JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 25 No. 8, pp. 39-45, August 2020
https://doi.org/10.9708/jksci.2020.25.08.039

A Fuzzy Rule-based System for Automatically Generating Customized Training Scenarios in Cyber Security

Su Man Nam*

*Researcher, DuDu Information Technologies, Ltd., Seoul, Korea

[Abstract]

Despite the increasing interest in cyber security in recent years, the emergence of new technologies has led to a shortage of professional personnel to efficiently perform the cyber security. Although various methods such as cyber rage are being used to cultivate cyber security experts, there are problems of limitation of virtual training system, scenario-based practice content development and operation, unit content-oriented development, and lack of consideration of learner level. In this paper, we develop a fuzzy rule-based user-customized training scenario automatic generation system for improving user's ability to respond to infringement. The proposed system creates and provides scenarios based on advanced persistent threats according to fuzzy rules. Thus, the proposed system can improve the trainee's ability to respond to the bed through the generated scenario.

▸ **Key words**: Cyber security, Virtual environment, Scenario automatic generation, Fuzzy Logic, Advanced persistent threats

[요 약]

최근에 사이버 보안에 대한 관심이 많이 증가함에도 불구하고 신기술들의 등장으로 사이버 보안을 효율적으로 수행할 전문적인 인력이 부족한 실정이다. 사이버 보안 전문인력 양성을 위해 사이버 레이지와 같은 다양한 방법이 활용하고 있음에도 가상훈련 시스템의 한계성, 시나리오 기반의 실습 콘텐츠 개발과 운용상, 단위 콘텐츠 중심 개발, 학습자 수준 고려 부족의 문제점이 있다. 본 논문에서는 사이버보안 훈련체계 사용자의 침해대응 능력을 향상하는 목적으로 퍼지 규칙 기반의 사용자 맞춤형 훈련 시나리오 자동 생성 시스템을 개발한다. 제안하는 시스템은 퍼지 규칙을 따라 지능형 지속 위협 기반으로 시나리오를 생성하고 제공한다. 그리하여 제안 시스템은 생성된 시나리오를 통해 훈련생의 침해 대응 능력을 향상시킬 수 있다.

▸ **주제어**: 사이버 보안, 가상 환경, 시나리오 자동 생성, 퍼지 로직, 지능형 지속 위협

• First Author: Su Man Nam, Corresponding Author: Su Man Nam
*Su Man Nam (sumannam@gmail.com), DuDu Information Technologies, Ltd.
• Received: 2020. 05. 04, Revised: 2020. 08. 15, Accepted: 2020. 08. 19.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

최근 전 세계적으로 기하급수적으로 늘어나는 사이버 공격에 대응하기 위해 사이버 전장을 규정하고 여러 가지 대책을 세우고 있다. 이러한 사이버 보안에 대한 관심이 많이 증가함에도 불구하고, 이에 대응하는 사이버 보안을 효율적으로 수행할 전문적인 인력은 부족한 실정이다[1-4]. 게다가, 모바일, 클라우드, IoT 등과 같은 신기술들의 등장으로 사이버 범죄는 급증하였지만, 이에 대응하는 전문 인력 또한 부족하다[1-3]. 이를 위해 실제 훈련 환경에서는 실제와 유사한 상황을 모의할 수 있으나 실제 시스템이 운영 중에 훈련이 쉽지 않을 뿐만 아니라 다양한 훈련을 구성하는 데 많은 비용이 든다.

실제 시스템에서 사이버 훈련을 보완하기 위해 사이버 레인지는 사이버 보안 인력 양성 목적으로 가상과 실 환경을 모의할 수 있는 LVC(Live-Virtual and Constructive, 실 가상) 환경으로써, 실무 사이버 기술(hands-on cyber skills)을 습득하기 위한 안전하고 적법한(safe and legal) 환경을 제공한다[5]. 이를 위해 세계 각 국에서는 SecGen(Security Scenario Generator)[6], MetaCTF[7], 자동화 문제 생성[8], 사이버 해킹 대응 시스템[9, 10] 등과 같은 다양한 사이버 레인지 시스템을 출시하고 있다.

상기 사이버 레이지들이 인력 양성을 위한 다양한 훈련 콘텐츠를 제공하고 있음에도 다음과 같이 네가지 문제점이 있다. 첫째, 가상훈련 시스템의 한계이다. 사전 정의된 콘텐츠의 훈련만 가능하므로, 정의되지 않은 공격(변형된 공격, 미래 위협 등)에 대한 훈련이 불가능하다[5]. 둘째, 시나리오 기반 실습 콘텐츠 개발과 운용상 문제점이다. 대부분의 시나리오 기반 실습 콘텐츠는 다양한 컴퓨팅과 네트워킹 자원 및 공격과 방어 기술이 포함된 복합 콘텐츠로, 설계 및 개발에 많은 시간 및 인원 투입이 필요하다[3]. 게다가, 시나리오 콘텐츠는 설계 단계에서 사전 정의된 시나리오에 따라 실습하는 형태이므로, 사실상 1회성 실습용으로 운용되는 것이 현실이다[11]. 셋째, 단위 콘텐츠 개발 문제점이다. 시나리오 콘텐츠에 다수의 단위 콘텐츠와 동일(또는 유사) 실습이 포함되는 형태로 개발되는 것이 일반적이나, 단위 콘텐츠가 결합 가능한 형태로 제작되지 않아 시나리오 콘텐츠 개발 시 직접적으로 재사용되지 않고 있다[5]. 마지막으로, 학습자 수준 고려 부족이다. 시나리오 콘텐츠는 대상 학습자들의 지식과 기술 수준을 세심하게 고려하지 않고 설계되는 경우가 흔하며, 이에 따른 실습 문제 난이도 조절 실패로 개발한 콘텐츠를 제대로 활용하지 못하는 경우도 종종 발생한다.

본 논문에서는 사이버 보안 훈련체계 사용자의 침해대응 능력을 향상시키기 위해 퍼지 규칙 기반의 사용자 맞춤형 훈련 시나리오 자동 생성 시스템을 제안한다. 제안 시스템은 사용자 그룹의 강점 및 약점을 기반으로 퍼지 규칙을 통해 지능형 지속 위협(Advanced Persistent Threat; 이하 APT) 공격 단계에 따라 훈련 시나리오를 생성한다. 따라서 제안 시스템은 훈련생이 보안 대응능력이 취약한 분야 또는 대응이 부족했던 공격을 중심으로 사이버 침투 시나리오를 플래닝할 수 있으며, 훈련생 강점을 피하고 약점을 공략하는 방식으로 훈련생의 침해 대응 능력을 향상시킨다.

본 논문의 구성은 2장에서 관련 연구를 소개하고, 3장에서 제안 시스템을 설명한다. 마지막으로 4장에서는 전반적인 결론을 요약한다.

II. Preliminaries

본 장에서는 2.1에서 대표적인 사이버보안 훈련 시스템을 소개하고, 2.2에서 APT 공격 단계를 살펴본다.

1. Related works

기존 사이버보안 훈련 시스템의 대표적인 시스템은 SecGen [6], MetaCTF [7], 자동화 문제 생성[8], 사이버 해킹 대응 시스템[9], [10] 등이 있다.

SecGen는 영국 Schreuders 등을 통해 제안되었다. SecGen는 임의의 시나리오를 기반으로 자동으로 보안 시나리오를 생성한다. 또한, 임의의 시나리오를 생성하기 위해 가상 머신(Virtual Machine)을 사용하여 모의 해킹, 보안 교육, CTF(capture-the-flag) 등에 사용한다. 이 시스템은 기반(base), 취약점, 서비스, 유틸리티, 네트워크, 생성기, 인코더를 컴포넌트로 구분하여 가상 머신들을 생성할 수 있다. 그러나 SecGEN은 임의의 한 가상 머신만 생성함으로 사용자 맞춤형 시나리오 등을 위해 사용하는 것은 한계가 있다.

Feng이 제안한 MetaCTF는 바이너리 역공학(binary reverse engineering) 중심의 CTF 문제를 자동 생성한다. 이 시스템은 기본 문제들로부터 다형(polymorphic) 및 변성(metamorphic) 문제들을 생성하여 서로 다른 사용자들에게 다른 문제들을 제공한다. 다만, 매개변수(parameter) 변경을 통해 바이너리 역공학 문제들만 생성하므로 시나리오 기반의 사이버 훈련 시스템에 적용하기는 쉽지 않다. 자동화 문제 생성 기법(Automated problem generation)은 Burket 등이 제안하였으며, 기

본 문제들을 기반으로 여러 가지 문제들을 자동으로 생성하는 기법이다. 자동화 문제 생성 기법은 2014년 PicoCTF라는 대규모 CTF 행사에 시범적으로 사용됐다. 이 기법은 매개변수를 통해 문제들이 변경됨에도 불구하고 MetaCTF와 유사하게 시나리오 기반의 문제들을 적용하기에는 어렵다.

두두아이티의 사이버이지스는 사이버 침해대응에 관한 이론과 실제 정보시스템과 유사한 상황 하에서 대응 능력을 숙달시키는 모의훈련 시스템이다.

Fig. 1. Cyber Aegis

Fig. 1과 같이 사이버이지스 훈련 환경(training environment), 훈련 체계(training system), 그리고 훈련 콘텐츠(training contents)로 구성된다. 훈련환경은 웹 기반의 교육환경에서 교육과정, 교육생 및 훈련콘텐츠를 관리하며 가상화 프로그램과 연동하여 콘텐츠들을 실습할 수 있다. 훈련체계는 가상화 기반의 훈련체계로 다수 훈련자 동시 실습이 가능하며 네트워크, 서버 등의 가상시스템을 직접 조작할 수 있다. 훈련콘텐츠는 원격 교육, 취약점조치, 해킹방어, 시나이로 기반 침해대응을 실습할 수 있다. 이 시스템은 사이버 보안에 대한 이론과 실습을 병행할 수 있음에도 사용자 맞춤형 훈련 시나리오 구성이 어렵다.

상기 시스템들 외에도 가상머신을 이용한 시나리오 기반 사이버보안 교육 시스템이 개발되었다[11]. 이 교육 시스템은 한 시나리오를 대상으로 이메일 첨부파일을 이용한 악성코드, Carbanak APT, 그리고 Mirai 악성코드 문제들을 사용하여 가상머신을 사용하였음에도 사용자 맞춤형 해킹보안 복합 시나리오를 구성하는 데는 한계가 있다.

2. APT

미국 표준기술연구소(National Institute of Standards and Technology, NIST)에서는 APT 공격[12]은 전문지식과 많은 자원을 가진 공격자가 여러 다른 공격 경로를 통해 그들의 목적을 달성하는 공격으로 정의한다. APT 공격은 방어자의 노력에 적응하면서, 목적을 실행하기 위해 필요한 수준의 상호 작용을 유지하고 오랜 기간 동안 반복적으로 목적을 달성한다.

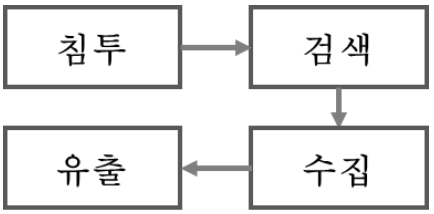


Fig. 2. Four steps of APT

Fig. 2는 APT 공격의 네 단계(침투, 검색, 수집, 유출)를 보여준다. 침투 단계는 공격자가 취약한 시스템을 통해 네트워크 내부로 침투한다. 검색 단계는 침투한 내부 시스템 및 인프라 구조에 대한 정보를 수집한 후 다음 단계를 계획한다. 수집 단계는 보호되지 않은 시스템 상의 데이터 수집 또는 시스템 운영을 방해한다. 마지막으로 유출 단계는 공격자의 근거자료 데이터 전용 시스템운영 방해 또는 장비 파괴한다.

III. The Proposed Scheme

본 장에서는 3.1에서 제안 시스템의 개요를 설명하고, 3.2에서 제안 시스템의 상세 과정을 소개한다.

1. Overview

제안 시스템은 사이버 보안에서 효율적으로 해킹 대응을 위한 퍼지 규칙 기반의 사용자 맞춤형 훈련 시나리오를 제공한다. 생성된 시나리오는 APT 공격 단계에 따라 콘텐츠들 재배열한다. 그러므로 제안 시스템은 사용자가 시도한 콘텐츠들을 대상으로 사용자의 수준을 분류하고 퍼지 로직 기반으로 APT 공격 단계를 따라 훈련 시나리오를 구성한다.

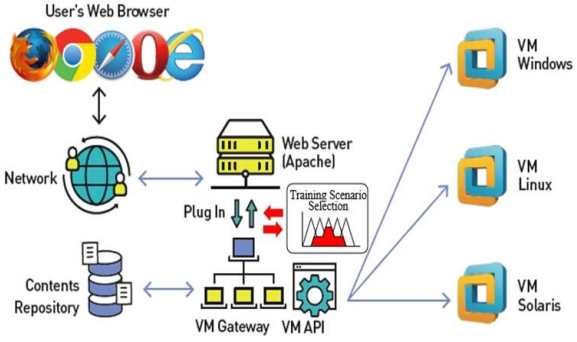


Fig. 3. Procedures of the proposed system

Fig. 3은 제안 시스템의 전체 동작 순서를 보여준다. 제안 시스템은 크게 4 단계(사용자 접속, 콘텐츠 선택 및 풀기, 퍼지 로직 실행, 맞춤형 시나리오 생성)로 구성된다. 사용자 접속 단계에서는 시스템 사용자는 웹 브라우저(web browser)을 통해 웹 서버(web server)에 접근한다. 콘텐츠 선택 및 풀기 단계에서는 사용자는 웹 페이지에 제공하는 콘텐츠들 중에 자신이 원하는 콘텐츠를 선택하고 푼다. 각 콘텐츠들은 시스템, 네트워크, 웹/응용, 악성코드로 분류되어 있는데, 각 분류에 따라 사용자 수준(예: 상, 중, 하)이 평가된다. 사용자가 선택한 콘텐츠들은 웹 브라우저에서 VM 게이트웨이와 응용 프로그램 프로그래밍 인터페이스(application programming interface)를 통해 VM 이미지들(Windows, Linux, Solaris 등)을 보여준다. 제안 시스템은 사용자가 풀었던 콘텐츠들에 따라 사용자 수준을 분류한다. 퍼지 로직 실행 단계에서는 분류된 수준을 입력 받아 정의된 퍼지 규칙을 기반으로 한 시나리오를 선택한다. 맞춤형 시나리오 생성 단계에서는 선택된 시나리오를 바탕으로 APT 공격 단계에 따라 콘텐츠들을 시나리오 형태로 제공한다. 따라서 본 시스템은 훈련생의 수준에 따라 사이버 훈련 시나리오를 자동 생성하여 훈련생의 사이버 침해 대응 능력을 향상시킬 수 있다.

2. Detailed Procedures

제안 시스템은 사용자 접속, 콘텐츠 풀기 및 사용자 수준 분류, 퍼지 로직 실행, 맞춤형 시나리오 생성으로 구성된다. Table 1은 제안 시스템의 의사코드(pseudocode)를 보여준다. 한 사용자는 시스템에 접근하고 콘텐츠들을 푼 다음(Table 1의 1~6줄), 한 사용자의 콘텐츠를 해결한 결과를 얻는다(Table 1의 8줄). 랜덤포레스트 기반으로 사용자 수준을 판단하고(Table 1의 9줄), 퍼지 시스템을 기반으로 사용자 맞춤형 시나리오를 제공한다(Table 1의 11~13줄).

Table 1. Pseudocode of proposed system

```
// Algorithm 1
// ExecuteProposedSystem(user_id)
1: for content.count do
2:    SolveContent(user_id, content_id);
3:    if exit_selection then
4:       break;
5:    end if
6: end for
7:
8: content_info=GetContentInfo(user_id);
9: contents_lv=RandomForest(content_info);
10:
11: user_scenario=RunFuzzy(contents_lv);
12:
13: ShowScenario(user_scenario);
```

2.1 User Access

제안 시스템의 사용자 접속 단계는 시스템 사용자는 웹 브라우저(web browser)을 통해 웹 서버(web server)에 접근한다.

Fig. 4. Main homepage of the proposed system

Fig. 4는 제안 시스템의 메인 화면을 보여준다. 메인 화면에서는 대분류로 원격교육, 취약점보안설정, 해킹방어가 분류되어 있다. 각 대분류는 그림 5와 같이 시스템 보호, 네트워크 보호, 웹 보호, 악성코드 분석으로 분류되어 있다.

2.2 Content Solving and Level Classification

제안 시스템의 콘텐츠들은 대/중 분류로 나누어져 있고, Table 2와 같이 총 300개의 콘텐츠로 구성되어 있다. 사용자는 각 콘텐츠의 가상 환경에 접속하는데 [13,14]에서는 '사용자 계정의 UID 확인'과 '비인가 계정 접속을 탐지' 콘텐츠에 대해 상세하게 소개하고 있다.

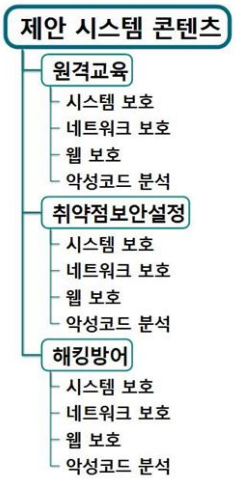


Fig. 5. Content of the proposed system

Table 2. Content of the proposed system

No.	Category	Field	Content Title
1	VSC	System	Verify UID of a user account
2	VSC	System	Create an account with a password, and change the password
3	VSC	System	Limit remote administrator login and session allowed time
4	VSC	System	Set IP Access Control Policy
5	VSC	System	Set and modify UMASK, PATH values for the system (Windows)
6	VSC	System	Set and modify UMASK, PATH values for the system (Linux)
7	VSC	System	Set and modify UMASK, PATH values for the system (Unix)
8	VSC	Network	Create an account with a password, and change the password
9	VSC	Network	Check the configuration values of the equipment, back up
10	VSC	Network	Set up and verify permissions for accounts and commands
11	HD	Web/App	Change the security-vulnerable preference value of a Web server
12	HD	Web/App	Check the logs on the web server
13	HD	Web/App	Setting up time synchronization for the Web server
14	HD	Malware	Check and set the Allow/Block policy
15	HD	Malware	Create an account with a password, and change the password and account permissions
16	HD	악성코드 분석	Set the number of failed remote connection and login for your account
17	HD	Malware	Set session connection time for account
18	HD	Malware	Performs Time Synchronization of Equipment
...	...	...	...
292	Online Education	System	Introduction to the Operating System
293	Online Education	System	Memory-Registry Introduction
294	Online Education	Network	Snort Introduction
295	Online Education	Network	Wireshark
296	Online Education	Web/App	Secure coding
297	Online Education	Web/App	Internet of Things Security
298	Online Education	Malware	Introduction to the virus protection system
299	Online Education	Malware	Static analysis of malicious code
300	Online Education	Malware	Dynamic Analysis of Malicious Codes

* VSC: Vulnerability Security Configuration
* HD: Hacking defense

제안 시스템은 한 사용자로부터 맞춤형 시나리오를 요청받으면 시스템은 Random Forest 기반으로 입력 변수들(콘텐츠 번호, 콘텐츠 난이도 등)에 따라 사용자 수준(상, 중, 하)을 분류한다[15]. 제안 시스템은 사용자 수준에 따라 퍼지 시스템을 통해 사용자 맞춤형 시나리오를 결정한다.

2.3 Execution of Fuzzy Rules

제안 시스템에서는사용자 수준에 따라 사용자 맞춤형 시나리오를 결정하기 위해 퍼지 논리 기법을 이용한다. Fig. 6은 퍼지 기법을 이용한 입력, 퍼지 if-then 규칙들, 출력 과정을 보여준다.

퍼지 논리의 입력 매개변수는 다음과 같다.

- 시스템 보호 수준(SYS_LEVEL): {BG(Beginner), IM(Intermediate), EX(Expert)}
- 네트워크 보호 수준(NET_LEVEL): {BG(Beginner), IM(Intermediate), EX(Expert)}
- 웹 보호 수준(WEB_LEVEL): {BG(Beginner), IM(Intermediate), EX(Expert)}
- 악성코드 분석 수준(MAL_LEVEL): {BG(Beginner), IM(Intermediate), EX(Expert)}

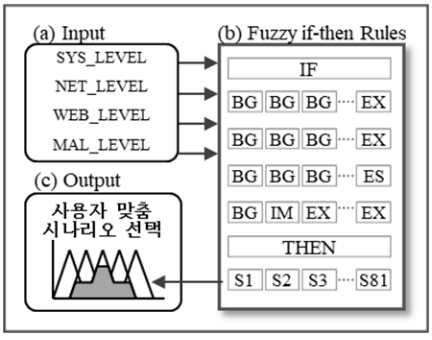
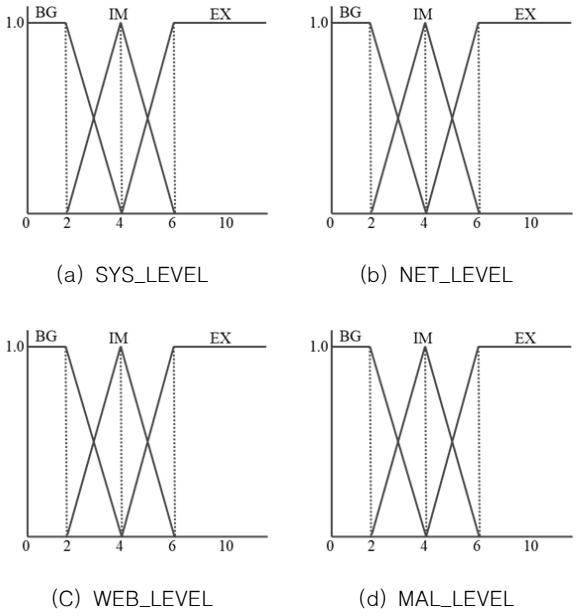


Fig. 6. Fuzzy rules

Fig. 6은 제안 시스템의 입력 값 4가지에 대한 퍼지 멤버십 함수를 보여준다. 퍼지 논리 기법의 추론은 맘다니 모델의 min-max 합성방법[16]을 사용하며, 출력을 위한 역 퍼지화 방법에서는 무게 중심법[17]을 사용한다.



(a) SYS_LEVEL (b) NET_LEVEL

(C) WEB_LEVEL (d) MAL_LEVEL

Fig. 7. Fuzzy membership functions

표 2는 제안 시스템의 퍼지 if-then 규칙들을 보여준다. 퍼지 규칙들은 4개의 입력 변수의 각 3가지 입력 값으로 총 81개(=3×3×3×3)의 규칙들로 구성되어 있다.

Table 3. if-then Rules

RULE 0: IF (SYS IS S_BG) AND (NET IS N_BG) AND (WEB IS W_BG) AND (MAL IS M_BG) THEN (RST IS SCN01) **RULE 1**: IF (SYS IS S_BG) AND (NET IS N_BG) AND (WEB IS W_BG) AND (MAL IS M_IM) THEN (RST IS SCN02) **RULE 2**: IF (SYS IS S_BG) AND (NET IS N_BG) AND (WEB IS W_BG) AND (MAL IS M_EX) THEN (RST IS SCN03) **RULE 3**: IF (SYS IS S_BG) AND (NET IS N_BG) AND (WEB IS W_IM) AND (MAL IS M_BG) THEN (RST IS SCN04) … **RULE 80**: IF (SYS IS S_EX) AND (NET IS N_EX) AND (WEB IS W_EX) AND (MAL IS M_EX) THEN (RST IS SCN81)

예를 들어, Table 3에서 보는 것과 같이 시스템 보호 수준이 초보자, 네트워크 보호 수준이 초보자, 웹 보호 수준이 초보자, 악성코드 분석이 초보자일 경우 시나리오 1번(SCN01)이 선택된다(RULE 0).

2.4 Scenario Automatic Generation

Fig. 8은 제안 시스템에서 콘텐츠 사용자 수준에 따라 퍼지 규칙에서 선택된 맞춤형 시나리오를 보여준다. Fig. 8의 사용자는 시스템, 네트워크, 웹, 악성코드 수준이 초보자인 경우이다.

Fig. 8. Example of APT based user-customized scenario

Fig. 9은 시스템 취약점의 '계정 원격 접속을 탐지하고 대응' 콘텐츠를 보여준다. 사용자는 '문제풀이 접속하기'를 통해 실습 콘텐츠에 접근하여 해당 문제를 풀 수 있다.

Fig. 9. Content of “Create a password-set account and change its password” in user-customized scenario

IV. Conclusions

최근에 사이버 보안에 대한 관심이 많이 증가함에도 불구하고 신기술들의 등장으로 사이버 보안을 효율적으로 수행할 전문적인 인력이 부족한 실정이다. 사이버 보안 전문 인력을 양성하기 위해 사이버 레이지를 활용하고 있지만, 다음과 같은 문제점이 있다.

- 가상훈련 시스템의 한계성
- 시나리오 기반의 실습 콘텐츠 개발과 운용상 문제점
- 단위 콘텐츠 개발 문제점
- 학습자 수준 고려 부족

본 논문에서는 상기 문제점을 해결하기 위해 사이버보안 훈련체계 사용자의 침해대응 능력을 향상하는 목적으로 퍼지 규칙 기반의 사용자 맞춤형 훈련 시나리오 자동 생성 시스템을 개발했다. 사용자 맞춤형 훈련 시나리오 자동 생성 시스템은 사용자 그룹의 강점 및 약점을 기반으로 퍼지 규칙을 통해 사이버공격 환경 및 시나리오 후보들을 생성한다. 그러므로 본 시스템은 훈련생의 수준에 따라 사이버 훈련 시나리오를 자동 생성하여 훈련생의 사이버 침해 대응 능력을 향상시킨다.

ACKNOWLEDGEMENT

This work was supported by the Technology development Program(S2591452) funded by the Ministry of SMEs and Startups(MSS, Korea)

REFERENCES

[1] Joint Publication 3-12, “Cyberspace Operations,” 8 June 2019

[2] Whitehouse.gov, “The National Cyber Range,” Whitehouse, 2009. [Online]. Available: https://obamawhitehouse.archives.gov/files/documents/cyber/DARPA - NationalCyberRange_FactSheet.pdf.

[3] D. Kim and Y. Kim, “A Study of Administration of Cyber Range,” J. Internet Comput. Serv., vol. 18, no. 5, pp. 9-15, 2017.

[4] Yong Goo Kang, Jeong Do Yoo, Eunji Pa가, Dong Hwa Kim, and Hyu Kang Kim, “Design and Implementation of Cyber Attack Simulator based on Attack Techniques Modeling,” Jounrnal of The Korea Society of Computer and Information, Vol. 25, No. 3, pp. 65-72, March 2020.

[5] H. Y. Lee, Y. S. Park, J. M. Ryoo, T. Korea, and S. For, “Generation of Random Virtual Environments for Cyber Kill Chain Training,” in The Korea Society For Simulation, 2018, pp. 15-18.

[6] Z. C. Schreuders, T. Shaw, M. Shan-A-Khuda, G. Ravichandran, J. Keighley, and M. Ordean, “Security Scenario Generator (SecGen): A Framework for Generating Randomly Vulnerable Rich-scenario VMs for Learning Computer Security and Hosting CTF Events,” in 2017 USENIX$ Workshop on Advances in Security Education (ASE), 2017.

[7] W. Feng, “A Scaffolded, Metamorphic CTF for Reverse Engineering,” in 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE), 2015.

[8] J. Burket, P. Chapman, T. Becker, C. Ganas, and D. Brumley, “Automatic problem generation for capture-the-flag competitions,” in 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE), 2015.

[9] DuDuIT, “Cyber-hacking response training system.” [Online]. Available: http://duduit.co.kr.

[10] Y. S. Park, J. M. Yyoo, H. Y. Lee, “Virtualization-based training content delivery system”. Kor. Patent No. 10-2020-0023934, 2020.

[11] J. Park, S. Yeom, S. Nam, D. Shin, and D. Shin, “Scenario-based Cyber Attack / Defense Education System Using Virtual Machine,” 2019 Korean Society For Internet Information Conference, 2019.

[12] D. Moon, H. Lee, and I. Kim, “Host based Feature Description Method for Detecting APT Attack-APT,” Journal of The Korea Institute of Information Security and Cryptology (JKIISC), vol. 24, no. 5, pp. 839-850, 2014. DOI: 10.13089/JKIISC.2014.24.5.839

[13] S. Nam, J. Ryoo, and Y. Park, “Virtual training system for checking user account and detecting unauthorized account access to counter cyber attacks,” 2019 Korea Convergence Security Association Conference, Oct. 2019.

[14] S. M. Nam, Y. S. Park, "Cyber Security Simulated Training System and Cyber Aegis", Bookk, Feb. 2020.

[15] J. Noh, D. Shin, and D. Shin, “Automated Classification by Efficient Learner Level based on Machine Learning,” 2019 Korean Society for Internet Information Conference, Nov. 2019.

[16] R. Babuška, “Fuzzy systems, modeling and identification,” Delft Univ. Technol. Dep. Electr. Eng. Control Lab. Mekelweg, vol. 4, 1996.

[17] S. H. Chi and T. H. Cho, “Fuzzy logic based propagation limiting method for message routing in wireless sensor networks,” in International Conference on Computational Science and Its Applications, 2006, pp. 58-67.

Authors

Su Man Nam received the B.S. degree in Computer Information from Hanseo University, Korea, and M.S. and Ph.D. degree in Electrical and Computer Engineering from SungkyunkwanUniversity, Korea, in 2013 and 2017 respectively. Dr. Nam joined a researcher in the Department of Biomedical Informatics, Ajou University, Suwon, Korea, in 2018. He is currently a senior researcher in DuDu IT, Ltd., Seoul, Korea. He is interested in modeling and simulation, WSN, and IoT.