원자력시설의 취약점 정보관리시스템 구축 및 활용방안에 관한 연구

김상우*, 이채창*, 송동훈*, 박재만**
*한국원자력통제기술원
**(주)SNTWorks
kjoey@kinac.re.kr

A Study on the Building & Application Method of Vulnerability Information Management Systems at Nuclear Facility

Sangwoo Kim*, Chae-Chang LEE*, Dong-Hoon Song*, Jae-Man Park**,
*Korea Institute of Nuclear Nonproliferation And Control
**SNTWorks

요 약

최근 기반시설의 제어시스템을 대상으로하는 악성코드와 취약점 등이 지속적으로 보고됨에 따라 기반시설의 사이버위협에 대한 긴장감 고조되고 있다. 이와 같은 최신 사이버위협들을 예방하기 위해서는 주기적인 취약점 점검 및 제거가 필수적이며, 이를 위해서는 먼저 해당 제어시스템에 대해 기 알려진 취약점 정보를 수집할 필요가 있다. 이에 본 논문에서는 공개 취약점 정보들을 활용해 제어시스템과 관계된 취약점 정보의 수집, 관리 및 활용을 위한 제어시스템 취약점 정보관리시스템의 설계 및 구축 방안을 제시하였다. 또한, 정보관리시스템 구축 시 필수디지털자산의 정보유출 사고를 예방을 위해 고려해야할 사항을 제안한다.

1. 서론

최근 IronGate, PLCWorm 등 제어시스템을 목표로 하는 악성코드가 지속적으로 보고되고 있으며, 유명 보안 컨퍼런스에서는 현재 국외 발전소에서 사용 중인 방사선감시 시스템의 취약점이 발표 되는 등 기반시설의 사이버보안 위협에 활용되는 취약점 발견 사례들이 꾸준히 증가하고 있다.

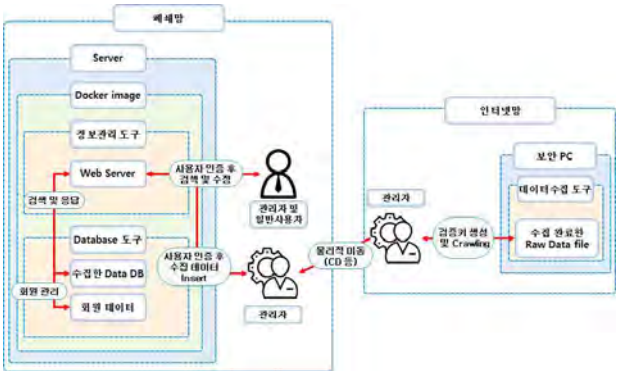
한국 원자력시설의 경우 이와 같은 최신 사이버위협들을 예방하기 위해 '원자력시설의 컴퓨터 및 정보시스템 보안 규정(RS-015)에 따라 필수디지털자산의 취약점 존재 여부를 주기적으로 평가하고 제거하도록 규제하고 있으며, 미국 또한 이와 동일한 내용의 규제를 수행하고 있다[1, 2]. 이를 위해 원자력사업자는 우선 해당 제어시스템의 기 알려진 취약점 정보를 수집할 필요가 있다.

본 논문에서는 주기적인 취약점 및 제거를 위해 공개 취약점 정보 중 기반시설 제어시스템과 관계된 정보를 수집하고, 수집된 정보들로부터 원자력시설의 필수디지털 자산과 관계된 정보를 추출 및 분석하기 위한 제어시스템 취약점 정보관리 시스템(이하 CV-IMS)의 구축 방법을 제시하였다. 또한, 설계 및 구현 시 동 시스템을 통해 정보 유출사고가 일어나는 것을 방지하기 위한 데이터 검증 및 망분리 방안을 적용하였으며, 최종적으로 원자력시설의 사이버보안을 위한 동 정보시스템의 활용 방안을 제시하였다.

2. 시스템 설계 및 구현

2.1 정보관리시스템 개발 요구사항

본 논문에서 제안하는 CV-IMS는 인터넷 상에서 정보를 수집하는 수집도구, 수집한 데이터를 가공하여 데이터베이스에 삽입하기 위한 데이터베이스 도구, 정보 검색, 삽입, 삭제가 가능한 정보관리 도구로 구성된다. 이와 같은 구성은 일반적인 데이터수집 서버와 유사하다. 그러나 제어시스템 관련 취약점 수집을 위해 웹 크롤링 및 데이터 파싱을 수행하는 점과, 사이버공격으로 인한 필수디지털자산 목록 유출 예방을 위해 [그림 1]과 같이 크롤러와 데이터베이스의 네트워크를 분리하고, 원시 데이터를 통해 데이터를 입력 시 무결성 검증을 위한 보안 기능 부분에 있어 차이점이 존재한다.

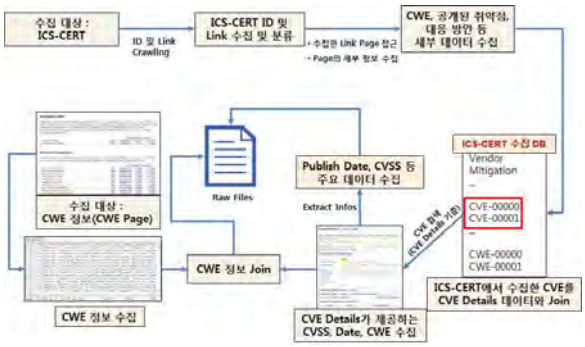


(그림 1) CV-IMS 시스템 구조

2.2 정보관리시스템 구축 방법 연구

CV-IMS의 시스템 구조는 크게 정보수집도구(크롤러), 데이터베이스 도구와 정보관리 도구 세 가지로 구분할 수 있다.

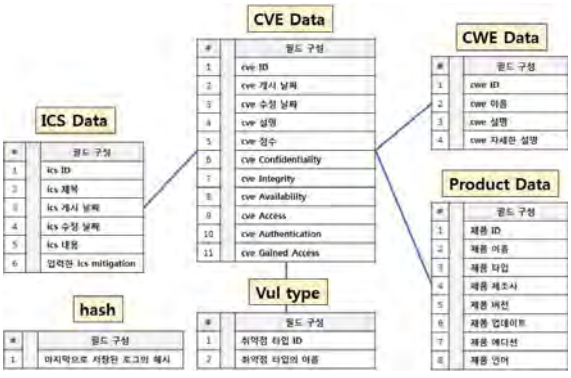
우선 수집 도구는 인터넷이 연결된 PC 환경에서 크롤러 프로그램을 통해 기반시설 취약점 데이터베이스를 운영중인 ICS-CERT의 모든 정보를 수집한다. 또한, 데이터 파싱을 통해 해당 취약점 정보와 관련된 CVE(Common Vulnerabilities and Exposures)가 정보가 존재할 경우, 관련 정보를 CVE-Details에서 해당 정보를 수집한다. 최종적으로 CWE에서 제어시스템에 주로 사용되는 실시간 운영체제 등의 플랫폼을 키워드로 검색된 데이터와 ICS-CERT를 통해 수집된 데이터를 조인 구문을 통해 중복 데이터를 제거한 후 원시 데이터 파일로 저장한다. [그림 2]는 이와 같은 과정을 그림으로 표현한 것이다[3,4,5].



(그림 2) 데이터 크롤링 과정

추가적으로 크롤러는 데이터를 수집하기 전 사용자로부터 검증키를 입력받으며, 입력받은 값은 해시 데이터로 변환되어 함께 저장된다. 이를 통해 생성된 원시 데이터파일 변조를 통해 폐쇄망으로 구축된 정보관리시스템에 대한 사이버공격이 수행되는 것을 예방할 수 있다.

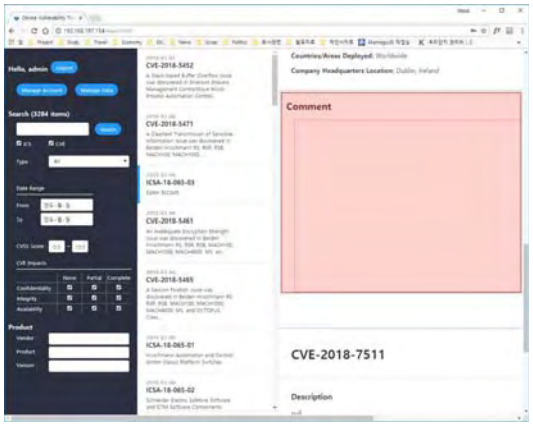
데이터베이스도구는 수집도구로부터 생성된 원시 데이터파일을 가공 및 데이터베이스에 삽입하는 역할을 수행한다.



(그림 3) 데이터베이스 구조

관리자는 데이터베이스를 삽입하는 과정에서 수집 도구에서 입력하였던 검증키를 입력해야 하며, 이를 통해 생성된 해시 데이터가 일치하는 경우에만 데이터베이스 삽입이 이루어진다. 데이터베이스 구조는 [그림 3]과 같다.

정보관리 도구는 데이터의 삽입, 삭제가 가능한 관리자 기능과 검색만이 가능한 사용자 기능으로 권한이 분리되어 있다. 취약점, 제조사, 플랫폼 등을 키워드로 검색이 가능한 검색 기능이 포함한다. 또한, 기 입력된 취약점 정보에 대한 추가적인 대응방안 등의 정보 입력을 위해 [그림 4]와 같은 취약점 별 메모 기능을 제공한다.



(그림 4) CV-IMS 취약점 별 메모 기능

정보관리 도구는 다중 사용자 접속 및 편의성 증대를 위해 웹서버 형태로 구성되며, 호스트 운영체제의 외부 노출을 최소화하기 위해 코드와 종속성을 함께 패키징 하는 도커와 같은 응용프로그램 계층의 가상환경을 활용한다.

3. 결론 및 활용 방안

본 논문에서는 공개 취약점 정보 중 기반시설 제어시스템과 관계된 정보를 수집하는 정보수집 도구, 원자력시설의 필수디지털 자산과 관계된 정보 관리 및 검색을 위한 데이터베이스 도구, 정보관리 도구로 구성된 제어시스템 취약점 정보관리 시스템(CV-IMS)의 구축 방법을 제시하였다. CV-IMS와 같은 구조로 취약점 정보관리시스템을 구현할 경우, 신규 취약점정보를 주기적으로 수집 및 관리할 수 있을 뿐만 아니라 수집도구와 정보관리 도구의 네트워크 망 분리와 원시 데이터파일 무결성 검증을 통해 인터넷을 통해 수행되는 정보관리시스템에 대한 사이버공격을 예방할 수 있다.

본 연구에서는 CV-IMS(제어시스템 취약점 정보관리 시스템)의 정보수집도구, 데이터베이스 도구, 정보관리

도구 구축 방안에 따라 구현된 [그림 4]와 같은 프로토타입의 정보관리시스템을 구현하였으며, 그 결과 3000개 이상의 제어시스템과 관련된 취약점 정보들을 수집하였다.

한국의 원자력사업자는 규제기준에 따라 주기적으로 취약점을 분석하고 제거해야할 의무가 있다. 시스템 보안 담당자들은 본인이 담당하는 시스템의 취약점을 분석하기에 앞서 CV-IMS와 같은 시스템을 활용해 담당 시스템에 존재하는 취약점과 대응방안에 관련된 정보를 취득할 수 있을 것이다. 또한, 원자력시설의 사건 탐지방안 마련 시 알려진 공격들에 탐지절차를 마련에 동 시스템의 정보들을 활용할 수 있다. 규제기관의 경우 원자력시설의 방호 및 방재법에 따라 정기적으로 수행되는 정기검사 시 동 시스템을 활용해 사업자의 취약점 점검 및 제거를 평가할 수 있을 것이다.

참고문헌

[1] 한국원자력통제기술원, “원자력시설등의 컴퓨터 및 정보시스템 보안 기술기준”, KINAC/RS-015, 2016.
기술기준”, KINAC/RS-015, 2016.
[2] Guide, Regulatory. "5.71." Cyber Security Programs for Nuclear Facilities, US Nuclear Regulatory Commission (2010).
[3] ICS-CERT. https://ics-cert.us-cert.gov/advisories
[4] MITRE. https://www.cvedetails.com
[5] MITRE, https://cwe.mitre.org