한국정보보호학회
Korea Institute of Information Security & Cryptology

2023년 한국정보보호학회 하계학술대회

CISC-S'23

Conference on Information Security and Cryptography Summer 2023

2023년 6월 22일(목)~23일(금)

강원대학교 춘천캠퍼스 60주년 기념관

주최 한국정보보호학회 Korea Institute of Information Security & Cryptology
주관 KNU 강원대학교 KANGWON NATIONAL UNIVERSITY
후원 국가정보원 NATIONAL INTELLIGENCE SERVICE, 과학기술정보통신부, 행정안전부, KISA 한국인터넷진흥원, ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute, NSR 국가보안기술연구소 National Security Research Institute, Google

2023년 한국정보보호학회 하계학술대회 CISC-S'23

Conference on Information Security and Cryptography Summer 2023

시간/세션	논문번호	발표논문	페이지
09:00~10:30 **포스터 1** 좌장 : 최석환 (연세대학교)	1	서버리스 환경에서 동작하는 크립토재킹 악성코드 분석 이석민, 신영주(고려대학교)	659
	3	블록체인 기반의 토큰증권 플랫폼을 위한 암호기술 제언 양수오(페어스퀘어랩), 서병완(산업정책연구원)	663
	12	반입금지 물품의 X-ray 데이터에 대한 딥러닝 모델의 instance segmentation 결과 비교 및 검증 이한주, 김광남, 박희준(연세대학교), 고광만(상지대학교), 최석환(연세대학교)	667
	13	산업기술 유출 방지를 위한 시나리오 기반 포렌식 아티팩트 분석에 관한 연구 김민정, 김소희, 이일구(성신여자대학교)	670
	89	최신 하드웨어 트레이싱 기술에 관한 조사 및 분석 윤희헌, 진지요, 루스다, 지라, 박용수(한양대학교)	674
	30	생성형 인공지능의 보안 위험과 대책방안 김정진, 서해인(청운대학교)	678
	32	메타버스 환경에서의 프라이버시 침해 행위 자동 탐지 모델 연구 김경연, 김기연, 박채령, 우영주, 한재영, 김형종(서울여자대학교)	682
	34	IoT 펌웨어 정적 취약점 분석 연구 동향 박찬희, 한창희, 신영주(고려대학교)	686
	36	Crowd-Analysis: 다각적인 사이버 침해사고 분석을 위한 협업식 분석 플랫폼 설계 가하늘, 고현승, 김준오, 김태환, 박정훈, 이지영(세종대학교), 김원철(국방부), 이세한, 박기웅(세종대학교)	690
	44	A Survey of Limitations of Re-Entrancy Vulnerability Analysis Approach Yu-Guang Jin, Hee-Kuck Oh(Hanyang University)	694
	45	IaC(Infrastructure as Code) 상에서 발생할 수 있는 보안 위협 연구 - Terraform을 중심으로 배경석(소속없음), 차유담(중앙대학교), 정금종(소속없음), 임태인(중앙대학교), 박병제(광운대학교)	698
	49	개인정보 보호를 고려하는 이미지 분류 모델 기반 리사이클 생태계 지원 안드로이드 앱 개발 김유진, 박채원, 이유진, 추연지, 김형종(서울여자대학교)	702
	73	코드 레벨 임베딩 기술 동향 분석 김찬형, 윤종희(영남대학교)	706
	77	망분리 환경에서의 보안 강화를 위한 온북 신인준, 박종현(대구대학교), 권상오(포위즈시스템), 김창훈(대구대학교)	710
	92	미 대통령 행정명령에 의한 Critical Software 보안 조치와 제로 트러스트 Capability 매핑에 대한 연구 정윤정, 조은정, 이만희(한남대학교)	714
	105	블록체인에서의 양자 내성 전자서명 연구 동향 김원웅, 강예준, 김현지, 서화정(한성대학교)	718
	113	빅 블러 시대 금융산업의 보안 위협에 관한 연구: 메타분석을 중심으로 변재욱, 최예지, 장항배(중앙대학교)	722

Crowd-Analysis: 다각적인 사이버 침해사고 분석을 위한 협업식 분석 플랫폼 설계

가하늘*, 고현승*, 김준오*, 김태환*, 박정훈*, 이지영*, 김원철[1], 이세한[2], 박기웅†

, † 세종대학교 정보보호학과 (학부생, 교수†)
[1] 대한민국 국방부 사이버작전사령부
[2] 세종대학교 시스템보안연구실 (지능형드론 융합전공) (대학원생)

Crowd-Analysis: Collaborative Analysis Platform Design for a Multilateral Cyber Incident Analysis

Ha-Neul Ka*, Hyun-Seung Ko*, Juno Kim*. Tae-Hwan Kim*, Jung-Hun Park*, Ji-Young Lee*, Won-Chul Kim[1], Se-Han Lee[2], Ki-Woong Park†

, † Dept. of Computer and Information Security, Sejong University (Undergraduate Student, Professor†)
[1] Cyber Operations Command, Ministry of National Defense
[2] SysCore Lab. (Convergence Engineering for Intelligent Drone), Sejong University (Graduate Student)

요 약

최근 APT 또는 사이버 공격의 치밀도와 공격 수준이 올라감에 따라 침해사고 발생량이 증가하였고, 이에 그 피해 수준 또한 매년 증가하고 있다. 특히 중소기업의 경우, 기술 보호 역량이 미흡한 상황이며, 이에 대한 대응책으로 정보공유체계가 중요한 과제로 인식되고 있다. 그러나 정보 공유체계의 단점으로 개인은 쉽게 접근할 수 없으며, 정보 유출에 대한 우려가 있어 정보 공유에 대한 가용성이 떨어지는 문제가 있다. 본 논문에서는 데이터 분석 및 시각화 도구를 활용하여 다각적인 정보를 수집하고 시각화하며 개인이 쉽게 접근 가능한 협업 분석 플랫폼을 설계한다. 이를 통해 사용자 간 정보 공유를 활성화하고, 집단지성을 활용하여 다각적인 사이버 침해사고를 분석을 수행한다. 이를 통해 정보 공유체계의 인식개선 및 개인의 해당 관련 분야 분석의 접근성을 높일 수 있다.

I. 서론

침해사고의 정의는 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'에 따르면 '해킹, 컴퓨터바이러스, 논리 폭탄, 메일 폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태'이다[1]. 현재 침해사고의 실태를 살펴보면, 국가 간 사이버전, 정치적 목적의 불만 표출, 금전 획득 등 다양한 이유로 사이버 공격이 활용되면서, 국내에서 신고된 사이버 보안 침해사고 건수만 2019년 418건, 2020년 603건, 2021년 640건, 2022년 1,045건으로 증가하는 추세이다[2].

이러한 상황에서 우리나라의 대기업 대비 중소기업의 기술 보호 역량을 살펴보면 대기업이 69.3점, 중견기업이 66.8점을 기록한 데에 비해 중소기업은 47.5점을 기록하여 중소기업이 상대적으로 침해사고 대응 역량이 미흡한 상황이다[3]. 정부는 이 문제를 극복하기 위해 한국인터넷진흥원(KISA)에서 운영 중인 사이버 위협 정보 분석·공유시스템(C-TAS)을 정보 공유를 원

†교신저자: 박기웅 (세종대학교 정보보호학과 교수)
본 연구는 과학기술정보통신부 및 정보통신기획평가원의 정보통신방송기술국제공동연구사업(Project No. RS-2022-00165794, 40%), 국방ICT융합사업(Project No. Project No.2022-0-00701, 10%), 실감콘텐츠핵심기술개발사업(Project No. RS-2023-00228996, 10%), 대학ICT연구센터 육성지원사업(Project No. 2023-2021-0-01816, 10%) 및 한국연구재단 개인기초연구과제(Project No. RS-2023-00208460, 30%)의 지원을 받아 수행된 연구임.

하는 모든 기업이 참여할 수 있는 '개방형' 체계로 바꾸었다[4].

이와 같이 사이버 위협에 효율적으로 대응하기 위한 정보공유체계를 구축하는 것은 해외에서도 중요한 과제로 인식되고 있다. 예시로 우리나라뿐만 아니라 미국이나 일본에서도 침해사고 발생 시 해당 단체들은 침해사고 정보를 공유하여 효율적인 공격을 방어하기 위한 ISAC(Information Sharing & Analysis Center)를 구축했다[5].

그러나 위의 정보공유체계는 침해사고 관련 정보를 개인이 쉽게 접할 수 없다는 단점이 존재한다. 또한, 이러한 정보공유체계에 대한 인식은 정보 유출에 대한 우려가 발생하는 가장 큰 요인이 되어, 정보 공유에 대한 필요성을 느끼지 못하는 문제를 야기하고 있다. 따라서 개인적으로도 편리하게 접근이 가능하며, 실시간으로 여러 분석가와 침해사고를 토론할 수 있는 플랫폼을 구축하여 접근성을 높이고, 관련 분야의 전문가가 아니더라도 침해사고 관련 정보를 편리하게 얻을 수 있도록 정보 공유를 활성화하는 플랫폼이 요구된다.

이를 위해 데이터 분석과 시각화 도구 등을 활용하여 누구나 침해사고의 전체적인 시나리오를 등록하고, 관련 정보를 쉽게 얻을 수 있으며 서로 의견을 나누어 집단지성을 통한 다각적인 사이버 침해사고 분석을 위한 협업식 분석 플랫폼을 설계하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 협업식 분석 플랫폼 개발을 위한 시스템 설계를 설명한다. 3장에서는 위 플랫폼의 구현 방식 및 등록된 침해사고에 대해 서로 의견을 추가하고, 수정하는 등 부가적인 기능에 관해서 설명한다. 4장에서는 결론 및 향후 연구계획에 대하여 설명한다.

II. 플랫폼 개발을 위한 시스템 설계

본 논문에서는 침해사고 대응을 위한 대시보드에 사용될 시각화, 데이터 분석, 게시판 기능을 MVC 모델을 활용하여 설계하고자 한다.

2.1 데이터 시각화 기반 대시보드

사용자가 침해사고의 흐름을 잘 파악할 수 있도록 침해사고 시나리오 생성 시 필수 데이터를 입력하고 해당 데이터를 활용하여 침해사고 시나리오를 시각화하여 생성할 수 있다.

초기 시나리오 생성 시, 사용자는 침해사고를 지칭하는 시나리오 제목과 사건 발생 시점 등을 입력한다. 이후 시나리오의 대시보드에 노드를 추가한다. 이 노드의 종류는 공격자, 라우터, PC, 이용자, 서버, 파일, 계정으로 6가지가 있다. 각각의 노드는 고유번호가 존재하고, 사용자의 편의성을 위해 따로 명칭을 부여할 수 있다.

이후 입력한 노드들을 화살표로 연결한다. 동시다발적으로 공격을 시도하거나 여러 방향에서 하나를 공격하기도 하는 등의 공격 패턴은 시간의 흐름과 사건의 순서를 한눈에 파악하기 어려워 사건 분석이 힘들어지는 경우가 많다. 시나리오를 분석하는 사용자의 해석을 돕기 위해 화살표로 시간의 흐름과 공격 방향을 표시하여 노드와 노드 사이를 연결해 서로의 관계를 보여준다. 위와 같은 방식으로 시나리오를 생성할 시 [그림 1]과 같은 모습이 된다.

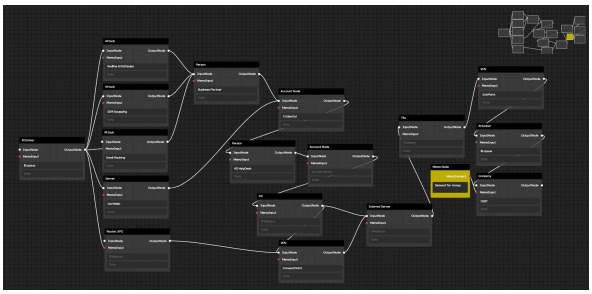

그림 1. 시나리오 시각화 대시보드의 노드 연결 예시

2.2 시나리오 데이터 분석

시나리오 생성 시 입력한 데이터를 통해 공격의 유형 및 공격자를 분석하고 발생 건수, 빈도 등을 분석하여 표로 수치화한 뒤 대시보드를 통해 보여준다. 시나리오와 노드에 관한 정보는 사전 작업, 서버 침투, 침투 후 작업, 작업 후 결과라는 4단계로 구분해 놓는다. 사전 작업은 공격자가 침투를 위해 필요한 정보를 얻는 단계고, 서버 침투는 공격자가 탈취한 권한, 혹은 이미 가지고 있던 정보로 서버에 침투하는 단계를 말한다. 또한, 침투 후 작업은 공격자가

침투에 성공한 경우, 서버에서 어떤 작업을 목표로 했는지 명시하는 단계이고, 작업 후 결과는 공격자가 작업 후 어떤 결과가 일어났는지에 대한 단계이다. 이 데이터를 활용하여 특정 공격자 및 조직의 특징, 성향 등을 분석하여 추후 발생하는 사건들을 분석할 때 도움을 줄 수 있다.

2.3 메모 및 게시판을 활용한 다각적 분석

시나리오 생성 시 시각화 대시보드에서 노드마다 즉각적으로 파악하기 힘든 추가적 정보를 넣어둘 수 있게 한다. 짧은 문장을 넣을 수 있는 메모 형태로 단순한 정보나 참고 사항 등을 적을 수 있다. 단, 시나리오를 입력하는 사용자만 시나리오에 메모를 끼워 넣을 수 있다. 그 이유는 여러 사용자가 시나리오에 간섭하면 오히려 간단하고 직관적으로 이용자에게 시나리오를 보여주기 위한 목적에 어긋나기 때문이다.

메모 기능에서는 시나리오를 생성하는 사용자만 입력할 수 있다. 반대로, 시나리오를 읽는 사용자가 침해사고에 관해 정보를 추가하고 싶을 때는 게시판을 이용할 수 있다.

게시판은 시각화 대시보드 옆에 사이드바 형태로 여닫을 수 있게 제작하여 대시보드와 게시판을 함께 확인할 수 있다. 추가로 대시보드 아래에서 게시판의 글만 읽을 수 있다.

게시판은 한 시나리오 당 하나의 게시판이 존재한다. 게시판에는 여러 게시글이 존재하며 사용자는 원하는 주제의 글에 들어가 관련 정보를 확인할 수 있다.

위처럼 게시판을 여러 게시글로 분리해 놓은 이유는 이용자가 시나리오와 관련하여 정리해 놓은 명확한 실제 정보와 관련해서 토론하고 싶은 토론글을 분리하기 위해서이다. 실제 분석가들이 하나의 시나리오를 보았을 때 그 대응책이나 예방책은 여러 방향으로 달라질 수 있다. 이러한 예방책들을 혼용하여 작성할 경우 사용자가 관련 정보 및 대응책을 혼동할 수 있으므로 게시글 내용을 서로 분리하여 사용자가 필요한 정보를 명확히 얻을 수 있다.

III. 플랫폼 제공 기능 및 활용 방안

본 장에서는 침해사고 대응을 위한 대시보드 플랫폼의 주요 기능을 구현한 방식을 설명하고 사용자의 관점에서 플랫폼을 활용할 수 있는 기본적인 절차를 안내한다.

3.1 시나리오 생성 및 활용 기능

위에 앞서 설명한 내용과 같이 시나리오를 생성하기 위해 시나리오 데이터베이스를 생성하고 Front-End 단에서 해당 데이터베이스 내용을 필요로 할 때마다 Back-End 단의 컨트롤러를 통해 데이터를 전달하는 방식으로 기능을 구현하였다. 시나리오는 JSON 형식으로 데이터베이스에 저장되며, 데이터값의 변환 없이 그대로 호출 및 변환이 가능하다. 또한 시나리오 데이터베이스는 시나리오의 단순 데이터 값만이 아닌 여러 속성들을 명시한다. 기본 인덱스, 시나리오 이름, 생성 날짜, 시나리오 기본 정보(사전 작업, 서버 침투, 침투 후 작업, 작업 후 결과) 등이 이에 속한다. 시나리오의 데이터베이스 및 정보처리 과정은 [그림 2]와 같다.

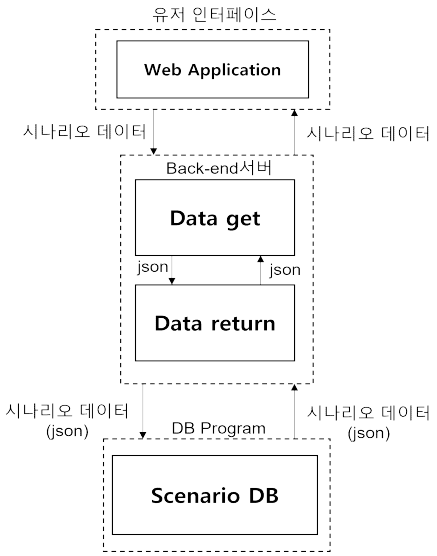

그림 2. 시나리오 분석 플랫폼 설계도

3.2 게시판 기능

기본적으로 게시판은 하나의 시나리오마다 하나가 존재하고 해당 게시판 내에 사용자가 직접 입력하는 게시글들이 포함될 수 있다. 따라서 게시판 데이터베이스는 시나리오의 기본 인덱스를 외래키로 참조하고 해당 게시판에 포함될 게시물들을 새로운 테이블들을 추가 또는 삭제하여 게시판을 제어할 수 있다. 게시물 테

이블의 칼럼으로는 제목, 작성자, 작성 날짜, 텍스트 등이 있다.

3.3 플랫폼의 전반적 활용 절차

사용자가 처음 플랫폼에 접속하면 회원가입을 진행한 뒤 로그인을 하여 홈 화면에 접속한다. 이후 시나리오 제작 또는 시나리오 선택 옵션을 선택할 수 있다. 시나리오 제작을 선택할 경우 새로운 시나리오를 생성하여 플랫폼에 새로운 사건을 추가하여 다른 사용자들과 정보를 공유할 수 있다. 시나리오 선택을 선택할 경우 시나리오 목록 중에서 하나를 선택하여 해당 시나리오의 내용을 대시보드를 통해 시각적으로 확인할 수 있고, 해당 시나리오의 게시판에서 다른 사용자들과 게시물을 통해 정보를 공유할 수 있다. 위의 절차들을 정리하면 [그림 3]과 같다.

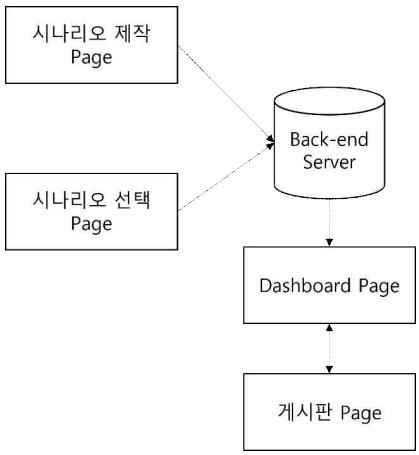

그림 3. 시나리오 분석 플랫폼 활용 절차

IV. 결론

APT와 사이버 공격의 치밀도와 공격 수준이 올라감에 따라 침해사고가 증가하고 그 피해 또한 범위가 늘어나고 있는 가운데, 이를 극복하기 위한 정보공유체계의 도입은 매우 중요하다. 따라서, 본 논문에서는 정보공유체계에서 집단지성을 활용한 정보 공유의 활성화를 목표로 하였고, 이를 위해 정보 공유체계의 인식을 개선하여 개인이 쉽게 접근이 가능한 방식을 도입하고 침해사고를 다각적으로 분석할 수 있는 플랫폼의 설계를 제안하였다. 이 설계는 침해사고를 방지하는 목적을 가진 조직뿐만 아니라, 침해사고와 관련된 여러 분야의 조직 및 개인에게도 활용될 수 있다.

위의 침해사고 대응 플랫폼은 누구나 쉽게 접근이 가능하도록 시각화를 활용한 대시보드를 제작하였고 해당 데이터를 기반으로 통계자료 및 비교분석을 수행하였다. 또한 침해사고의 다각적 분석을 위해 집단지성을 활용한 정보 공유체계를 구축하여 방대하고 다각적인 정보 수집이 가능하다. 추후 해당 플랫폼을 기반으로, 사용자들이 모여 제작한 시나리오의 정확도 및 신뢰도를 분석하여 개선점을 찾아보고자 한다.

[참고문헌]

[1] 정보통신망법 (정보통신망 이용촉진 및 정보보호 등에 관한 법률) 제2조 7항.

[2] 곽현아, “사이버 보안 침해사고 1천건 넘어”, 통계뉴스, 데이터 솜, 2023.01.

[3] 중소벤처기업부, “2020년도 중소기업기술보호수준 실태조사 보고서”, 2021.02.

[4] 김윤희, “사이버위협 정보 공유 ‘C-TAS’, 일반 기업도 가입 가능해진다”, ZDNET Korea, 2021.12.

[5] 진희승, 심미나, 양민호, “소프트웨어안전 정보공유체계에 관한 연구 - 해외 사례 중심으로”, 연구보고서 2017-009, 소프트웨어정책연구소, 2018.04.