사이버 위협 대응

전 세계적으로 4차 산업혁명의 성패를 좌우할 5G, 사물인터넷, 클라우드, 인공지능, 블록체인 등과 같은 ICT 신기술 확보와 시장을 선점하기 위한 경쟁이 나날이 치열해지고 있다. 우리나라도 초연결 지능정보화 사회 구현을 위한 핵심 인프라 기술 확보를 위해 세계 최초로 5G 상용 서비스가 개시되었고, 데이터 경제 및 인공지능 활성화 전략 등 4차 산업혁명의 핵심기술 확보를 위한 전략과 투자를 적극적으로 추진하고 있다. 이러한 4차 산업혁명의 ICT 신기술로 인해 우리의 삶은 보다 편해질 것으로 기대하고 있으나, 동전의 양면과 같이 개인정보 침해, 정보유출, 랜섬웨어 등 사이버공격 피해도 나날이 증가하고, 신기술을 악용한 개인정보 침해, 정보유출, 랜섬웨어 등 지능화된 사이버공격의 강도에 대한 우려 역시 크다. 따라서 보안 내재화가 고려되지 않은 ICT 기술은 정보통신 서비스의 안전과 디지털 경제발전의 걸림돌로 작용하여, 미래 디지털 사회의 신뢰위기를 야기할 수 있다. 이에 정부는 민간부문 정보보호 종합계획 2019, 국가사이버안보전략(2019년 8월), 5G+ 전략 등을 통해 정보보호가 정보통신 서비스의 일부 요소기술이 아닌 초연결지능정보화 사회의 Key Enabler로서 중요성과 역할이 매우 커지고 있다. 이번 특집호에서는 4차 산업혁명의 핵심기술 연관된 사이버위협대응 분야의 기술이슈와 표준화 동향을 다루었다.

김환국 _ TTA 사이버보안 프로젝트그룹(PG503) 의장

사이버위협대응에 대한 소개 부탁드리며, 최근 관심이 되고 있는 기술은 무엇이 있는지...

사이버보안은 사이버공간 영역 확장과 보호대상 증가로 인해 개념과 정의가 점차 확대되고 있다. 전통적으로 정보보호는 네트워크에 연결된 IT 자산과 정보를 보호하기 위한 기밀성, 무결성, 가용성 중심의 정보보호(Security) 개념에서 ICT 기술과 전통적인 산업의 융합이 가속화되면서 인터넷에 연결되는 모든 영역을 사이버공격으로부터 물리적 공간의 실생활, 생명과 안전(Safety)하게 보호하는 사이버보안(Cyber Security) 개념으로 진화하고 있다.

사이버보안 기술의 구성요소는 보호대상 관점에서 살펴보면 공통기반보안, 시스템보안, 네트워크보안, 데이터보안, 응용서비스 및 플랫폼 보안으로 구분하고 있으며, 최근에는 사이버공간의 확장에 따라 ICT 정보자산에서 IoT 기기, 자율주행차, 의료기기, 산업제어시스템(ICS) 등 전통적인 산업분야의 기기들로 확장되고 있다.

특히 사이버위협대응기술은 진화하는 사이버공격에 신속하게 대응하기 위한 방어기술 개념을 갖는다는 점에서 ICT 기술과는 다른 특징을 갖는다. 사이버공격은 다양한 기기들이 인터넷에 연결되고 전 산업분야에 ICT 기술과 융합이 가속화되면서 새로운 보안위협이 출현하거나 기존 보안기술을 우회하는 방향으로 진화하고 있다. 반면 사이버위협대응기술은 보호대상과 분석해야 할 데이터의 증가로 탐지 정확도 저하와 수동분석의 한계 등 해결해야 할 도전과제가 끊이지 않고 있다. 따라서 진화하는 사이버위협에 신속하게 대응하기 위해 현재 보안기술 수준과 성능을 향상시키 위한 지능형 사이버위협대응기술과 표준화에 관심을 두어야 할 것으로 생각된다.

사이버위협대응기술과 관련된 국내외 표준화 현황을 말씀해 주신다면…

사이버위협대응기술의 국제 표준화는 ITU-T SG 17(정보보호), ISO/IEC JTC 1 SC 27, IETF I2NSF에서 주로 담당하고 있으며, 국내는 TTA 정보보호기술위원회(TC5) 사이버보안 프로젝트그룹(PG503)에서 사이버위협대응기술과 관련된 표준을 개발하고 있다. 최근 국내외 표준화 기구에서 다루고 있는 주요 아이템들은 4차 산업혁명과 관련하여 신규 보안이슈를 해결하기 위해 IoT 보안, 빅데이터 보안, ITS 보안, SDN/NFV 보안, 개인정보보호, 클라우드 컴퓨팅 보안, 5G 보안 등에 관심도가 높은 편이다.

사이버위협대응분야 대표적인 해외 표준화 현황을 살펴보면, ITU-T SG 17 Q2(보안구조 및 프레임워크)에서, SDN 보안 서비스 기능 체인에 대한 보안위협 분석과 이를 해결하기 위한 보안 요구사항 표준들이 제정되었다. Q4(사이버보안)는 국가 간, 유관 기관 간에 사이버 위협 정보 공유 및 분석을 신속히 처리할 수 있는 사이버보안관제 표준화에 포커스를 두고 있으며, 최근에는 랜섬웨어, 가상화폐거래소 해킹 등에 대한 사이버 위협 정보 표현 규격(STIX) 활용 표준이 제정되었다. Q6(통신 서비스 및 사물인터넷 보안)에서는 IoT 보안 위협 및 도전 과제들을 분석하고, 이를 감소시키거나 해결할 수 있는 방법론에 대한 표준이 제정되었다. ISO/IEC JTC 1 SC 27에서 사이버보안 침해 관리에 대한 표준(ISO/IEC 27035-2011)을 제정 후, 2016년에는 ISO/IEC 27035-1 및 ISO/IEC 27035-2 분리하여 개정을 완료하였다. 사이버침해대응 오퍼레이션을 위한 가이드라인(ISO/IEC 27035-3) 개발이 진행 중이다. IETF I2NSF에서는 SDN/NFV 인터페이스 보안 표준이 개발되었다(※ 출처: 오흥룡, 'ITU-T SG17 보안국제표준화 동향', 정보보호학회지 Vol.29, No.4).

국내 표준화는 TTA TC5 PG503(사이버보안)에서 담당하고 있으며, 클라우드 보안, 네트워크 보안, 해킹대응, 악성코드 대응, 스팸대응, 디지털 포렌식 및 사이버 범죄 대응 기술 분야의 표준을 다루고 있다. 최근에는 SDN 보안, 디지털 포렌식을 위한 이기종 증거의 통합정보처리규격, 사이버위협정보공유규격(STIX) 및 정보공유 유스케이스 등 표준을 제정하고 있다.

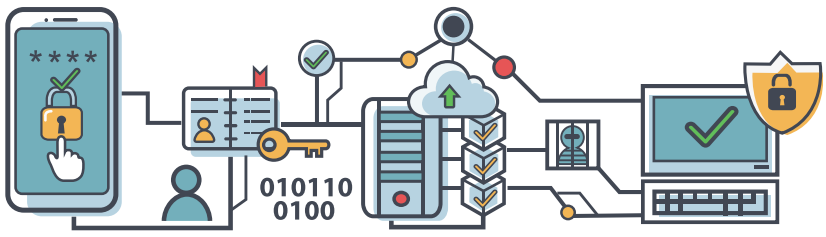
사이버위협대응기술에서 다루고 있는 주요 표준화 아이템은 무엇이 있는지?

사이버위협대응기술의 주요 표준화 아이템은 사이버위협 정보공유, 디지털 포렌식, 악성코드 및 보안 취약점 분석 등 신속한 사이버공격대응과 사이버범죄수사를 위해 이기종 보안시스템 간 정보규격 및 연동 인터페이스와 관련된 표준화 아이템이 많은 편이다.

사이버침해사고 발생 시 신속한 대응과 공격확산 방지를 위해 서로 다른 조직(시스템, 사람)간 사이버위협정보(악성코드 정보, 보안 취약점 정보, 침해사고 정보)를 상호 교환하는 것이 매우 중요하다. 특히, 각 기관과 시스템별 위협정보와 탐지 결과의 표현 체계가 서로 다르고, 타 기관 간 실시간 공유·전파 체계가 상이하기 때문에, 사이버위협에 적절하면서 신속하게 대응하기 위해서는 사이버위협정보 교환은 필수적이며, 정보공유 체계를 수립하기 위해서는 표준화된 정보 규격과 연동 인터페이스의 표준화가 매우 중요하다.

또한 지능형 사이버범죄 수사를 위한 디지털 증거의 증거능력 확보를 위한 절차와 도구의 신뢰성 검증에 대한 표준화가 중요하며, 최신 형사소송법과 각종 판례의 요구사항을 반영한 가이드라인 개정과 네트워크 패킷을 처리하는 절차를 규정하는 지침과 관련된 표준이 TTA 단체표준으로 제정되었다.

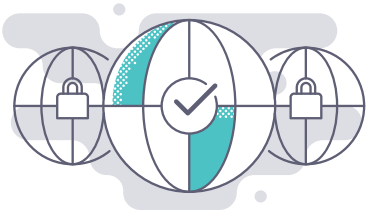
최근에는 소프트웨어 및 하드웨어 공급망 취약점을 이용한 사이버공격이 이슈가 되고 있어, 제품 개발 및 운영단계에서 보안 취약점을 사전에 진단하고 제거하는 것이 필요하며 이를 위해서는 다양한 보안 솔루션들이 각 벤더별로 그 취약점을 평가하기 위한 식별 체계들을 표준화하여 공통적인 식별 체계 및 진단 프로세스 관련 표준화가 중점적으로 다뤄지고 있다.



초연결 5G 시대를 대비해 주목해야 할 사이버위협 대응분야 이슈와 표준화 역할은?

5G 네트워크, 사용자 트래픽과 서비스를 안전하게 보호하기 위해서는 이전 세대 보안기술과는 차별화된 새로운 보안기술이 설계되고 솔루션이 개발되어 네트워크에 구축·운영되어야 한다. 이를 위해서는 표준화, 장비개발, 네트워크 구축 및 운영의 각 단계별 보안 내재화를 위해서는 표준화 역할이 매우 중요하다. 먼저 표준화 단계에서는 국가 간 네트워크 및 시스템의 상호 연동을 위해 통신 프로토콜과 인터페이스가 안전하게 설계되어야 한다. 5G 관련 보안 표준화는 국제표준기구와 사실표준단체에서 5G 기본적 보안 요구사항과 아키텍처에 관한 표준 연구가 활발하게 진행 중이다. 3GPP 표준에서는 사용자와 네트워크 간에 상호인증을 위한 인증 및 키 관리, 제어 평면(Control Plane)의 시그널링 메시지와 사용자 평면(User Plane)의 데이터 보호를 위한 보안 표준들이 개발되어 모바일 네트워크의 보안성을 지속적으로 강화해 왔다. 그러나 표준화는 최소한 기본적인 보안 요구사항과 스펙만을 정의하기 때문에 표준 프로토콜 상의 취약점이 상시 발생할 수 있다는 우려가 존재한다. 둘째, 장비 개발 제조사들은 표준에서 요구하는 보안 기준과 목표 수준에 맞는 장비를 개발해야 한다. 예를 들어, 각 장비 제조사별로 보안 기능이 다르게 구현되거나 SW로 구현된 장비들이 SW 오류를 내포하거나 장비 구현 당시 알려지지 않았던 보안 취약점(Unknown Vulnerabilities)이 시간이 지나면서 지속적으로 발견되는 장비 구현 상 보안 취약점 이슈가 지속적으로 발생한다. 셋째, 통신 사업자는 장비 제조사들의 통신장비와 서비스 애플리케이션들이 보안요구사항에 맞게 구현되었는지 공급망 제품을 검증하여 안전한 네트워크와 서비스를 설계하고 구축해야 한다. 그럼에도 불구하고 네트워크와 서비스를 구축하는 과정에서 구성설정 오류가 존재할 수 있

고, 통신 사업자가 아닌 3rd 애플리케이션 등의 보안 이슈는 지속적으로 제기되고 있다. 마지막 서비스 운영 단계에서는 고도화되고 지능화된 사이버공격에 대한 취약점 제거와 침해사고 발생 후 복원력이 중요하다. 또한, 각 단계별 보안 이슈사항을 해결하는데 소요되는 대응조치 시간도 장애요소가 될 수 있으므로, 표준 프로토콜 상의 보안 취약점의 경우 표준에 반영되기까지 수년의 시간이 소요되며, 장비 구현 취약점은 SW 패치부터 안전성 검증까지 약 6개월 이상의 시간이 소요되기 때문에 각 단계 간 보안 갭(Security Gap)을 줄여나가기 위해서는 5G 보안 관련 국내외 표준의 역할이 매우 중요하다.



5G 보안 관련된 주목해야 할 표준과 기술은 무엇이며 그 이유는?

앞에서 설명하였듯이, 5G 보안은 5G 설계 시 보안 및 프라이버시 내재화가 기본적으로 적용되어야 한다. 이를 위해 SDN 보안, NFV 보안, 네트워크 슬라이싱 보안이 고려되어야 하고, 보안 관리를 위한 오케스트레이션이 필요하다. 또한 AI/ML 기술을 이용한 침입 탐지 및 위협 대책 수립과 5G 보안 프레임워크 등 5G 보안내재화를 위한 연구와 표준화가 중요하다.

해외에서는 3GPP, 5G PPP(유럽 집행위, 제조사, 통신사, 서비스사업자, 연구기관 참여)의 Security WG에서 5G 보안 아키텍처 연구가, 이동통신사업자 중심의 NGMN(Next Generation Mobile Networks) 5G 워킹그룹에서는 네트워크 슬라이싱, MEC 보안 요구사항을 다루고 있다. ETSI(유럽전기표준협회) NFV SEC(NFV Security) WG에서 NFV 보안 스펙을 주로 다루고 있다. ITU(SG 17)에서 5G 보안에 관한 보안 표준화 연구를 본격적으로 개시하였다.

5G 핵심기술로 소프트웨어 정의 네트워킹(SDN)과 네트워크 기능 가상화(NFV)를 기반으로 한 클라우드 컴퓨팅과 에지 컴퓨팅이 5G의 핵심기술로 이용될 전망이다. 이러한 클라우드와 에지 컴퓨팅에서 있어서 안전하고 안정적인 네트워크 서비스를 제공하기 위해 클라우드 기반 보안 서비스(SeCAAS) 시스템이 필요하다. 이러한 클라우드 기반 보안 서비스 시스템에서 다양한 보안 솔루션 벤더들이 제공하는 보안 솔루션을 효과적으로 운용하기 위해서는 I2NSF의 프레임워크와 표준 인터페이스가 중요하다.

IoT 보안과 관련된 시험 인증과 융합보안 표준 사례를 소개해주신다면?

IoT 기기는 산업군 서비스별 기기 유형(스마트공장 기기, 스마트시티 센서, CCTV 등)과 탑재 애플리케이션, 공급망 생태계가 다양하기 때문에 공통된 보안 표준이나 아키텍처 설계가 쉽지 않다. 또한 저사양 IoT 기기의 경우 고수준의 보안 기능을 탑재하기 어려워 취약한 패스워드 및 오래된 보안 취약점을 내포한 채 방치되거나 디바이스 템퍼링에 의한 변조에 취약하고 악성 애플리케이션에 의한 부적절한 접근 또는 중간자공격으로 인한 가입자 정보 정보유출 등의 보안위협에 취약한 환경에 노출될 가능성이 상대적으로 높다.

과학기술정보통신부와 한국인터넷진흥원은 IoT 기기 및 제품에 대한 침해위협이 증가함에 따라 IoT 제조사가 제품 개발단계부터 보안을 고려하여 출시할 수 있도록 민간 자율의 'IoT 보안인증 서비스'를 2017년 12월부터 실시하고 있다. IoT 제품들이 기본적인 보안 요건을 만족하는지 5개 시험영역인 인증(사용자 인증, 인증정보의 안전한 사용, 제품인증 등), 암호(안전한 암호 알고리즘 사용 등), 데이터보호(전송 및 저장 데이터 보호 등), 플랫폼보호(SW 보안, 업데이트, 보안관리 등), 물리적 보호(물리적 인터페이스 보호 등)별로 시험 평가하고 기준 충족 시 등급별 인증서를 발급해주는 민간 자율 인증 서비스를 운영 중이다.

또한 과학기술정보통신부 5G+ 핵심서비스 융합보안 강화방안(2019년 10월)을 발표하면서 5G 통신 기반 핵심 융합 서비스(스마트공장, 자율주행차, 스마트시티, 디지털 헬스케어, 실감콘텐츠) 보안 내재화 논의가 본격적으로 개시되고 있으며, 5G+ 융합서비스 관련된 보안 표준화 역할이 한층 커질 것으로 기대된다. 대표적으로 자율주행 자동차 보안 표준은 ISO TC 22 WG, ITU-T 등에서 협력자율주행을 위한 V2X 통신 보안, 자동차 사이버보안 요구사항과 규제, 자동차 서비스 보안(예: car-to-cloud 보안, 차량 소프트웨어·펌웨어 원격 업데이트 등) 등 다양한 분야에서 표준화 논의가 활발하게 진행되고 있는 분야이다. TTA