Journal of KIIT. Vol. 18, No. 4, pp. 129-136, Apr. 30, 2020. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2020.18.4.129

정보보안산업 기반 스마트시티 사이버 보안

김성민*, 정혜선**, 이용우***

Smart City Cyber Security Based on Information Security Industry

Sung-Min Kim*, Hae-Sun Jung**, and Yong-Woo Lee***

이 논문은 2019년도 서울시립대학교 학술연구비에 의하여 지원되었음

요 약

본 논문에서는, 저자들이 속한 연구 그룹에서 스마트시티의 전체적인 사이버 보안에 관하여 수행한 연구의 일부로서, 저자들이 속한 연구 그룹의 축적된 연구결과를 바탕으로 하여 저자들에 의해 개발된 국내의 정보보안제품 기반 스마트시티-사이버-보안-메트릭스를 소개한다. 국내의 정보보안제품 기반 스마트시티-사이버-보안-메트릭스를 개발하기 위한 첫 번째 단계로서, 사이버 보안에 관한 지금까지의 전 세계적인 연구와 스마트시티에 관한 본 연구팀의 지속적인 연구 및 실제 구축 참여 경험을 바탕으로 하여, 스마트시티에서의 사이버 보안 위협요소들을 선정하였다. 다음 단계로서, 선정된 사이버 보안 위협요소들을 기반으로 하여, 스마트시티 사이버 보안 요구사항들을 도출하였다. 스마트시티-사이버-보안-메트릭스는 이 도출된 보안 요구사항들을 사용한다. 국내의 정보보안제품들과 연동된 스마트시티-사이버-보안-메트릭스를 이용하면, 국내의 정보보안제품들을 사용하여 스마트시티의 사이버-보안-시스템을 구축하는 경우에, 구축되는 스마트시티의 사이버 보안 정도를 일목요연하게 점검할 수 있어서, 스마트시티 사이버 보안의 구축과 운영관리가 용이해지고 체계화된다.

Abstract

As part of our research result for the overall cyber security of smart city, this paper presents the Korean information security market based smart-city-cyber-security-matrix developed by our research group. As the first step to develop our Korean information security market based smart-city-cyber-security-matrix, cyber security threats in smart city were examined and selected based on worldwide research on cyber security and research on smart city. In the next step, based on this, cyber security requirements in smart city were derived. The smart-city-cyber-security-matrix developed in this study uses these derived security requirements. With the developed smart-city-cyber-security-matrix, when building a cyber-security-system of a smart city using domestic information security products, the degree of cyber security of the built smart city can be checked at a glance, and smart city cyber security system construction and operation management will be easier and systematized.

Keywords
smart city, smart-city-cyber-security, smart-city-cyber-security-matrix

* 서울시립대학교 전자전기컴퓨터공학과 박사과정
- ORCID: https://orcid.org/0000-0002-9503-5614
** 서울시립대학교 전자전기컴퓨터공학과 연구교수
- ORCID: https://orcid.org/0000-0002-5866-3507
*** 서울시립대학교 전자전기컴퓨터공학과 교수(교신저자)
- ORCID: https://orcid.org/0000-0002-0219-8650

· Received: Mar. 31, 2020, Revised: Apr. 16, 2020, Accepted: Apr. 19, 2020
· Corresponding Author: Yong-Woo Lee
Department of EECE,. University of Seoul, Seoul, Korea
Tel.: +82-2-6490-2335, Email: ywlee@uos.ac.kr

Ⅰ. 서 론

ICT를 기반으로 하는 스마트시티의 특성상 사이버 보안이 매우 중요하다. 스마트시티 이전에 시행되었던 유시티 기간 중에 전국의 백여 개가 넘는 유시티 건설에 참여해 오면서 수행해온 스마트시티 연구의 결실 하나를 본 논문에서 발표한다. 지난 20년간 컴퓨터와 컴퓨터 네트워크 그리고 컴퓨터 통신 그리고 보조 장비들로 이루어지는 사이버 세계에서의 보안은 엄청난 변화를 보였다. 본 논문의 기반이 되는 연구에서 이 위협들과 해결책들을 모두 추적해왔다. 스마트시티에서의 사이버 보안에 대한 스마트 메트릭스 방법론을 본 논문에서 제시한다.

본 논문에서 발표하는 내용은, 본 논문의 연구진이 2000년 서울시 프로젝트인 상암동 소재의 디지털미디어시티(Digital media city) 건설 및 운영 프로젝트에 참여한 이래, 2005년도에 서울시의 대규모 지원을 받아서 시작하여 지금까지 이어온 연구의 산물이다. 또한, 유럽의 스마트시티와 기타 다른 국가들에 제공했던 자문 협력과 세계의 주요 스마트시티들에 대한 지속적인 연구 분석의 산물이다.

본 연구의 목표는 일 단계 목표로서, 스마트시티에서의 사이버 보안 위협요소들을 찾아내는 것이다. 이 단계 목표로, 스마트시티 시스템을 위한 사이버 보안 요구사항들을 도출하는 것이다. 삼 단계 목표로, 스마트시티-사이버-보안-메트릭스 방법론을 개발하여 소개하는 것이다. 사 단계 목표로서, 스마트시티-사이버-보안-메트릭스 방법론을 국내의 정보 보안제품 시장에 적용하여, 국내 정보보안제품에 연동된 스마트시티-사이버-보안-메트릭스를 개발하는 것이다. 오 단계 목표로서, 스마트시티-사이버-보안-메트릭스 방법론의 유용함을 입증하는 것이다.

본 논문은 다음과 같이 구성되었다. Ⅱ장에서는 관련연구를 서술한다. Ⅲ장에서는 본 논문의 대상이 되는 스마트시티를 정의한다. Ⅳ장에서는 스마트시티의 사이버 보안 위협요소들을 설명한다. Ⅴ장에서는 스마트시티 사이버 보안 요구사항(SCCSR, Smart City Cyber Security Requirement)을 설명한다. Ⅵ장에서는, 국내의 보안 산업에 기반한 스마트시티-사이버-보안-메트릭스를 제시한다. 마지막으로 Ⅶ장에서는 결론과 향후 연구 방향을 설명한다.

Ⅱ. 관련연구

스마트시티에는 많은 세부 분야가 있다. 요즈음의 스마트시티 붐에 힘입어 일부 세부 분야들에 관한 보안 연구보고서가 존재한다. 그러나 스마트시티의 총체적인 보안에 관한 연구는 찾아보기 어렵다. 현재의 스마트시티 붐을 일으킨 유럽연합의 유럽연합 사이버 보안기구(ENISA)에서 스마트시티-공공교통[1]과 스마트-병원[2]에서의 모델에 대한 사이버 보안에 관한 연구를 선보였다.

본 논문에서는 한국인터넷진흥원(KISA)의 국가정보보호백서[3]들과, 한국정보보호산업협회(KISIA)의 국내 정보보호산업 및 실태조사[4]와 2019년 4월 3일에 청와대 국가안보실에서 발표한 국가 사이버안보전략[5]을 반영하였다. 스마트시티의 많은 세부 분야의 일부에 대하여 국내의 KISA에서 제공하는 가이드라인이 돋보인다. KISA[6]은 스마트의료, 스마트교통, 스마트공장, 스마트안전·재난·환경, 스마트에너지에서의 보안 가이드를 제공하고 있으며, 스마트시티에 필수적인 IoT에 관한 보안 가이드도 제공하고 있다.

참고문헌 [7]은 스마트시티에서의 전체적인 통합 사용자 인증 보안관리를, 참고문헌 [8]는 IoT를 사용하는 스마트시티-인프라스트럭쳐-티어의 보안을 위한 시스템을 소개하고 있다.

국제표준기구(ISO)와 국제전자기술위원회(IEC)는 사이버 보안 표준들을 제정해오고 있다[9]. 대한민국 국가보안기술연구소(NSRI)는 정보보호제품 평가·인증을 수행하고 있는데, 이 정보보호제품 평가·인증은 ISO/IEC 15408 국제표준의 정보보호시스템 공통평가기준을 기준으로 ISO/IEC 18045 국제표준의 정보보호시스템 공통평가방법론에 기반을 두어 수행되고 있다.

미국 표준기술연구소(NIST)와 미국인터넷보안센터(CIS)는 미국의 사실상 표준화된 사이버 보안 프레임워크를 제공하고 있다. 유럽연합 사이버 보안기구는 매년 사이버 보안에 관한 보고서를 발간하고 있다[10]. 이들은 연구 분석되어서 본 논문에 반영되었다.

III. 스마트시티

대한민국의 스마트시트 법률은 스마트시티를 “도시의 경쟁력과 삶의 질의 향상을 위하여 건설·정보통신기술 등을 융·복합하여 건설된 도시 기반 시설을 바탕으로 다양한 도시서비스를 제공하는 지속 가능한 도시를 말한다.”라고 정의하고 있다[11].

본 논문의 저자들이 소속된 기관에서 2000년도에 시작하여, 지금까지 지속되고 있는 연구를 수행하면서, 스마트시티 패러다임으로 유토피아(UTOPIA) 스마트시티를 제안하였고 지금까지 발전시켜 오고 있다. 이 패러다임은 현재 스마트시티의 대부분에서 사용되고 있다. 이 패러다임이 본 논문이 대상으로 하는 스마트시티이다. 대상으로 하는 유토피아 스마트시티 패러다임은 그림 1에서처럼 세 개의 티어로 이루어져 있다[12].

스마트시티-포탈-티어는 사용자들이 온라인으로 다양한 스마트시티 서비스들을 이용할 수 있게 해주는 역할을 한다. 스마트시티를 하나의 시스템으로 유기적으로 관리하기 위하여, 통합 플랫폼을 스마트시티 통합 서버에 의하여 제공하는 것이 현재의 스마트시티에서의 일반적인 경향이다. 본 연구는 이 패러다임에 기반을 두고 있으며, 더욱더 강력한 통합 플랫폼 서비스를 제공 하는 스마트시티-플랫폼(미들웨어)-티어를 제공한다.

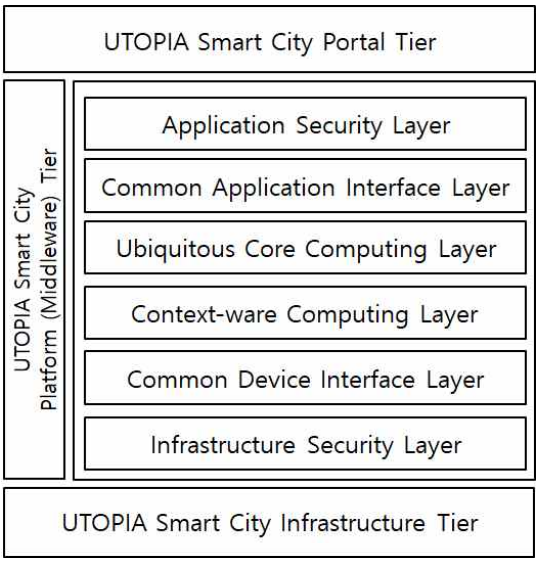

그림 1. 유토피아 스마트시티 구조
Fig. 1. UTOPIA smart city architecture

이 티어는 스마트시티의 중심의 되는 역할을 하며, 지능적인 다양한 융복합 솔루션을 제공하고, 클라우드 컴퓨팅을 포함한다. 스마트시티-인프라스트럭처-티어는 스마트시티로 연결되어 통합 운영되는 스마트시티의 각 구성요소들로 구성되어져 있다. 스마트시티-인프라-스트럭처-티어는 도시의 인프라-스트럭처에 사물인터넷(IoT) 기능을 널리 적용하여 스마트시티-인프라-스트럭처를 만들어 낸다. 이를 통하여 지능적이고, 스스로 작동하게 할 수 있는 스마트시티 시민에게 유용한 역할을 하게 된다. 그러나 이 때문에, 스마트시티 보안이 더욱 중요해지고, 어려운 임무가 되었다.

IV. 스마트시티 사이버 보안 위협요소

본장에서는, 스마트시티 사이버 보안 위협요소들을 설명한다. 선행되었던 전 세계의 뛰어난 연구결과들이 반영되었다[3][10][13]-[15].

본 연구에서는 멀웨어(Malware)에 의한 공격들을 스마트시티에 심각한 위협요소로 분류한다. 2018년도에 제일 많이 발생한 사이버 공격이라고 보고한 참고문헌 [10]에서는 특정 멀웨어를 개별적으로 순위 표기하였으나, 본 논문에서는 모든 멀웨어들을 하나의 항목으로 표기한다. 스마트시티는 사물인터넷을 기반 기술로 사용하는데, 이를 노리는 멀웨어가 2018년에 크게 증가하였다[10].

멀웨어 항목은 다시 4개로 분류하여 설명하면 다음과 같다. 웹 어플리케이션-공격, 크립토재킹, 랜섬웨어(Ransomware), 기타 대표적인 멀웨어들의 4개로 세분한다. 웜(Worms)과 트로이-목마(Trojans)는 2012년에 2위를 차지했던, 스마트시티에 대한 심각한 위협요소이다. 루트킷(Rootkit) 멀웨어도. 그들과 함께 번들 된 페이로드가 악의적이기 때문에 스마트시티에 대한 심각한 위협요소이다. 본 연구의 대상이 되는 스마트시티는 유비쿼터스 컴퓨팅을 지원한다.

따라서 모바일 스마트 기기로서 모든 일을 할 수 있기 때문에, 모바일 스마트 기기에 멀웨어를 심고 이를 통하여 스마트시티를 공격하는 위협은 심각한 위협요소이다. 인가되지 않은 권한 상승을 통하여 컴퓨터 자원들에 대한 접근 권한을 높여서 시스템

을 공격하는 멀웨어들도 스마트시티에 대한 심각한 위협요소이다. 가짜 백신 프로그램은 백신 소프트웨어를 사칭해서 이득을 얻는 악성 소프트웨어로서, 스마트시티에 대한 심각한 위협요소이다. 취약점 공격 도구인 익스플로잇 킷(Exploit kit)도 스마트시티에 대한 심각한 위협요소이다. 멀웨어에는 상기에 기술한 것들 외에 각종 바이러스 프로그램들이 있다. 이들도 스마트시티에 대한 심각한 위협요소이다.

비인가-소프트웨어-설치-공격은 대부분 웹-기반-공격 형태를 취한다. 스마트시티에 대한 심각한 위협요소이다. 사회공학적-공격은 기술적인 방법이 아닌 사람들 간의 기본적인 신뢰를 기반으로 사람을 속여 비밀 정보를 획득하는 공격으로서, 피싱(Phishing)과 스피어-피싱(Spear-phishing)이 대표적이다. 스마트시티에 대한 심각한 위협요소이다. 분산 서비스 거부(DDoS) 공격은, 스팸(Spam) 공격이라고도 불리는 원하지 않는 이메일(E-mail) 수신 공격과 함께 스마트시티에 대한 위협요소이다. 봇넷(Botnets)에 의한 공격 등과 같은 원격-활동-공격(원격-수행-공격)은 스마트시티에 대한 위협요소이다. 데이터-유출은 기밀정보의 유출을 말하는데, 스마트시티에 대한 위협요소이다.

정보 누설은 비의도적으로 정보가 외부로 누설되는 것을 말하는데, 정보의 누설 사고는 스마트시티에 대한 심각한 위협요소이다. 개인 정보를 탈취하여 신원을 도용하는 공격도 스마트시티에 대한 심각한 위협요소이다. 가짜 인증서를 생성하여 사용하는 공격은 스마트시티에 대한 심각한 위협요소이다. 하드웨어와 소프트웨어의 인가를 받지 않은 조작에 의한 공격, 정보의 조작에 의한 위협, 감사 도구(Audit tool)의 악용에 의한 위협과 공격, 정보와 모바일 앱을 포함하는 정보시스템의 오용에 의한 위협, 비인가 행위에 의한 위협, 거짓 정보에 의한 위협은 모두 스마트시티에 대한 큰 위협요소이다.

APT(Advanced Persistent Threat) 등에 의한 목표된 공격, 가짜 백신 프로그램, 브루트 포스 공격(Brute force attack), 남발된 승인을 통해 접속하여 공격 하는 승인 남용 위협과 함께, 스마트시티에 대한 심각한 위협요소이다.

정보의 가로채기는 특정한 사람이나 기관에 대한 정보를 수집하려는 의도를 가진 스파이웨어 또는 기만하는 프로그램에 의한 공격으로서, 스마트시티에 대한 심각한 위협요소이다. 정보를 가로채 가는 공격과 유사한 공격행위나 위협요소로 워-드라이빙(War driving), 방출자료-가로채기, 메시지-재생, 네트워크 조작, 세션 도용 등과 같은 공격과 위협요소가 유명하다. 이들은 모두 스마트시티에 대한 심각한 위협요소이다. 워-드라이빙은 무선 네트워크를 이용한 해킹 수법이다. 정보를 갖는 시그널을 방사하는 것을 자료 방출이라고 한다. 스마트시티에는 IoT를 사용하는 등의 이유로 방출자료-가로채기는 큰 위협이 되고 있다. 특히, 스마트시티-인프라-스트럭처에 큰 위협이 되고 있다.

메시지 재생 공격, 네트워크-조작-공격, 세션-도용은 스마트시티에 대한 심각한 위협요소이다. 유선이나 무선 네트워크 액세스를 통해 신뢰할 수 없는 기기나 정보에 의한 스마트시티 시스템에 접근하여 공격할 수 있다. 예를 들어, 스마트시티에서, 집에 있는 스마트 TV를 통해 정상적인 방송 신호를 가장하여 침입하여 스마트시티를 공격할 수 있다. 이와 같은 신뢰할 수 없는 출처의 정보를 사용한 공격은 스마트시티에 대한 큰 위협요소이다.

Ⅴ. SCCSR

스마트시티 사이버 보안에 위협을 가하는 요소들을 여러 카테고리로 분류하였다. 스마트시티에 직접적으로 위협을 가하는 요소들은 [카테고리 1]으로 분류하였다. [카테고리 2]는 물리적인 공격에 의한 위협요소들을 담고 있다. [카테고리 3]는 재난에 의한 위협요소들을 담고 있다. [카테고리 4]는 시스템과 기기들의 이상과 고장에 의한 위협들을 담고 있다. [카테고리 5]는 정전 등과 같은 전기 공급 이상에 의한 위협들을 담고 있다. 여기서는[카테고리 1]에 기반한 SCCSR들을 제시한다. 본 연구에서 추구하는 스마트시티에서의 사이버 보안을 확보하기 위한 SCCSR들은 표 1과 같다.

표 1. 스마트시티 사이버 보안 요구사항
Table 1. Smart city cyber security requirement

SCCSR	스마트시티가 방어해야하는 사이버 보안 공격과 사이버 보안 사고
SCCSR-01	멀웨어에 의한 공격
SCCSR-02	비인가 소프트웨어 설치 공격
SCCSR-03	피싱과 스피어-피싱과 같은 사회공학적 공격
SCCSR-04	분산 서비스 거부 (DDoS) 공격
SCCSR-05	원하지 않는 E-mail 수신 공격
SCCSR-06	원격활동 공격
SCCSR-07	데이터 유출 사고
SCCSR-08	정보의 누설 사고
SCCSR-09	개인 정보 탈취를 통한 신원 도용 공격
SCCSR-10	가짜 인증서의 생성과 사용에 의한 공격.
SCCSR-11	하드웨어와 소프트웨어의 인가를 받지 않은 조작에 의한 공격
SCCSR-12	정보의 조작에 의한 공격
SCCSR-13	감사도구의 악용에 의한 공격
SCCSR-14	비인가 행위에 의한 공격
SCCSR-15	거짓 정보에 의한 공격
SCCSR-16	목표된 공격
SCCSR-17	무차별 공격
SCCSR-18	승인 남용에 의한 공격.
SCCSR-19	정보의 가로채기 공격
SCCSR-20	워-드라이빙 공격
SCCSR-21	방출자료 가로채기 공격
SCCSR-22	메시지 재생 공격
SCCSR-23	네트워크 조작 공격
SCCSR-24	세션 도용 공격.
SCCSR-25	신뢰할 수 없는 정보사용이나 출처미상 정보사용에 의한 공격

VI. 스마트시티 사이버 보안 메트릭스

개발된 스마트시티-사이버-보안-메트릭스는 앞장에서 도출된 스마트시티 보안 요구사항을 세로축의 항목으로 사용한다. 본장에서는, 이것을 국내 정보보호산업 시장에 적용하여 표 2와 같은 국내 정보보호산업 기반 스마트시티-사이버-보안-메트릭스를 개발하여 제시한다. 표 2에서는 가독성을 위하여 개발된 메트릭스의 일부를 실었다.

KISIA에서 발간한 2018년 국내 정보보호 시장 분석 보고서에는 2018년 국내에서 유통되고 있는 정보보안 제품을 크게 5개로 대분류하고, 각각의 시스템을 다시 중분류하고, 각 중분류 항목을 다시 소분류 하였다[4].

표 2에서 표시한 사용상품은 (1) 웹 방화벽, (2) 네트워크(시스템) 방화벽, (3) 침입방지시스템(IPS), (4) DDoS 차단 시스템, (5) 통합보안시스템(UTM), (6) 가상 사설망(VPN), (7) 네트워크 접근제어(MAC), (8) 무선네트워크, (9) 망분리(가상화), (10) 시스템 접근통제 (PC방화벽 포함), (11) Anti 멀웨어, (12) 스팸차단 SW, (13) 보안운영체제(Secure OS), (14) APT 대응, (15) 모바일 보안, (16) DB보안 (접근통제), (17) DB 암호, (18) 보안 USB, (19) 네트워크 DLP, (20) 단말 DLP 등이다

표 2의 동그라미를 친 부분의 의미는 가로항목에 표시된 국내 보안 시장에 유통되는 제품을 사용하여 스마트시티의 사이버 보안을 구축하는 경우에 세로항목에 표시된 스마트시티-사이버-보안-요구사항을 만족하는가에 대한 점검을 한 결과를 표시하는데, 만족한다는 뜻이다. 동그라미 대신에, 퍼센트 값으로 표시할 수도 있는데, 이럴 경우 훨씬 상세한 국내 정보보호 산업 기반 스마트시티-사이버-보안-메트릭스가 된다. 본 논문에서는 80프로 이상의 만족 가능성이 있으면 만족한다고 동그라미로 표시하였다. 표시에는 이견이 있을 수 있다. 보수적으로 작성되었으며, 어떤 제품은 표시된 것 이상을 방어할 수도 있다. 현장에서 사용 시, 목표로 하는 제품들에 대한 보다 면밀한 분석이 필요하다.

표 2는 제시한 국내 정보보호 산업 기반 스마트시티-사이버-보안-메트릭스로서, 국내 정보보안제품들을 이용하여 스마트시티의 사이버 보안을 구축할 때, 사이버 보안을 할 수 있는 정도를 보여주고 있다. 각 스마트시티는 이 메트릭스를 활용하여 원하는 수준의 스마트시티 사이버 보안을 구현할 수 있게 계획을 수립하고 집행하고 확인하고 유지보수할 수 있으며, 각 스마트시티의 현 상태의 사이버 보안 수준을 검증할 수 있다.

표 2. 스마트시티 사이버 보안 그리드 메트릭스
Table 2 Smart city cyber security grid matrix

Product / Requirement	Network security (%)									System security (%)						Contents/Information leakage prevention (%)				
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)	(18)	(19)	(20)
SCCSR-01	△ (50)				△ (30)						△ (80)				△ (50)					
SCCSR-02											O				△ (50)					
SCCSR-03																				
SCCSR-04				O																
SCCSR-05												O								
SCCSR-06				△ (70)																
SCCSR-07	△ (50)				△ (50)	O	△ (30)			△ (70)					△ (50)	△ (50)	△ (50)		△ (50)	△ (50)
SCCSR-08													△ (50)		△ (50)					
SCCSR-09	△ (50)				△ (50)	△ (50)									△ (50)					
SCCSR-10																				
SCCSR-11	△ (50)				△ (50)															
SCCSR-12	△ (50)				△ (50)															
SCCSR-13																				
SCCSR-14	△ (50)		△ (50)		△ (50)			△ (30)	O						△ (50)					
SCCSR-15																				
SCCSR-16														O						
SCCSR-17																				
SCCSR-18													△ (50)							
SCCSR-19		△ (50)				△ (50)									△ (50)					
SCCSR-20								O												
SCCSR-21		△ (50)			△ (50)															
SCCSR-22	△ (30)	O			△ (30)															
SCCSR-23	△ (50)	O	O	△ (30)	△ (70)			△ (50)												
SCCSR-24	△ (50)	△ (30)			△ (30)	O														
SCCSR-25																				

Ⅶ. 결론 및 향후 과제

본 연구의 목표는, 스마트시티에서의 사이버 보안 위협요소들을 찾아내어, 스마트시티를 위한 사이버 보안 요구사항들을 도출하여 이를 사용하여, 스마트시티-사이버-보안-메트릭스를 개발하여, 이를 국내의 정보보안제품과 연동시킨 스마트시티-사이버-보안-메트릭스를 개발하고, 우수함을 검증하는 것이다. 스마트시티-사이버-보안-메트릭스를 제시하고 설명하였다. 스마트시티 사이버 보안 연구 위협요소들을 설명하였다. 그리고 이를 바탕으로 도출된 25가지의 SCCSR들을 설명하였다. 제시된 메트릭스를

이용하면, 국내의 정보보안제품들을 사용하였을 때, 스마트시티의 사이버 보안 요구사항의 만족도를 알 수 있다. 개발한 국내의 정보보안제품들을 사용하였을 때의 스마트시티-사이버-보안-그리드-메트릭스를 이용하여, 대한민국 정보보안 시장을 이용하여, 원하는 수준의 스마트시티 사이버 보안을 구현할 수 있게 계획을 수립하고 집행하고, 확인하고, 유지 보수를 할 수 있음을 검증하였다. 향후에는 미국 표준기술연구소의 사이버 보안 프레임워크에 적용하는 연구 등을 수행할 예정이다.

감사의 글

박종원 박사, 윤철상 연구원과 스마트시티 사업단, 서울그리드센터, 유비쿼터스-그리드(클라우드) 컴퓨팅 연구실원들에게 감사를 표합니다.

References

[1] "Cyber security for Smart Cities – An architecture model for public transport", European Union Agency For Network And Information Security, Greece, pp. 1-54, Dec. 2015.

[2] "Smart Hospitals – Security and Resilience for Smart Health Service and Infrastructures", European Union Agency For Network and Information Security, Greece, pp. 1-56, Nov. 2016.

[3] "2019 National Information Protection White Paper", Korea Internet Security Agency, https://www.kisa.or.kr/public/library/etc_View.jsp?regno=0012001&searchType=&searchKeyword=&pageIndex=1. [accessed: Mar. 01, 2020]

[4] "Survey for Information Security Industry in Korea : Year 2019", Korea Information Security Industry Association, pp. 1-227, Dec. 2019.

[5] "National Cybersecurity Strategy", Korea National Security Office, pp. 1-27, Apr. 2019.

[6] Korea Internet Security Agency, https://www.kisa.or.kr/public/laws/laws3.jsp. [accessed: Mar. 01, 2020]

[7] E. D. Hwang and Y. W. Lee, "User Authentication of a Smart City Management System", Journal of the Korea Convergence Society, Vol. 10, No. 1, pp. 53-59, Feb. 2019.

[8] E. D. Hwang and Y. W. Lee, "Smart City Security Management in Three Tier Smart City Management System", Journal of the Korea Convergence Society, Vol. 10 No. 1, pp. 25-33, Feb. 2019.

[9] "ISO/IEC TR 27103:2018—Information technology—Security techniques—Cybersecurity and ISO and IEC standards“, https://www.iso27001security.com/html/27103.html. [accessed: Mar. 01, 2020]

[10] "ENISA Threat Landscape Report 2018", European Union Agency For Network And Information Security, Greece, pp. 24-115, Jan. 2019.

[11] Korean Ministry of Land, Infrastructure and Transport, “Act on Smart City Creation and Industry Promotion, etc”, This Decree enter into force on Sep. 22, 2017, Law No.14718.

[12] H. S. Jung, C. S. Jeong, Y. W. LEE, and P. D. Hong, "An Intelligent Ubiquitous Middleware for U-city: SmartUM", Journal of Information Science and Engineering, Vol. 25, No. 2, pp. 375-388, Mar. 2009.

[13] "ENISA Threat Taxonomy", European Union Agency For Network And Information Security, Greece, Dec. 2016.

[14] "Threat Classification Taxonomy Cross Reference View", http://projects.webappsec.org/w/page/13246977/Threat%20Classification%20Views. [accessed: Mar. 01, 2020]

[15] "CIF Taxonomy Assesment v1", https://code.google.com/p/collective-intelligence-framework/wiki/TaxonomyAssessment_v1. [accessed: Jul. 01, 2016]

저자소개

김 성 민 (Sung-Min Kim)

1996년 ~ 2007년 : 중앙정보처리 학원, 교육부 강사
2006년 : 단국대학교 정보통신대학원 IT학과(공학석사)
2007년 ~ 2011년 : ㈜데카소프트, 개발팀 과장
2010년 ~ 현재 : 서울시립대학교 전자전기컴퓨터공학과 박사과정
2011년 ~ 현재 : ㈜이테크밸리플러스, 개발팀 차장
관심분야 : 스마트시티, 보안관리

정 혜 선 (Hae-Sun Jung)

2001년 : 고려대학교 전자컴퓨터공학과(공학석사)
2011년 : 고려대학교 전자컴퓨터공학과(공학박사)
2015년 ~ 현재 : 서울시립대학교 연구교수
관심분야 : 인터넷, 클라우드 컴퓨팅, 시스템 소프트웨어, 스마트시티, 보안관리, ICT융합시스템, IoT

이 용 우 (Yong-Woo Lee)

1981년 : 서울대학교 전기공학과(학사)
1981년 : Schlumberger Inc., International Engineer
1982년 ~ 1998년 : KIST (한국과학기술연구원) 선임연구원
1997년 : 영국 에딘버러대학교 컴퓨터학과 (박사)
1998년 : 한국교육학술정보연구원, 책임연구원
1999년 ~ 현재 : 서울시립대학교 전자전기컴퓨터공학부 교수
2005년 ~ 현재 : 지능형도시(스마트시티)사업단 단장
2002년 ~ 현재 : 서울그리드(클라우드)센터 센터장
관심분야 : 스마트시티, ICT 기반 융합, 4차산업혁명, 시스템 소프트웨어, 초고속 통신, 클라우드 컴퓨팅, 그리드 컴퓨팅, 차세대 컴퓨팅. 보안관리