JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 22, No. 10: 1392~1397, Oct. 2018

원전 적용을 위한 네트워크 기반 취약점 스캐너의 비교 분석

임수창[1] · 김도연[1*]

Comparative Analysis of Network-based Vulnerability Scanner for application in Nuclear Power Plants

Su-chang Lim[1] · Do-yeon Kim[1*]

[1*]Department of Computer Engineering, Sunchon National University, Sunchon 57922, Korea

요 약

원자력 발전소는 주요 국가에서 관리하는 핵심 시설로 보호되고 있으며, 원자력 발전소의 설비들에 일반적인 IT 기술을 적용하여 기존에 설치된 아날로그 방식의 운용자원을 제외한 나머지 자산에 대해 디지털화된 자원을 활용하는 비중이 높아지고 있다. 네트워크를 사용하여 원전의 IT자산을 제어하는 것은 상당한 이점을 제공할 수 있지만 기존 IT자원이 지닌 잠정적인 보안 취약점(Vulnerability)으로 인해 원자력 시설 전반을 위협하는 중대한 사이버 보안 침해사고를 야기할 수 있다. 이에 본 논문에서는 원전 사이버 보안 취약점 규제 요건과 기존 취약점 스캐너의 특징 및 이들이 지닌 요건들을 분석하였고, 상용 및 무료 취약점 스캐너를 조사 하였다. 제안된 적용 방안을 바탕으로 취약점 스캐너를 원전에 적용할 시 원전의 네트워크 보안 취약점 점검 효율성을 향상시킬 수 있을 것으로 판단된다.

ABSTRACT

Nuclear power plants(NPPs) are protected as core facilities managed by major countries. Applying general IT technology to facilities of NPPs, the proportion of utilizing the digitized resources for the rest of the assets except for the existing installed analog type operating resources is increasing. Using the network to control the IT assets of NPPs can provide significant benefits, but the potential vulnerability of existing IT resources can lead to significant cyber security breaches that threaten the entire NPPs. In this paper, we analyze the nuclear cyber security vulnerability regulatory requirements, characteristics of existing vulnerability scanners and their requirements and investigate commercial and free vulnerability scanners. Based on the proposed application method, we can improve the efficiency of checking the network security vulnerability of NPPs when applying vulnerability scanner to NPPs.

키워드 : 원자력 발전소, 네트워크 보안, 보안 취약점, 네트워크 기반 취약점 스캐너

Key word : Nuclear Power Plants, Network Security, Security Vulnerability, Network based Vulnerability Scanner

Received 31 August 2018, **Revised** 31 August 2018, **Accepted** 11 September 2018

*** Corresponding Author** Do-Yeon Kim(E-mail:dykim@scnu.ac.kr, Tel:+82-61-750-3628)
Department of Computer Engineering, Sunchon National University, Sunchon 57922, Korea

Open Access http://doi.org/10.6109/jkiice.2018.22.10.1392 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

진보화된 IT 산업은 기존 아날로그 방식의 정보처리 과정을 적용하던 산업현장을 디지털화 및 자동화하는데 도움을 주었으며, 이러한 산업을 다양한 분야에 적용함으로써 이 시대의 핵심기술로 자리잡고 있다. 이러한 동향은 국가기반시설로 통제받고 있는 원전에서도 나타나는데, 기존 원전 설계시 장착되는 아날로그 방식의 운용자원을 제외한 나머지 자산에 대해 디지털화된 자원을 활용하는 비중이 높아지고 있다[1-2]. 이러한 경향으로 IT 자원이 지니고 있는 보안 취약점(Vulnerability)으로 인해 원자력 시설 전반을 위협하는 중대한 사이버 보안 침해사고가 발생할 수 있다. 이러한 결과는 원전 사고에서 더 나아가, 원전 운전중단과 파손을 야기함으로써 국가적 재난에 이르는 심각한 사고를 일으킬 수 있다는 문제가 제기되고 있다[3-6].

네트워크를 사용하여 원전의 IT자산을 제어하는 것은 관리자에게 상당한 이점을 제공할 수 있지만, 네트워크가 지닌 잠재적인 보안 취약점으로 인해 치명적인 결과를 초래할 수 있다. 이러한 문제점을 해결하기 위해, 네트워크기반 취약점 스캐너(Network based vulnerability scanner)를 원전에 적용할 필요가 있다. 취약점 스캐너는 컴퓨터 시스템, 네트워크 또는 응용프로그램들의 약점을 평가하고 찾아내기 위해 제작된 컴퓨터 프로그램으로서, 방화벽, 라우터, 웹서버, 응용 프로그램 서버와 같은 네트워크 기반 자산에 있는 잘못 구성된 시스템, 결함이 있는 소프트웨어와 관련된 취약성을 식별하고 탐지하는데 사용된다. 또한 시스템 공급자, 시스템 관리 활동 또는 사용자 활동에서 비롯될 수 있는 정보 시스템(컴퓨터, 네트워크 시스템, 운영체제 및 소프트웨어 응용프로그램 등)의 다양한 취약점을 평가 할 수 있다[7].

시스템 공급자에 의한 취약점은 소프트웨어 버그, 운영체제 패치 누락, 취약한 서비스, 안전하지 않은 시스템 구성, 웹 응용프로그램 취약성을 포함하며 시스템 관리 활동에 의한 취약점은 적절치 않은 시스템 구성 및 승인되지 않은 시스템 변경, 암호 보호 정책 부재 등을 포함하고 있다. 또한 사용자 활동에 의한 취약점은 허가받지 않은 사용자와 디렉토리 공유, 바이러스 검색 소프트웨어 실행 실패, 시스템 백도어 도입 등의 악성 활동 등을 포함하고 있다.

본 논문에서는 원전에 적용하기 위한 네트워크 기반 취약점 스캐너를 비교 분석하였다. 논문의 Ⅱ장에서는 취약점 형태에 따라 호스트기반, 네트워크기반 스캐너를 분석하였고, Ⅲ장에서는 네트워크 스캐너의 장단점에 대하여 서술하였으며, Ⅳ장에서 네트워크 기반 상용, 오픈형 스캐너에 대하여 서술한다. Ⅴ장에서는 네트워크 기반 취약점 스캐너 선정 기준 및 운영상의 문제점을 분석하고, 마지막 Ⅵ장 네트워크기반 취약점 스캐너의 원전 적용방안을 끝으로 논문을 마무리하였다.

Ⅱ. 취약점 스캐너 분류

2.1. 호스트 기반

호스트 기반 스캐너는 스캔 대상이 되는 호스트에 설치되며, 운영체제의 특정 서비스 및 구성 세부 정보와 같은 하위 수준의 데이터에 직접 접근 할 수 있다. 따라서 쉽게 예측 가능한 암호를 사용하거나 암호 없이도 위험한 사용자 활동을 파악할 수 있다. 또한 의심스러운 파일 명, 예상치 못한 시스템 파일 또는 장치 파일, 예정에 없던 상위 권한이 부여된 프로그램 검색 등 적절한 절차를 거치지 않는 사용자가 시스템에 침입하여 시스템을 손상 시켰음을 나타내는 징조를 감지 할 수 있다. 호스트 기반 스캐너는 시스템(또는 파일 시스템)에 대한 검사를 수행할 수 있다.

2.2. 네트워크 기반

네트워크 기반 스캐너는 일반적으로 네트워크상의 다른 호스트를 검색하는 단일 시스템에 설치된다. 취약한 웹 서버, 공급 업체가 제공하는 소프트웨어의 위험성 및 네트워크 및 시스템 관리와 관련된 위험과 같은 치명적인 취약점을 탐지하는데 도움을 준다.

네트워크 기반 스캐너의 다른 유형은 다음과 같다[8]. 첫 번째로 원격 시스템의 열린 네트워크 포트 목록을 결정하는 포트 스캐너가 있으며, 두 번째로 웹 서버 원격 웹 서버에서 발생할 수 있는 잠재적 취약성 (예 : 잠재적으로 위험한 파일 또는 CGI)을 평가하는 스캐너를 제공한다. 웹 응용 프로그램 스캐너 (예 : 크로스 사이트 스크립팅 및 SQL 삽입)가 웹 서버에서 실행되는 웹 응용 프로그램의 보안 측면을 평가한다. 웹 응용 프로그램 스캐너는 프로그램의 모든 측면에 대해 포괄적인 보안 검사를 제공 하지 못한다. 웹 응용 프로그램의 테스트를 보

완하기 위해 수동으로 추가 검사 (예 : 로그인 시도가 여러 번 잘못된 로그인 시도 후에 잠겨 있는지 여부)가 필요하다.

Ⅲ. 네트워크 기반 취약점 스캐너의 장단점

3.1. 취약점 스캐너의 장점

취약점 스캐너의 장점은 세 가지 정도로 축약 할 수 있다. 첫 번째로, 알려진 취약점을 사전에 탐지하고 처리 할 수 있다. 스캐너를 사용하여 지속적으로 보안평가를 수행함으로써 시스템 내부 및 외부 관점 모두에서 네트워크에 존재 가능한 보안 취약점을 쉽게 식별 할 수 있다. 두 번째로, 새로운 장치 또는 새로운 시스템의 승인없이 네트워크에 연결되어 전체 시스템 및 네트워크 보안을 위태롭게 만드는 악의적 목적을 지닌 시스템을 식별하는데에 도움을 준다. 마지막으로, 취약성 스캐너는 네트워크상의 모든 장치의 인벤토리를 확인하는 데에 도움을 준다. 인벤토리에는 장치 유형, 운영 체제 버전 및 패치 수준, 하드웨어 구성 및 기타 관련 시스템 정보를 포함하고 있다. 이러한 정보는 보안 이력 관리 및 침입 발생 및 사후 처리 추적에 유용하다.

3.2. 취약점 스캐너의 단점

네트워크 기반 취약점 검색에는 몇 가지 중요한 단점이 존재한다[9]. 네트워크 스니핑 및 탐색과 마찬가지로 이러한 유형의 검색은 활성화된 시스템에 대해서만 취약점을 발견할 수 있다. 이는 일반적으로 표면 취약점 (surface vulnerabilities)을 다루며, 검색된 네트워크에 내재된 전반적인 위험 수준을 해결할 수 없다. 프로세스 자체는 고도로 자동화되어 있지만 취약성 검색 프로그램은 높은 오 탐지율 (false positive error rate)을 지닐 수 있다. 즉, 취약점 데이터베이스에 발견된 취약점이 존재하지 않는 경우 이것이 취약점인지 아닌지에 관계없이 취약점으로 판단하여 관리자에게 보고한다. 또한, 네트워킹 및 OS 보안 전문 지식을 갖춘 사용자가 이 결과를 자체적으로 해석해야한다. 또한 네트워크 기반 취약점 검색은 포트 검색보다 많은 정보를 필요하기 때문에 호스트의 취약점을 쉽게 식별 할 수 있지만 포트 검색보다 훨씬 많은 네트워크 트래픽을 발생시키는 경향이 존재한다. 이는 검색 대상이 되는 호스트, 네트워크, 스캔 트래픽이 통과하는 네트워크 세그먼트에 부정적인 형향을 미칠 수 있다. 취약성 검사기에는 비 전문가에 의해 스캔된 네트워크에 부정적인 영향을 줄 수 있는 DoS 공격에 대한 네트워크 기반 검사도 포함 되어있다. 네트워크 기반 스캐너는 때때로 DoS 공격 테스트를 억제하여 호스트에 영향을 주는 위험을 감소시킨다.

Ⅳ. 상용 또는 오픈형 네트워크 기반 취약점 스캐너

4.1. 상용 네트워크 기반 취약점 스캐너

- ImmuniWeb[10] : High-Tech Bridge사에서 제작한 스캐너로서, 기계학습 및 인공지능을 기반으로 취약점 검색을 수행한다. 지능화된 침입 테스트를 사용하여 웹 사이트 및 응용프로그램의 결함을 감지한다. 취약점 검색에 사용되는 기계 학습 알고리즘은 3주마다 업데이트 되므로, 새로 발생 되는 위협요인에 강건히 대응 할 수 있다.
- Netsparker[11] : Windows 응용 프로그램 또는 웹 응용 프로그램에 사용할 수 있는 침투 테스트 도구와 보고(report) 도구가 포함 되어있다. 클라우드 기반 스캐너를 제공하며, 수 천개의 프로그램에 대한 보안 결함 및 잠재적 취약성을 스캔 할 수 있는 엔터프라이즈 워크 플로우 도구가 내장되어 있다.
- Nessus[12] : 시스템의 중요한 데이터, 잘못된 시스템 구성, 기본 암호 등을 제어하거나 액세스 할 수 있는 취약점을 검색하기 위한 도구를 제공한다. 응용 프로그램 뿐만 아니라 운영체제, 데이터베이스의 취약점을 검색하는 도구 또한 제공한다.

4.2. 오픈형 네트워크 기반 취약점 스캐너

- OpenVAS[13] : Linux에 한정된 취약점 스캐너로서, 네트워크 검사(Network Vulerability Tests)를 매일 업데이트 한다. 설치 및 사용에 접근성이 어렵지만 무료 프로그램으로서 가장 많은 기능을 지닌 보안 스캐너이다. 수 천개의 취약점을 검사하고 이와 동시에 검사 결과에 대한 기록, 오 탐지 검사를 제공한다.
- Retina CS Community[14] : 상용 공급 업체가 무료로 제공하는 프로그램으로, 최대 256개의 IP를 검색

및 관리를 지원한다. 이 프로그램은 Windows Server 2008이상에 설치되며 IIS 서버를 활성화 하기 위해선 Microsoft SQL 2008 이상을 설치해야 사용가능하다. 하지만 상용 프로그램에 비해 제한된 기능을 지니고 있다.

- Microsoft Baseline Security Analyzer (MBSA)[15] : Windows에 기반한 취약점 검색 프로그램으로서 네트워크의 특정 컴퓨터를 지정하거나 IP 주소를 지정하여 IIS 및 SQL 관리 취약점, 암호, Windwos 업데이트 등의 보안 구성 오류를 식별한다. 비록 고급 Windows 설정, 드라이버, Microsoft 이외의 회사에서 제작한 소프트웨어 및 네트워크 관련 취약점을 검색하지 못하지만 일반적인 보안 위험을 최소화 하는데 도움을 준다.

Ⅴ. 원전 사이버보안 취약점 점검 규제 요건

5.1. 원전 사이버보안 규제지침

미국 원자력규제위원회(Nuclear Regulatory Commission)에서 발간한 R.G. 5.71[16]은 악의적 목적을 지닌 사용자 또는 단체의 사이버 공격으로부터 원자력발전소의 컴퓨터, 통신 시스템 및 네트워크 등 디지털화된 설비를 보호하기 위해 규정된 규제 지침으로 미 연방법 10CFR73.54에 명시된 사이버 보안 법령을 세분화 한 것이다. R.G. 5.71은 디지털 자산이 지닌 중요도에 따라 보호되어야 할 요소들을 선정하여 주요 디지털 자산(CDA : Critical Digital Asset)으로 구분하고 있다.

사이버 보안 위협으로부터 CDA를 보호하기 위해 다양한 보안 통제수단과 방어 요소를 적용하고 있으며, CDA의 SSEP(Safety, Security, Emergency Preparedness) 기능 수행 여부에 따라 사이버 보안 적용 범위를 정의하고 있다. R.G. 5.71은 CDA 식별과 방어 요소 적용, 디지털 컴퓨터, 통신시스템 및 네트워크 분석 이외에 잠재적인 사이버 위협으로부터 CDA를 보호하고 보안 수명주기(Security Life Cycle)활동을 수행하기 위한 보안 프로그램을 설치/유지하도록 명시하고 있다.

5.2. 취약점 점검 규제 요건

원전의 안전계통과 안전 유지를 위해 필수적인 계통, 보안 기능 및 비상대응 설비, 그리고 이들을 보완하는 계통, 네트워크 와 통신계통 및 디지털 컴퓨터를 보호하기 위해 적용되는 R.G. 5.71에서는 원전의 기술적/운영적/관리적 측면에서 통제하기 위한 원전 사이버 보안 계획서를 작성하도록 규정하고 있다.

5.3. 취약점 점검 규제 요건 분류

R.G. 5.71 규제지침에 정의된 다양한 요건 중, 취약점에 관련한 내용은 총 42개 항목으로 나열되어 있으며, 관련 내용에 따라 다음 4가지 요건으로 축약하여 분류하였다.

- 취약점 평가 및 스캔 수행 필요성에 관련한 요건
- 취약점 스캔과 관련된 세부사항에 대한 요건
- 소스코드 분석을 통한 취약점 점검 요건
- SSEP 기능 및 성능과 보안 통제에 대한 요건

5.4. 취약점 점검 규제 요건 분석

4개의 항목으로 분류된 각각의 취약점 요건 분석의 내용은 다음과 같다[4].

5.4.1. 취약점 평가 및 스캔 수행 필요성에 관련한 요건

이 유형의 요건은 원전 계통에 설치된 IT 설비들에 대한 사이버 보안 유지를 위해 취약점 평가와 스캔이 필요하다는 점을 강조한다. 보안 프로그램이 마련된 후, 라이센시(Licensee)는 반드시 사이버 위험에 대한 평가와 관리를 수행하여야 하며, 보안수명주기 안에 취약점 검사 및 평가를 포함해야 한다. 이러한 이유는 끊임없이 변화하고 새로이 발생하는 다양한 사이버 위협과 취약점에 대응하여 강건히 시스템을 유지하도록 취약점 점검 도구가 반드시 갖추어야할 요건이다.

5.4.2. 취약점 스캔과 관련된 세부사항에 대한 요건

이 요건은 취약점 스캔의 주기적 수행, 취약점 스캔 도구 및 기술 적용과 같은 취약점 스캔의 전반 내용에 관한 내용을 서술하고 있다. 라이센시는 CDA 보안에 영향을 미칠 수 있는 잠재적 취약점이 발견된 경우 모든 CDA에 대해 정기적적으로 취약점 스캔을 수행하여야 하고, 도구 간의 상호 운용성 촉진 및 관리 프로세스의 일부를 자동화할 수 있는 취약점 스캔 도구와 방법을 채택하여야 한다. 또한 취약점 스캔 결과 보고서를 분석해야 한다. 특히, 취약점 스캔이 SSEP 기능에 악영향을 주어서는 안되며, 악영향을 주는 경우 스캔 대상이 되는 CDA를 서비

스(online)에서 제외시켜야 함을 명시하고 있다. 이러한 내용들은 취약점 스캔이 일시적으로 수행되어서는 안 되며, 점검내용, 도구 및 제한요소, 취약점 스캔 주기에 대한 계획을 바탕으로 수행되어야 함을 강조한다.

5.4.3. 소스코드 분석을 통한 취약점 점검 요건

이 요건은 소스코드에 잠재된 취약점을 점검하기 위한 정적・동적 분석에 관한 요건이다. CDA 시스템 개발자 및 통합자로부터 해당 제품이 새로운 기술에 영향을 받아 변경될 수 있는 몇 가지 취약점 및 취약점 제거 요구사항을 충족하는지 확인하고, 알려진 모든 테스트 가능한 취약점과 악성코드로부터 안전한지 식별하고, 이와 관련한 내용을 문서화하여 정리해야할 것을 명시하고 있다. 이 때 점검해야할 내용은 가동 중인 시스템에서 안전하지 않은 네트워크 프로토콜 및 라이브러리 사용 여부, 비표준 암호화 모듈 사용 여부, 부적절한 접근 로직 등을 소스코드 레벨에서 분석하여야 한다고 규정 하고 있다.

5.4.4. SSEP 기능 및 성능과 보안 통제에 대한 요건

해당 요건의 주된 내용은 SSEP 기능 및 성능에 악영향을 미치는 보안 통제 접근 방법을 적용해서는 안 되며, CDA 기능 또는 성능에 미치는 악영향으로 인해 보안 통제를 수행하지 않음으로써 발생할 수 있는 CDA의 잔여 취약점은 다른 통제방법을 사용하여 제거하거나 완화 시켜야 하는 것이다. 하지만, 개발하고자하는 취약점 점검 기술 또는 점검 도구를 해당 계통에 적용하기 위해, 해당 계통이 지닌 기능의 일부분으로 점검 영역을 구현하여 적용하는 것은 시스템 및 도구사이의 호환성 등의 다양한 어려움이 있을 것으로 보이기 때문에 온라인 형태의 도구 개발을 위한 별도의 추가적인 작업이 필요하다.

Ⅵ. 네트워크 기반 취약점 스캐너의 원전 적용 방안

원자력발전소의 데이터 네트워크와 연관된 안전 계통들은 다양한 IT 네트워크 및 응용프로그램들을 적용하여 현대화되고 있다. 발전소 데이터 네트워크의 출현과 더불어 원전 계측제어시스템들은 최신의 디지털화된 마이크로프로세서에 근간을 둔 시스템으로 진화하고 있다. 고도로 발전된 IT 및 네트워크 관련 기술들이 원전 계측제어시스템에 적용되고 있는 관계로, 일반적인 IT 환경에서의 각종 정보시스템이 가지는 사이버 보안 위협, 보안 취약성 및 사고의 가능성이 증대되는 단점을 가지게 되었다. 이러한 단점을 극복하고자 하는 대책으로 네트워크 기반 취약점 스캐너를 활용하는 것을 고려하고 있다[5].

취약점 스캐너를 원전에 적용하는 경우 다음과 같은 요소를 고려해야 한다.

첫 번째로, 업데이트 주기 및 플러그인 업데이트 방법을 고려해야한다. 일반적으로 취약점 스캐너는 취약점 검색 전용 플러그인을 사용할 수없는 경우에 취약점을 식별 할 수 없다. 결과적으로, 공급업체가 업데이트하고 새로운 플러그인을 생산할수록, 새로운 결함을 발견 할 수 있는 스캐너의 능력이 향상된다. 또한 자동 업데이트 기능이 있는 스캐너는 정기적으로 최신 플러그인을 다운로드하고 설치할 수 있다. 이것은 취약점 스캐너를 선택할 때 고려되어야 한다.

둘째로 탐지된 취약점의 갯수와 정확도를 고려해야 한다. 동일한 취약점이 스캐너에 의해 두 번 이상 발견되기 때문에 치명적인 취약점이 식별되는 정확성은 취약점 검사의 횟수보다 중요하다. CVE (Common Vulnerabilities and Exposure)의 유효 취약점 갯수는 취약점 및 기타 정보 보안 노출에 대한 표준화 된 데이터베이스 목록에서 비교할 수 있다.

마지막으로, 검색된 취약점에 대해 산출된 결과 보고서의 품질을 고려해야 한다. 발견 된 취약점의 세부 사항 외에도 검사 보고서는 발견된 문제를 해결하기 위한 명확하고 간결한 정보를 사용자, 전문가 및 관리자에게 제공해야한다. 관리자가 초기 검색 또는 구성 변경 후 후속 스캔을 수행하거나 이전 스캔 결과를 비교해야하는 경우 추세 분석을 위해 아카이브 검색 결과를 보관할 수 있는 데이터베이스 시스템이 있는 스캐너가 필요하다.

위에서 나열한 취약점 스캐너 선택 요소들을 포함하고 있는 제품은 IBM의 QRadar 보안 지능형 플랫폼[17]을 예로 들 수 있다. 이 제품은 고급 분석 및 기계학습 알고리즘 기반으로 구성되어 있으며, 이 알고리즘을 사용하여 제품이 설치된 시스템을 스캔하는 과정중에 발생된 이벤트를 정규화하고 내장된 분석 규칙에 따라 이벤트를 매칭 시킨다. 하지만 이 제품이 요구하는 운용환경과 원전에서 사용 중인 운용 환경과 호환이 되는지, 호환이 되

더라도 이 제품이 원전 네트워크에 영향을 미치는 지를 R.G. 5.71을 기준으로 분석할 필요성이 존재한다.

ACKNOWLEDGEMENT

This work was supported by National Research Foundation of Korea(NRF) grant funded by the Korea government(Ministry of Science and ICT) (No. 2016M2A8A4952280, Development of Vulnerability Analysis for Nuclear Plant Instrument & Control)

References

[1] G. I. Jeong, J. K. Lee, and G. O. Park, “Application Trend of Cyber Security in Nuclear Power Plant Measurement Control System,“ *Journal of the Korea Information Processing Society Review*, vol. 19, no. 5, pp. 69-77, Sept. 2012.

[2] S. S. Kang, T. H. Lim, J. Y. Choo, H. T. Kim, D. H. Kim, G. G. Byun, J. E. Park, J. Y. Lee, and H. S. Choo, "Analysis on the EMC evaluating method for applying wireless communications in NPP," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 21, no. 12, pp. 2221-2231, Dec. 2017.

[3] D. Kim, “Vulnerability Analysis for Industrial Control System Cyber Security,” *Journal of the Korea Institute of Electronic Communication Sciences*, vol. 9, no. 1, pp. 137- 142, Jan. 2013.

[4] S. H. Kim, S. C. Lim and D. Y. Kim, “Regulatory Requirements Analysis for Development of Nuclear Power Plants Cyber Security Vulnerability Inspection Tool,” *Journal of the Korea Institute of Electronic Communication Sciences*, vol. 12, no. 5, pp. 725-730, Oct. 2017.

[5] D. Y. Kim, “Security Criteria for Design and Evaluation of Secure Plant Data Network on Nuclear Power Plants,” *Journal of the Korea Institute of Electronic Communication Sciences*, vol. 9, no. 2, pp. 267-271, Feb. 2014.

[6] D. Y. Kim, “Cyber security issues imposed on nuclear power plants,” *Annals of Nuclear Energy*, vol. 65, pp. 141-143, Nov. 2014.

[7] The Government of the Hong Kong Special Administrative Region [Internet]. Available: https://www.infosec.gov.hk/english/technical/files/vulnerability.pdf.

[8] P. Lindstrom, (2004, July). Network VS. Host-based Vulnerability Management. *A Spire Research Report* [Internet]. Available : http://spiresecurity.com/?page_id=1307.

[9] K. Scarfone, S. Murugiah, C. Amanda, and O. Angela, "Technical guide to information security testing and assessment." *NIST Special Publication 800*, no. 115, pp. 2-25, Sept. 2008.

[10] High-Tech Bridge Web Security Company [Internet]. Available: https://www.htbridge.com/immuniweb/.

[11] Netsparker Web Application Security Scanner [Internet]. Available: https://www.netsparker.com/.

[12] Tenable - Nessus [Internet]. Available: https://www.tenable.com/.

[13] OpenVAS [Internet]. Available: http://www.openvas.org/.

[14] BeyondTrust – Retina CS Community [Internet]. Available: https://www.beyondtrust.com/products/retina-network-community/.

[15] Microsoft - MBSA [Internet]. Available: https://www.microsoft.com/en-us/download/details.aspx?id=7558.

[16] US Nuclear Regulatory Commission, “Syber Security Programs for Nuclear Power Facilities,” Nuclear Regulatory Commission Regulatory Guide 5.71, Jan. 2010.

[17] IBM QRadar [Internet]. Available : https://www.ibm.com/security/security-intelligence/qradar.

임수창(Su-Chang Lim)

2015년 순천대학교 컴퓨터공학과 졸업(공학사)
2017년 순천대학교 대학원 컴퓨터공학과 졸업 (공학석사)
2017년 ~ 현재 순천대학교 대학원 컴퓨터공학과 박사과정
※관심분야 : 컴퓨터비전, 딥러닝, 기계학습

김도연(Do-Yeon Kim)

1986년 충남대학교 계산통계학과 졸업(이학사)
2000년 충남대학교 대학원 정보통신공학과 졸업 (공학석사)
2003년 충남대학교 대학원 컴퓨터공학과 졸업 (공학박사)
1986년 ~ 1996 한국원자력연구원 선임연구원
1997년 ~ 2008 한국전력기술(주) 책임연구원
2008년 ~ 현재 순천대학교 컴퓨터공학과 교수
※관심분야 : 컴퓨터비전, 딥러닝, 기계학습, 컴퓨터보안