Journal of The Korea Society of Computer and Information
Vol. 23 No. 11, pp. 75-84, November 2018
www.ksci.re.kr
https://doi.org/10.9708/jksci.2018.23.11.075

Social Engineering Attack Graph for Security Risk Assessment: Social Engineering Attack Graph framework(SEAG)

Jun Seok Kim*, Hyunjae Kang*, Jinsoo Kim**, Huy Kang Kim*

Abstract

Social engineering attack means to get information of Social engineering attack means to get information of opponent without technical attack or to induce opponent to provide information directly. In particular, social engineering does not approach opponents through technical attacks, so it is difficult to prevent all attacks with high-tech security equipment. Each company plans employee education and social training as a countermeasure to prevent social engineering. However, it is difficult for a security officer to obtain a practical education(training) effect, and it is also difficult to measure it visually. Therefore, to measure the social engineering threat, we use the results of social engineering training result to calculate the risk by system asset and propose a attack graph based probability. The security officer uses the results of social engineering training to analyze the security threats by asset and suggests a framework for quick security response. Through the framework presented in this paper, we measure the qualitative social engineering threats, collect system asset information, and calculate the asset risk to generate probability based attack graphs. As a result, the security officer can graphically monitor the degree of vulnerability of the asset's authority system, asset information and preferences along with social engineering training results. It aims to make it practical for companies to utilize as a key indicator for establishing a systematic security strategy in the enterprise.

▸Keyword: Attack graph, Social engineering, Risk assessment, Network security, APT attack

I. Introduction

사회공학이라는 용어는 처음에 정보 보안 분야뿐만 아니라 사회, 정치 분야 등 여러 분야에서도 다양하게 사용되고 있다. 사회·정치 분야에서 사용된 '사회공학'의 의미는 특정 단체를 대상으로 하여 원하는 결과물이나 행동을 대규모로 취하게끔 영향을 행사하는 것을 의미했다. 이때의 사회공학은 개인과 문화에 폭넓게 영향력을 행사할 수 있는 권위를 가진 중앙 정부 주도로 이루어졌으며, 이것이 사회공학의 시초라고 할 수 있다. 반면, 정보 보안 분야의 사회공학은 케빈 미트닉[1]과 크리스 헤드내기[2]로 인해 사회공학 공격이라는 분야가 부각됐고, 사람들은 보안 기술이 아닌 사람을 이용한 휴먼 해킹에 집중하게 되었다. 그들의 시작으로 지금의 사회공학 공격은 제조, 생산, 발전, 가공, 제련 등과 같은 주요 국가 기반의 산업 시설을 대상으로 공격하는 APT(Advanced Persistent Threat) 공격들의 정보 수집 단계로 가장 많이 사용되는 기술이기도 하다. 예를 들어, 기업 내 채용 담당자 메일 주소로 악성코드가 담긴 이력서 파일을 첨부하여 메일을 보낸다거나, 국가 고위 간부를 사칭하여 공격자가 원하는 정보를 빼내는 것이 그에 해당한다.

사회공학 공격은 고도의 해킹 기술이 필요하지 않아, 대부분

• First Author: Jun Seok Kim, Corresponding Author: Huy Kang Kim
*Jun Seok Kim (junskim8@gmail.com), Graduate School of Information Security, Korea University
*Hyunjae Kang (trifle19@korea.ac.kr), Graduate School of Information Security, Korea University
**Jinsoo Kim (niravan421@naver.com), Senior Researcher, Agency for Defense Development
*Huy Kang Kim (cenda@korea.ac.kr), Graduate School of Information Security, Korea University
• Received: 2018. 08. 30, Revised: 2018. 10. 06, Accepted: 2018. 10. 22.
• This work was supported by Agency for Defense Development research grant. (UD180011ED)

Table 1. Overview of related work

Keyword	Category	Contents
Attack graph	Generation the graph	- Network security planning architecture [3] - Logical generation the attack graph [4, 5, 6] - Attack graph using bayesian network [7]
	Risk evaluation	- Attack graph-based probabilistic security metric [8] - CVSS-based security metrics [9] - Unknown vulnerabilities based security metrics [10] - Security assessment in dynamic(multi-layer) networks [11,12, 13]
Social engineering	Definition & Classification	- Social engineering attack technique classification [1,2,15,18] - Social engineering using attack graph [19]
	Attack research	- The penetration test using social engineering [14,16] - Social engineering attack through SNS [17]

기업에서는 사회공학 공격에 대한 중요함을 인식하지만, 대응하기가 어렵다는 입장이다. 국가 정부, 기업 내에서는 연 1회 이상 사회공학 공격에 대비한 교육과 훈련을 병행하고 있다. 보안 담당자는 이를 통해 사내 보안 수준을 높이고, 외부 공격자로부터의 APT 공격에 위협을 최소화하기를 원한다. 하지만, 사회공학 공격은 사람의 심리, 사회·정치·경제 이슈, 상호 신뢰 관계(rapport) 등을 통해 공격을 하기 때문에 가시적인 교육 및 훈련 효과를 얻기가 어렵다. 이러한 점에서 기업 담당자 입장에서는 사회공학 위협에 대한 실질적인 대응 방안과 현존하는 위협을 식별하고 빠르게 의사 결정할 수 있는 도구 등이 필요하다.

기존의 사회공학 연구는 주로 사회공학 기법 정의와 공격 유형별 분류를 주로 연구했으며, 공격자 관점에서의 연구는 사회공학 기법을 이용한 공격 도구 개발 등이 연구가 되었다. 이 중 사회공학을 공격 그래프와 결합한 경우는 사회 공학을 하나의 경로 요소로 모델링하여 공격 경로를 측정했다. 사회공학 공격을 패턴화하여 하나의 인스턴스로 공격 그래프 상에 중간 경로로 추가했고, 사회 공학 공격에 필요한 사전 권한, 공격 성공(exploit) 결과 등을 정의하여 모델링했다. 하지만, 실제 공격자 관점에서는 사회공학 공격을 최초 공격 시작 지점으로 주로 활용하며, 이미 침입한 네트워크에서 사회공학을 이용하지 않는다는 점에서 실제 기업 침해 사고와 다르다는 한계가 존재한다.

따라서, 본 논문에서는 실제 기업에서 이루어지는 침해 사고 시나리오를 바탕으로 사회공학 공격을 시작 시점으로 하여 공격 그래프를 생성하는 사회공학 공격 그래프 프레임워크를 제안한다. 사회공학 공격 대응 훈련을 통해 평가한 임직원들의 훈련 결과를 바탕으로 임직원 PC를 공격 시작점으로 하여 이와 연결된 자산별 위험도를 산정하여 공격 경로를 예측하는 그래프를 생성한다. 보안 담당자는 훈련 결과가 저조한 임직원의 자산의 권한, 기본 정보, 환경설정에 따라 공격자의 예상 경로를 그래프 형태로 모니터링 할 수 있게 된다. 이를 활용하여 담당자가 기업 내 체계적인 보안 전략을 세우는 데 주요 지표로 활용할 수 있게 하는 프레임워크를 제안한다.

II. Preliminaries

1. Related works

1.1 Attack graph

공격 그래프는 네트워크가 구성되어 있는 환경에서 취약성 분석 및 예상 공격 경로 분석에 주로 활용되고 있다. Artz 등[3]은 공격 시나리오를 기반으로 하여 목표한 시스템에 침투하기 위해 사용 될 수 있는 가능한 공격 경로를 표시하는 방법을 제안하였다. 이를 NetSPA(network security planning architecture)라는 도구로 개발하여 공격 그래프를 효율적으로 그릴 수 있는 방법을 제안하였다. 그 이후 Ou 등[4] 네트워크 보안성을 논리적으로 분석할 수 있는 도구인 MulVAL를 개발하여 자산의 정보를 수집하고, 이에 대한 취약성을 분석할 수 있는 도구를 개발한 것이다. 그 후에 도구를 이용한 확장된 네트워크 상에서 사용 가능한 공격 그래프 생성 알고리즘을 추가로 제안했다[5]. 또한, Ingols 등[6]은 공격자가 네트워크에 접근하는 데 이용할 수 있는 공격 경로를 보여주고, 해당 공격에 필요한 전제 조건도 함께 제시하고, 공격 그래프를 계산했다. Poolsappasit 등[7]은 다양한 자산들이 포함된 네트워크 환경에서 정량화 할 수 있는 베이지안(bayesian) 네트워크를 사용하는 위험 관리 프레임워크를 제안했다. 특히, 동적 분석에 적합하여, 리소스가 제약된 환경에서 의사 결정을 할 때 필요한 정보를 관리자에게 효율적으로 제공할 수 있다.

공격 그래프 생성 연구와 함께 그래프 생성에 반드시 필요한 정보인 자산 위험 평가 방법 요소에 관한 연구가 활발히 진행되었다. Wang 등[8]은 여러 가지 보안 취약점을 취합하여, 공격 가능성을 정량화 했다. 예를 들어, 각 자산별 도달 가능성을 확률적인 메트릭으로 공격 그래프를 계산하는 방법을 제안했다. Keramati 등[9]은 알려진 CVSS(Common Vulnerability Scoring System)의 보안 지표를 활용하여 공격 그래프를 확률적으로 생성하였다. Wang [10]등은 기존의 공격 메트릭에서 제로 데이(0-day) 공격에 대한 영향을 배제한 것을 문제로 삼아, 제로 데이를 새로운 평가 메트릭으로 제안했다. 자산별 가장 최악의 경우를 고려하여 해당 자산에 침입하기 위해 얼마나 많은 제로 데이 취약점이 필요한지를 측정하여, 개수가 많으면

Table 2. Classification of social engineering attack

Keyword	Attack techniques	Description
Personal	Piggy backing	It is a technique in which people are identified in an access controlled system or are followed by people who have access rights.
	Shoulder surfing	It is a technique of gathering information while stealing the work or document that the object performs through the shoulder by direct observation around the attacked object.
	Direct approach	It is a technique in which an attacker accesses an object directly and masquerades as if it is someone else or creates a situation in which the information is obtained.
Phone	Vishing	It is a combination of voice and phishing. It is a technique for taking sensitive information by setting arbitrary situation or impersonating another person by using a fixed telephone or internet telephone.
	Smishing	It is a compound word of SMS and Phishing, and it induces the installation of mobile malicious code through the URL address in the text message to seize sensitive information of the victim.
Online	Evil twin (fake access point)	It is a technique to capture information by impersonating a legitimate network in order to gather desired information and accessing the wireless AP created by the attacker.
	Baiting	This technique, called Trojan-Throat in the real world, is a technique of taking information by using the curiosity of the victim and the physical medium to put the virus and file together and open the file to the user.
	Impersonation account	It is a technique to steal victims 'acquaintances' information by acting like a certain person on the SNS, such as a doppelganger.
	Pharming	It is a technique to infect the user's PC with malicious code or farm the DNS server so that the hacker can steal the domain from the middle and get the real site address to connect to the fake site address.
	Phishing	It is a combination of private data and fishing. It is a technique to seize information through e-mail or Internet site by assuming financial institution or public institution.

안전한 네트워크로 평가하는 식의 방법으로 공격 그래프를 생성하는 것을 제안하였다.

최근에는 동적 네트워크 환경에서의 공격 그래프 생성을 위한 평가 방법들이 연구되었다. Yusuf [11]등은 동적 네트워크 환경에서의 공격 그래프 생성을 위한 보안 평가 모델을 개발했다. 특히 전통적인 네트워크 환경이 아닌 동적 네트워크 환경에서의 자산 변화를 캡처하는 보안 모델인 Temporal-Hierarchical Attack Representation Model (T-HARM)을 개발했다. Moon [12]등은 다계층(multi-layer) 네트워크 환경에서 IT 시스템의 자산 중요도와 라우터와 서버 간의 인증 수단에 따른 경로 생성 방법을 제안하였다. Ge [13]등은 서버 복제(redundancy)에 따른 서버 가용에 기반한 보안성 평가를 제안하였다. 자산을 대상으로 패치 적용 전후의 공격에 보안성을 평가하는 모델을 개발했다.

1.2 Social engineering

정보 보안 분야의 초기 사회공학 연구는 사회공학 공격을 이용하여 물리적인 침입이 가능한지에 대해 연구되었다. Dimkov 등[14]은 실제 조직 내에서 IT 보안 시스템을 대상으로 침투 테스트를 하여, 물리적 보안 및 직원들의 보안 인식 평가를 제안했다. 이 때, 사회공학을 사용한 침투 테스트가 실제로 이루어졌으며, 관리 중심의 방법론과 환경(물리 보안) 중심의 방법론을 제시하여 조직 환경에 맞는 방법론을 제안하였다. Ivaturi 등[15]와 Mouton 등[18]은 사회공학 공격의 분류를 통해 공격 기법별 사회 공학 용어를 정의하였다. 사회공학 공격을 유형별로 분류하고, 알려진 사회공학 공격에 대한 대응 방법을 제안했다. 이 때, 우리가 많이 알고 있는 피싱(phishing), 스미싱(SMSishing), 악성코드(malware), 바이싱(vishing) 등의 표현이 사용되었다. Pavković 등[16]은 정보 자산을 보호하는 보안 시스템의 가장 취약한 요소인 사람을 활용하는 공격 기법을 사회공학이라고 설명하고, 이 공격을 실제 테스트할 수 있도록 소프트웨어로 구현하였다. 그래서 SET(social engineering toolkit)라는 이름으로, 현재까지 사용되고 있는 메타스플로잇(metasploit)에도 포함되어 무료로 배포되고 있다.

Algarni 등[17]은 SNS를 통해 사회공학 공격에 이용될 수 있는 개인들의 사생활 정보가 많이 노출되어 있다고 위험성을 알리고, 실제 공격에 활용될 수 있는 시나리오를 보였다. Beckers 등[19]은 사회공학 취약점과 함께 기술적인 취약점을 함께 고려하여 공격 그래프를 생성하는 것을 제안했다. 이는 보안 전략을 세우는 데 도움이 될 수 있으며, 사회공학을 정량적인 분석을 통해 공격 경로를 제시하였다. 하지만, 공격자 관점에서 사회공학을 정량적인 요소로 측정한 시도는 좋았으나, 실제 침입 사고 사례를 보면, 공격자는 사회공학 공격을 최초 공격 시작 지점으로 주로 활용하며, 이미 침입한 네트워크에서 사회공학을 이용하지 않는다는 점에서 실제 사례와 다르다는 한계가 존재한다.

지금까지 사회공학 기반의 연구는 주로 공격 관점에서의 연구 또는 공격 기법에 대한 정의나 분류에 그쳤다. 하지만, 현재 사회공학 공격은 공격자들의 랜섬웨어, APT 공격을 위한 사전 공격으로 매우 활발하게 이루어지고 있다. 이러한 상황에서 기업과 정부는 방어적인 관점에서 사회공학 공격을 바라볼 필요가 있다. 본 논문은 방어적인 관점에서의 사회공학 위협을 공격 그래프로 나타내어 보안 담당자가 유사시 빠른 의사 결정과 판단을 할 수 있는 프레임워크를 제안한다.

III. The Proposed Scheme

1. Defiition of social engineering techniques

사회공학 공격 기법의 절차는 의사 소통 모델과 유사하게 진행된다. 사회공학 공격에 앞서 공격자가 원하는 정보를 어디에서 얻을 것인지에 대해 정해야 한다. 즉, 믿을 수 있는 정보의 출처가 분명해야 신뢰할 수 있는 정보를 얻을 수 있기 때문이다. 신뢰할 수 있는 정보의 출처가 정해졌다면, 정보 출처와의 상호적인 신뢰 관계를 형성하기 위한 채널을 어떻게 할 것인지를 선택해야 한다. 예를 들면, 이메일이나 전화 또는 직접 대면을 통해 채널을 형성할 수 있다. 다음은 채널을 통해 어떤 메시지를 누구에게 보낼 것인가를 정해야 한다. 이 단계가 가장 중요하다고 할 수 있다. 메시지를 보낼 때는 반드시 받는 대상 상호 신뢰 관계를 통해 얻은 정보를 바탕으로 알맞게 전달해야 한다. 긴밀한 관계를 통해 얻은 정보를 활용해야 상대방에게 민감한 정보를 얻을 수 있고, 이러한 정보들이 활용도가 높기 때문이다. 최종적으로 피드백 단계에서 공격자가 원하는 정보를 얻을 수 있게 된다. 이러한 일련의 과정을 통해 사회공학 공격이 이루어진다[Fig 1. 참조].

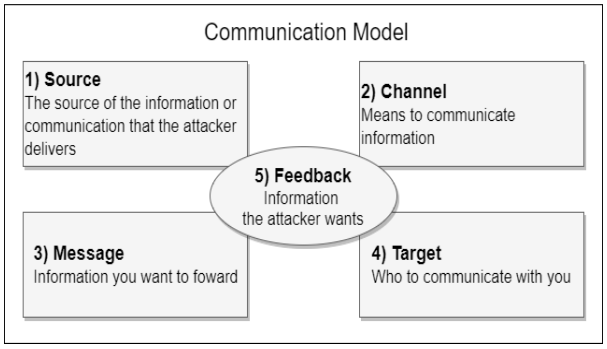


Fig. 1. The communication model of social engineering

사회공학 기법은 크게 정보 전달 채널에 따라 분류할 수 있다. 총 3개의 분류로 나눌 수 있는데, 1) 대면, 2) 전화, 3) 온라인 구분한다[Table 2. 참조]. 본 논문에서는 네트워크 환경에서의 사회공학 공격을 통한 공격 예상 경로를 보여주기 때문에 다양한 공격 기법 중에 온라인을 통한 피싱(phsihing) 공격으로 한정한다. 실제 기업 내에서도 피싱 메일을 통한 랜섬웨어 감염, 기업 내부 정보 유출 등의 사고가 발생하므로, 가장 위험도가 높은 사회공학 공격 기법이라고 할 수 있다. 따라서, 사회공학 기법 중 피싱 메일을 통한 공격 시나리오로 진행한다.

2. Social engineering training

사회공학 대응 훈련으로 가장 대표적인 것이 피싱 메일 훈련이다. 일반적으로 피싱 메일 대응 훈련은 시스템을 통해 발송하고, 각 임직원들이 열람 여부에 따라 훈련 결과가 담당자에게 발송되는 프로세스로 진행된다[Fig 2. 참조]. 이 훈련은 모든 기업에서 매년 또는 2년에 한번 씩 진행되고 있지만, 실질적인 효과를 얻기는 어렵다. 얻어진 결과를 통해 직접적으로 인사 점수에 반영하기도 어려울 뿐만 아니라, 개별적인 교육을 한다 해도 업무 특성상 열람해야 하는 악성 코드가 담긴 인사 채용 지원서를 첨부한 메일 공격에는 무용지물이다. 따라서, 이를 보완하기 위해 사회공학에 기반으로 한 공격이 어떻게 이루어질 수 있는지를 분석하고, 실질적인 사회공학 공격 대응이 필요하다. 본 논문에서는 제안하는 프레임워크가 기존 훈련 프로세스와 더불어 훈련 결과를 바탕으로 직원들에게 실제 기업이 공격을 당할 수 있는 예상 공격 경로를 그래프로 보여줌으로써, 임직원 보안 의식을 높이는데 활용할 수 있다.

사회공학 공격 훈련을 할 때에는 여러 가지의 시나리오를 활용할 수 있다. 주로 훈련에 사용되는 시나리오는 당시 이슈가 되었던 뉴스, 사내 이벤트, 입사 지원, 은행 서비스, 시스템 비밀번호 변경 등이 활용된다. 또한, 각 시나리오에 따라 사용자가 메일을 열람한 이후에 영향을 파악하기 위한 목적으로 첨부 파일을 넣는 등과 같이 메일 내용을 다양하게 설정할 수 있다. 예를 들면, 랜섬웨어와 같은 파급력을 주기 위해 메일 첨부파일에 훈련용 악성코드를 삽입하여 사용자가 실행하도록 유도하기도 한다. 또 다른 경우로는 임직원의 이름, 연락처, 메일 주소 정보를 얻기 위한 목적으로 일종의 이벤트 형태의 메일을 보내 사용자가 자신의 정보를 입력하게 한다. 본 논문에서는 이러한 각 시나리오 특성들을 고려하여, 공격 가능 경로를 생성할 때 위협 지표로 활용하여 평가 요소에 반영한다[Table 3. 참조].

Table 3. Social engineering scenario

ID	Scenario	Weight
SES-01	Attaching the malware (ex, ransomware, backdoor)	0.9
SES-02	Attaching the malicious link(script) (ex. dropper)	0.7
SES-03	Link manipulation (ex. phishing site, watering hole)	0.5
SES-04	Enticing to input information (ex. Impersonation, event)	0.3

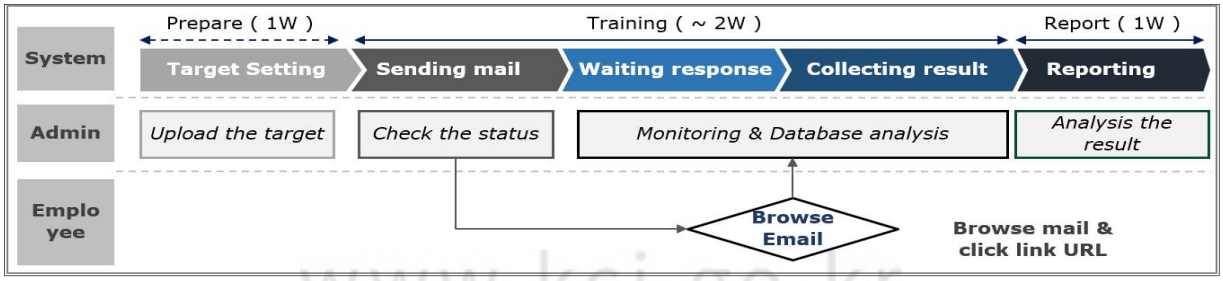


Fig. 2. The procedure of social engineering attack response training

3. Anlaysis of attack graph

기업 내 네트워크는 점차 확대되고, 복잡해지면서 공격에 대한 취약한 곳을 식별하고 대응하는 데에 어려움이 있다. 이러한 어려움을 해결하기 위해 기업 내 네트워크 환경에서 가능한 공격 방법과 공격을 구체화하는 방법으로 공격 그래프에 대한 연구가 활발히 진행되고 있다. 공격 그래프는 시스템 취약점 정보를 바탕으로 공격 경로를 모델링하여 분석할 수 있다.

공격 그래프를 통해 시스템 내 존재하는 취약점을 확인하고, 발생 가능한 공격 경로에 대해 보여주기 때문에 기업 내 보안 전략을 수립하는데 많은 정보를 제공한다. 이러한 정보를 바탕으로 기업 내 담당자들이 보안 전략을 수립하고, 대안을 마련하는데 좋은 의사 결정 도구가 될 수 있다. 그래프 생성 시, 공격자의 침입 경로를 예측을 위해 자산들의 취약점들을 점수화(scoring)하여, 공격자가 목표 시스템에 도달할 확률을 기반으로 공격 예상 경로를 그려준다. 그러기 위해서는 일반적으로 4단계의 작업이 필요하며, 각 단계는 다음과 같다[Fig. 3. 참조].

1) 네트워크 환경 정보 수집
2) 자산별 취약점 식별
3) 자산별 위험도 평가
4) 공격 경로 생성

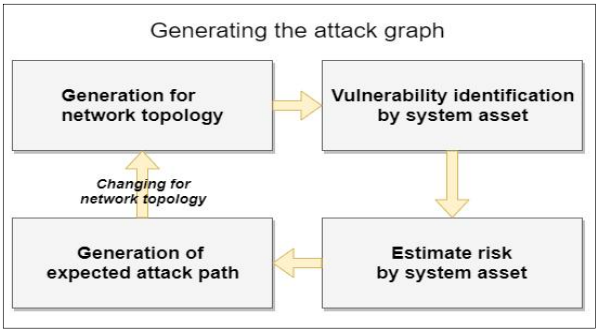


Fig. 3. Generation of the attack graph

위의 프로세스는 일반적인 공격 그래프 생성 프로세스를 나타낸 것이며, 기존에 공격 그래프 연구들은 주로 자산별 위험도 평가를 다르게 하거나, 기존에 없던 SDN (Software Defined Networking)과 같은 동적인 네트워크 환경에서의 공격 그래프를 생성하는 기법들에 대해 연구되어 왔다.

4. Social Engineering Attack Graph framework (SEAG)

사회공학 공격 그래프(Social Engineering Attack Graph framework, SEAG)는 기업에서 실제 활용이 가능한 프레임워크 모델을 제안한다. 본 논문에서 제안하는 사회공학 공격 그래프 모델은 기업 내에서 수행하고 있는 사회공학 훈련을 기반으로 구축되었다[Fig. 4. 참조].

4.1 Vulnerability of social engineering

사회공학 취약점은 주로 실제 근무하고 있는 임직원들을 이용하여 발생하기 때문에 실제 공격과 유사한 사회공학 훈련을 통해 식별할 수 있다. 예를 들어, 공격자가 악성코드로 사내 PC를 감염시키는 시나리오로 설정하여 공격에 필요한 메일을 직원들에게 보내게 된다. 그러면 메일을 열람한 직원들은 악성코드에 감염되게 되고, 감염된 PC를 공격자가 제어할 수 있게 된다. 최종적으로 제어 권한을 얻은 PC를 공격의 시작 지점으로 하여, 공격 그래프를 그리게 된다. 따라서, 우리는 사회공학 취약점을 계산하기 위한 방법으로 크게 메일 시나리오 유형과 감염된 직원의 권한, 메일 열람 디바이스 총 3개의 요소를 활용하여 사회공학 위험도를 평가하고, 이를 공격 경로의 시작 지점으로 활용한다. 가중치는 각각 0~1 사이의 확률(P)로 나타내며, 확률 값이 클수록 위험도가 높은 것을 나타낸다.

시나리오에 따른 위험도(Social Engineering Scenario, SES)는 훈련 메일 시나리오에 따라 결정되며, 첨부 파일의 기능 또는 메일 내 링크 종류에 따라 위험도를 다르게 산정한다. 직원 권한에 따른 위험도(User Access Control, UAC)는 임직원의 직급 또는 직무에 따라 부여되며, 웹 서버, 데이터베이스 서버 등과 같은 주요 시스템에 접근할 수 있는 권한 여부에 따라 위험도를 부여된다. 훈련 결과에 따라 메일을 열람하여 링크 또는 파일에 접근한 경우에 이용한 디바이스(device, DEV)에 따라 위험도를 산정한다. 모바일의 경우, Android와 iOS로 나눌 수 있는데, 이 중 Android는 상대적으로 취약하며, 외부 패키지(apk) 설치로 인하여 공격이 발생할 수 있기 때문에 0.5의 가중치를 부여했다[Table 4. 참조].

Table 4. Social engineering vulnerability

ID	Scenario	Weight
SES-01	Attaching the malware (ex, ransomware, backdoor)	0.9
SES-02	Attaching the malicious link(script) (ex. dropper)	0.7
SES-03	Link manipulation (ex. phishing site, watering hole)	0.5
SES-04	Enticing to input information (ex. Impersonation, event)	0.3
UAC-01	Administrator (all accessible)	0.9
UAC-02	Manager (partially accessible)	0.7
UAC-03	Engineer (specifically accessible)	0.3
UAC-04	General user (No access)	0.1
DEV-01	Employees who viewed mail on their enterprise computers	1
DEV-02	Employees who read email on their mobile phone	0.5
DEV-03	An employee who did not access the mail.	0

예를 들면, SES-01은 공격 시나리오(Social Engineering Scenario)의 의미로 악성 코드를 첨부하는 훈련 시나리오를 의미한다. 훈련 시, 활용 가능한 첨부 파일로는 랜섬웨어나 백도

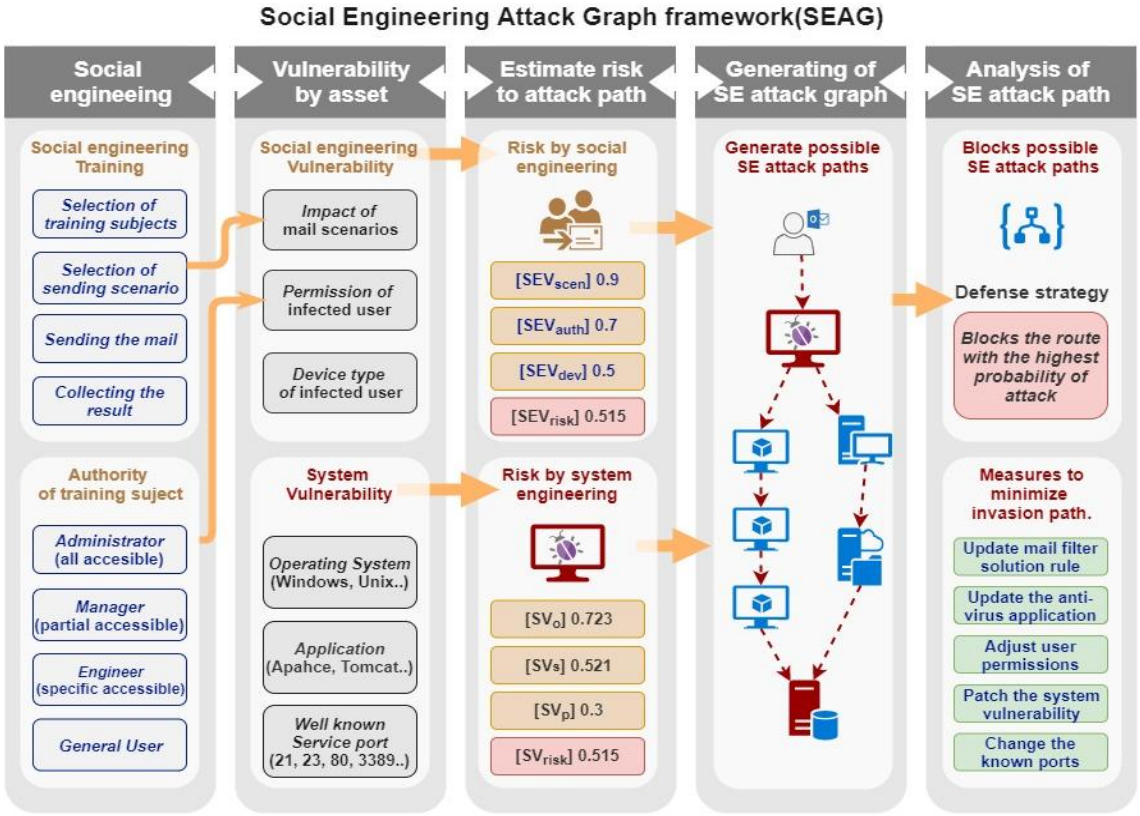


Fig. 4. Overview of the Social Engineering Attack Graph framework(SEAG)

어 역할을 하는 등의 훈련용 악성코드가 활용될 수 있다. 이 때, 가중치(weight)는 해당 공격 시나리오로 인한 사용자의 영향력을 파악하여 0~1 사이의 확률(P)로 표시했다. 따라서, SES-01의 경우, 랜섬웨어나 백도어로 인해 사용자에게 2차 피해를 일으킬 수 있을 만큼 영향력이 큰 것으로 판단하여 0.9의 가중치를 부여했다.

UAC-01은 사용자의 접근 권한(User Access Control)을 나타낸 것으로, 훈련을 통해 감염된 사용자의 접근 권한을 의미한다. 감염된 사용자의 권한이 관리자(Administrator)인 경우, 일반 유저의 권한보다 높은 접근 권한을 갖고 있기 때문에 그로 인한 위험도를 높아지게 된다. 따라서, UAC-01의 경우에는 가중치를 0~1 사이의 가장 높은 0.9의 가중치를 부여했다.

마지막 DEV-01의 경우는 감염된 사용자가 사용한 디바이스(Device)를 의미한다. 해당 취약성은 사용자가 악성 메일을 열람한 디바이스에 따라 중요 정보의 노출 또는 공격자가 의도한 공격에 감염 여부가 결정되기 때문에 사회공학 기법에서는 중요한 요소로 작용한다. 따라서, DEV-01 의 경우, 민감한 정보를 가장 많이 저장하고 있는 사내의 PC에서 열람한 경우를 가장 가중치를 높게 부여(0.9)하고, 모바일은 PC와 비교하여 상대적으로 감염될 수 있는 확률이 낮고, 민감 정보를 모바일에는 저장하지 않기 때문에 가중치를 0.5로 부여했다.

사회공학 취약점은 SEV_{risk}로 나타내며, 시나리오 확률(SEV_{scen}), 사용자 권한(SEV_{auth})에 따른 확률, 메일을 열람한 디바이스(SEV_{dev})의 확률로 계산한다.

$$SEV_{risk} = SEV_{scen} * SEV_{auth} * SEV_{dev} \quad (1)$$

위의 수식을 구하기 위한 각각의 확률은 반드시 훈련을 진행한 임직원을 대상으로 구할 수 있으며, 훈련 결과에 따라 대상별 사회공학 위험도가 다르게 나올 수 계산될 수 있다.

특히, 훈련 결과에 따라 read, access(click, download), execution으로 구분할 수 있는데, 메일 시나리오와 함께 고려하여 위험도를 고려한다. 예를 들어, 시나리오가 malware인 경우에는 사용자가 실행(execution)까지 해야 위험도 산정이 가능하지만, Link manipulation의 경우에는 접근(link click)까지만 진행이 되어도 위험으로 산정된다.

Table 5. Example of social engineering training results and risks

name	Dep	Attach	Auth	Act	Agent	Vul(P)
user A	IT	malware	adm	A	PC	-
user B	IT	malware	mng	E	PC	0.63
user C	IT	link	eng	A	mobile	0.075
user D	IT	malware	eng	A	PC	-
user E	IT	malware	eng	R	PC	-
user F	HR	malware	mng	R	mobile	-
user G	HR	malware	user	R	PC	-
user H	Plan	malware	user	R	PC	-
user I	Plan	malware	user	R	mobile	-
user J	CS	link	mng	A	PC	0.35
user K	CS	malware	user	E	PC	0.09

악성코드가 담긴 메일과 악성 링크가 담긴 시나리오로 훈련을 한 결과가 [Table 5]와 같다고 하면, link에 감염된 사용자는 user C, J이며, malware에 감염된 사용자는 user A, B, D, E, F, G, H, I , K이다[Table 5. 참조]. 이 중에 실제 공격 시작 지점으로 공격 경로가 산출될 수 있는 경우는 user B, C, J, K만 가능하다. user B의 경우를 예로 들면, user B는 malware 메일에 감염되었고, 그의 직급은 관리자(mng)의 권한을 가진다. 또한, 메일에 담긴 malware를 실행(execution, E)까지 하였다. 사용자의 Act 결과는 사용자의 행위를 나타낸 것으로 읽기(read, R), 링크 접속(access, A), 실행(execution, E)으로 구분했다. 결과표에 따라 user B의 SEV_{risk}를 계산하면 다음과 같다.

$$SEV_{risk} = SEV_{scen} * SEV_{auth} * SEV_{dev} \quad (2)$$
$$0.63 = 0.9 * 0.7 * 1$$

여기서, 사용자의 행위에 따라 SEV_{risk}이 결정되게 되는데, malware 시나리오 경우는 실행(execution, E)까지의 행위가 나타나지 않으면 실제 공격 확률로 산정하지 않는다. 마찬가지로 link인 경우에는 링크 접속(access, A)까지 한 경우에만 공격 시작 지점으로 SEV_{risk}를 계산한다.

4.2 System vulnerability

Moon 등[20]이 제안한 공격 그래프 모델을 활용하여 시스템 취약점을 각 시스템에 설치되어 있는 운영체제(operate system), 애플리케이션(application, service), 포트(port)를 이용하여 취약성을 평가했다. 운영체제와 애플리케이션의 취약성 평가 지표는 NVD(National Vulnerability Database)에서 제공하는 CVSS의 점수를 이용하여 평가한다.

운영체제의 경우, 시스템 자산에서 사용하는 운영체제의 가중치(W_o)와 해당 운영체제에 존재하는 취약점의 평균 CVSS 점수($avgc_o$)로 취약성을 평가한다. 이 때, 운영체제의 가중치(W_o)는 운영체제 종류에 따라 발견된 CVE 개수가 많을수록 높은 가중치를 부여했다. 예를 들어, 특정 자산에서 Mac OS X 10.5 버전의 운영체제가 확인되었다면, CVE 데이터베이스에서 Mac OS X 10.5에 해당하는 CVE 취약점이 총 127개가 나타나게 된다. 이처럼 각각 운영체제 종류에 따라 CVE 개수를 통해 가중치를 부여하는 방식이다. 그리고 각각의 점수를 곱으로 계산하여 시스템 운영체제의 가중치(sv_o)를 계산한다.

$$SV_o = W_o * avgc_o \quad (3)$$

애플리케이션은 시스템 자산에 설치되어 있는 애플리케이션의 가중치(W_s)와 해당 애플리케이션에 존재하는 취약점의 평균 CVSS 점수($avgc_s$)로 취약성을 평가한다. 이 때, 애플리케이션의 가중치(W_s)는 애플리케이션에 따라 발견된 CVE 개수가 많을수록 높은 가중치를 부여했다. 그리고 각각의 점수를 곱으로 계산하여 시스템 애플리케이션의 가중치(sv_s)를 계산한다.

$$SV_s = W_s * avgc_s \quad (4)$$

마지막으로 시스템 포트는 잘 알려진 포트를 제한하고, 알려지지 않는 포트를 사용하는 것이 공격자의 공격 확률을 낮추는 역할을 하므로 이것을 취약성으로 판단하고 산정한다. IANA(Internet Assigned Numbers Authority)에서 권고하는 포트-서비스와 일치 여부를 피하도록 설정해야하며, 이와 같은 경우 공격자에게 노출될 확률이 높으므로 시스템 포트와 일치한 개수를 계산하여 포트 가중치(sv_p)로 평가한다. 최종적으로 평가된 운영체제, 애플리케이션, 포트 가중치들의 평균값을 구하여 최종 시스템 취약성(SV_{risk})을 평가하게 된다.

$$SV_{risk} = \frac{S_o + S_s + S_p}{3} \quad (5)$$

4.3 Generation social engineering attack graph

공격 그래프는 기업 또는 조직 환경에서 이미 구축되어 있는 네트워크 구성도를 기반으로 생성한다. 네트워크 구성도를 기반으로 공격 그래프를 생성하고, 공격 그래프를 생성할 때에는 백본, 라우터, 스위치 등과 같은 네트워크 장비들은 제외하고 생성한다. 공격 그래프에서 가장 핵심이 되는 자산인 서버, 데이터베이스, 워크스테이션 등의 호스트를 노드(node)로 그리고, 각 호스트 간의 연결을 엣지(edge)로 나타낸다. 실선으로 연결된 무방향성(undirected) 엣지는 실제 네트워크 환경에서의 물리적인 연결을 의미하고, 점선으로 연결된 방향성(directed) 엣지는 사용자가 해당 시스템의 접근 권한을 가지고 있다는 것을 의미한다. 기존의 공격 그래프와 다르게 사용자의 접근 권한이 사회공학 취약점에 중요한 요소로 작용하기 때문에 네트워크 토폴로지에 함께 표시해야 한다[Fig. 5. 참조].

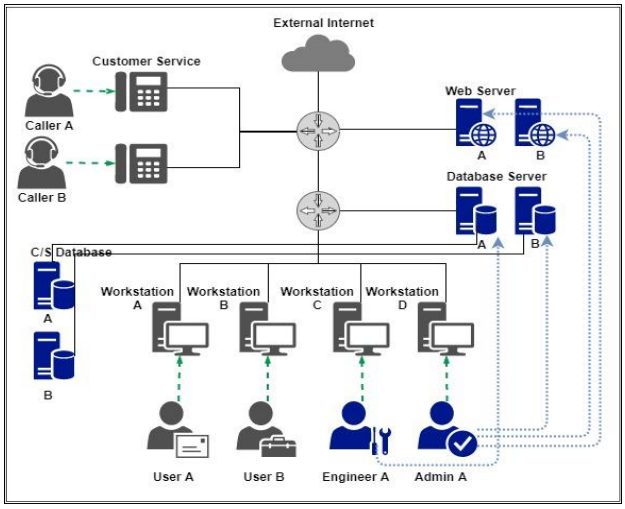


Fig. 5. Example of network topology

네트워크 토폴로지가 완성되면, 사전에 계산한 사회공학 취약성과 시스템 취약성을 이용하여 공격 그래프를 생성한다. 공격 그래프는 공격 예상 경로를 표시하는데, 경로를 표시하기 위해서는 반드시 출발 지점(start point)과 목표 지점(target point)이 필요하다. 본 논문에서 제안하는 사회공학 공격 그래프에서는 외부의 공격자가 침입 가능한 경로로 사회공학 취약성을 이용한다고 가정한다. 사회공학 훈련은 malware 시나리오로 진행되었으며, 악성 메일을 자신의 사내 Workstation PC로 열람하고 실행했다고 가정한다. 따라서, 공격 경로의 모든 시작 지점은 사회공학 취약 지점으로 각 사용자가 이용하는 워크스테이션 등이 시작 지점이 된다. 그 이후부터는 각 시스템의 취약성을 이용하여, 목표 지점까지의 가능한 경로를 계산하게 된다. 공격 그래프 예시로 시작 지점을 각 유저가 사용하는 워크스테이션이라고 하면, 시작 노드에서 목표지점 노드까지의 경로는 [Fig. 6.]과 같이 그려진다.

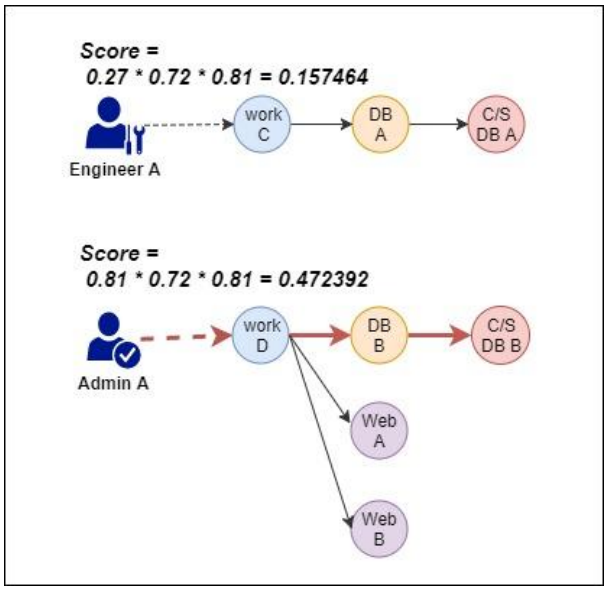


Fig. 6. Example of attack graph generation

생성된 공격 그래프에서 최적의 공격 경로를 선정하려면 각 호스트들의 가중치를 계산해야 한다. 사회공학 공격 그래프에서는 처음 공격 접점을 사회공학 취약성을 이용하기 때문에 모든 시작 경로는 사람이 된다. 시작 지점은 사회공학 훈련에서 메일을 열람하고 실행한 직원들이 되며, 목표 지점은 C/S database A 또는 B로 설정한다. 사회공학 훈련 시나리오(malware)는 위에서 언급한 것과 같으며, 악성 메일을 열람하고 실행한 직원은 Engineer A와 Admin A 이다. 위에 시나리오를 통한 공격 경로는 [Fig. 6.]와 같다. [Fig. 6.]에서 Engineer A로 시작되는 공격 경로는 {Engineer A(Workstation C) → Database A → C/S Database A}로 그려진다. 위의 경로의 대한 취약성을 계산하면다음과 같다.

$$SEV_{risk} = SEV_{scen} * SEV_{auth} * SEV_{dev} \quad (6)$$
$$0.27 = 0.9 * 0.3 * 1$$

사회공학 취약성은 위의 계산식에 따라 malware 시나리오의 가중치와 Engineer A의 권한 가중치, 메일 열람 및 실행한 장치에 따른 가중치를 각각 곱하여 0.27로 나타난다. 다음 경로는 각각의 workstation, database, C/S database들은 시스템 취약성 계산식에 따라 계산한다. Database A의 자산 위험도는 0.72이며, C/S Database A는 0.81이라고 하면, 최종적으로 공격 경로 확률은 {0.27 * 0.72 * 0.81 = 0.157464 }이다. 반면에 Admin A로 시작되는 공격 경로는 {Engineer A(Workstation D) → Database B → C/S Database B}로 그려진다. 위의 경로의 대한 취약성을 계산하면다음과 같다.

$$SEV_{risk} = SEV_{scen} * SEV_{auth} * SEV_{dev} \quad (7)$$
$$0.81 = 0.9 * 0.9 * 1$$

사회공학 취약성은 위의 계산식에 따라 malware 시나리오의 가중치와 Engineer A의 권한 가중치, 메일 열람 및 실행한 장치에 따른 가중치를 각각 곱하여 0.81로 나타난다. 다음 경로는 각각의 workstation, database, C/S database들은 시스템 취약성 계산식에 따라 계산한다. Database B의 자산 위험도는 0.72이며, C/S Database B는 0.81이라고 하면, 최종적으로 공격 경로 확률은 {0.81 * 0.72 * 0.81 = 0.472392 }이다. 따라서, 기업 보안 담당자는 생성된 공격 그래프를 통해 Admin A를 통한 공격 경로가 취약한 공격 경로로 판단할 수 있다.

4.4 Analysis of social engineering attack path

사회공학 공격 그래프는 사회공학 취약성을 시작 지점으로 각 시스템 취약성을 통해 목표 지점까지의 도달 확률을 계산하여 외부의 공격자가 침입해 올 경로를 미리 예측해준다. 기업 입장에서 좋은 보안 대책은 각각의 가장 높은 확률로 계산된 공격 경로에 활용된 사회공학 취약성 및 시스템 취약성을 낮추는 방식으로 보안 대책을 수립할 수 있다.

사회공학 취약성을 낮추는 방법으로는 메일 필터 솔루션을 이용한 규칙을 추가하는 것이다. 최근에는 메일에 첨부된 파일, 내용에 포함된 링크 등을 솔루션에서 검사하여 악성 여부를 판단하는 방식의 솔루션이 출시되고 있다. 이를 활용하여 메일 공격으로 인한 사회공학 취약성을 낮추는 방법이 있다. 그 외에는 불필요한 사용자의 권한 조정으로 무분별하게 접근 권한이 부여되어 있는 주요 자산에 대한 접근을 제한하는 방법이 있다. 마지막으로는 지속적인 훈련과 교육으로 기업 내 임직원 모두가 의심되는 메일에 대한 열람을 지양하고, 내부 보안팀으로 신고하는 등과 같은 체계적인 교육이 수립되어야 한다.

시스템 취약성을 낮추는 방법으로는 가장 위험도가 높게 산정된 자산을 식별하여 우선적으로 운영체제와 애플리케이션 패치, 알려진 포트 사용 제한, 자산 내 안티 바이러스 설치 및 업데이트를 통해 위험도를 낮출 수 있다. 기업은 수없이 많은 서버와 데이터베이스 등과 같은 자산을 관리해야하기 때문에 담당자는 모든 자산의 취약성을 낮추기가 어렵다. 따라서, 실제 공격에 활용될 수 있는 매우 취약한 자산 위주로 조치해나가며, 중장기적

으로 보안 전략을 세우는데 좋은 지표로 활용될 수 있다.

IV. Conclusions

본 논문은 기업에서 진행하고 있는 사회공학 훈련 결과를 바탕으로 공격 그래프를 생성하는 프레임워크를 제시했다. 기존의 사회공학과 공격 그래프를 함께 나타낸 연구에서는 사회공학을 시스템과 동일한 하나의 평가 메트릭으로 내부 임직원을 통한 사회공학 취약성을 모델링하여 경로에 추가하는 형태였다. 하지만, 이러한 연구는 공격자 측면에서 현실적인 한계가 존재한다. 공격자 관점에서 기존 연구는 이미 공격자가 네트워크에 침입한 상황을 가정한 것이고, 이미 탈취한 상황에서 사회공학을 이용하여 원하는 목표 지점까지의 경로를 계산한다. 그러나, 실제 기업에서의 침해 사고를 보면, 주로 사회공학 공격으로 시작으로 내부 네트워크에 접속하는 경우가 많기 때문에 오히려 사회공학 취약성을 시작으로 침입이 이루어지는 경우가 많다.

따라서, 본 논문에서 제안하는 프레임워크와 같이 사회공학을 시작으로 하여 생성하는 공격 그래프가 공격 관점이 필요한 것이다. 사회공학 공격 그래프는 현재의 네트워크 구성 및 모든 자산의 정보와 직원들의 보안 수준을 모두 고려하여 외부의 공격자가 침입해 올 가장 높은 확률의 경로를 보여주기 때문에 기업 보안 측면에서 선제적인 공격 대응이 가능하다. 특히, 보안 관점에서 가장 관리하기 어려운 인적 보안을 정량적으로 측정해 볼 수 있다는 점에서 논문에서는 제안하는 프레임워크는 매우 활용도가 높다. 또한, 제안한 그래프를 활용하면, 직원들이 본인 자신으로 인해 회사에 큰 피해를 입을 수 있다는 경각심과 나로 인해 발생할 수 있는 공격 경로를 보여주어 교육 및 훈련 효과를 높일 수 있다. 나아가 보안 관련 부서의 성과 측면에서도 효과적인 지표로 활용될 수 있다. 기존의 국내 보안 인증에 국한되어 있던 성과를 실제 공격 가능한 경로를 측정함으로써 전략적인 요소로 활용해볼 수 있는 좋은 지표가 될 수 있다.

하지만, 본 논문에서 제안하는 사회공학 공격 시나리오로 피싱 메일에 한정되어있는 것이 사회공학 공격 그래프의 다양성 측면에서 보면 분명한 한계가 존재한다. 이는 기업에서 실시되고 있는 사회공학 훈련과 함께 구체적인 대안이 필요한 사항이며, 갈수록 교묘해지는 공격자의 사회공학 공격들을 반영하기 위해서는 다양한 공격 시나리오가 반드시 필요하다. 최근에는 클라우드, SDN, VM 등과 같이 다양한 네트워크 환경이 기업에 적용되면서 이러한 환경에서도 적용 가능한 사회공학 공격 그래프 모델을 고려해야한다. 최근에는 기업 내 네트워크 환경도 다양해지면서, 기존에 시스템 취약점 평가 요소도 바뀌고, 측정해야하는 지표들도 보완되거나 다양해지고 있다. 따라서, 향후에는 사회공학 훈련 시나리오와 더불어 다양한 네트워크 환경에 맞는 공격 그래프를 생성해야한다. 향후 연구 과제로 다양해지는 네트워크 환경에 적용 가능한 프레임워크로 보완하고, 사회공학 취약성을 측정할 수 있는 시나리오를 추가하여 더 다양한 기업 환경에 맞는 사회공학 프레임워크 모델을 지속적으로 연구할 예정이다.

REFERENCES

[1] Mitnick, Kevin D. and William L. Simon. The art of deception: Controlling the human element of security. John Wiley & Sons, 2011.

[2] Hadnagy, Christopher. Social engineering: The art of human hacking. John Wiley & Sons, 2010.

[3] Artz, Michael Lyle. Netspa: A network security planning architecture. Diss. Massachusetts Institute of Technology, 2002.

[4] Ou, Xinming, Sudhakar Govindavajhala, and Andrew W. Appel. "MulVAL: A Logic-based Network Security Analyzer." USENIX Security Symposium. Vol. 8. 2005.

[5] Ou, Xinming, Wayne F. Boyer, and Miles A. McQueen. "A scalable approach to attack graph generation." Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006.

[6] Ingols, Kyle, Richard Lippmann, and Keith Piwowarski. "Practical attack graph generation for network defense." Computer Security Applications Conference, 2006. ACSAC'06. 22nd Annual. IEEE, 2006.

[7] Poolsappasit, Nayot, Rinku Dewri, and Indrajit Ray. "Dynamic security risk management using bayesian attack graphs." IEEE Transactions on Dependable and Secure Computing 9.1 (2012): 61-74.

[8] Wang, Lingyu, et al. "An attack graph-based probabilistic security metric." IFIP Annual Conference on Data and Applications Security and Privacy. Springer, Berlin, Heidelberg, 2008.

[9] Keramati, Marjan, Ahmad Akbari, and Mahsa Keramati. "CVSS-based security metrics for quantitative analysis of attack graphs." Computer and Knowledge Engineering (ICCKE), 2013 3th International eConference on. IEEE, 2013.

[10] Wang, Lingyu, et al. "k-zero day safety: A network security metric for measuring the risk of unknown vulnerabilities." IEEE Transactions on Dependable and Secure Computing 11.1 (2014): 30-44.

[11] Yusuf, Simon Enoch, et al. "Security Modelling and Analysis of Dynamic Enterprise Networks." Computer and Information Technology (CIT), 2016 IEEE International Conference on. IEEE, 2016.

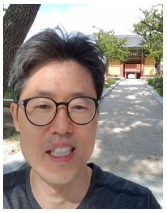
[12] Moon, Young Hoon, et al. "Hybrid Attack Path Enumeration System Based on Reputation Scores." Computer and Information Technology (CIT), 2016 IEEE International Conference on. IEEE, 2016.

[13] Ge, Mengmeng, et al. "Evaluating Security and Availability of Multiple Redundancy Designs when Applying Security Patches." Dependable Systems and Networks Workshop (DSN-W), 2017 47th Annual IEEE/IFIP International Conference on. IEEE, 2017.
[14] Dimkov, Trajce, et al. "Two methodologies for physical penetration testing using social engineering." Proceedings of the 26th annual computer security applications conference. ACM, 2010.
[15] Ivaturi, Koteswara, and Lech Janczewski. "A taxonomy for social engineering attacks." International Conference on Information Resources Management. Centre for Information Technology, Organizations, and People, 2011.
[16] Pavković, Nikola, and Luka Perkov. "Social Engineering Toolkit—A systematic approach to social engineering." MIPRO, 2011 Proceedings of the 34th International Convention. IEEE, 2011.
[17] Algarni, Abdullah, et al. "Social engineering in social networking sites: Affect-based model." Internet technology and secured transactions (icitst), 2013 8th international conference for. IEEE, 2013.
[18] Mouton, Francois, et al. "Social engineering attack framework." Information Security for South Africa (ISSA), 2014. IEEE, 2014.
[19] Beckers, Kristian, Leanid Krautsevich, and Artsiom Yautsiukhin. "Analysis of social engineering threats with attack graphs." Data privacy management, autonomous spontaneous security, and security assurance. Springer, Cham, 2015. 216-232.
[20] Moon, Joo Yeon, et al. "An Attack Graph Model for Dynamic Network Environment" Journal of The Korea Institue of Information Security & Cryptology 28.2 (2018): 485-500.

Authors

Jun Seok Kim received the B.S. degree in Computer Science from Sejong University, Korea, in 2015. Jun Seok Kim is currently a M.S course student in the Graduate School of Information Security, Korea University. He is interested in network security, vehicle security and system security on cyber security. Before joining Korea University, he was a consultant in Risk Advisory department of Deloitte(2014~2017).

Hyunjae Kang received the B.S. degree in mathematics and M.S. degree in information security from Korea University, Korea, in 2012 and 2014, respectively. Hyunjae Kang is currently a Ph.D. course student in the Graduate School of Information Security, Korea University. She is interested in data mining and machine learning on cyber security.



Jinsoo Kim received the B.S. degree in computer science from Chonnam Nat'l Univ. and M.S. degree in computer science from KAIST in 1999, 2002 respectively. Kim is currently a senior researcher in Agency for Defense Development. He is interested in cyber command control and malware analysis.

Huy Kang Kim received his B.S. degree in Industrial Management in 1998, M.S. and Ph.D degrees in industrial and systems engineering from KAIST in 2000 and 2009. He founded A3 Security Consulting, the first information security consulting company in Korea in 1999. Currently he is an associate professor in Graduate School of Information Security, Korea University. Before joining Korea University, he was a technical director (TD) and a head of information security department of NCSOFT (2004~2010). His research interests include solving security problems in online games based on the user behavior analysis and data mining.