

2019년 2월 셋째주

해외 ICT 표준화 동향

목 차

본문	**1. NIST, 스마트제조를 위한 보안과 추적을 제공하는 블록체인** **2. NIST, 포스트-양자암호(PQC) 26개 후보 알고리즘 공개**
단신	1. ETSI, NFV(네트워크기능가상화) 배치 탬플릿을 위한 표준 발표 2. ETSI, 'MCPTT, MCData, MCVideo' 플러그 테스트 이벤트 완료

※ 게시물 보기

TTA 홈페이지 ▷ 자료마당 ▷ TTA 간행물 ▷ 표준화 이슈 및 해외 동향

1. NIST, 스마트제조를 위한 보안과 추적을 제공하는 블록체인

NIST: Blockchain Provides Security, Traceability for Smart Manufacturing

보도날짜 19. 02. 11.
출 처 NIST
사 이 트 https://www.nist.gov/news-events/news/2019/02/nist-blockchain-provides-security-traceability-smart-manufacturing

◆ 2019년 2월, NIST(National Institute of Standards and Technology, 미국국립표준기술연구소)는 스마트 제조를 위한 보안과 추적성을 제공하는 블록체인 기술에 대한 보고서[1]를 발표하였고 스마트제조 시스템에 있어서 블록체인을 이용한 디지털스레드(Digital Thread) 프로젝트[2]를 소개함

◆ 이 보고서에 따르면 블록체인을 이용한 보안 시스템은 제조 데이터의 변조 방지 전송 기능을 제공할 뿐만 아니라 생산 과정에서 사용자에게 추적 가능한 정보를 제공하여 블록체인을 통해 디지털 제조 네트워크의 신뢰성을 높일 수 있다고 언급

- 또한, 스마트 제조 네트워크에 블록체인을 적용하는데 필요한 컴퓨터 모델링 시스템인 UML(Unified Modeling Language, 통합 모델링 언어)에 대해 자세히 설명하고 있음

◆ 디지털화된 과정을 통해 생산된 제품은 각 수명주기 단계마다 데이터를 생성하기 때문에 제품 수명주기 동안 지속적으로 생성된 데이터의 원활한 흐름이 중요해짐 따라서 이 기간 동안 블록체인을 통해 안전하게 정보를 보호하며 전달하도록 도와주는 것을 디지털스레드(Digital Thread)라고 함

- 디지털스레드(Digital Thread)는 설계에서 제조에 이르기까지 정보가 컴퓨터에서 컴퓨터로, 기계에서 기계로 전달될 때 제품의 설계 및 제조 정보를 오류 없이 작성, 교환 및 처리 할 수 있는 방법을 파악하여 제공함

- 사용자는 데이터를 주고받는 사람, 데이터를 교환하는 사람, 교환이 이루어지는 시기, 교환되는 대상 및 방법 등 각 단계에서 인증된 블록을 이용하게 됨

◆ NIST는 스마트제조를 위한 블록체인 사용을 촉진하고 홍보하기 위해 노력하고 있음

1) https://nvlpubs.nist.gov/nistpubs/ams/NIST.AMS.300-6.pdf
2) https://www.nist.gov/video/digital-thread-manufacturing

2. NIST, PQC(포스트-양자암호) 26개 후보 알고리즘 공개

NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto 'Semifinals'

보도날짜 19. 01. 30.
출 처 NIST
사 이 트 https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals

◆ 2019년 1월 30일, NIST(National Institute of Standards and Technology, 미국국립표준기술연구소)는 양자컴퓨팅 환경에서 안전한 암호알고리즘으로 정보를 보호할 수 있는 일련의 표준을 만들기 위한 프로젝트의 일환으로 26개의 후보 PQC(Post-Quantum Cryptography, 포스트-양자암호) 알고리즘[3]을 발표함

* 양자 컴퓨팅을 실행할 수 있는 양자컴퓨터를 이용할 수 있더라도 그 암호의 안전성이 본질적으로 쉽게 해독되지 않는 암호를 "포스트-양자 암호"라 함

- 2017년 11월 NIST에 제출된 82건의 알고리즘 후보를 검토하는 첫 번째 단계에서 69건이 최소 수용기준과 요구사항을 모두 충족하였고, 이중 PQC 후보 알고리즘으로 2019년 1월에 26개가 선정됨

- 포스트-양자암호 중 공개키 암호 후보로 언급되는 것은 lattice-based cryptography (격자기반암호), Code-based cryptograph(코드기반암호), Multivariate cryptography (다변수암호)등이 있음

◆ NIST PQC 표준화 과정 단계가 완료되고 나면 선정된 PQC 후보 알고리즘은 NIST에서 양자공격에 취약한 것으로 간주되는 세 개의 표준(FIPS 186-4, NIST SP 800-56A 및 NIST SP 800-56B)을 보완하거나 대체할 것이라고 언급함

- PQC 표준화는 AES나 SHA-3 표준화와 같이 하나의 표준 알고리즘이 아닌 여러 개의 알고리즘을 제정하는 방향으로 진행될 것으로 예상

◆ 26개의 후보 알고리즘을 검토하는 이번 단계에서는 광범위한 시스템 전반에서 이 알고리즘이 외부 공격에 대응하는 성능을 평가하는데 더욱 중점을 둘 예정이며, 대형 컴퓨터와 스마트폰뿐만 아니라 프로세서 기능이 제한적인 장치에서도 이 알고리즘이 어떻게 작동하는지 검토할 예정임

3) https://csrc.nist.gov/publications/detail/nistir/8240/final

기타 소식

1. ETSI, NFV(네트워크기능가상화) 배치 탬플릿을 위한 표준 발표

▷ 발 행 일 : 19. 01. 30.

▷ 원문제목 : ETSI RELEASES A STANDARD FOR NFV DEPLOYMENT TEMPLATES

▷ 원 문 : https://www.etsi.org/newsroom/press-releases/1540-2019-01-etsi-releases-a-standard-for-nfv-deployment-templates

▷ 내용요약

◦ 2019년 1월 30일, ETSI ISG NFV(ETSI Industry Specification Group Network Functions Vertualization, 네트워크기능가상화 산업규격그룹)는 ETSI GS(Group Specification) NFV-SOL 001 표준의 첫 번째 버전을 발표

◦ ETSI GS NFV-SOL 001은 YAML 명세의 TOSCA Simple Profile에 따라 NFV 기술자를 구조화하는 규칙을 규정하고 있음

1. ETSI, 'MCPTT, MCData, MCVideo' 플러그 테스트 이벤트 완료

▷ 발 행 일 : 19. 02. 11.

▷ 원문제목 : ETSI COMPLETED ITS FIRST REMOTE MISSION CRITICAL PLUGTESTS EVENT

▷ 원 문 : https://www.etsi.org/newsroom/news/1547-2019-02-etsi-completed-its-first-remote-mission-critical-plugtests-event

▷ 내용요약

◦ 2019년 2월 11일, ETSI(European Telecommunications Standards Institute, 유럽전기통신표준협회)는 2018년 12월 3일부터 2019년 1월 31일 까지 있었던 세 번째 MCX(MCPTT, MCData, MCVideo) Plugtests™를 완료하였다고 발표함

◦ 이번 테스트는 2개월 동안 1000여건의 테스트를 26개 업체와 진행하였으며 92%의 성공률을 달성함

◦ MCX 플러그 테스트(Plugtests) 다음 회의는 2019년 9월 유럽에서 개최될 예정임