

2017. 9

해외 ICT 표준화 동향

4th week

목차

본문 1. OASIS, 사이버 위협 대응 관련 OpenC2 표준 작업 착수

기타 - IEEE·UL, 무선 당뇨병 기기 보안 표준개발 협력 체결
- ITU, 지능형 교통 시스템 보안 관점 워크숍 개최

* 게시물 보기

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

TTA 한국정보통신기술협회 Telecommunications Technology Association

1. OASIS, 사이버 위협 대응 관련 OpenC2 표준 작업 착수

(International Community Comes Together at OASIS to Advance OpenC2 Standard for Automated Defense Against Cyber-Attacks)

보도날짜 2017. 9. 5.
출 처 OASIS
사 이 트 https://www.oasis-open.org/news/pr/international-community-comes-together-at-oasis-to-advance-openc2-standard-for-automated-def

■ 2017년 9월 5일, OASIS는 사이버 운영 명령 및 제어(Cyber Operations Command and Control) 표준 언어 개발에 착수함

- OASIS의 OpenC2(개방형 명령 및 제어, Open Command and Control) 기술위원회는 사이버 방어 기술에 명확한 명령과 제어를 위한 표준화된 언어를 정의하는 곳으로, 이번 작업은 사이버 위협에 대해 빠른 속도로 대응이 가능하며, 제품들 간 높은 상호운용성을 보장함

■ 사이버 위협은 사람이 인지하는 데 몇 주 이상 걸리지만 공격은 몇 초 만에 실행 되므로, OpenC2는 기계 간 통신의 공통 언어를 제공함으로써 자동화되고 전략적인 사이버 위협에 빠르고 정확한 대응을 가능케 함

- 대부분의 환경은 수백 가지의 시스템 및 기기로 구성되어있고, 이러한 모든 장비는 수동으로 구성하거나 실시간 명령을 보내야 하므로 사고 대응 속도가 감소되며, 수동적 조작 시 실수를 야기할 수 있음

- 따라서 OpenC2 작업은 환경 내 취약한 장치에 자동적으로 방어적 조치를 가능케 함

■ OpenC2는 플랫폼과 제품에 상관없이 사이버 방어 접근을 능동적으로 지원함

- OpenC2를 사용함으로써 특정 위협을 예방 하는 방법을 고안할 수 있고, 기계가 읽을 수 있는 간결한 언어로 다른 사람과 공유하는 방법을 개발할 수 있음

- 이 방식을 사용하는 기관은 상호운용성에 대한 걱정 없이 기관 환경에 적절히 적용하여 사이버 위협을 경감시킬 수 있음

■ OpenC2에는 현재 산업, 정부, 학계, 재정 분야의 전력망 및 기타 주요 이해관계자 54개의 조직이 참여하고 있음

- STIX[1] 및 TAXII[2] 표준 작업을 수행하는 지능형 사이버 위협대응(CTI, Cyber Threat Intelligence)[3] 기술위원회도 OpenC2에 참여하고 있음

1) STIX(Structured Threat Information Expression): 사이버 위협 지능 교환(CTI)을 위해 사용되는 언어와 연속된 포맷. 조직들이 기계가 해석할 수 있는 방법으로 CTI를 공유하고 보안 커뮤니티들이 컴퓨터 기반 공격에 더욱 빠르고 효과적으로 반응하도록 한다. STIX는 협력 위협 분석, 자동 위협 교환, 자동 감지와 대응 등의 다른 능력 향상을 위해 설계됨. <출처: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti-stix>

2) TAXII(Trusted Automated Exchange of Indicator Information): 사이버 위협 정보를 단순한 방식으로 통신하는 애플리케이션 층 프로토콜. Https의 사이버 위협 지능(CTI)을 교환하는데 사용하는 프로토콜이며, 특히 STIX에서 나타나는 CTI 교환을 지원하기 위해 설계됨. <출처: https://oasis-open.github.io/cti-documentation/>

3) 지능형 사이버 위협대응(CTI, Cyber Threat Intelligence): 조직의 정보(information) 자산에 위협이 될 수 있는 취약 요소, 과거 공격 등 관련 정보를 기반으로 사이버 보안 위협에 효과적으로 대응하는 방법. 지능형 사이버 위협 대응(CTI)은 과거 조직 내부뿐만 아니라 여러 외부 조직에서 겪었던 많은 위협 정보를 수집·분석·활용하여, 지능형 지속 위협(APT)과 같은 공격을 사전에 방어한다. < 출처: 정보통신용어사전, http://term.tta.or.kr>

기타 소식

IEEE·UL, 무선 당뇨병 기기 보안 표준개발 협력 체결

▶ 출처 : http://www.cellular-news.com/story/Operators/72601.php (2017. 8. 25.)

ㅇ 2017년 8월 25일, IEEE와 안전과학인증기관인 UL(Underwriters Laborataories Inc.)[1]은 무선 당뇨병 기기 보안에 대한 공동 표준개발에 대해 협력키로 함

- 이번 협력으로, 무선 당뇨병 기기의 안전을 지원하는 표준 협력체 결성을 통해 환자의 데이터와 개인정보 보안에 대한 의학 기기의 안전성을 제공케 할 것임

ITU, 지능형 교통 시스템(ITS)의 보안 관점 워크숍 개최

▶ 출처 : http://newslog.itu.int/archives/1613 (2017. 8. 30.)

ㅇ 2017년 8월 28일, ITU는 '지능형 교통 시스템(ITS, Intelligent Transport Systems) 보안에 대한 관점'이라는 주제로 스위스 제네바에서 워크숍 개최

- 이번 워크숍에서는 ITS 산업의 가치사슬 내 모든 분야의 보안 요구사항에 대해 논의하고, ITS 보안 문제의 생태계적 관점을 독려하였음

1) UL(Underwriters Laboratories Inc. , 이하 UL) : 미국 일리노이주 노스 브룩에 본거지를 두고 있는 미국 최초의 안전 규격 개발 기관이자 인증 회사이다. UL은 글로벌 안전 과학 회사로서, 제품 안전 시험 및 인증 발행, 환경 시험, 제품 성능 시험, 헬스 케어 및 의료기기 인증 발행, 교육 및 세미나 등의 서비스를 제공하고 있다. UL 제품 성능 시험에 합격한 제품은 UL 인증 마크의 사용이 허가된다.< 출처: 위키백과 >