2018년 11월 넷째주

해외 ICT 표준화 동향

목 차

※ 게시물 보기

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

TTA 한국정보통신기술협회 Telecommunications Technology Association

1. ETSI, 기업 보안 및 데이터 센터 관리 표준 발표

ETSI releases standards for enterprise security and data centre management

보도날짜 18. 11. 05.
출 처 ETSI
사 이 트 https://www.etsi.org/news-events/news/1358-2018-11-press-etsi-releases-standards-for-enterprise-security-and-data-centre-management

◆ 2018년 11월 5일, ETSI CYBER TC(Technical Committee, 기술위원회)는 eTLS(Enterprise Transport Layer Security, 기업 전송계층보안)로 알려진 중간장비(middlebox)[1] 보안 프로토콜 규격(ETSI TS 103 523-3 v1.1.1. profile for enterprise network and data centre access control)을 발표하였다고 보도함

◆ 이 기술 규격은 TLS 1.3 버전의 특정키 교환 방식에 대한 변경을 반영함

- 수동으로 TLS 1.3 세션의 암호를 해독할 수 있는 방법 중 하나는 각 TLS 세션에 대해 생성된 임시키를 중간장비로 보내는 것이지만, 이러한 접근방식의 개선사항이 요구되어 eTLS는 여러 세션에서 재사용되는 수명이 긴 정적 Diffie-Hellman(디피-헬먼)[2]키를 사용함

- 이는 키를 실시간 해독하여 중간장비에 미리 배포할 수 있으므로 저장 및 암호화된 패킷 저장 시스템과 관련된 키 수를 크게 줄일 수 있음

- 세션의 수동 암호 해독이 필요한 운영 환경에서는 이러한 사용 사례를 지원하는 키 교환 메시지를 사용하고 연결 인증서를 사용하여 최종 사용자에게 공개 정보를 전달

◆ eTLS를 통해 데이터 센터 및 엔터프라이즈 네트워크 운영자는 서비스 계약 및 법적 의무를 준수 할 수 있으며 누가 데이터에 접근하는지 알 수 있도록 보호할 수 있음

1) 중간장비, middlebox : 특정 지능적 기능을 가진 네트워크 중간자로서의 서비스를 수행하는 장비 방화벽이다. [http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=049049-1 TTA 용어사전 참고]
2) 디피(Diffe)와 헬만(Hellman)이 1976년에 발명한 공용 키(public key) 분배법이며, 두 사람이 소수(素數) p와 원시근(原始根) g를 공유하고, 각각 자신의 비밀 정보를 생성, 비밀 정보와 g, p로부터 모듈러 연산(p로 나눈 나머지를 계산)한 결과를 상대방에게 보낸다. 각자 받은 정보와 자신의 비밀 정보를 이용하여 계산함으로서, 두 사람은 동일키를 공유할 수 있다. [http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=053217-4 TTA 용어사전 참고]

1. CEN 및 CENELEC, 유럽사이버보안기구와 MOU 체결

▷ 발 행 일 : 18. 11. 13.

▷ 원문제목 : Memorandum of Understanding between CEN, CENELEC and the European Cyber Security Organisation (ECSO)

▷ 원 문 : https://www.cencenelec.eu/News/Press_Releases/Pages/PR-2018-09.aspx

▷ 내용요약

◦ 2018년 11월 13일, CEN 및 CENELEC은 유럽사이버보안기구(European Cyber Security Organization, ECSO)와 MOU(양해각서) 체결

◦ 이번 MOU를 통해 공식적으로 인정된 유럽 및 국제기구의 표준화가 사이버 보안 분야 인증 제도의 기초로서 효과적으로 고려되도록 하기 위함.