정 보 보 호 학 회 지
제 30 권 제5호, 2020. 10

원전 사이버 보안 취약점 점검 기술 동향 및 개발 사례

최 양 서*, 안 개 일**

요 약

정보화 시대의 도래와 함께 원자력발전소 등 사회 간접자본의 중요 시설에서 운영되는 각종 장치들 역시 디지털화되면서 기존에 존재하지 않았던 사이버 공격에 대한 위협이 현실화되고 있다. 이러한 중요 사회 간접자본 등의 운영에 위협을 가하는 행위는 사회적으로 경제적으로 매우 큰 재난을 발생시킬 수 있기 때문에 공격 발생 이전에 사전 방어 체계를 구축해야 하는데, 이때, 실질적으로 위협이 되는 취약점의 존재 여부를 사전 인지하는 것이 매우 중요하다. 이를 위하여 본 논문에서는 원자력발전소의 계측제어계통에서 운영되는 국산화된 디지털 장치에 대하여 관련 취약점을 확인하고 확인된 취약점의 실질적인 위험도를 장치의 운영환경 특징을 반영하여 도출하며, 주요 기기의 운영 규제지침의 준수 여부를 점검하는 도구의 개발 결과를 소개한다. 본 논문은 원자력발전소 상에서 운영되는 시스템을 주요 대상으로 작성되었다.

Ⅰ. 서 론

정보화 시대가 도래하면서 IT 기술 발전에 따라 기존에 기계식으로 존재하던 다양한 산업 기기들의 동작 방식이 디지털화되었다. 원자력발전소 역시 계측제어시스템뿐만 아니라 보안 시스템, 비상대응 시스템 등에 많은 디지털 기기들이 활용되고 있다.

특히, 최근에 건설되어 운용이 예정되어있는 신한울 1, 2호기 원자력발전소의 경우 APR-1400 노형[1]으로 건설되면서 세계 최초로 100% 디지털화된 인간-기계연계시스템(MMIS, Man Machine Interface System)을 도입하였고, 계측제어계통 기기들을 포함한 주제어실의 많은 기기들이 디지털화되어 운영되고 있다.

디지털 기기들이 널리 활용되고, 스턱스넷(Stuxnet)[2] 등의 사이버 공격으로 실질적 피해 발생이 가능하다는 것이 확인되면서 원전 내 디지털 기기에 대한 사이버 보안 이슈가 크게 강조되기 시작하였다.

원자력발전소 운영 기기에 대한 사이버 보안 대응을 위해 한국원자력통제기술원(KINAC)에서는 “원자력시설의 컴퓨터 및 정보시스템 보안(RS-015)”[3]이라는 원전 디지털 기기에 대한 보안 기준을 마련하고 사이버 보안 요구사항을 제시하였다.

이와 같은 보안 위협에 대응하기 위해서는 실제 공격 발생 시 해당 공격을 신속히 탐지하고 이를 차단하는 것도 중요하지만, 더불어서 원자력발전소의 운영 요원들이 운영하는 기기에 존재할 수 있는 사이버 보안 취약점에 대한 정보를 손쉽게 얻을 수 있어야 한다. 또한, RS-015 등에서 요구하는 보안 지침을 해당 기기들이 준수하고 있는지를 손쉽게 확인할 수 있어야 한다.

그러나, 원전과 관련된 취약점 정보의 경우 외부 기관을 통해 관련 취약점에 대한 정보를 관련 인원들이 획득하고는 있으나, 운영 요원 자체적으로 관련 취약점 정보를 손쉽게 획득하거나 확보된 취약점에 대한 실질적인 위험도를 파악하기는 쉽지 않은 상황이다. 또한, RS-015에서 요구하는 규제지침의 준수 여부 확인은 운영 장치의 안정성 유지를 위해 매우 중요하나 해당 규제지침이 준수되고 있는지를 확인하는 과정은 오랜 시간이 소요되고 있어 규제지침 준수 여부를 신속하게 확인할 수 있는 방법이 요구되는 상황이다.

이를 위해 본 논문에서는 운영 장치 관련 키워드에 기반한 취약점 검색, 검색된 취약점에 대한 장치 운영환경 특징을 반영한 취약점 위험도 재평가 그리고 자동화된 방식으로 점검이 가능한 RS-015 규제지침 항목에 대해 규제지침 점검을 수행하는 도구 개발 사례를 소개

본 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2016M2A8A4952280, 원전 계측제어 사이버보안 취약점 점검 기술).
* 한국전자통신연구원 (책임연구원, yschoi92@etri.re.kr)
** 한국전자통신연구원 (책임연구원, fogone@etri.re.kr)

함으로써 관련 요구에 부응할 수 있도록 한다.

본 문서는 2장에서 원자력발전소에 대한 사이버 보안 위협, 관련 규제지침과 점검 방안 그리고 취약점 관리 관련 동향에 대해 알아보고, 3장에서 기기 규제지침 점검 및 취약점 위험도 재평가를 위한 도구의 구성과 기능을 소개하며, 4장에서 개발 결과물의 시험 내용을 소개하도록 한다. 그리고 5장에서 결론 및 향후 연구 방향을 제시하면서 본 논문을 마치도록 한다.

Ⅱ. 원전 사이버보안 위협 및 대응 방안 동향

2.1. 원전 사이버 보안 위협 동향

2003년 슬래머웜[4] 발생 이래로 지금까지 원자력발전소에 대한 사이버 보안 위협은 지속적으로 발견되고 있다. 특히, 2010년 스턱스넷은 이란의 원자력발전소에서 운영되는 지멘스 S7 PLC에 대해 공격을 수행하였고, 이로 인해 우라늄 원심분리기를 오동작하게 함으로써 사고를 발생시켰다. 이는 그동안 인터넷과 물리적으로 분리된 장치에 대한 공격은 불가능하다는 인식을 종식시키게 되었으며, 비록 직접적인 네트워크 연결이 제공되지 않더라도 다양한 매체들을 이용하여 공격 코드의 원자력발전소 내부 침투가 가능하며, 이로 인한 공격이 성공될 수 있는 사례를 보여주게 되었다. 또한, 2014년 한국수력원자력의 상업용 네트워크 침투를 통한 데이터 유출, 2016년 독일 Gundremmingen 원전 내 일부 시스템의 악성코드 감염 등의 공격이 전 세계적으로 원자력발전소 및 관련 시설에 대해 다양한 형태의 공격이 지속적으로 발견되고 있다([그림 1]참조).

특히, 최근에는 네트워크 뿐만 아니라 다양한 이동저장 매체 등을 통해 EWS(Engineering Work Station)에 접근하고, 이를 통해 PLC 또는 DCS 등에서 동작하는 펌웨어 변조를 시도하거나, 해당 기기에 대한 공격 정보 획득을 위한 사전 준비 단계에서 악성코드가 발견되는 등 다양한 공격들이 나타나고 있다.

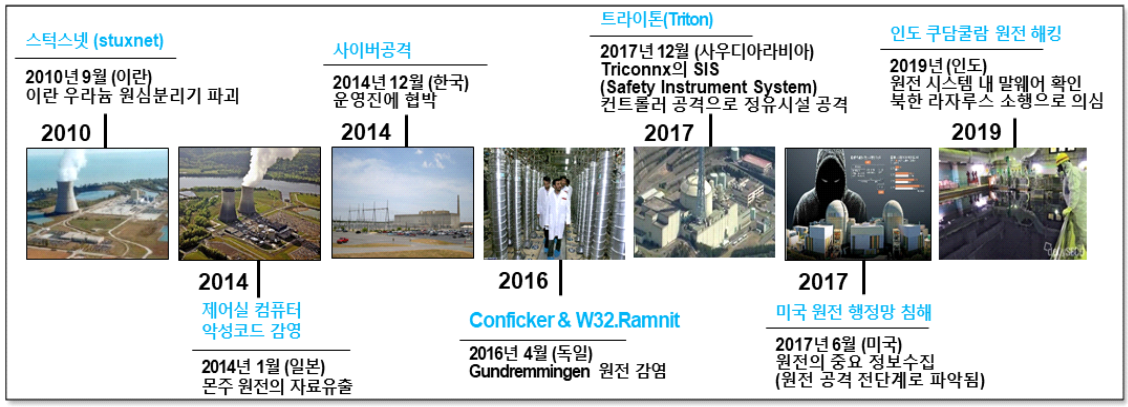
이러한 원자력발전소에 대한 침해 시도는 원자력이라는 특수 물질을 활용하는 핵심 국가 시설의 파괴라는 재앙적인 상황을 야기시킬 수 있는 것으로, 이러한 문제 발생 시 그 피해는 사회 모든 분야에서 전방위적으로 감당할 수 없을 정도의 규모로 나타나게 된다.

이와 같이, 실제 공격으로 인한 피해가 나타나기 시작하면서, 원자력발전소뿐만 아니라 다양한 산업제어시스템이 운영되는 사회 주요 기반시설의 사이버 안전의 중요성이 크게 대두되고 있고, 각 기업의 관련 기술 개발 시도뿐만 아니라 세계 주요 국가들은 정부 차원에서 대응 방안을 모색하고 관련 정책 및 기술 개발에 노력하고 있다.

2.2. 원전 사이버 보안 위협 대응 동향

2.2.1. 국가기관의 보안위협 대응 동향

핵물질 및 원자력시설의 물리적방호 체제를 구축하기 위하여 정부는 2003년 “원자력시설 등의 방호 및 방사능 방재 대책법”[5]을 제정하였다. 관련법과 시행령, 시행규칙의 개정에 따라 사업자의 사이버보안 요건이



〔그림 1〕 원자력발전소 및 사회기반시설 사이버 보안 위협 및 침해 동향

추가되었으며, 관련 고시 “물리적방호규정등의 작성내용의 항목별 세부작성기준”의 개정으로 물리적방호규정에 “원자력시설등의 컴퓨터 및 정보시스템의 보안 대책을 위한 시설·설비 및 그 운영체제에 관한 사항”을 물리적방호규정과 방호비상계획에 포함하여 작성하도록 기준을 제시하였다. 이에 따라 한국원자력통제기술원(KINAC)은 사이버보안에 관한 기술기준인 KINAC/RS-015 “원자력시설등의 컴퓨터 및 정보시스템 보안 기술기준”을 2016년 12월에 개정하여 원자력 사업자들이 기술기준에 따라 정보시스템 보안규정을 작성하도록 기준을 제시하였다.

RS-015는 [그림 2]와 같이 IAEA 기술지침(Technical Guidance)인 NSS 17 “Computer Security at Nuclear Facilities”[6]와 NST 038 “Computer Security Incident Response”[7] 및 미국 원자력규제원회(NRC)에서 발표한 규정(Regulatory Guide)인 RG 5.71 “Cyber Security Programs for Nuclear Facilities”[8]를 기반으로 작성되었다. RG 5.71은 사이버 공격으로부터 원전 디지털 장비를 보호하기 위한 보안 조치로 원전 사이버보안 조직, 대상분석, 심층방호, 보안조치 및 위험평가 등을 통한 원전 디지털 시스템 보호 규제지침이다.

IAEA의 NSS 17은 원자력시설의 사이버보안에 대한 보안 체계로서 원자력시설의 디지털시스템을 보호하기 위한 사이버보안 프로그램 수립방안을 제시하고 있으며, 사이버보안을 위한 관리적 및 이행적 사항을 기술하고 있다. NST 038은 원자력 보안에 영향을 미칠 수 있는 컴퓨터 보안 사고에 대한 비상 계획을 개발 구현 실행하는 것에 관한 내용을 기술한다.

2.2.2. 원전 운영기기 개발 업체 보안위협 대응 동향

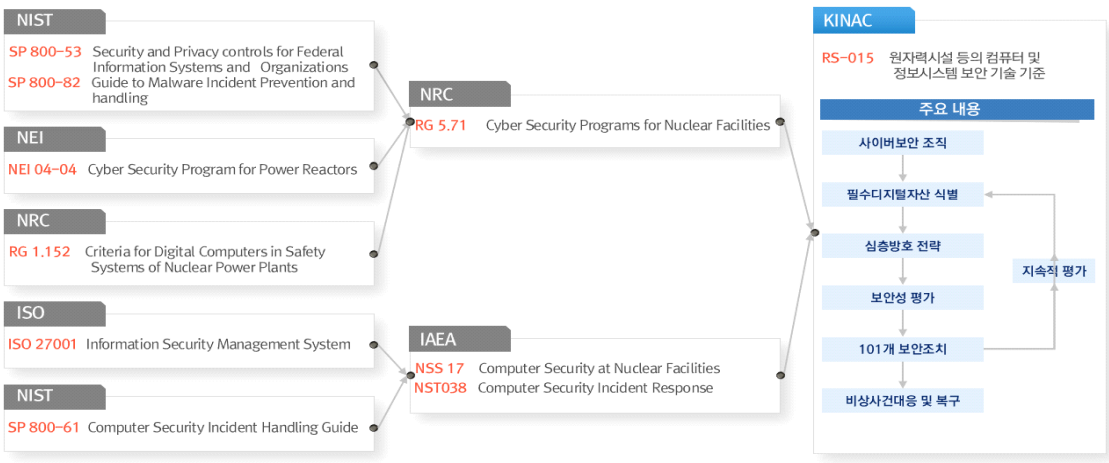
웨스팅하우스(Westinghouse)는 보안업체인 McAfee와 협력을 통해 McAfee의 ESM 등을 웨스팅하우스 제품과 함께 제공함으로써 보안성을 강화하기 위해 노력하고 있다. 또한, SIEM 시스템을 이용하여 기기에서 생성되는 로그를 수집하고 연관성 분석을 통해 RG 5.71과 NEI 08-09[9]에서 요구하는 항목을 만족시킬 수 있도록 지원하고 있다.

슈나이더(Schneider Electronic)는 자체 사이버보안팀을 운영하면서, 제어기를 운영하는 사이트에 대한 보안 컨설팅을 수행하고 있다. 컨설팅에는 기기에 대한 접근제어, 로깅, 패칭 및 성능 감시와 경보 발생처리, 안전한 원격 접속 기능 등과 함께 보안 취약점 확인 등이 포함된다.

지멘스는 기기 단위로 요구되는 다양한 보안 기능을 추가하여 위협에 대비하는 것에 집중하고 있다. 이는 오류 입력에 대한 관리, 비밀정보의 보안성 강화, 접근제어, 펌웨어 무결성 검증, 프로그램 신뢰성 검증, 통신 암호화 등이 포함된다.

2.2.3. 취약점 관리 기술 동향

일반적인 IT환경에서 사용되는 취약점 점검 또는 취



〔그림 2〕 RS-015 개발 개념

약점 스캐닝 도구들은 점검 대상 시스템에 사전에 정의된 점검용 네트워크 패킷을 전달하고, 해당 패킷에 대한 응답을 분석함으로써 해당 시스템의 운영체제, 외부로 제공되는 서비스의 종류 및 버전 등을 확인하는 과정을 통해 취약점을 점검하였다.

그러나, 원자력발전소와 같이 OT(Operational Technology) 환경에서 동작하는 매우 중요한 사회 간접자본 시설 등에 대해서는 직접적인 네트워크 패킷 전송을 통한 취약점 점검이 사실상 매우 어려운 상황이다. 이는 해당 장비들이 매우 오래전에 설치되어 사전에 정의되지 않은 입력이 발생하는 경우 오동작할 가능성이 크기 때문에 네트워크 취약점 분석과정으로 해당 기기에 문제가 발생할 수 있기 때문이다.

따라서, 최근에는 직접적인 취약점 점검이 아닌 수동적인 취약점 점검에 초점이 맞춰져 있다. OT 환경에서의 대부분의 취약점 수집행위는 사전에 수집한 점검대상 정보를 활용한 Off-line 형태의 취약점 확인 또는 점검 대상이 생성하는 네트워크 패킷 수집을 통해 관련된 정보를 수집하여 취약점의 존재 여부를 결정하는 수동적인 취약점 점검행위가 주류를 이루고 있다.

그리고, 취약점 자체를 수집하는 행위보다 수집된 취약점이 얼마나 위험한지를 판단하는 기술 개발이 중요시되고 있다. CVE[10] 형태로 발표되는 취약점은 대부분 IT 환경에서 수집되고, IT 환경에 기반하여 위험도가 CVSS[11] 형태로 제공되는데, OT 환경에서 운영되는 시스템은 IT환경과는 매우 다르기 때문에 동일한 위험도 측정방식을 사용하는 것은 한계가 있기 때문이다. Nessus라는 취약점 점검도구 개발 업체로 유명한 Tenable의 경우, VPR(Vulnerability Priority Rating)[12]이라는 취약점 위험도 레벨을 자체적으로 평가하는 방법을 적용하고 있다. VPR은 취약점이 미칠 수 있는 영향과 실제 해당 취약점이 공격에 활용될 수 있는 정도를 기준으로 취약점의 우선 순위를 지정하기 위해 개발되었다.

ETRI에서는 원전 운영 장치들의 실제 운영 환경 특징과 외부 접근 가능 인터페이스 등을 반영하여 취약점의 위험도를 재계산하고 있다.

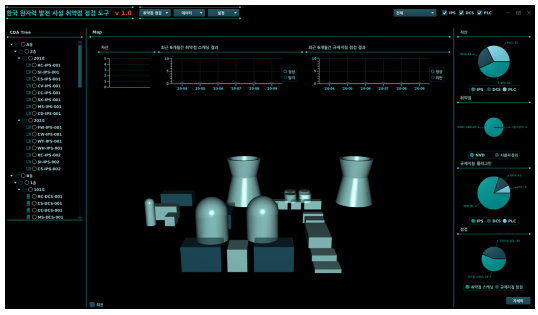
2.3. 규제지침 점검 도구 동향

우리나라에서 원자력발전소에 사이버 보안과 관련하여 적용해야 하는 규제지침은 RS-015가 있다. 현재 이 규제지침의 준수 여부를 판단하는 방식은 검사자가 개별 점검대상 시스템에 접근하여 시스템 설정 등을 확인하고, 관리적인 측면에 대해서는 사전에 준비된 문서를 확인하는 방식 등으로 판단하고 있다.

일부 이 과정을 지원하기 위한 도구가 제공되고는 있으나, 역시 점검행위 자체를 자동화하지는 못했다. 해외에서는 CSET (Cyber Security Evaluation Tool)[13]이라는 도구를 이용하여 ICS 환경과 IT 환경의 운영 자산에 대한 보안성 평가를 지원하는 도구가 활용되고 있는데, NRC RG 5.71 등과 같은 다양한 규제지침들을 선택하고 각 규제지침 항목 준수를 위해 필요한 항목을 제시함으로써 현재 해당 자산이 규제지침을 준수하고 있는지를 체크할 수 있도록 지원하는 도구이다. 국내에는 ㈜이공감의 CSAMS(Cyber Security Assessment and Management System)[14]가 있다. CSAMS는 사이버보안 규제요건 부합성 평가 도구로 평가 시간 단축, 평가 절차 안내, 평가 보고서 생성 및 평가 일관성 확보 지원 등의 특징이 있다.

Ⅲ. 기기 규제지침 점검 및 취약점 위험도 재평가를 위한 도구

ETRI에서 개발한 원전 디지털 I&C 계통 운영장치 취약점 점검도구는 지정된 기기의 RS-015 규제지침 준수 여부를 판단하거나 판단에 필요한 정보를 제공하고 발견된 취약점에 대한 점검대상 기기의 운영환경 특징을 반영하여 위험도를 계산하는 기능을 포함하고 있다. 실제로 상기 점검 도구는 네트워크를 통해 점검 대상 장치가 가지고 있을 것으로 예상되는 취약점을 도출하는 기능과, CDA(Critical Digital Asset)를 건물별로 관



〔그림 3〕 원전 I&C 계통 운영장치 취약점 점검도구

리할 수 있는 기능, 특정 기기에 대한 취약점 검색 및 위험도 재평가 기능 그리고 규제지침 점검 기능 등을 포함하고 있다. [그림 3]은 원전 취약점 점검 도구 초기 화면이다.

3.1. 취약점 검색 및 위험도 재평가 기능

3.1.1. 취약점 검색

본 도구에서는 NVD(National Vulnerability Database)[20]에서 제공하는 최신 취약점 정보를 on/off-line 형태로 자동 업데이트하여, 취약점 확인의 편리성 확보를 위해 키워드 기반으로 검색 가능하도록 제공하고, 검색된 취약점에 대한 위험도를 재평가하는 기능을 제공한다. 특히, 이와 같은 취약점 검색 기능은 앞서 언급한 CDA 정보에 기반하여 자동검색이 가능한 형태로 개발되어, 사용자가 손쉽게 운영 중인 기기와 관련된 취약점 정보를 손쉽게 확인할 수 있다.

NVD에서 제공하는 취약점 정보는 JSON (JavaScript Object Notation)[21] 타입으로 제공되는데, 이를 자체적으로 설계한 취약점 데이터베이스에 이관하여 신속한 검색을 지원한다. 취약점 정보는 인터넷 연결이 가능한 경우 실시간으로 최신 정보를 획득할 수 있으며, 인터넷 접속이 불가능한 경우에는 내려받은 JSON 파일을 이용하여 업데이트를 수행한다.

이렇게 업데이트된 취약점 정보에 대해 제조사, 응용프로그램 또는 서비스명 등의 키워드를 이용하여 관련 취약점 검색 후 확인이 가능하다.

3.1.2. 취약점 위험도 재평가

NVD에서 제공하는 취약점 정보는 기본적으로 CVSS V2 또는 V3 형태의 위험도가 제공되고 있다. 그러나, 이 위험도는 기존 IT 환경에서의 위험도를 도출한 것으로 원전 운영 환경과는 맞지 않는 경우가 많다. 이를 극복하기 위해 원전 운영환경 특징을 반영한 위험도 재평가를 진행하였다. 여기서 원전 운영기기의 운영환경 특징을 정의하기 위한 질의를 [표 1]에 나열한다.

〔표 1〕에 포함되어 있는 질문들은 해당 운영기기의 운영 환경 특징을 표현하는 것으로 공격 벡터를 결정하기 위한 것이다. 해당 질문에 대한 답에 따라 운영환경의 구분이 직접 네트워크 연결, 무선네트워크 연결, 휴대용 매체 및 장비 연결, 공급망 연결, 직접 물리적 접근으로 구분되며, 해당 값에 기반하여 해당 기기의 통신 인터페이스와 사용하는 통신 프로토콜에 따라 공격벡터를 결정한다. 이렇게 결정된 공격벡터를 기반으로 CVSS에서 제공하는 위험도 계산방식을 활용하여 위험도를 재계산하게 된다.

이와 같은 방법으로 실제 취약점에 대하여 관련 접속 및 접근이 불가능한 환경에서 운영되는 기기의 경우 그 취약점의 위험도가 기존 7.5에서 5.7로 감소함을 볼 수 있었다.

〔표 1〕 원전 운영기기 운영환경 특징 질의

운용환경 구분	운용환경 특징값 결정을 위한 질의
직접 네트워크 연결	(1)레벨 3과 4의 CDA 네트워크 인터페이스와 유선 통신 보안이 레벨 1과 2의 통신과 결정적으로 분리되어 있는가? (2)CDA가 같은 보안 레벨의 네트워크 공격 취약점으로부터 보호되고 있는가?
무선 네트워크 연결	(1)CDA가 무선 네트워킹 기능이 없는가? (2)CDA나 CDA 그룹에 무선 통신 어댑터가 있는 경우, 비활성화 되어있는가? (3)CDA나 CDA 그룹에 무선 기능이 활성화 되었을 때, 디자인 혹은 엔지니어링 패키지가 공격벡터를 충분히 무효화 할만큼 암호화를 특정하고 있는가?
휴대용 매체 및 장비 연결	(1)오직 물리적으로만 통제, 식별, 인증, 추적되는 휴대용 저장 장치나 컴퓨터만 CDA나 CDA 그룹에 연결할 수 있게 되어있는가? (2)CDA가 물리적 공격 벡터로부터 안전한 곳에 위치하고 있는가? 혹은 자물쇠나 USB 구멍을 막는 등의 대안적인 물리적 보호 장비가 설치되어 있는가?(노트 : 만약 물리적 접근 공격 벡터가 상위 내용과 무관하다면 YES, 아니면 NO) (3)원자력 사업자가 CDA의 운영 및 유지와 관계 없는 휴대용 저장 매체의 소프트웨어를 제거 혹은 비활성화했는가? (4)원자력 사업자가 CDA의 운영 및 유지와 관계 없는 휴대용 저장 매체의 하드웨어를 제거 혹은 비활성화했는가?

운용환경 구분	운용환경 특징값 결정을 위한 질의
공급망 기반 연결	(1)공급자가 CDA나 CDA 그룹에 설치된 제3자의 모든 소트트웨어 어플리케이션을 승인했는가? (2)소프트웨어 패치나 업데이트를 하기 전에 분리된 지원 시스템이나 테스트 환경에서 검증을 하고 있는가? (3)CDA 공급자를 CDA나 CDA 그룹에 원격접근하지 못하도록 제한하고 있는가? (4)시스템 설치와 운영에 대한 로그 기록을 하고 있는가? (5)사용하는 리커버리 명령이 대체할 부분의 설정을 구체적으로 명시하고 있는가? (6)CDA를 입수 상세 보안이 적용된 장소로 이동시키면서 관리 연속성을 유지하고 있는가?
직접 물리적 접근	(1)CDA나 CDA그룹이 중요 구역(VA)에 위치하고 있는가? (2)CDA나 CDA그룹에 대한 물리적 접근을 영구적 발전소 접근 배지를 지닌 인원과 배지를 지닌 검증된 인원과 동행하는 방문자들에게만 허용하고있는가? (3)CDA나 CDA그룹에 대한 조작을 접근 인증 프로그램을 통해 검증받은 인원에게만 허용하고 있는가? (4)CDA나 CDA 그룹의 HMI 사용을 접근 인증 프로그램을 통해 검증받은 인원에게만 허용하고 있는가? (5)CDA나 CDA 그룹이 보호 구역(PA) 안, 중요 구역(VA) 밖에 위치하는가? (6)CDA나 CDA 그룹이 잠금장치가 있는 방이나 캐비닛에 위치하는가? (7)CDA나 CDA 그룹에 대한 조작을 승인받은 업무 계획을 통해 검증받은 인원에게만 허용하고 있는가? (8)CDA나 CDA 그룹의 HMI 사용을 승인받은 업무 계획을 통해 검증받은 인원에게만 허용하고 있는가?

3.2. 원전 규제지침 자동 점검 기능

원전 규제지침 자동 점검 기능은 RS-015에서 요구하는 규제지침 중 자동 점검이 가능한 항목을 선정하여, 해당 항목에 대한 점검을 자동화하였다. 자동화 방식은 점검 대상 장치에 접근 가능한 프로토콜을 활용하여 해당 규제지침을 준수 여부를 해당 시스템 내의 정보를 활용하여 판단한다. 이는 에이전트를 설치하지 않는 방식으로 검사자가 직접 점검하는 방식과 동일한 방식으로 점검함으로써, 점검 대상 시스템에 미칠 수 있는 영향을 최소화하였다. RS-015는 기술적보안조치, 운영적보안조치, 관리적보안조치로 구분되어 있으며, 각각의 조치에는 각각 5, 6, 2개의 통제 분야가 존재하고 이에 포함되는 통제 항목은 총 101개이다. 이러한 규제지침 중 많은 부분이 컴퓨터 프로그램을 이용한 자동화된 방식으로는 점검이 불가능한 항목들이다. 본 도구는 이러한 자동점검이 불가능한 항목을 제외하고 나머지 항목에 대하여 점검 플러그인을 개발하고 이를 바탕으로 점검을 수행하였다.

점검 플러그인은 운영 장비에서 사용하는 4종의 운영체제별로 구분되어 개발되었으며, 총 DCS용 12개, IPS1용 42개, IPS2용 39개, PLC용 8개의 총 105개 플러그인을 개발하였다.

규제지침 점검 방식은 점검 대상 시스템에 지정된 네트워크 서비스를 통해 접속하고 점검에 필요한 정보를 획득하여 규제지침의 준수 여부를 점검하게 된다. 이때, 어떤 플러그인의 경우에는 직접적으로 준수 여부를 판단하기 어려운 경우가 있으며, 이러한 경우에는 해당 항목의 준수여부를 판단하기 위해 필요한 정보를 수집하여 사용자에게 전달함으로써 사용자가 판단할 수 있게 지원한다.

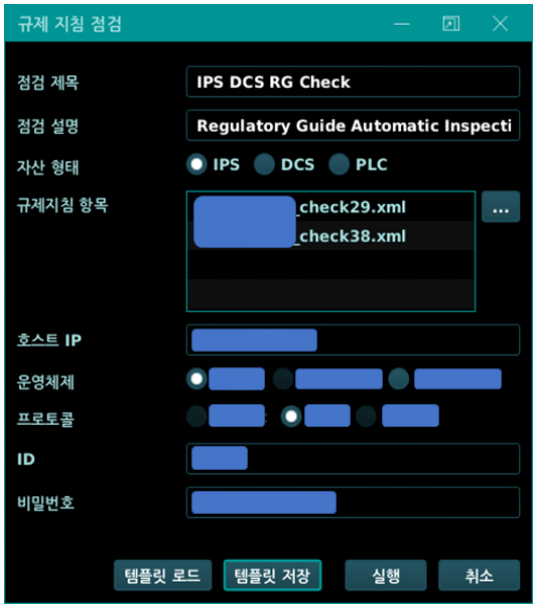
이와 같은 방식의 규제지침 준수 여부 확인 방법은

〔그림 4〕 취약점 위험도 재계산 기능 화면

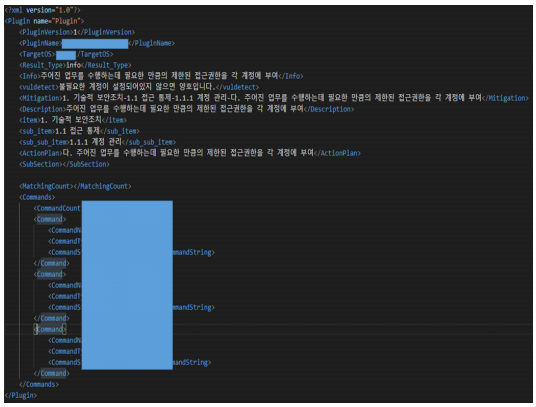
기존에 매우 많은 시간이 소요되던 것을 단축시키는 효과가 있으며, 특별한 에이전트 프로그램을 점검대상 시스템에 설치하지 않기 때문에 미치는 영향을 최소화했다고 할 수 있다. [그림 5]는 점검하고자 하는 규제지침을 선택하는 설정화면이다.

본 규제지침 자동 점검 기능은 새로운 점검 방법이 확인되는 경우, 해당 점검 방법을 플러그인 형태로 구성하여 추가 가능하도록 설계되었다.

플러그인 형태는 xml 형태로 구성되며([그림 6] 참조), 각각의 점검 방법에 따라 점검 방법이 포함되도록



〔그림 5〕 RS-015 규제지침 점검 기능 화면



〔그림 6〕 규제지침 점검 플러그인 예

〔표 2〕 규제지침 점검 플러그인 구성 (xml 타입)

Tag 명	설 명
Plugin	규제지침 플러그인 시작
PluginVersion	플러그인의 버전정보
PluginName	플러그인 명
TargetOS	규제지침 점검 대상 OS 타입
Result_Type	점검 결과타입(info, rs015)
Info	플러그인 정보
vuldetect	점검 결과 판단기준
Mitigation	점검 결과 조치방안
Description	플러그인 설명
item	대분류
sub_item	중분류
sub_sub_item	소분류
ActionPlan	조치항목
SubSection	세부항목
MatchingCount	점검항목의 준수 여부판단 기준 항목 개수
Commands	점검항목 목록
CommandCount	점검항목 개수
Command	점검항목
CommandName	점검항목 명
CommandType	점검항목 타입(CMD Registry)
CommandString	점검항목 명령어
ConditionItem	점검항목 조건
ConditionName	조건 명
ConditionType	조건 타입(int, float, hex, string)
Condition	조건(same : ==, notsame : !=, big : 〉, small : 〈, bigsame : 〉=, smallsame : 〈=, have : +, nothave : *)
ConditionValue	조건 값

구성된다. 실제 점검 플러그인의 일 예를 보면 [표 2]와 같이 구성된다.

Ⅳ. 원전 취약점 점검도구 시험 결과

개발된 취약점 점검도구는 자체 테스트베드와 한국

원자력연구원의 사이버보안 테스트베드에서 시험되었다. 다만, 한국원자력연구원에서 수행한 시험 결과는 공개할 수 없기 때문에 ETRI 내부 테스트베드에서의 점검 결과만을 제시한다. 따라서, 시험 결과는 실제 운영되고 있는 원전 기기에 대한 점검 수행 결과와는 상이할 수 있다.

시험을 위한 테스트베드 구성은 [그림 7]과 같다. 대표적인 IPS, DCS 및 PLC 제품을 활용하여 구성하였으며, 해당 기기는 최초 기본 설정 상태에서 시험이 진행되었다.

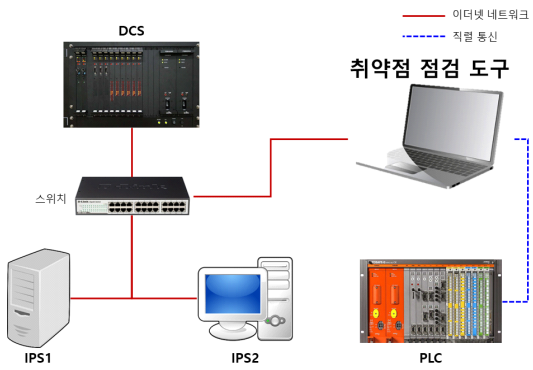
각 기기의 제조사와 제품명 그리고 운영체제 정보는 실제 원자력발전소에서 운영되는 것과 동일하기 때문에 정보보호 차원에서 공개하지 않는다.

취약점 점검도구는 네트워크를 통해 DCS 및 IPS1, IPS2에 대하여 점검을 수행하였으며, PLC에 대해서는 직렬통신(Serial Communication)을 통해 진행되었다. 먼저, 각각의 점검 대상 시스템에 대하여 키워드를 이용한 존재 가능한 관련 취약점을 확인하였고, 도출된 취약점에 대하여, 해당 기기의 운영환경 특징값을 지정하여 위험도를 재계산하였다.

또한, 현재 본 도구에 포함되어있는 규제지침 자동점검을 수행하였고, 그 결과는 각각 [표 3] 및 [표 4]와 같다.

[표 3]을 보면 관련 취약점의 평균 위험도가 대부분 재계산 후 낮아진 것을 볼 수 있다. 이는 기본적으로 제공되는 취약점의 위험도에 비해 운영환경 특징을 반영하여 해당 취약점의 공격 벡터가 제외되면서 위험도가 낮아졌기 때문이다.

규제지침 점검 결과인 [표 4]에서 “정보제공” 부분은 실제로 특정 규제지침을 준수하는지 혹은 준수하지 않는지를 자체적으로 판단하기 어려운 경우, 시험자가 해당 항목의 준수 여부를 판단하기위해 필요한 정보를 수집하여 전달하는 경우를 의미한다. 세부 준수 및 미준수 항목에 대한 설명은 생략한다.



〔그림 7〕 원전 취약점 점검도구 시험 테스트베드

〔표 3〕 점검 대상 관련 취약점 위험도 재계산 결과

점검 대상	평균 위험도	재계산 평균 위험도
DCS	8.4	7.1
IPS1	5.3	5.1
IPS2	8.3	6.9
PLC	-	-

〔표 4〕 RS-015 규제지침 점검 결과

점검 대상	점검 항목 개수	점검여부 판단		정보 제공	점검 소요시간 (분:초)
		준수	미준수		
DCS	12	0	0	12	1:23
IPS1	42	2	2	38	4:36
IPS2	39	4	3	32	6:38
PLC	8	7	0	1	10:35

V. 결 론

본 논문에서는 원자력발전소 계측제어계통에서 운영되는 디지털 장치에 대한 취약점 점검 특히 관련된 취약점의 위험도 재평가와 RS-015 규제지침 점검을 위해 개발된 원전 취약점 점검도구 개발 결과를 소개하였다. 현재 제공되고 있는 취약점 정보에 포함되어있는 위험도는 일반적인 IT환경에 적합한 위험도로 특수한 운영환경에서 동작하는 원자력발전소 계측제어계통의 디지털 장치들의 위험도로 사용하기에는 맞지 않는 부분들이 많았다. 하여, 본 논문에서는 다양한 운영환경 특징을 도출하고 이를 위험도 계산에 반영함으로써 원전 운영환경의 특징이 반영된 실질적인 위험도 측정이 가능한 기술을 개발하였다.

또한, 각 기기의 정보보호 규제지침 준수 여부를 판단하기 위한 도구로 RS-015 규제지침 자동점검 도구를 제시하였다. 기존에 규제지침의 준수 여부를 판단하기 위해서는 점검 대상 장치에 점검자가 직접 로그인을 하여 해당 기기의 설정값을 확인하거나 관련 정보를 수집하여 판단하였는데, 이러한 점검 방식은 매우 오랜 시간

이 소요되었다. 이를 극복하기 위해 본 도구에서는 점검 대상과 점검 방법 항목을 지정하면 해당 점검 항목 점검을 위해 사전에 정의된 플러그인을 이용하여 자동화된 점검 방식으로 수행한다. 이때 모든 점검 항목이 해당 규제지침을 준수하는 지를 판단하는 것은 아니고, 직접적으로 판단이 어려운 경우에는 관련 정보를 수집하여 점검자가 판단할 수 있도록 제공하는 방식을 취한다. 이렇게 개발된 도구는 ETRI 테스트베드와 한국원자력연구원 테스트베드 상에서 시험이 진행되었으며, ETRI 테스트베드 상에서 진행한 점검 결과를 제시하였다.

향후에는 보다 실질적인 위험도 계산을 위한 계산식 보완이 진행될 예정이며, 동시에 점검 가능한 규제지침 항목 증대를 위한 연구가 진행될 예정이다.

참 고 문 헌

[1] APR-1400 노형, 한국전력기술, 원자력사업 APR-1400, https://www.kepco-enc.com/ portal/contents.do?key=1240

[2] 허재준, 이상철, “스턱스넷의 감염 경로와 대응방안”, 정보보호학회지, 제21권 제7호 pp. 23-29, 2011.10

[3] 한국원자력통제기술원, *“원자력 시설 등의 컴퓨터 및 정보시스템 보안 기술기준,”* KINAC RS-015, 2016.

[4] 김우년, “원전 사이버보안 체계 개발 추진방안”, NUPIC2012, 2012.11.

[5] 법률 제 17347호, 2020.6.9. 개정, *원자력 시설 등의 방호 및 방사능 방재 대책법,* 2020, http://law.go.kr/법령/원자력시설등의방호및방사능방재대책법

[6] IAEA, *Computer Security at Nuclear Facilities,* IAEA Nuclear Security Series No.17, Technical Guidance, 2011

[7] International Atomic Energy Agency. *“Computer Security Incident Response Planning at Nuclear Facilities TDL005 (NST-038)”,* (2016).

[8] U,S.Nuclear Regulatory commission (U.S.NRC), *Regulatory Guide 5.71(R.G 5.71), “Cyber Security Programs for Nuclear Facilities”,* 2010.

[9] Nuclear Energy Institute(NEI), NEI 08-09(rev.6) *“Cyber Security Plan for Nuclear Power Reactors.”,* 2010.

[10] CVE Board, *Common Vulnerabilities and Exposures (CVE®) Numbering Authority (CNA) Rules version 3.0,* 2020.02

[11] First, CVSS, *Common Vulnerability Scoring System version 3.1, User Guide Revision 1,* https://www.first.org/cvss/v3.1/user-guide

[12] Wei Tai, *“What is VPR and How is it different from CVSS?”*, Tenable, 2020. 04., https://www.tenable.com/blog/what-is-vpr-and-how-is-it-different-from-cvss

[13] CSET, Cybersecurity and Infrastructure Security Agency, https://github.com/cisagov

[14] E공감, CSAMS 브로셔, 가동중 원자력 시설에 대한 사이버보안 규제요건 부합성 평가 도구

[15] 김도연, “원전 계측제어계통의 안전 네트워크 설계 및 평가를 위한 보안 기준,” 한국전자통신학회, *한국전자통신학회 논문지,* 제9권, 제2호, 2014, pp.267-272.

[16] 정성민·박기용, “원전 계측제어시스템에 적합한 운영적 및 관리적 보안 요건,” 디지털산업정보학회 공동학술대회, 서울, 2019, pp.175-178.

[17] 이철권, “원전 계측제어시스템 사이버보안 기술동향,” 한국정보보호학회, *정보보호학회지,* 제22권, 제5호, 2012, pp.28-34.

[18] 정성민, “원전 안전계통의 사이버보안 위협 및 대응”, *디지털산업정보학회 논문지* 제16권 제1호, pp. 99-109, 2020. 3

[19] 김인경, 변예은, 권국희, “원전디지털자산 사이버보안 규제 요건 개발을 위한 보안조치 적용 방안에 대한 분석”, *정보보호학회 논문지,* 제29권, 제5호, pp. 1077-1088, 2019.10

[20] NVD, National Vulnerability Database, NIST Information Technology Laboratory, https://nvd.nist.gov

[21] JSON, JavaScript Object Notation, https://www.json.org/json-ko.html

〈저 자 소 개〉

최 양 서 (Choi, Yangseo)

정회원

1996년 2월 : 강원대학교 전자계산학과 졸업
2000년 8월 : 서강대학교 컴퓨터공학과 석사
2011년 8월 : 충남대학교 컴퓨터공학과 컴퓨터통신 및 보안 박사
2000년 6월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원
<관심분야> 정보보안, ICS보안, 네트워크 보안, 취약점분석

안 개 일 (An, Gaeil)

정회원

1993년 2월 : 충남대학교 컴퓨터공학과 졸업
1995년 2월 : 충남대학교 컴퓨터공학과 석사
2001년 8월 : 충남대학교 컴퓨터공학과 박사
2001년 8월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원
<관심분야> 네트워크보안, 제어시스템보안, 국민생활사이버안전