Regular paper
Journal of the KIECS. pp. 449-456, vol. 13, no. 2, Apr. 30 2018, t. 88, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2018.13.2.449

칼라 페트리 네트를 이용한 랜섬웨어의 모델링

이요섭*

Modeling of Ransomware using Colored Petri Net

Yo-Seob Lee*

요 약

암호화폐의 등장은 해커에게 실제 금전적 이득을 취득할 수 있는 수단이 되었고, 이에 따라 최근 랜섬웨어가 급증하며 관련 피해가 크게 늘어나고 있다. 악성코드가 암호화폐를 만나 새로운 영역으로 확장되고 있으며, 앞으로 랜섬웨어가 더욱 증가할 것으로 예측된다. 이러한 문제들을 해결하기 위해 랜섬웨어의 침입 경로를 분석하여 랜섬웨어의 침입을 탐지하고 차단할 수 있는 모델이 필요하다. 본 논문에서는 최근 랜섬웨어들의 자료를 수집하여, 이를 토대로 랜섬웨어의 칼라 페트리 네트 모델을 작성하고, 분석하고자 한다.

ABSTRACT

The advent of cryptography has become a means of obtaining real monetary benefits to hackers, which has recently led to a surge in the number of Ransomware and the associated damage has increased significantly. It is expected that malicious codes will be expanded to new areas by meeting passwords, and Ransomware will be further increased in the future. To solve these problems, we need a model that can detect and block intrusion of Ransomware by analyzing the intrusion path of Ransomware. In this paper, we collect and analyze the data of Ransomware, and create and analyze Ransomware 's color Petri net model.

키워드

Ransomware, Colored Petri Net, Hacking, Modeling
랜섬웨어, 칼라 페트리 네트, 해킹, 모델링

Ⅰ. 서 론

랜섬웨어(Ransomware)는 컴퓨터에 침입해 문서나 다양한 파일들을 암호화한 후 돈을 요구하는 악성 프로그램이다. 사용자가 돈을 보내주면 복호화해 준다고 하지만 원례의 파일을 복구하는 사례가 없다. 공격대상은 PC뿐 아니라 스마트폰, IoT까지 대상으로 하고 있다.

랜섬웨어의 감염경로는 신뢰할 수 없는 사이트, 스팸메일이나 스피어피싱, 파일 공유 사이트, 눈, 네트워크 등을 통해 이루어진다.

현재 버전들의 랜섬웨어 복구 방법은 해커에게 키 값을 지불하여 해결하고 있다. 이러한 문제들을 해결하기 위해 랜섬웨어의 침입 경로를 분석하여 랜섬웨어의 침입을 탐지하고 차단할 수 있는 모델이 필요하다.

이 모델을 통하여 랜섬웨어의 침입을 탐지하고 차단할 수 있는 소프트웨어를 손쉽게 개발할 수 있는

* 교신저자 : 평택대학교 ICT 융합학부 스마트컨텐츠전공
• 접 수 일 : 2018. 02. 12
• 수정완료일 : 2018. 03. 15
• 게재확정일 : 2018. 04. 15
• Received : Feb. 12, 2018, Revised : Mar. 15, 2018, Accepted : Apr. 15, 2018
• Corresponding Author : Yo-Seob Lee
School of ICT Convergence Smart Contents Major, Pyeongtaek University,
Email : yslee@ptu.ac.kr

토대를 제공할 수 있으며, 차후 신종 랜섬웨어의 대처에도 손쉽게 대응할 수 있다.

본 논문에서는 최근 랜섬웨어들의 자료를 수집하여 공격 흐름에 대해 분석하고, 이 흐름도를 표현하기 위해 칼라 페트리 네트를 이용하여 랜섬웨어 모델을 작성하고, 시뮬레이션을 수행하여 분석하고자 한다[1-6].

향후에는 이 모델을 통하여 랜섬웨어의 침입을 탐지하고 차단할 수 있는 소프트웨어를 손쉽게 개발할 수 있는 토대를 제공할 수 있으며, 차후 신종 랜섬웨어의 대처에도 손쉽게 대응할 수 있다

II. 랜섬웨어의 개념과 공격 흐름도

2.1 랜섬웨어의 개념

랜섬웨어(Ransomware)는 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류로서, 사용자의 동의없이 해당 컴퓨터에 불법으로 설치된다. 컴퓨터로의 접근이 제한되기 때문에 제한을 없애려면 해당 악성 프로그램을 개발한 자에게 값을 지불해야 한다[1].

2.2 랜섬웨어의 공격 흐름도

랜섬웨어는 일반적인 공격 흐름은 그림 1과 같이 이루어진다[2]. 일단 랜섬웨어에 감염이 되면 중요한 정보를 포함하는 파일들을 검색하여 최대한 많이 확보한 후에 이 파일들을 암호화하게 된다. 피해자에게 꼭 필요한 파일들인 경우에는 복원을 위해 피해자가 요금을 지급할 수 있기 때문이다.

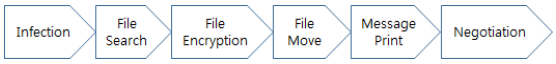

그림 1. 랜섬웨어의 일반적인 공격 흐름
Fig. 1 Typical attack flow for Ransomware

1) Ransomware, https://en.wikipedia.org/wiki/ Ransomware.

2) Hacking Security: Understanding Ransomware Purpose and Principles #02, http://blog.kinesis.kr/136.

파일들의 암호화가 이루어진 후에 감염된 파일들을 바탕화면 위치 등으로 이동시켜서 많은 중요 자료들이 손상되어 복원을 해야 할 필요성이 있다는 것을 알려준다.

피해자가 바탕화면에 옮겨진 파일들을 발견하고 이상하다는 증상을 알게 된 후, 공격자는 피해자에게 중요 자료의 복원을 위해 금전적인 비용을 지불하라는 메시지를 전달한다. 이후에 협상을 통해 비용을 전달하고 중요 파일의 복원을 시도하게 된다.

III. 랜섬웨어 모델

3.1 랜섬웨어 모델

랜섬웨어 모델은 랜섬웨어가 처리되는 흐름도를 나타내는 모델로, 그림 3과 같이 여러 단계들로 이루어진다.

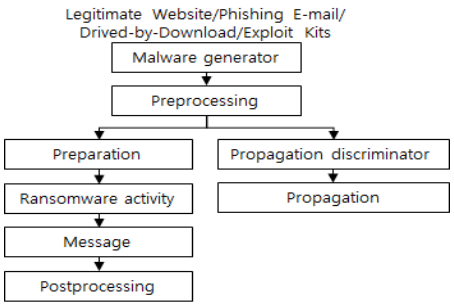

그림 2. 랜섬웨어 모델
Fig. 2 Ransomware Model

Malware generator는 악성코드를 생성시키는 부분을 나타낸다. Preprocessing은 랜섬웨어가 동작하기 전에 킬스위치와 같이 미리 처리되는 부분을 나타낸다. Propagation dicsriminator는 악성코드를 네트워크를 통해 전파되는지의 여부를 판별한다. Preparation은 랜섬웨어를 동작시키기 위한 코드와 토르와 비트코인 정보, 공개키와 AES 키 등을 준비한다. Ransomware activity는 파일에 대한 암호화가 이루어지는 부분이다. Message는 랜섬 노트를 출력하는 부분이다. Postprocessing은 랜섬웨어에 감염된 이후의 처리, 기간이 지난 후에 모든 파일을 삭제하는 등의 부분을 나타낸다.

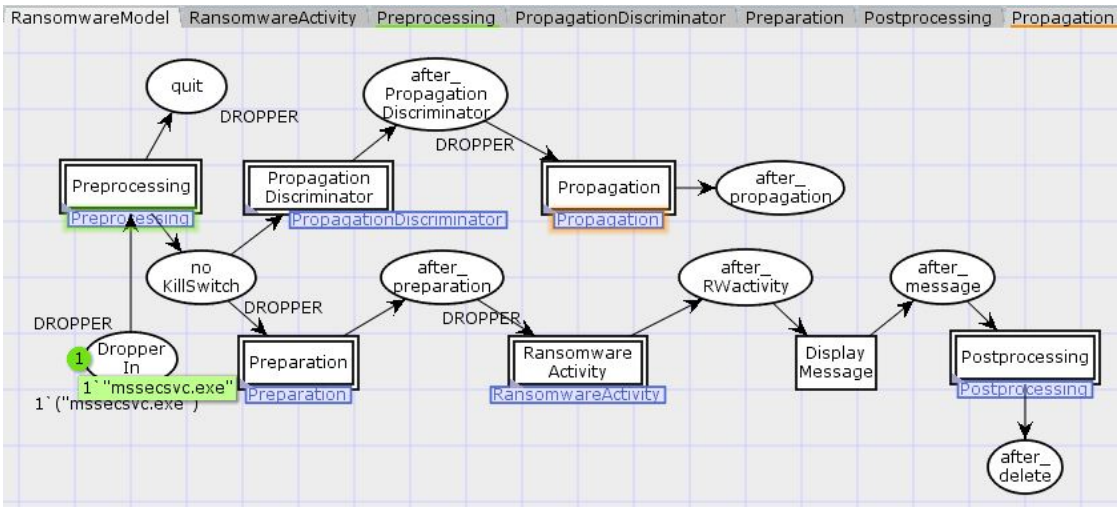

그림 3. Design/CPN의 랜섬웨어 모델
Fig. 3 Ransomware model in Design/CPN

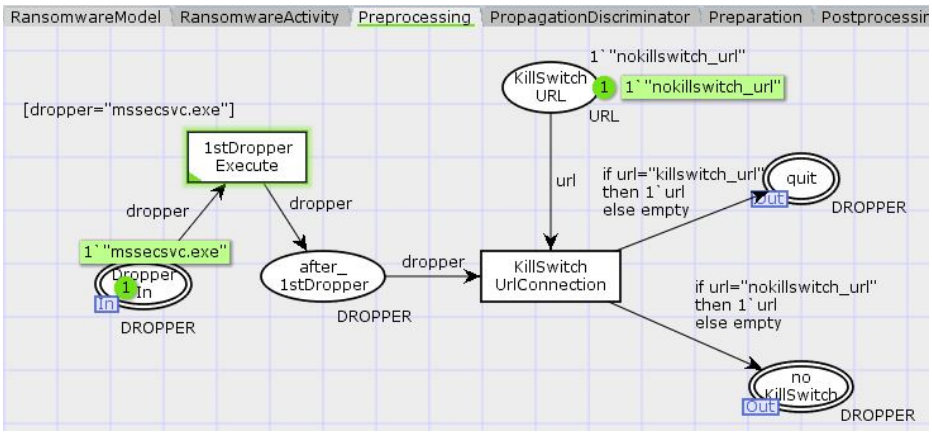

그림 4. Prepocessing 모듈
Fig. 4 Preprocessing module

3.2 Design/CPN을 이용한 랜섬웨어모델의 표현

랜섬웨어 모델은 Jensen에 의한 칼라 페트리 네트를 기반으로 구성되며[7], 랜섬웨어 모델은 Design/CPN이라는 도구를 사용하여 모델링한다[3]. Design/CPN은 칼라 페트리 네트로 모델링하고 시뮬레이션을 수행할 수 있도록 해주는 프로그램이다. 그림 4는 랜섬웨어 모델을 칼라 페트리 네트로 표현한 것이다.

입력 패턴은 (Dropper)의 형태로 표현된다. 그림 4의 입력 패턴의 1`("mssecsvc.exe")를 보면, mssecsvc.exe 파일이 dropper로 동작하는 것을 알 수 있다. mssecsvc.exe 파일은 워너크라이 랜섬웨어를 발생시키는 dropper이다.

랜섬웨어 모델은 킬 스위치의 존재여부를 체크하는 Preprocessing 모듈과 랜섬웨어 전파와 관련된 Propagation Discriminator, Propagation 모듈, 악성코드 생성과 실행과 관련된 Preparation,

3) Design/CPN, http://cpntools.org/.

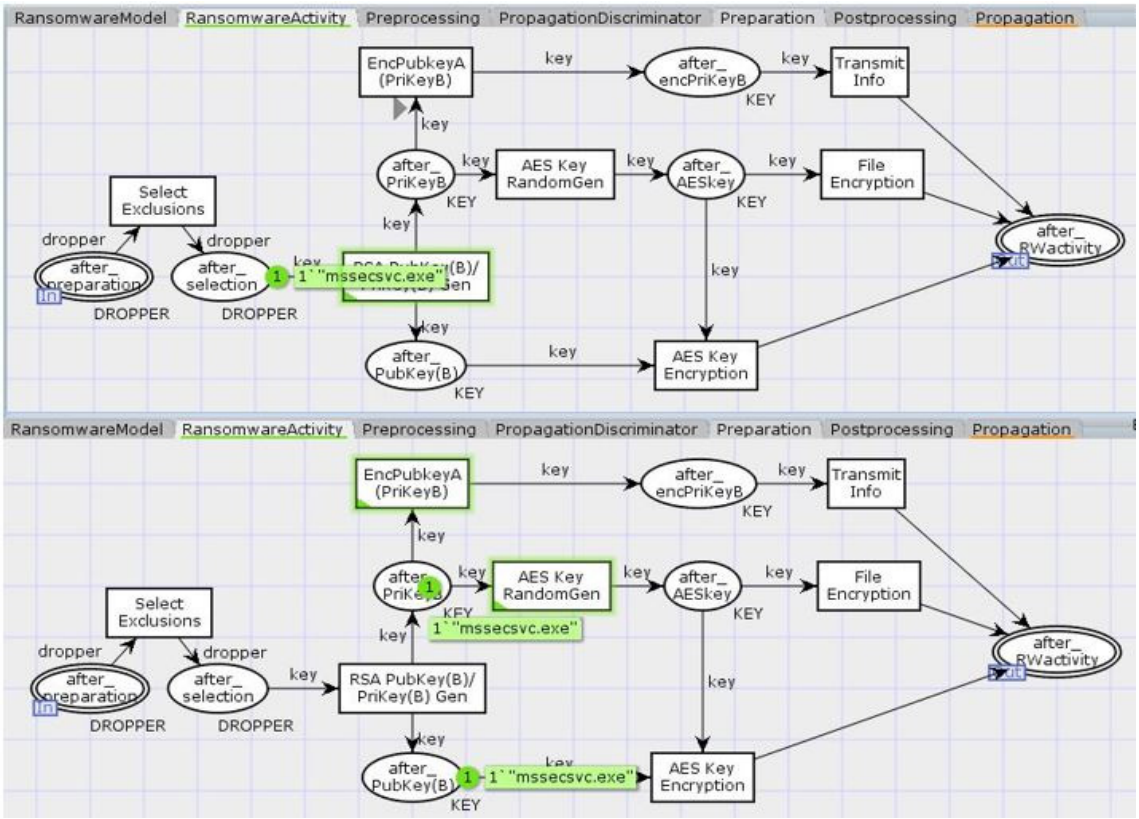

그림 5. Ransomware Activity 모듈(1)
Fig. 5 Ransomware Activity module(1)

Ransomware Activity 모듈, 해커에게 비용을 지불하지 않으면 암호화된 파일을 모두 삭제하는 Postprocessing 모듈로 구성되어 있다.

킬스위치는 랜섬웨어 진입 함수(WinMain)에 위치해 있으며, 특정 도메인과의 연결 상태만 체크한다. 그림 5의 Preprocessing 모듈의 킬 스위치 체크 루틴에서 악성코드가 특정 도메인에 접속이 되지 않을 경우 랜섬웨어는 감염 시스템 대상으로 악성행위를 진행하게 된다.

Propagation Discriminator 모듈에서 랜섬웨어 악성코드(mssecsvc.exe)는 전파와 관련하여 내부망을 대상으로 하는 공격과 외부망을 대상으로 하는 공격 2가지로 나누어져 있다. 내부망에서는 감염시스템 IP와 NetMask 정보를 이용하여 동일 대역에 위치한 공격 대상 IP를 계산하여 배열을 생성하고 해당 IP들을 대상으로 순차적 공격을 진행한다. 이후, 랜덤한 공인 IP 대역을 생성한 후 외부로 취약점 공격을 진행한다.

Preparation 모듈은 최초 드랍퍼 악성코드(mssecsvc.exe)에서 추가 악성코드(tasksche.exe)를 생성하는데, 이 파일이 실제 랜섬웨어 행위를 수행한다. 파일 암호화와 비트코인 결제 등 랜섬웨어 동작에 필요한 추가 코드를 생성한다.

그림 6과 그림7의 Ransonware Activity 모듈은 폴더 등 암호화 제외 대상을 선별한다. 특히, 윈도우의 정상적인 동작에 필요한 기본 폴더, 파일들과 비트코인 결제와 관련된 인터넷 익스플로러 등 관련 파일들이 제외된다. 비교적 속도가 빠른 대칭키 알고리즘으로 다수의 파일을 암호화시키고, 해커만 해독이 가능하도록 공개키를 이용하여 암호화에 사용한 대칭키들을 암호화 시켜 해커에게 전송한다.

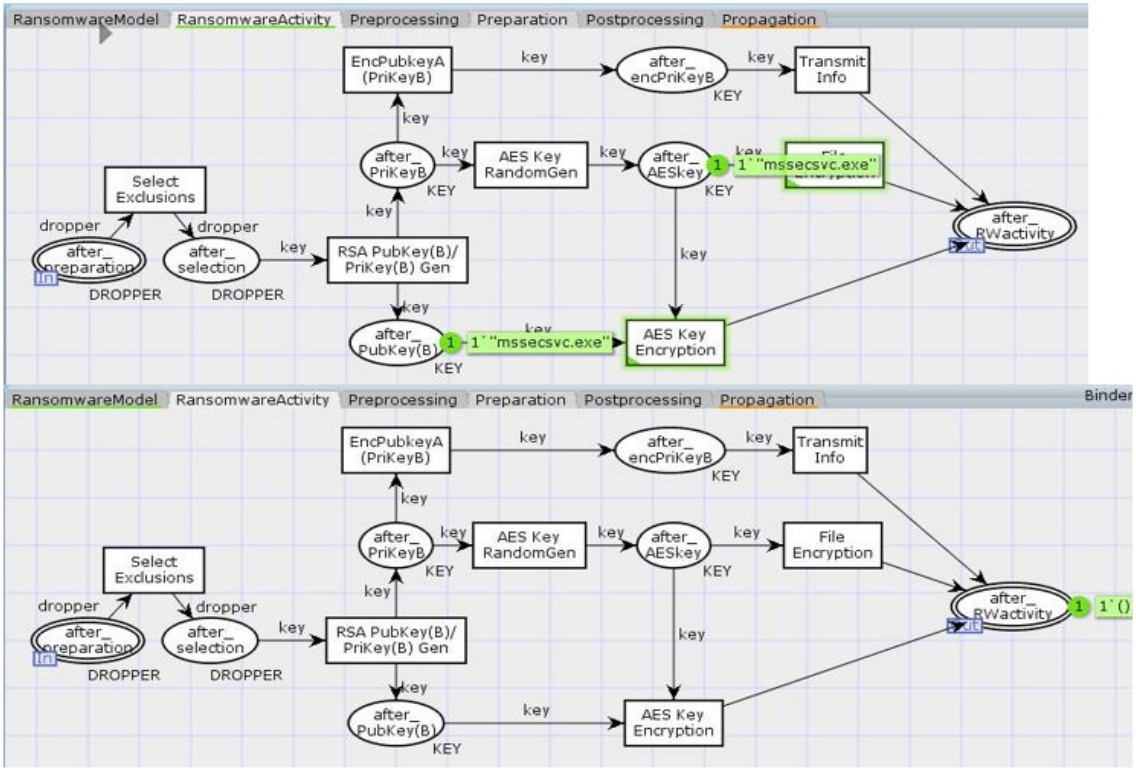

그림 6. Ransomware Activity 모듈(2)
Fig. 6 Ransomware Activity module(2)

IV. 랜섬웨어 CPN 모델의 분석

4.1 랜섬웨어 모델의 변종 모델링

랜섬웨어 모델은 랜섬웨어의 행위 이전과 이후에 Preprocessing과 Postprocessing 모듈을 통해 랜섬웨어의 다양한 변종들을 모델링하여 랜섬웨어에 대처하는데 도움을 줄 수 있다. 워너크라이 랜섬웨어의 경우에 Preprocessing에서 킬스위치의 존재여부를 처리하는 부분을 모델링하였으며, Postprocessing에서 기한이 지난 경우 모든 암호화 파일을 삭제하는 부분을 모델링하였다.

4.2 발생 그래프를 이용한 제안한 모델의 분석

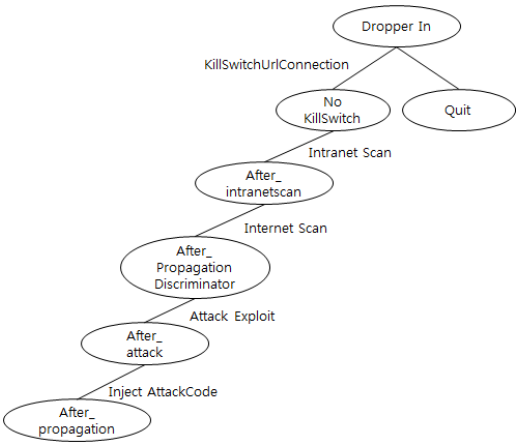

그림 8. 악성코드가 전파되는 경우의 발생그래프
Fig. 8 Occurrence graph when malicious code is propagated

랜섬웨어 모델은 칼라 페트리 네트에 의해 모델링되며, 사건 발생 그래프(occurrence graph)를 사용하여 노드가 도달 가능한 시스템 상태를 나타내고 아크가 변경 가능한 상태를 나타내는 방향성 그래프를 구축한다. 이 그래프를 이용하여 모델의 완벽한 분석이 가능하다.

그림 8에서는 악성코드가 전파되는 경우의 발생그래프를 나타낸다. 킬스위치가 존재하지 않는 경우 내부 네트워크를 먼저 취약점을 스캔하고 그 후에 외부 인터넷을 스캔하여 취약점을 발견하는 경우 취약점을 공격하여 공격코드를 주입하는 것을 알 수 있다. 단계별로 네트워크 상황을 감시하면 악성코드의 전파 단계를 탐지하는데 도움을 줄 수 있다.

그림 9에서 악성코드가 동작하는 경우의 발생그래프를 나타낸다. 킬스위치가 존재하는 않는 경우 최초 dropper 악성코드가 새로운 dropper 악성코드를 생성하고, 이 악성코드가 공개키, AES 키, 토르 등 필요한 추가 코드를 생성하고, 암호화 제외 대상을 선별한다. AES 키로 다수의 파일을 암호화시키고, 암호화에 사용한 대칭키들을 공개키로 암호화 시켜 해커에게 전송하는 것을 알 수 있다. 단계별로 시스템의 프로세스를 감시하면 악성코드의 동작을 탐지하여 대응책을 세우는데 도움을 줄 수 있다.

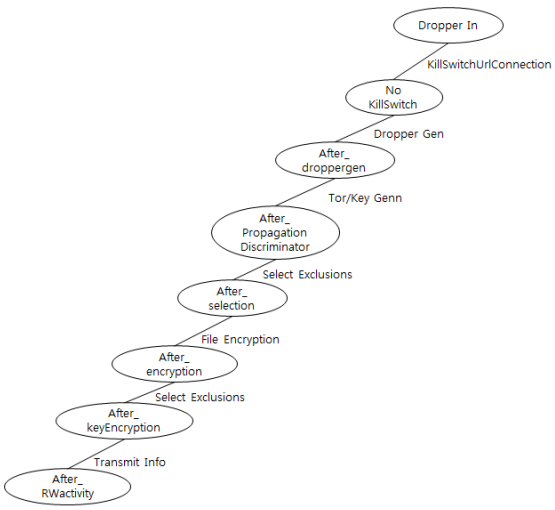

그림 9. 악성코드가 동작하는 경우의 발생그래프
Fig. 9 Occurrence graph when malicious code is running

V. 결 론

암호화폐의 등장으로 앞으로 랜섬웨어가 더욱 증가할 것으로 예측된다. 이러한 문제들을 해결하기 위해 랜섬웨어의 침입 경로를 분석하여 랜섬웨어의 침입을 탐지하고 차단할 수 있는 모델이 필요하다. 본 논문에서는 최근 랜섬웨어들의 자료를 수집하여, 이를 토대로 랜섬웨어의 칼라 페트리 네트 모델을 작성하여 분석하였다. 이 모델을 통하여 랜섬웨어의 침입을 탐지하고 차단할 수 있는 소프트웨어를 손쉽게 개발할 수 있는 토대를 제공할 수 있으며, 차후 신종 랜섬웨어의 대처에도 손쉽게 대응할 수 있다.

향후에는 새로운 형태의 랜섬웨어에 대한 추가 연구와 딥 러닝을 위한 모델에 대한 연구가 필요할 것으로 생각된다[8].

감사의 글

이 논문은 2016학년도 평택대학교 학술연구비의 지원에 의하여 연구되었음.

References

[1] Y. Lee, “Design and Analysis of Multiple Intrusion Detection Model,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 6, 2016, pp. 619-626.

[2] Y. Chun, “Hacking Detection Mechanism of Cyber Attacks Modeling,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 8, no. 9, 2013, pp. 1313-1318.

[3] S. Park, “Current Status and Analysis of Domestic Security Monitoring Systems,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 9, no. 2, 2014, pp. 261-266.

[4] W. Li, R. Wu, and H. Huang, “Colored Petri Nets Based Modeling of Information Flow Security,” *2009 Second International Workshop on Knowledge Discovery and Data Mining*, Moscow, Russia, 23-25 Jan. 2009.

[5] B. Jasiul, M. Szpyrka, and J. Śliwa, "Malware Behavior Modeling with Colored Petri Nets," *Computer Information Systems and Industrial Management Volume 8838 of the Series Lecture Notes in Computer Science,* 5-7 Nov. 2014, pp 667-679.

[6] B. Jasiul, M. Szpyrka, and J. Śliwa, "Formal Specification of Malware Models in the Form of Colored Petri Nets," *Computer Science and its Applications Volume 330 of the series Lecture Notes in Electrical Engineering,* 2015, pp 475-482.

[7] K. Jensen and L. Kristensen, *"Colored Petri Nets – Modeling and Validation of Concurrent Systems.* Berlin: Springer-Verlag, 2009.

[8] Y. Lee and P. Moon, "A Comparison and Analysis of Deep Learning Framework," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 12, no. 1, 2017, pp. 115-122.

저자 소개

이요섭(Yo-Seob Lee)

1990년 숭실대학교 전자계산학과 졸업(공학사)
1992년 숭실대학교 대학원 컴퓨터학과 졸업(공학석사)
1999년 숭실대학교 대학원 컴퓨터학과 졸업(공학박사)
2016년 ~ 현재 평택대학교 ICT융합학부 스마트컨텐츠전공 교수
※ 관심분야 : 모바일 애플리케이션, 네트워크보안, 딥 러닝, IoT