해외 ICT 표준화 동향

2018년 10월

(2018.10.1.~2018.10.31.)

*** 게시물 보기**

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

TTA 한국정보통신기술협회
Telecommunications Technology Association

목차

Ⅰ. 지역 표준화 기구

1. 유럽
   1.1 ETSI, 사이버대응을 위한 보안통제 기술보고서 발표
   1.2 ETSI CYBER TC, 양자-안전 가상 사설망 기술보고서 발표

2. 미국
   2.1 ANSI, IoT 기반 스마트시티 프레임워크 발표
   2.2 TIA, 5G와 차세대 공공안전을 위한 정책 포럼 개최
   2.3 TIA, 에지 데이터 센터에 대한 새로운 보고서 발표

Ⅱ. 기타 사실 표준화 기구

1. ISA, 컨트롤시스템 부품 사이버보안 성능을 위한 표준 발표
2. SNIA, 클라우드 데이터관리 인터페이스 오픈소스 표준 발표
3. W3C, 웹 폰트모듈 Lv3 권고안 발표
4. IEEE, IEEE 802.11TM EHT SG와 RTA TIG 출범
5. IETF, 인증 토큰 보안을 위한 새로운 인터넷 표준 승인

Ⅰ. 지역 표준화 기구

1. 유럽

1.1 ETSI, 사이버대응을 위한 보안통제 기술보고서 발표

2018년 10월 3일, ETSI CYBER 기술위원회(Technical Committee)는 "효과적인 사이버 대응을 위한 효과적인 보안 통제(Critical Security Controls for Effective Cyber Defence)" 기술보고서(Technical Report, TR)를 발표하였다.

이 보고서는 네트워크 제공 업체가 최신 사이버 보안 위협에 대응하고, GDPR(General Data Protection Regulation, 개인정보보호 규정) 준수 및 클라우드 데이터 센터 강화와 같은 새로운 요구 사항을 충족할 수 있도록 CIS Controls v7 및 관련 자료를 최신 버전으로 업데이트하였다.

TR 103 305-1은 "중요한 보안 통제(The Critical Security Controls)"를 다루며 시스템 및 네트워크에 대한 가장 일반적인 공격을 완화하는 모범 사례의 심층방어 작업을 설명한다.

TR 103 305-2는 효과적인 사이버 방어를 위한 중요한 보안 조정에서 "측정 및 감사(measurement and auditing)"를 다룬다.

TR 103 305-3은 모바일 장치 및 IoT(Internet of Things, 사물인터넷)의 "서비스 부분 구현(Service Sector Implementations)"을 다룬다

TR 103 305-4는 "여러 메커니즘에 대한 유용한 정보(Facilitation Mechanisms)" 제공한다.

TR 103 305-5는 유럽 GDPR의 조항을 충족시키는데 도움이 되는 "개인 정보 보호 강화(Privacy enhancement)"에 대해 설명한다.

ETSI 기술위원회 의장인 Alex Leadbeater는 ETSI 기술보고서가 실제 공격에 대한 종합 지식과 사이버 보안 생태계 부분에서 전문가의 효과적인 대응을 반영한다고 언급하였다.

☞ https://www.etsi.org/news-events/news/1342-2018-10-news-etsi-publishes-critical-security-controls-for-effective-cyber-defence-as-technical-reports

1.2 ETSI CYBER TC, 양자-안전 가상 사설망 기술보고서 발표

2018년 10월 16일 ETSI CYBER TC(Technical Committee, 기술위원회)는 "양자-안전 가상 사설망(Quantum-Safe Virtual Private Networks)"에 관한 기술보고서(ETSI TR 103 617 V1.1.1)를 발표하였다.

ETSI TR 103 617 V1.1.1 보고서를 발표한 ETSI CYBER 기술위원회는 효율적이고 시기적절한 해결책을 제공하기 위해 3년 이상 양자-안전 암호화 기술을 연구해오고 있다.

이번에 발표한 기술 보고서는 클라이언트, 서버 및 아키텍처 고려 사항과 같은 VPN 기술에 양자 저항성(resistance)을 추가하는데 필요한 프로토콜 요구 사항에 대해 설명한다.

일반적인 VPN 요구사항 중 특히 양자 컴퓨터에 보호 기능을 추가하면서 기존의 고전적인 핸드셰이크(handshake)가 제공하는 속성을 유지할 필요성을 검토하였으며, 양자 안전 및 고전적인 키 설정 기술을 결합하여 보안에 대한 복합적인 접근 방식을 권장한다.

☞ https://www.etsi.org/news-events/news/1346-2018-10-press-etsi-tc-cyber-re

2. 미국

2.1 ANSI, IoT 기반 스마트시티 프레임워크 발표

2018년 9월 30일, ANSI(American National Standards Institute, 미국국가표준협회)와 IST(National Institute of Standards and Technology, 국립표준기술연구소)를 함한 여러 파트너*는 IoT기반 스마트시티 프레임워크(IoT-Enabled Smart City ramework or IES-City Framework)1)를 발표하였다.

* ETSI(European Telecommunications Standards Institute, 유럽전기통신표준협회), MIST(Korea's Ministry of Science and ICT, 과학기술정보통신부), TIA(Telecommunications Industry Association, 전기통신산업협회) 등

이 프레임워크는 스마트시티 배치를 위한 융합 및 조화의 방법 모색을 위해 개발되었다. IoT 기반 스마트시티 프레임워크는 기존 스마트시티 애플리케이션(응용프로그램) 및 아키텍처의 기술적 분석을 통한 고비용 애플리케이션의 통합 비용을 줄이기 위한 개방적이고 국제적인 공공 워킹그룹(Working Group, WG)의 산물이다.

부적절한 정보 및 지식이전, 표준의 다양성, 확장성 부족, 자원 부족, 우선순위에 대한 명확한 원칙의 부재, 제한된 접근 방법 등과 같은 장벽을 낮추기 위해 NIST와 파트너는 국제 공공 워킹그룹을 소집하여 합의된 언어, 분류(taxonomy), 공통 아키텍처 기능의 프레임워크를 비교하고 추출하여 현대 사회의 요구를 충족시키는 스마트시티 프레임워크를 구현한다.

구체적으로 이 프레임워크에는 스마트시티 애플리케이션의 현 상황, ANSI와 ETSI등 여러 파트너의 역할, IES-City 프레임워크 유스케이스 등의 내용을 담고 있다.

☞ https://www.ansi.org/news_publications/news_story?menuid=7&articleid=e9065100-3718-4444-9fa2-9a3515304dbf

2.2 TIA, 5G와 차세대 공공안전을 위한 정책 포럼 개최

2018년 10월 2일, TIA(Telecommunications Industry Association, 미국통신산업협회)는 워싱턴 D.C.의 버라이즌(Verizon) 기술정책센터에서 열린 5G와 차세대 공공안전을 위한 정책 포럼에서 기술 및 통신 산업 전문가는 함께 기술 투자, 연방 정책 및 관련 혁신과 관련된 긴급한 문제를 논의하였다.

새로운 솔루션에 대한 안정적이고 일관된 연결성을 보장하려면 5G에 대비한 강력한 공공 안전 통신 네트워크가 필수적이며 정부와 산업계가 차세대 기술의 잠재력을 최대한 발휘 할 수 있는 탄력적인 공공 안전 네트워크를 구축 할 수 있는지 논의하였다.

☞ https://www.tiaonline.org/press-release/tia-policy-forum-to-explore-public-safety-benefits-of-5g-and-next-generation-technologies/

2.3 TIA, 에지 데이터 센터에 대한 새로운 보고서 발표

2018년 10월 10일, TIA(Telecommunications Industry Association, 미국통신산업협회)는 현재 및 미래의 기술이 요구하는 빠르고 신뢰성 있는 정보를 제공하기 위해 에지 데이터 센터(Edge Data Center, EDCs) 개발, 이행 및 운영 기능에 대한 고려 사항을 간략히 설명하는 새로운 포지션 보고서를 발표하였다.

이 보고서는 계획, 설계 개발, 운영 및 유지 보수 요구를 포함하여 기존의 데이터 센터와 비교할 때 새로운 에지 데이터 센터에 대한 기술 요구사항 및 고려사항에 대해 설명하고 있다.

☞ https://www.tiaonline.org/press-release/tia-releases-new-position-paper-on-edge-data-centers/

Ⅱ. 기타 사실 표준화 기구

1. ISA, 컨트롤시스템 부품 사이버보안 성능을 위한 표준 발표

2018년 9월 25일, ISA(International Society of Automation, 국제자동제어협회)는 SA/IEC 62443-4-2-2018 표준(Security for Industrial Automation and Control Systems: Technical

Security Requirements for IACS Components, 산업 자동화 및 제어 시스템 보안 : IACS 요소를 위한 기술적 보안 요구사항)을 발표하였다.

이 표준은 ISA/IEC 62443 표준 시리즈로 ISA99 위원회가 미국국가표준(ANS)으로 개발하고, 동시에 IEC(International Electrotechnical Commission, 국제 전자기술 위원회)에서 국제표준으로 채택되었다.

이 표준은 유연한 프레임 워크 IACS(Industrial Automation and Control Systems, 산업 자동화 및 제어시스템)의 현재 및 미래의 보안 취약점을 해결하고 완화하였으며 제어 시스템 구성 요소에 대한 사이버 보안 기능을 지정한다.

IACS를 구성하는 구성 요소 중 특히 내장 장치, 네트워크 구성 요소, 호스트 구성 요소 및 소프트웨어 응용 프로그램에 대한 사이버 보안 기술 요구 사항을 제공하며 또한, 구성 요소가 보상 대책의 도움 없이 주어진 보안 수준에 대한 위협을 완화할 수 있도록 하는 보안 기능을 설명한다.

☞ https://www.isa.org/news-and-press-releases/isa-press-releases/2018/sept/new-isa-iec-standard-specifies-cybersecurity-capabilities-for-control-system-components/

2. SNIA, 클라우드 데이터관리 인터페이스 오픈소스 표준 발표

2018년 9월 24일, SNIA(Storage Networking Industry Association, 스토리지 네트워킹 산업 협회)는 스토리지 개발자 컨퍼런스에서 CDMI 2.0(Cloud Data Management Interface, 클라우드 데이터 관리 인터페이스) 규격이 오픈소스 표준이 되었음을 발표하였다.

이로써, SNIA 작성자 라이선스 약정서(Contributors License Agreement)1)에 가입함으로써 ISO 표준에 기여할 수 있게 되었다.

CDMI 개발은 표준을 이루는 오픈소스 툴을 사용하여 가능하며, SNIA 클라우드 스토리지 기술 작업반이 비 SNIA 회원으로부터도 CDMI 규격에 대한 충분한 개정 요구를 수용할 수 있어서, 광범위한 커뮤니티가 CDMI를 개선하는 작업에 참여할 수 있다는 데에 중요한 의미가 있다.

이러한 CDMI 2.0 규격에 대한 오픈소스 커뮤티니 접근방법은 CDMI RI(Reference Implementation)를 위한 오픈소스 제공을 완성시켜 준다.

CDMI는 앤드 유저가 데이터 상태를 통제할 수 있도록 하고, 불편 없는 데이터 액세스, 데이터 보호 및 클라우드 서버 간 데이터 이전 형식을 보장한다.

CDMI는 응용 프로그램이 클라우드에서 데이터 요소를 생성, 검색, 업데이트 및 삭제하는 기능 인터페이스를 정의하는 국제표준인 ISO/IEC 17826 : 2016(Information technology - Cloud Data Management Interface , CDMI)이며, 컨테이너 및 컨테이너에 배치된 데이터의 관리를 조정할 수 있는 CMDI 클라이언트 기능과 OpenStack Swift 및 Amazon S3 모델과 함께 작업할 수 있는 기능을 제공한다.

CDMA 2.0 규격의 첫 번째 릴리즈는 2019년도 하반기에 개발될 예정이다.

☞ https://www.snia.org/news_events/newsroom/cloud-data-management-interface-now-open-source-standard

3. W3C, 웹 폰트모듈 Lv3 권고안 발표

2018년 9월 20일 W3C CSS(Cascading Style Sheets) WG(Working Group)[1)]은 CSS 글꼴 모듈 Lv3 권고안(Recommendation)을 발표하였다.

이 CSS Lv3 모듈은 글꼴 속성을 지정하는 방법과 글꼴 리소스를 동적으로 로드하는 방법을 설명하며, 이 규격의 내용은 이전에 CSS3 글꼴 및 CSS3 웹 글꼴 모듈로 분할된 내용을 통합한 버전이다.

☞ https://www.w3.org/blog/news/archives/7300

4. IEEE, IEEE 802.11TM EHT SG와 RTA TIG 출범

2018년 10월 9일, IEEE-SA(IEEE Standards Association)는 새로운 IEEE 802.11™ EHT(Extremely High Throughput) SG(Study Group, 연구반)과 RTA(Real Time Application, 실시간 응용프로그램) TIG(Technical Interest Group)를 발표하였다.

IEEE 802.11TM EHT SG는 1 ~ 7.125GHz 대역의 새로운 IEEE 802.11기능에 대한 논의를 시작하기 위한 그룹이다.

EHT 스터디그룹은 무선랜 환경에서의 AR(Augmented Reality, 증강현실), VR(Virtual Reality, 가상현실)과 같은 대용량의 응용 프로그램을 지원하기 위해 데이터 처리량을 증가시키고자하며, 멀티-AP(Access Point), 공간스트림(spatial streams), 더 넓은 대역폭(higher bandwidth), data aggregation(데이터 집합) 기술과 같은 기능에 대해 논의 예정이다.

1) 종속 스타일 시트(Cascading Style Sheets, CSS) : HMTL, XML 등 마크업 언어로 작성된 웹 문서에서 레이아웃이나 구성 요소들의 스타일을 담당하는 언어이며 웹 페이지의 개발과 수정을 용이하게 한다. 일반적으로 약어 시에스에스(CSS)로 사용한다. <TTA용어사전(http://word.tta.or.kr) 참고>

The IEEE 802.11TM RTA(Real Time Applications, 실시간 응용프로그램) TIG는 실시간 응용프로그램에 대한 사용 모델 및 요구 사항 메트릭을 문서화하기 위해 노력하고 있다.

모바일 및 멀티 플레이어 게임, 로봇 및 산업 자동화와 같은 실시간 응용 프로그램과 이러한 주제를 다루기 위한 산업계의 다양한 메커니즘에서 관찰된 성능 지연 및 안정성 문제를 정량화 한다.

☞ https://standards.ieee.org/news/2018/ieee-802_11-extremely-high-throughput-study-group.html

5. IETF, 인증 토큰 보안을 위한 새로운 인터넷 표준 승인

2018년 10월 12일, IETF(Internet Engineering Task Force, 국제인터넷표준화기구)는 “반복공격(REPLAY ATTACKS)”에 대한 인증 토큰의 보안을 향상시키기 한 세 가지 표준을 승인하였다.

이 세 가지 표준은 새로운 접근/인증 토큰을 생성하고 협상하는 프로세스에 대한 추가 보안을 제공하기 위함이며 IETF가 발표한 세 가지 표준은 다음과 같다.

* RFC 8471 – 토큰 바인딩 프로토콜 버전 1.0
: 토큰 바인딩 프로토콜을 사용하면 고객/서버 응용프로그램에서 여러 TLS (Transport Layer Security, 전송 계층 보안) 세션 및 연결에 걸쳐 장기적이며 고유하게 식별 가능한 TLS 바인딩을 생성할 수 있다.

* RFC 8472 – 토큰 바인딩 프로토콜 협상을 위한 TLS 확장
: RFC 8472는 토큰 바인딩 프로토콜 버전 및 주요 매개 변수 협상을 위한 TLS 확장을 설명하고 있음 단, TLS 1.3 이상의 버전의 토큰 바인딩에 대한 협상은 이 문서의 범위가 아니다.

* RFC 8473 – HTTP를 통한 토큰 바인딩
: HTTP 서버가 보안 토큰(예 : 쿠키 및 OAuth 토큰)을 TLS 연결 암호 방식으로 바인딩 할 수 있게 하는 메커니즘의 모음을 설명한다.

※ IETF는 TCP/IP와 같은 인터넷 관련 프로토콜을 제정·관리하는 사실 표준화 기구로서 전 세계 망 운용자(operators), 장비제조업체(vendors) 및 기술전문가들이 참여하는 개방형 표준기구이다.

☞ https://www.zdnet.com/article/ietf-approves-new-internet-standards-to-secure-authentication-tokens/