로 다른 점을 활용하여 사용자를 인증하는 기술이다. 별도의 조작 없이 말을 하는 것으로 인증이 된다는 편리성이 있으나, 주변의 잡음이나 감기 등으로 사용자의 목소리가 인증되지 않는 경우가 발생하기 때문에 보조적으로 사용할 인증수단이 추가로 필요하다.

2.5. 지문 인식

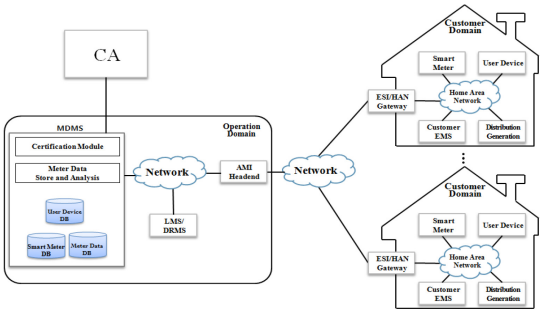
사용자의 지문을 인식하여 인증을 수행하는 지문인식을 통한 인증기술은 암호기반 인증기술에 비해 편리하다는 장점을 갖고 있어 최근 암호를 대체하는 인증수단으로 자리를 잡고 있다. 편리성으로 인해 지문인식을 통한 인증기술은 스마트폰 등 사용자와 접촉이 빈번한 장비에 적용이 되고 있다. 그러나 종종 사용자 인증에 실패하는 인식률과 관련된 이슈가 존재한다.

Ⅲ. 인증 기술 연구동향

본 장에서는 앞서 살펴본 사용자 인증 기술을 스마트그리드 제어시스템 및 HCI에 적용하기 위해 각 기술별로 수행되고 있는 연구동향을 알아본다.

3.1. 전자서명

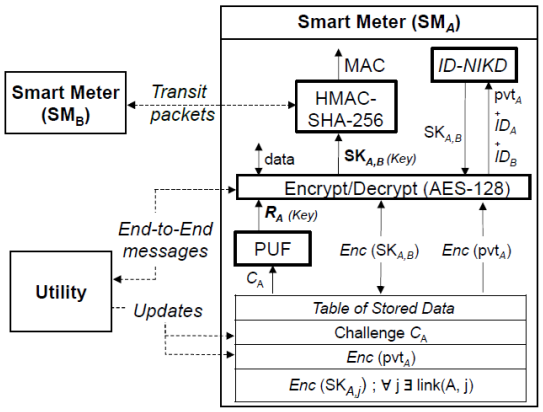
일반적인 ICT 환경에서 사용되고 있는 PKI 기반 전자서명 기술은 스마트그리드 환경에서 사용되기에 높은 연산처리능력과 연산시간이 요구된다. 이러한 요구사항을 충족시키고 스마트그리드 환경에 전자서명 기술을 적용할 수 있는지 여부를 시험하기 위해 T. Ward은 스마트그리드 환경에 PKI 기반 전자서명 기술을 적용 시켜 볼 수 있는 시뮬레이터를 개발하였다. 개발한 시뮬레이터를 통해 PKI 기반 전자서명 기술을 스마트그리드 환경에 적용하기 이전에 발생할 수 있는 병목현상, 가용성 침해 등의 문제점들을 사전에 파악 가능하며 이를 통해 PKI 기반 전자서명 기술을 스마트그리드 환경에 도입하기 이전 스마트그리드 환경을 고려한 기술 수정의 필요성과 방향에 대해 제시하였다[4]. S. Lee, et al.은 AMI 환경에서 인증을 위해 PKI 기반 전자서명 기술을 도입하기 위한 연구를 하였으며, 인증과정에서 발생한 다수의 인증요청 메시지로 인해 CA에서 발생하는 병목현상 등 스마트그리드의 가용성을 침해하게 되는 문제를 해결하기 위해 CA의 인증을 받은 MDMS (Meter Data Management System)들을 도입하여 인증서를 발급, CA의 병목현상을 해결하였으며 또한 인증메시지 교환 횟수를 감소시킨 상호인증구조를 제시하였다[5].



〔그림 1〕 MDMS를 이용한 공개키 기반 전자서명 인증

3.2. PUF

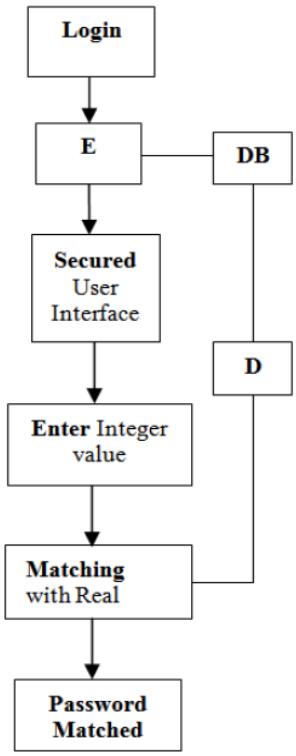
V. Seferian, et al. 은 스마트그리드를 구성하는 AMI(Advanced Metering Infrastructure)를 인증하기 위해 PUF와 공개된 ID 정보를 조합한 인증 프레임워크를 제안했다. 제안된 프레임워크는 인증된 스마트미터들만 알 수 있는 인증정보를 PUF를 이용해 암호화하여 스마트미터를 설치하기 전에 스마트미터 내부에 저장한다. 스마트미터 내부에 저장된 인증정보와 MAC address와 같이 공개된 ID 정보를 조합 및 연산하여 HMAC(Hashed Message Authentication Code)을 생성해 인증을 수행한다[6].



〔그림 2〕 PUF-based Smart Meter Authentication

3.3. IP/Password

ID/비밀번호 인증의 경우 키로그 공격과 훔쳐보기 공격에 취약하다. 키로그 공격에 대응하기 위해GUI가 들어간 가상키보드를 통해 ID/비밀번호를 입력하는 방식

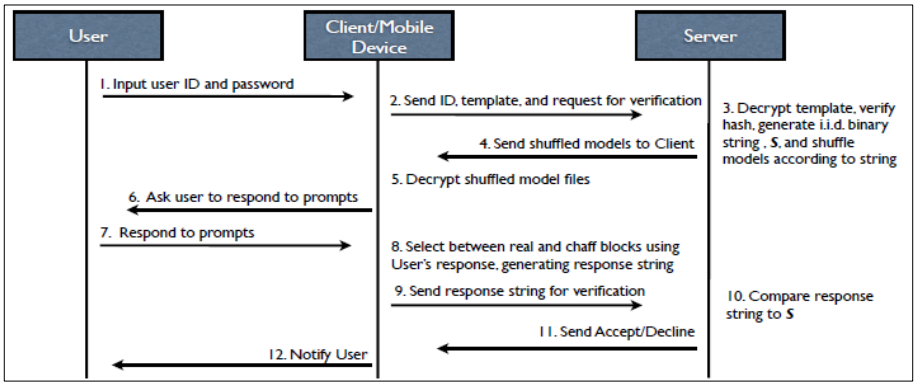


〔그림 3〕 Secured Password Authentication Module Architecture

이 사용될 수 있으나 여전히 훔쳐보기 공격에는 취약하다. 이러한 ID/비밀번호 인증의 취약성을 보완하기 위해 V. Agrawal, et al.은 키로그 공격과 훔쳐보기 공격에 모두 대응할 수 있는 로그인 보안 인터페이스를 개발하였으며, 인터페이스에서 알파벳 대/소문자와 특수문자는 각 1자리수의 숫자에 대응된다. 따라서 같은 숫자에 대응되는 알파벳 및 특수문자가 여럿 있을 수 있으며, 이를 통해 비밀번호 입력하여 훔쳐보기 공격에 대응 할 수 있다. 그러나 이 방법 또한 훔쳐보기 공격을 여러 번 수행하여 비밀번호를 알아낼 수 있는 여지가 있어 추가적인 연구가 필요하다[7].

3.4. 목소리 인식

음성 인증 기술의 경우 인증에 사용된 음성을 불법 취득하여 재전송 공격에 사용할 시 취약할 수 있다. 이를 보완하기 위해 R. Johnson, et al.은 텍스트 의존/비의존 질의를 결합한 음성 인증 체계를 제시하였으며 텍스트 의존 질의를 통해 예상되는 음성 대답을 사용자에

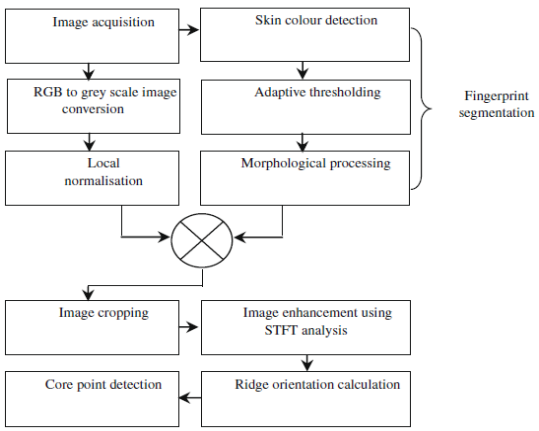


〔그림 4〕 Vaulted Voice Verification Process, Proposed by R. Johnson, et al.

게 받아 최대한 음성 정보를 취득하고, 텍스트 비의존 음성 질의를 통해 재전송 공격을 방지하여 사용자에게 과도한 인증을 요구하지 않으면서 재전송 공격에 대응하였다[8].

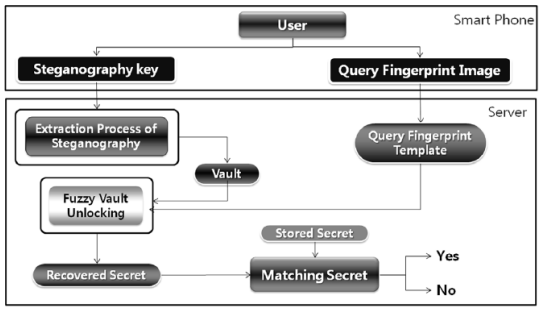
3.5. 지문 인식

모바일 환경에서 주로 지문인식 기술이 활용되고 있어 임베디드 장치들이 주로 사용되는 스마트그리드 환경에 즉시 적용하기 용이하다. 지문인식에 지문 스캐너가 아닌 일반 카메라를 이용할 경우 카메라의 성능에 크게 좌우된다는 문제점이 있다. 이러한 문제를 해결하기 위해 B.Y.Hiew, et al. 은 지문 인식률 향상을 위한 전처리 기법과 MRP-SVM을 제안하여 인식률을 향상시켰다[9]. 지문 인식은 한 번 노출 될 경우 적당한 대



〔그림 5〕 Flow chart of fingerprint preprocessing Proposed by B. Y. Hiew, et al.

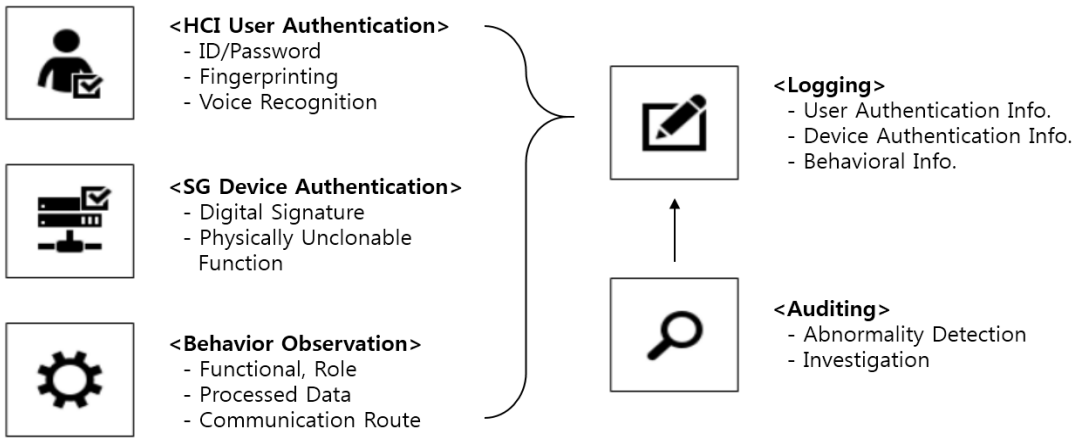
응책이 존재하지 않다는 또 다른 문제점을 가지고 있다. 이 문제점은 모든 바이오 인증 방식에 사용되는 생체정보들은 ID 및 Password 인증처럼 변경하는 것이 불가능하기 때문에 발생하는 문제점으로 생체정보를 들어나지 않도록 처리하는 것이 중요하다. 이러한 문제점에 대한 대안으로 H. Nam, et al. 은 퍼지볼트와 지문 인증 시스템을 결합하여 생체정보를 들어나지 않도록 하는 연구를 진행하였다[10]. 국외에서도 생체정보를 숨기는 기법 및 지문정보에 재사용이 불가능한 워터마크를 남기는 기법에 대한 연구들이 진행되고 있다.



〔그림 6〕 Fingerprint Authentication by using Fuzzy vault with steganography

Ⅳ. HCI 기반 제어시스템을 위한 인증방안

스마트그리드 제어시스템의 보안을 위해 적용되고 있는 IDS(Intrusion Detection System) /IPS(Intrusion Prevention System), 방화벽, UTM(Unified Threat Management) 등과 같은 보안 제품을 통해 스마트그리드 제어시스템을 대상으로 하는 대부분의 사이버공격에



〔그림 7〕 HCI가 적용된 스마트그리드 제어시스템에서의 강화된 인증 방안

대응할 수 있지만, 이러한 보안 제품으로 내부자에 의한 공격을 방지 및 검출하는 데에는 어려움이 있다.

따라서 HCI 차원에서 사용자인증을 수행하고 사용자가 사용하는 스마트그리드 제어시스템 구성 장비에 대해 다시 한 번의 인증하는 다중인증 기법을 사용해 사용자와 장비의 신뢰성을 검증할 필요성이 있다. HCI 차원에서 수행되는 사용자인증에는 ID/ Password 기반 인증, 지문 인식, 목소리 인식 등의 인증기술 중 2가지 이상을 조합한 Multi-factor Authentication을 사용하는 것을 권장한다. 스마트그리드 제어시스템 구성 장비를 인증하는 데에는 시스템 구축 환경에 따라 전자서명 또는 PUF 기반 인증을 사용할 수 있다. 또한 인증된 장비의 기능, 처리하는 정보, 통신 경로 등 행위정보를 분석하여, 정당한 권한을 보유하고 있는 사용자가 인증된 장비를 통해 정상적인 행위를 했는지 여부를 판단한다. 그리고 사용자 인증정보, 장비 인증정보, 행위정보를 로그화한 뒤, 데이터베이스에 저장하여 추후 스마트그리드 제어시스템에 대한 보안침해 사고 발생 시 참고 가능한 감사(Auditing) 자료로 활용한다.

V. 결 론

전력을 보다 효율적으로 관리하기 위해 제어시스템에 HCI 및 ICT 기술이 도입된 스마트그리드 환경에서는 조작의 편리함과 외부로부터의 접근이 용이해짐에 따라, 내·외부에 존재하는 보안위협이 증가하고 있다. 사이버공격으로 인해 스마트그리드 제어시스템이 장애 또는 오작동을 일으킬 경우, 전력공급에 차질이 생겨 경제적·사회적 피해를 야기할 수 있다. 따라서 스마트그리드 제어시스템에는 내·외부 환경에 대해 모두 높은 수준의 보안이 요구되는데, 외부로부터의 사이버공격은 IDS나 UTM 등과 같이 현재 적용되고 있는 보안 제품을 통해 대응할 수 있다. 그러나 내부자의 정보유출과 같이 내부에서 발생할 수 있는 보안 침해에 대응하기 위해서는 본 논문에서 제안하고 있는 방안과 같이 높은 수준의 인증 기술이 추가로 필요하다.

참 고 문 헌

[1] D. Kang, S. Park, “A conceptual Approach to Data Visualization for User Interface Design of Smart Grid Operation Tools,” International Journal of Energy, Information and Communications, Vol.1, Issue 1, 64-76, November 2010.

[2] J. Pierce, E. Paulos, “Beyond Energy Monitors: Interaction, Energy, and Emerging Energy Systems,” CHI 2012, Vol.1, pp.665-674, May 2012.

[3] S. Dang, R. Kakimzhanov, M. Zhang, and A. Gholamzadeh, “Smart Grid- oriented Graphical User Interface Design and Data Processing Algorithm Proposal Based on LabVIEW,” 14th International Conference on Environ ment and Electrical Engineering, Vol.1, pp. 323-327, May 2014.

[4] T. Ward, “Grid Cryptographic Simulation: A Simulator to Evaluate the Scalability of the

X.509 Standard in the Smart Grid," Senior Honors Thesis, Dartmouth College, Hanover, NH, USA, September 2013.

[5] S. Lee, J. Bong, S. Shin, and Y. Shin, "A Security Mechanism of Smart Grid AMI Network through Smart Device Mutual Authentication," International Conference on Information Networking, Vol.1, pp. 592-595, February, 2014.

[6] V. Seferian, R. Kanj, A. Chehab, and A. Kayssi, "PUF and ID-Based Key Distribution Security Framework for Advanced Metering Infrastructures," IEEE Conference on Smart Grid Communications, Vol.1, 939-944, November 2014.

[7] V. Agrawal, R. Bharti, "Password Authentication with Secured Login Interface at Application Layer," International Journal of Computer Science and Network Security, Vol.15, No.1, pp. 132-135, January 2015.

[8] R. Johnson, T. Boult, and W. Scheirer, "Voice Authentication Using Short Phrases: Examining Accuracy, Security and Privacy Issues," IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems, Vol.1, pp1-8, September, 2013.

[9] B. Hiew, A. Teoh, and O. Yin, "A secure digital camera based fingerprint verification system," J. Vis. Commun. Image R. Vol.21, pp. 219-231, December, 2009.

[10] 남한솔, 김애영, 이상호, "퍼지볼트와 스테가노그래피를 이용한 스마트폰 지문 인증 시스템", Journal of KIISE, Vol.42, No.4, pp419-426, 2015.

〈저자소개〉

이 석 철 (Seokcheol Lee)
학생회원
2012년 2월 : 아주대학교 정보 및 컴퓨터공학부 공학사
2012 3월~현재 : 아주대학교 컴퓨터공학과 석박사통합과정
관심분야 : 스마트그리드 보안, 디지털 포렌식, 네트워크 보안

권 성 문 (Sungmoon Kwon)
학생회원
2013년 2월 : 아주대학교 정보 및 컴퓨터공학부 공학사
2013 3월~현재 : 아주대학교 컴퓨터공학과 석박사통합과정
관심분야 : 제어시스템 보안

김 성 진 (Sungjin Kim)
학생회원
2014년 2월 : 아주대학교 정보 및 컴퓨터공학부 공학사
2014 3월~현재 : 아주대학교 컴퓨터공학과 석사과정
관심분야 : 제어시스템 보안

손 태 식 (Taeshik Shon)
정회원
2000년 2월 : 아주대학교 정보 및 컴퓨터공학부 공학사
2002년 2월 : 아주대학교 전보통신 전문대학 공학석사
2005년 8월 : 고려대학교 정보보호대학원 공학박사
2004년 2월~2005년 2월 : Research Scholar, University of Minnesota
2005년 8월~2011년 2월 : 삼전전자 DMC 연구소 책임연구원
2011년 3월~현재 : 아주대학교 정보통신대학 정보컴퓨터공학과 부교수
관심분야 : 전력제어시스템 보안, 디지털 포렌식, 비정상행위탐지, ICT융합보안