원자력시설의 사이버보안 규제 관점에서의 단방향 통신 보안 요구사항 연구

이채창*
한국원자력통제기술원, 대전광역시 유성구 유성대로 1534
*chiching@kinac.re.kr

1. 서론

원자력시설을 목표로 하는 악성코드 스턱스넷이 발견된 이후로, 원자력시설에 대한 사이버공격 위협이 지속되고 있다. 이에 따라 원자력시설 사업자들의 사이버보안 관련 규정 준수와 전문성 있는 규제가 함께 요구되고 있다.

미국 원자력규제위원회(NRC)는 원자력사업자의 사이버보안 방어 전략에 있어 필수디지털자산을 보호하기 위해 심층방호(defense-in-depth) 전략을 활용하도록 규제하고 있으며, 한국원자력통제기술원 또한 기술기준 및 사이버보안계획(CSP)을 통해 심층방호 전략을 원자력 사업자들에게 요구하고 있다. 아래 Fig. 1은 사이버보안 심층방호 구조의 예시를 보여 준다.

Fig. 1. An Example of a cyber security defensive architecture.

이러한 사이버보안 방호구조는 방화벽이나 다이오드와 같은 보안 경계에 의해 구분되는 다섯 가지의 사이버보안 방호등급으로 구성되어 있으며, 각 경계에서는 데이터 통신이 감시 및 제한된다. 이와 같은 방호구조 상에서 높은 수준의 사이버보안이 요구되는 시스템은 높은 등급의 구역에 배치되어 낮은 등급의 시스템 및 데이터 통신으로부터 보호되어야 한다. 따라서 4등급에서 3등급, 3등급에서 2등급으로의 데이터 흐름은 단방향(one-way) 통신만 허용된다.

2. 본론

2.1 단방향 통신 기술 동향 및 구성 방식

초기의 단방향 통신 매체는 데이터 다이오드(Data Diodes)로 불리며, 군사 기밀과 같은 높은 보안 등급의 네트워크에 있는 자료가 낮은 보안 등급의 네트워크로 전송되지 않도록 하기 위해 사용되었다. 최근에는 원자력시설을 비롯한 산업제어시스템 상에서 인터넷망 등 신뢰되지 않는 네트워크에 연결된 낮은 보안 등급 시스템의 데이터 및 프로그램 들이 높은 신뢰성이 요구되는 제어망 등 높은 보안 등급으로 유입되지 않도록 단방향 통신이 사용되고 있다.

2.1.1 케이블 방식

가장 일반적이며 전통적인 방식으로, RS-232 케이블의 송신 및 수신 두 가닥 중 한 가닥을 절제하여 단방향성을 제공한다. 이와 유사하게 UTP, USB 케이블 등의 양방향 회선을 조작하여 단방향이 되도록 구성하는 방식이 있으며, 이 밖에 Tap이나 Splitter와 같은 장치를 사용하여 두 시스템 사이의 양방향 통신 데이터를 단방향으로 유도할 수 있다. 미디어 컨버터를 사용하여 이더넷 신호를 광학 신호로 변환하여 단방향성을 제공하기도 한다.

2.1.2 전용 하드웨어 방식

Fox-IT, Watefall 등의 보안 업체에서는 단방향 통신을 구성하기 위해 단방향 전용 네트워크 카드를 사용하는 별도의 상용 하드웨어 장치를 통해 단방향 통신을 제공하고 있다.

2.1.3 논리적 방식

방화벽의 정책 설정을 통해 아웃바운드 트래픽만 허용하고 인바운드 트래픽을 차단하는 등의 방법으로 단방향 정책 설정을 할 수 있다. 또한 심층방호 구조의 경계 상에 별도의 시스템을 두고 접근 대상에 따라 데이터의 읽기 및 쓰기 권한을 구분하여 접근 제어 정책을 설정하거나, 비대칭키 암호 알고리즘을 사용하여 암호화키와 복호화키를 구분하는 방식으로 단방향성을 유지할 수 있다.

2.2 규제 관점에서의 보안 요구사항

2.2.1 매체 건전성

매체 건전성은 단방향 매체가 물리적으로 적법한

절차나 방법에 의해 설치 및 구성되었음을 뜻한다. 특히 케이블 방식의 단방향 통신의 경우 저렴한 비용과 구축 편의성으로 많은 제어시스템에서 사용되고 있으나 보안성은 고려되지 않아, 케이블 변경 및 이중 연결 등으로 단방향성이 훼손되지 않았는지 점검이 필요하다. 또한 적절한 케이블링을 통해 한 방향의 회선만 사용이 가능하도록 구성되었는지 여부는 육안으로 확인이 어려우므로, ping 테스트 등과 같은 방법으로 실제 역방향의 신호가 차단되는지 여부도 확인해야 한다.

2.2.2 정책 건전성

정책 건전성은 논리적 방식의 단방향 통신 매체에 적용되는 것으로 단방향성을 보장하는 규칙의 정의가 적절하게 설정되었음을 의미한다. 논리적 방식의 단방향 통신 매체를 사용하는 경우에는 특히 해당 매체에 대한 이해와 전문성을 갖춘 사용자가 정책을 설정해야 하며, 정책 설정을 변경할 수 있는 권한의 설정 및 관리가 무엇보다 중요하다. 또한 다른 third-party 프로그램이나 프로세스의 허가되지 않은 권한 상승(privilege escalation)에 의해 해당 정책이 변경되지 않도록 유의해야 한다.

암호화 방식의 단방향 매체의 경우에는 대칭키 암호 알고리즘을 사용하고 있지 않은지, 암호화 알고리즘 및 키 길이는 충분한 안전성을 보장하는지, 키 관리는 적절한지 등을 살펴보아야 한다.

2.2.3 프로토콜 건전성

전용 하드웨어를 통한 단방향 통신 매체에서는 TCP와 같이 신뢰성이 보장되는 연결이 제한되므로, UDP와 같은 비연결형 프로토콜을 사용한다. 이에 따라 필연적으로 오류 제어 및 검출이나 피드백을 위해 별도의 방식이나 독자적인 프로토콜을 사용하기도 한다. 오류 제어 및 검출을 위해 피드백 신호를 사용하는 경우 피드백 신호에 제어를 위한 기본적인 신호 외에 유의미한 신호가 검출되지 않는지, 오류 제어 및 검출 방식은 적절한지 등을 확인해야 한다.

2.2.4 인증

전용 하드웨어를 통한 단방향 통신 구성시 CC(Common Criteria)나 보안적합성검증 등의 인증 결과를 활용할 수 있다. 다만 CC의 경우 해당 장치(TOE, Target of Evaluation)의 특정 보안기능 요구사항(SFR, Security Function Requirement)에 부합하는 것에 대한 보증이므로, 해당 CC가 제어시스템에서 요구하는 단방향성이 SFR에 포함되어 있는지 살펴보아야 한다.

3. 결론

NRC는 원자력사업자의 사이버보안 방어 전략에 따른 방호구조에 있어 높은 보안 등급의 시스템에서 낮은 보안 등급의 시스템으로 단방향 통신을 구성할 것을 요구하였으며, 이에 따라 단방향 통신 규제시 고려해야할 보안 요구사항들을 살펴보았다. 보안 등급에 따른 단방향 통신 요구사항은 안전 등급에 따른 단방향 통신 요구사항으로 확장하여 적용할 수 있으며, 원자력시설 뿐 아니라 단방향 통신이 요구되는 산업제어시스템 현장의 운영이나 규제에도 활용될 수 있을 것이다.

4. 참고문헌

[1] NRC, “Cyber Security Programs for Nuclear Facilities”, Regulatory Guide 5.71 (2010).

[2] 한국원자력통제기술원, “원자력시설등의 컴퓨터 및 정보시스템 보안 기술기준”, KINAC/RS-015.01 (2014).

[3] Stevens M. and Pope M. “Data Didoes”, Electronics and Surveillance Research Laboratory(DSTO), DSTO-TR-0209 (1995).

[4] Jeffrey Menoher, “All Data Diodes Are Not Equal”, Owl Computing Technologies, white paper (2013).

[5] NIST, “Recommendation for Key Management - Part 1: General(rev.3)”, SP 800-57 (2012).

[6] IEEE, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Powr Generating Stations, 7-4.3.2-2010.