JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 21, No. 11 : 2199~2205 Nov. 2017

공격 원점 타격을 위한 사이버 킬체인 전략

유재원[1] · 박대우[2*]

Cyber kill chain strategy for hitting attacker origin

Jae-won Yoo[1] · Dea-woo Park[2*]

[1]Department of Convergence Technology, Hoseo Graduate School of Venture, Seoul 06724, Korea
[2*]Department of Convergence Technology, Hoseo Graduate School of Venture, Seoul 06724, Korea

요 약

현대 ICT 기술의 발달은, 국가와 사회에 인프라를 이용하여 사이버 세계를 구성하고 있다. 사이버 세계에서는 국경이 없다. 세계 각국들은 자국의 이익을 목적으로, 사이버 공격을 수행하고 있다. 사이버 공격을 방어하기 위해서는 사이버 킬체인 전략이 필요하다. 사이버 공격을 방어하거나, 공격책임을 판단하기 위해서는, 공격 원점지의 파악이 중요하다. 공격 원점지에 대한 타격을 하기 위해서는, 전략적인 사이버 킬체인이 필요하다. 본 논문에서는 공격 원점지를 분석하는 연구를 한다. 그리고 공격 원점지 타격을 위한 사이버 킬체인을 분석한다. 공격 원점지 타격을 위한 효율적이고 맞춤형 사이버 킬체인 전략을 연구한다. 사이버 킬체인 전략은 비대칭 전력으로, 핵과 미사일의 위력을 대치할 수 있는 실용적인 전략이 될 것이다.

ABSTRACT

The development of modern ICT technology constitutes cyber world by using infrastructure in country and society. There is no border in cyber world. Countries around the world are carrying out cyber attacks for their own benefit. A cyber killer strategy is needed to defend cyber attacks. In order to defend the cyber attack or to determine the responsibility of attack, it is important to grasp the attacker origin point. Strategic cyber kill chains are needed to strike against the attacker origin. In this paper, we study the analysis of attacker origin. And analyze the cyber kill chain for attacker origin point strike. Study the efficient and customized cyber kill chain strategy for attacking the origin point. The cyber kill chain strategy will be a practical strategy to replace the power of nuclear and missiles with asymmetric power.

키워드 : 공격원점, 사이버 공격 , 사이버 킬체인, 사이버보안

Key word : Attacker Origin, Cyber Attack, Cyber Kill Chain, Cybersecurity

Received 27 October 2017, **Revised** 31 October 2017, **Accepted** 04 November 2017

* **Corresponding Author** Dea-woo Park(E-mail:prof_pdw@naver.com, Tel:+82-2-2059-2352)
Department of Convergence Technology, Hoseo Graduate School of Venture, Seoul 06724, South Korea

Open Access https://doi.org/10.6109/jkiice.2017.21.11.2199 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

2017년 9월 13일 북한은 국제사회의 경고에도 불구 6차 핵실험을 실시하였다. 이후에도 미사일 발사시험을 하여 국제사회의 불안을 유발시키고 있다.

북한은 00년대 이후부터 한미 동맹 전력 대비 재래식 전력 열세를 극복하고 위해 노력을 하여왔다[1]. 비대칭 전력 일환으로 핵WMD 및 사이버 전력을 지속 증강하고 있다.

핵 WMD 전력에 대응하기 위하여 한국형 3축 체계를 구축하여 대응하고 있다. 핵 WMD을 사용하기 전에 식별해서 선제적 타격을 의미하는 Kill Chain, 핵 WMD 전력이 투사시 피해최소화를 위한 한국형 미사일방어체계(KAMD), 핵WMD 피해 발생이후 공격지휘세력에 대한 대량응징보복작전(KMPR)으로 개념이 마련되고 실현이 되고 있는 실정이다.

이에 반해, 북한의 사이버 전략에 대응하기 위한 전략 개발은 걸음마 단계라고 보고 있다. 이마저도 군이 아닌 록히드마틴, 베다시스 등 기업에서 마련되고 있는 실정이다.

본 논문에서는 사이버 공격에 대비하기 위한 식별하고 사전 공격을 무력화시키는 사이버 Kill Chain구축 전략에 대해 알아보고자 한다.

Ⅱ. Kill chain관련 연구 동향

2.1. Kill Chain 개념

킬체인은 미군이 1991년 걸프전 이후 중동지역에서 전쟁을 수행하면서 적 미사일이나 지도부 및 테러요원과 같은 기민하게 움직이는 시한성 표적에 대한 효과적인 타격방법을 모색하는 과정에서 등장한 개념 미군의 역동적인 표적처리절차(Dynamic Targeting Step)'에 대한 별칭이다[2]. 즉, 사전 식별되고 움직이지 않는 대상이 아니라 갑자기 나타나는 위협에 대해 긴급표적처리절차이다.

미군의 긴급표적처리절차는 그림 1과 같이 나타내고 있다[3, 4].

Fig. 1 Kill Chain Concept of USAF

그림 1에서 나와 있듯이 6단계로 절차를 볼 수 있다. 1단계는 위협에 대한 전장을 식별하는 과정(Find)이며 2단계는 위협요소가 식별되면 해당전장에 대해 집중적인 관찰을 통해 피아식별 과정(Fix)과정, 3단계는 지속적인 감시를 통해 최신화된 타겟 정보를 유지하고(Track), 4단계는 해당 타겟에 대해 적절한 전력을 결정하는 과정(Target), 5단계는 결정된 전력으로 타겟을 제거(Engage)하며, 6단계로 피해평가(Assess)를 실시하게 된다.

2.2. 한국형 Kill Chain 개념

한국형 Kill Chain은 북한 미사일에 대비하기 위해 미공군 Kill Chain 운용 개념과 유사하며 그림 2와 같이 4단계로 간략화[5]되어 있다.

Fig. 2 Kill Chain Concept of ROK MND[6]

그림 2와 같이 한국형 킬체인이란 북한이 핵, 미사일로 한국을 타격할 가능성이 커질 경우, 그림 2와 같이 실시간 탐지(Real-time detection) - 식별(Identification) - 결심(Decision-Making) - 타격(Strike)의 과정으로 미 공군의 킬체인 과정에서 나타난 추적(Track) 및 평가(Assess)과정을 생략하였다. 한국은 이런 징후를 조기에 포착하여 선제공격을 실시하여 제거하는 개념이다.

2.3. Kill Chain 구현요구 사항

Kill Chain 전략은 구현되기 위해서는 감시체계, 결심체계인 C4I체계, 그리고 타격/요격체계가 필요하다. 추가적으로 각 체계를 유기적으로 연동되는 체계, 즉 System of System이 필요하다고 알려져 있다.

전략은 목표와 수단, 운영개념으로 구성되며 Kill Chain은 공세적 방위전략이다. 즉, 목표는 우군 방위이며, 목표는 선제타격을 통한 위협 제거이고, 운영개념은 공세적 운용으로 볼 수 있다. 침략 임박시 행해지는 선제타격, 혹은 미래위협을 사전에 제거하는 예방전쟁이 대표적인 공세적 방위전략이다.

방위전략으로서 억제전략은 능력(Capability), 의사소통(Communication), 신뢰성(Credibility) 등 3C를 만족시켜야 성공이 가능하다. 능력은 필요시 타격을 할 수 있는 역량이며, 의사소통은 상대방에게 아군 네트워크를 공격하려는 징후가 식별될시 공격하겠다는 의사를 밝히고, 징후가 식별될 경우 실제로 타격을 감행하고 상대에게 공격당할 수 있다는 확신을 주어야 한다[3].

2.4. 사이버 Kill Chain 개념 등장

사이버 Kill Chain의 개념을 사용한 것은 록히드마틴사[7]에서 최초 도입한 이후 베다시스사[8] 등에서 개념을 발전시키고 있다.

록히드마틴社는 그림 3과 같이 APT 공격형태를 기반으로 Kill Chain 모델을 제시하였다. 정보를 통합하는 정찰(Reconnaisance)단계부터 목적 달성(Actions on Objectives)까지 7단계를 거치게 되어 있다. 록히드마틴社의 Kill Chain 모델은 단계별 공격 단계를 차단에 중점을 두고 있다.

7단계의 공격내용을 NTT Security에서[9] 다음과 같이 설명하고 있다.

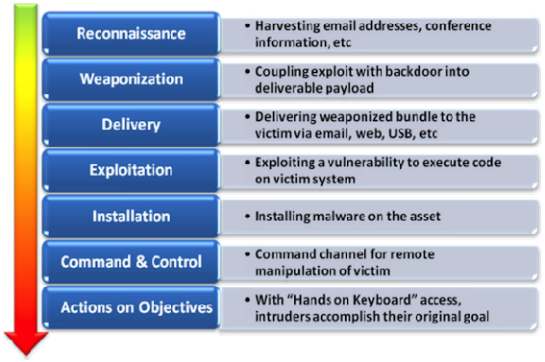

Fig. 3 Cyber Kill Chain Concept of LM

① 정찰(Reconnaissance): 목표물을 정하고 대상을 식별하여 정보를 연구하는 내용으로 이 과정은 대상 목표물의 공격에 활용할 수 있는 이메일 주소와 같은 정보를 인터넷으로부터 수집하고 사회적 관계 정보까지 획득할 수 있는 SNS 등의 다양한 여러 경로들을 활용하거나 그 외에 다양한 기술들을 활용하여 정보 수집을 하게 된다.

② 무기화(Weaponization) : 알려진 취약점 중 패치되지 않은 취약점(Adobe PDF 문서의 취약점 또는 Microsoft Office 문서의 취약점 등)을 알려진 취약점을 악용하는 익스플로잇을 활용하여 사용자에게 전달되어 유인할 수 있는 무기를 만든다.

③ 유포(Delivery) : 목표물 대상 사용자에게 발송하는 이메일의 파일 또는 링크 첨부, 웹사이트 링크, USB 미디어 장치 등 다양한 형태로 제작된 무기를 전달하게 된다. 최근 백신이나 보안 프로그램의 패치 기능에 대한 취약점을 이용하는 방식 등 보다 고도화된 방법도 증가 하고 있다.

④ 취약공격(Exploitation) : 대상 목표물에 전달된 무기(익스플로잇)가 구동되면서 공격자가 악의적으로 제작한 코드가 실행되어 대상물의 취약점을 이용하여 의도된 공격 방법이 활성화 된다.

⑤ 설치(Installation) : 공격자가 지속적으로 대상목적지를 장악할 수 있는 백도어(Backdoor)나 원격접근(Remote Access) 가능한 악성 프로그램을 설치한다.

⑥ 명령과 제어(Command and Control) : 공격자가 대상물을 제어할 수 있는 통신 채널(Command and Control)이 생기면서 의도적인 수동 조작 가능해지고 내부 목표에 접근 할 수 있게 된다.

⑦ 목적달성(Actions on Objectives) : 공격자는 목표 데이타를 수집, 암호화, 전달까지 성공하여 목표한 결과물을 획득할 수 있게 된다.

그림 4는 록히드마틴社 단계별 대응절차이다. 이 절차에서 근원지에 대한 공격(Destroy)은 현실적으로 제시하자 못하고 있다.

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Fig. 4 Courses of Action Matrix of LM

NTT Security에서도 사이버 킬체인에 대한 대응전략[10]을 Center for Internet Security (CIS)에서 정의한 Critical Security Controls (CSC)와 매핑[11] 하여 각 단계별 방어 전략을 제시하고CSC 기준을 참고하여 어떠한 대응을 할 수 있는지 제시하고 있으나 동일한 문제점을 가지고 있다. 또한, Verdasys사의 Kill Chain 모델은 그림 5과 같다. 방어(Protect), 탐지(Detect), 조사(Investigate), 억제(Contain)의 4단계 대응 절차에 초점이 맞추어져 있다.

Fig. 5 Cyber Kill Chain Concept of Verdasys

2.5. 사이버 Kill Chain의 한계[12,13]

록히드마틴社 및 베다시스社의 Kill Chain모델을 살펴보면 이동단계(Delivery) 이후 탐지시 이미 적이 네트워크 내부로 침입이 진행된 상태로 대부분의 방어체계는 통과하여 방어자에게 수세적 대응만 할 수 있도록 강요한다.

또한, 원점 타격을 위한 대응방법은 제시하지 못하고 있다. 따라서 공세적 대응을 위한 사이버 Kill Chain 전략이 필요한 실정이다.

Ⅲ. 사이버 Kill chain 구축 방안

3.1. 기존 Kill Chain 모델의 한계 및 의미

기존 록히드마틴社와 베다시스社에서 제안한 Kill Chain은 현실세계의 Kill Chain과 개념부터 차이를 보인다.

현실세계 Kill Chain은 선제적 억제개념이 반영되어 있어 공격자가 공격시도 자체를 못 하게 하는 전략이라며, 제시된 사이버 Kill Chain은 공격자 입장에서 침투단계를 모델화시켰으며 침투단계를 단절시켜서 Kill Chain을 무력화시키는데 중점을 두고 있다.

하지만, 기존 사이버 Kill Chain 모델연구의 성과는 우리가 제시한 구축 모델에서 통제가능 네트워크에서 필요한 기술요소들을 무엇인지 제시해주고 있다.

3.2. 제안하는 사이버 킬체인 구현 요소

사이버 Kill Chain 체계도 그림 6과 같이 현실 세계의 Kill Chain과 동일하게 감시정찰(Sensor) - 결심(Decision) - 타격체계(Strike)와 연동체계(System of Systems)가 필요로 한다.

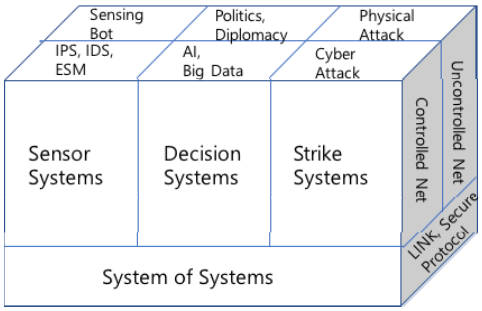

Fig. 6 Proposed Cyber Kill Chain Concept

제안되는 사이버 Kill Chain은 연동체계를 바탕으로 해서 감시정찰-결심-타계체계로 구성되며, 통제가능한 국내 영역의 네트워크(Controlled Net)와 외부 네트워크(Uncontrolled Net)로 구분하였다.

사이버 킬체인의 영역 중 통제가능 네트워크는 국내 네트워크와 국내 현실사회를 총괄하는 의미이며, 우리의 공권력이 미치는 영역이라 할 수 있다.

반면, 외부 네트워크로 표현된 부분은 물리적 현실 세계를 포함한 사이버 공간으로 우리가 임의대로 할 수 없는 영역을 총괄하였다. 즉, 적국의 사이버 공간 및 사회를 의미한다.

3.3. 사이버킬체인 감시체계(Sensor) 제안

감시정찰은 통제가능 네트워크(Controlled Net)뿐만 아니라 통제가 제한되는 네트워크(Uncontrolled Net)에 대한 감시정찰체계도 중요하다.

록히드마틴社가 제시한 킬체인 대응방안은 그림 4에서 제시된 기술들은 감시 체계에 활용할 수 있는 기술로 적합하다. 다만, 그림 6처럼 침입탐지체계(IDS), 침입방지체계(IPS), 통합보안관제체계(ESM) 등 통제가능 네트워크(Controlled Net)에서 수집되는 정보를 통해 공격자의 특이 행동을 점검・확인할 수 있다.

또한, 외부 네트워크(Uncontrolled Net)에 활동하는 아니라 감시 봇(Sensing Bot)이 필요하다. 외부 네트워크에서 식별되는 이상 현상에 대한 사전 탐지를 위해서는 사전 투입이 필요하다.

다만, 감시행위 자체가 상대방에게 위협이 되지 않기 위해서 위협행위를 최소화 혹은 하지 말아야 한다. 추가하여 주변국가에 발생하는 악성코드(Malware), 언론에서 거론되거나 조사 중인 사이버 범죄에 대해 현실 세계의 정보 등도 사이버공간에서 수집된 정보와 결합되어야 한다.

즉, 공격자의 네트워크 혹은 체계를 감시할 수 있는 사이버공간 감시체계와 현실 세계의 감시체계는 분리되어서는 안 된다.

3.4. 사이버 결심(Decision)체계 제안

결심 체계로는 각종 로그파일, 침입시도 패턴, 감시봇 등을 통해 수집되는 다양한 소스의 감시정보를 처리하고 분석할 수 있는 체계로 구축되어야 한다. 결심체계에서 필요한 기술들은 인공지능과 더불어 빅데이터 분석기술이다.

사이버상의 공격은 짧은 시간에 이루어지는 점을 감안, 인공지능 방식을 추천한다. 이는, 인공지능 결심체계로 구축시 특정 공격 행위에 대해 Kill Chain 작동하였으며, 이 과정에서 발생한 기록(로그)을 통해 정당성을 확보하여 준다.

다만, 결심체계에서 나오는 적국 공격 징후 대상 타격간 오류방지를 위해 최종결심은 현실 세계의 외교・정치적 판단이 필요하다.

사이버 킬체인 가동이후 추가적인 분쟁으로 확대되지 않기 위해서는 감시체계결과를 바탕으로 타격 근거를 제시해야 한다. 이를 위해 빅데이터 기술이 적용되야 한다.

3.5. 사이버킬체인 타격(Cyber Strike)체계 제안

타격 체계는 공격원점 타격, 지원세력 확대타격, 지휘세력 포함 타격으로 구분할 수 있다.

공격원점 타격은 실제 공격징후가 실제 식별되는 서버, 네트워크에 대한 타격이며 록히드마틴社의 대응방안 그림 4에서 식별되는 차단・거부 방안이다. 가장 간단하며 공격에 대응하는 소극적 방안으로 확전에 위험이 적다.

공격원점 타격과 더불어 지원세력까지 포함하여 타격방안은 공격징후가 식별된 네트워크를 대상으로 공격하는 방식이다. 대표적인 예는 분산서비스거부공격(DDoS) 징후 발생시 좀비PC 및 통제서버까지 타격해야 피해차단을 할수 있다. 차단・거부이외 공격징후 네트워크에 강제 백신유포, 악성코드 유포 등의 방법을 통해 무력화 시킬 수 있다.

마지막으로 지휘세력 포함타격은 사이버 공간과 현실 세계를 포함하며 위협행위를 설계하고 지휘한 세력을 타격하는 방안이다. 지원세력 타격에 추가하여 현실 세계의 인원, 조직에 대한 물리적 제압이 포함된다.

원점에서 지휘세력으로 타격범위가 확대 될수록 현실 세계의 분쟁으로 확대될 수 있음을 고려해야 한다.

3.6. 사이버킬체인 연동체계(System of Systems) 제안

감시-결심-타격 체계가 별개가 아닌 유기적으로 작동하기 위해서는 체계가 연동이 가장 중요하다고 볼 수 있다.

유사시 사이버 킬체인 작동을 위해서는 TCP/IP 방식 등 기존 프로토콜이 아닌 중앙통제적인 프로토콜이 필요할 것이다. 그림 6에서 통제가능 국내 네트워크(Controlled Net)는 평시에는 공개망의 기능을 수행하나, 유사시 전용 통제망으로 전환되어야 한다.

공개망의 성격을 가지며 유사시 통제망으로 변경할 수 있는 것이 LINK 관절[14]기술이다. LINK관절을 이용한 망구성을 통해 필요시 불필요한 트래픽은 제외하고 공격대상 네트워크에서 작동하게 되는 타격체계가 통제망에서는 작동하지 않도록 하여 부수적 피해를 차단한다. 또한, 공격원점으로 경로를 설정하여 바로 타격할 수 있다. 상대 공격을 차단하는 효과도 가진다. 추가하여, LINK 관절망이 적절하게 운용될 수 있기 위해서는 유사시 통용될 수 있는 별도의 프로토콜이 마련되어야 한다.

별도 프로토콜은 피아를 식별하는 용도와 전용 통제망을 위해 사용되며 공격의도를 가진 패킷을 역추적(Fingerprint/Backtrack) 기능도 있어야 한다. 유사시 사용되게 될 해당 프로토콜은 국가기관에 의해 통제되어야 한다[15].

Ⅳ. 결 론

사이버 킬체인은 공격 의도를 가진 대상에 대해 선제타격을 통해 우리의 망을 안전하게 지키는 데 목적이 있다.

사이버 킬체인을 구현하기 위한 기술들은 지속해서 개발 중이라 볼 수 있다. 또한, 기술을 활용간 발생할 수 있는 법적 문제도 해결해야 될 부분이라고 생각된다.

본 연구에서는 북한의 사이버 위협이 지속 증대되고 있는 실정에서 각종 정보보호 기술들이 개별적이고 독립적으로 연구되고 있어 사이버 킬체인 구축에 필요한 연구분야가 무엇인지 제시하였으며, 큰 그림에서 사이버 킬체인의 프레임워크를 제시하였다.

사이버 킬체인 프레임 워크에서 제시된 기술분야 이외 추가적인 기술 방안 및 운용간 발생할 수 있는 국제적 법적 문제에 대해서는 지속적인 연구가 필요한 분야이다.

REFERENCES

[1] J. W. Kim, “Interpretation of the ROK-U.S. Alliance and PSI,” *Journal of the Korea Institute of Information and Communication Engineering*, vol. 16, no. 5, pp. 1102-1112, May 2012.

[2] Edward H. S. Lo and T. Andrew Au, “Improving the Kill Chain for Prosecution of TimeSensitive Targets.” in Computer and Information Science, ch. 5, p. 95, Jan. 2010.

[3] U. K. Yang, Kill-Chain [Internet]. Available: http://terms.naver.com/entry.nhn?docId=3576761&cid=59087&categoryId=59087.

[4] F2T2EA Process Diagram, Available : http://rtf-ebooks.com/_/_/538584/the-evolution-of-time-sensitive-targeting-operation-iraqi-freedom-results-and-lessons-desert-storm-enduring-freedom-centcom-definitions-future-trends-adversary-focus-on-asymmetric-operations.

[5] Y. S. Kim, “Kilchen((Kill-Chain) and Korean missile defense system(KAMD) : Feasibility Assessment,” *New Asia*, vol.20, no.4, pp. 112-136, Dec. 2013.

[6] S. Korean military speeds up development of Kill Chain and other response capabilities [Internet]. Available: http://english.hani.co.kr/arti/english_edition/e_northkorea/790847.html.

[7] E. M. Hutchins, M. J. Cloppert, R. M. Amin, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains“, Lockheed Martin, Technical Report, 2014.

[8] Verdasys Kill Chain [Internet]. Available: https://www.vivit-germany.org/pdf/2013/vortraege/Application-Security-von-SAP-bis-DLP-die-Sicherung-von-Applikationen-mittels-HP-ArcSight_tcm_144_1428973.pdf.

[9] “The NTT Group 2016 GlobalThreat Intelligence Report,“ NTT Security, Technical Report, 2016

[10] Defense Strategies for Advanced Threats- White Paper: Mapping the SANS 20 Critical Security Controls to the Cyber Kill Chain, NTT Security [Internet]. Available: https://www.solutionary.com/resource-center/white-papers/advanced-threat-protection/.

[11] “Critical Security Controls for Effective Cyber Defense Version 6.1,” The Center for Internet Security, Technical Report, 2016.

[12] K. J. Kim, “Cyber Defense Development Plan Based on Cyber Kill Chain,” *Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities,* vol. 7, no.1. pp.277-285, Jan. 2017.

[13] Y. H. Kim, “Cyber Kill Chain Strategy for Offensive and Integrated Cyber Operations,” *Journal of Security Engineering* , vol. 13, no. 5. pp.325-340, Oct. 2016.

[14] J. W. Yoo, D. W. Park, “A Study of TCP LINK based Real-Time Secure Communication Research in the Ocean,”

Conference of The Korea Institute of Information and Communication Engineering, vol. 18, no. 1, pp.250-253, May 2015.

[15] J. W. Yoo, D. W. Park, “Cyber kill chain strategy for hitting attacker origin,” *Conference of The Korea Institute of Information and Communication Engineering*, vol.21, no.2. pp.158, Oct. 2017.

유재원(Jae-won Yoo)

1998년 : 공군사관학교 전자공학과 (공학학사)
2008년 : 오리건주립대학 컴퓨터학과 (공학석사)
2013년 ~ 현재 : 호서대학교 벤처대학원(박사과정)
※관심분야 : 정보보호, 사이버보안, 보안인증

박대우(Dea-woo Park)

1998년 : 숭실대학교 컴퓨터학과 (공학석사)
2004년 : 숭실대학교 컴퓨터학과 (공학박사)
2004년 : 숭실대학교 겸임교수
2006년 : 정보보호진흥원(KISA) 선임연구원
2007년 ~ 현재 : 호서대학교 벤처대학원 교수
※관심분야 : Hacking, CERT/CC, 침해사고 대응, e-Discoverty, Forensic, 사이버안보, 네트워크 보안, 스마트폰 보안