한국정보보호학회
Korea Institute of Information Security & Cryptology

Proceedings

2021년 한국정보보호학회 하계학술대회

CISC-S'21

Conference on Information Security and Cryptography Summer 2021

2021년 6월 24일(목)

온라인 컨퍼런스

(개회식 촬영: 한국과학기술회관 12F 아나이스홀)

주최 한국정보보호학회 Korea Institute of Information Security & Cryptology

주관 KAIST 한국과학기술원

후원 과학기술정보통신부 국가정보원 National Intelligence Service Korea 행정안전부

NSR 국가보안기술연구소 National Security Research Institute KISA 한국인터넷진흥원 ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute

쌍용정보통신주식회사 SsangYong Information & Communications Corp.

클라우드 보안 분류체계 설계를 위한 요구사항 도출

양주호*, 박기웅†

*세종대학교 시스템보안연구실, † 세종대학교 정보보호학과

Requirements for designing a cloud security taxonomy

Ju-Ho Yang*, Ki-Woong Park†

*SysCore Lab., Sejong University.

† Department of Computer and Information Security, Sejong University

요 약

클라우드 환경에서 보안 위협에 대한 가시성 확보는 보안 위협을 탐지하고 대응하는 데 필수적인 요소 중 하나이다. 하지만 클라우드 환경의 복잡한 구성으로 인해 보안 사고를 클라우드의 아키텍처와 연관 지어 표현하는 데 어려움이 있어, 보안 위협에 대응하기 위한 가시성을 확보하고 향상시키는 데 한계가 있다. 이에 따라 클라우드 환경에서 발생 가능한 보안 사고를 정의 및 분류하고 보안 위협에 대한 모델을 설계하는 다양한 연구들이 꾸준히 수행되어왔다. 클라우드 가시성을 확보하기 위해서는 클라우드 환경에서 발생 가능한 보안 사고를 클라우드 아키텍처와의 연관분석이 필요하다. 따라서 본 논문은 클라우드 환경의 발생 가능한 기존의 보안 사고를 하나의 도면에서 표식 및 분류에 특화된 방식으로 분석하기 위한 클라우드 보안 분류체계를 제안하여, 이에 대한 설계를 위해 요구사항을 도출하는 것에 목적이 있다. 본 논문을 통해 클라우드 환경에서 발생 가능한 보안 사고들을 표식하고 체계적으로 분류하는 체계의 설계를 위한 요구사항을 도출하며, 추후 연구에서 분석된 보안 사고들을 표식하기 위한 아키텍처와의 연관성 분석 및 정형화된 사고의 분류 조사를 통해 표식 및 분류할 수 있는 체계인 클라우드 분류체계를 제안한다.

I. 서론

온프레미스 환경에서 클라우드 환경으로 이전하는 기업의 비율이 늘어나고 있다. 기업이 클라우드를 이용하면 멀티 테넌시, 접근성, 탄력성과 같은 장점을 활용하여 비즈니스의 유연성과 민첩성을 높일 수 있기 때문이다. 이처럼 기업 내 IT 인프라에서 선택이 아닌 필수가 되어버린 클라우드 환경은 분산되고 동적인 특성으로 인해 복잡한 구성을 가지고 있다. 이러한 복잡한 클라우드 환경은 기존의 온프레미스 환경에 없었던 새로운 보안 위협 요소를 증가시킨다. 증가한 보안 위협에 따라, 이를 탐지하고 대응하기 위해선 새로운 보안 기술에 최적화된 보안 접근 전략을 수립하는 것 뿐 만 아니라 보안 위협하는 것들을 파악하는, 즉 보안 위협에 대한 가시성을 확보하는 것 또한 중요하다.

본 논문의 큰 그림은 보안 위협에 대한 가시성을 확보하기 위해, 클라우드 환경에서 발생 가능한 보안 사고들을 하나의 도면에서 표식 및 분류에 특화된 방식으로 분석하기 위한 클라우드 보안 분류체계를 설계하는 것이다. 기존의 클라우드컴퓨팅 기술 스택[1]이 클라우드에서 제공되는 서비스를 기반으로 설계된 하나의 도면이라면, 클라우드 보안 분류체계를 구성하는 도면은 클라우드 환경에서 발생 가능한 보안 위협을 기반으로 클라우드 환경 구성 요소

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

이 논문은 ETRI부설연구소의 위탁연구과제[2021-086]의 지원(50%)과 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(No.2019-0-00273,25%) 및 한국연구재단(No.NRF-2020R1A2C4002737. 25%)의 지원을 받아 수행된 연구임.

들을 설계한 아키텍처를 의미한다.

본 논문에서는 클라우드 환경에서 발생 가능한 보안 사고들을 표식하고 체계적으로 분류하는 프레임 워크를 설계하기 위한 요구사항을 도출하고자 한다. 본 논문의 구성은 다음과 같다. 2장에서는 클라우드 환경에서 발생 가능한 보안 사고들이 분류될 수 있는 보안 위협의 요소들을 설명한다. 3장에서는 클라우드 보안 표식체계를 설계하기 위해 필요한 요구사항들을 도출한다. 4장에서 결론 및 향후 연구를 기술한다.

II. 관련 연구 및 배경 지식

본 장에서는 클라우드에서 발생한 보안 사고를 육하 원칙에 따라 정의하기 위해 관련 연구[2-5]를 통해 배경 지식을 설명한다. 이를 통해, 하나의 보안 사고를 체계적으로 분류하기 위해 세 가지 요소들이 어떻게 정의될 수 있는지 분석한다.

2.1 보안 사고를 정의하기 위한 분류

2.1.1 인적 요소 분류

클라우드 환경에서 역할을 수행할 수 있는 주체들이다.

- Consumer - CSP와 비즈니스 관계를 유지하고 서비스를 사용하는 개인 또는 조직이다.
- Provider - 이해 당사자에게 서비스를 제공할 책임이 있는 개인 또는 조직이다.
- Auditor - 서비스, 정보 시스템 운영, 성능 및 보안 등 클라우드 구현의 전반적인 평가를 독립적으로 수행할 수 있는 당사자이다.
- Broker - 클라우드 서비스의 사용, 성능 및 제공을 관리하고 CSP와 사용자 간의 관계를 협상하는 기업이다.
- Carrier - CSP에서 사용자로의 클라우드 서비스 연결 및 전송을 제공하는 중개자이다.

2.1.2 표적 요소 분류

[표 1]은 클라우드 환경에서 발생 가능한 공격 유형을 클라우드의 표적이 되는 구성 요소 기반으로 분류하였다.

[표 1] 클라우드 환경에서의 표적 요소 분류

표적 요소	공격 유형
Virtual Machine	Cross VM side channel , Guest DoS, Information leakage, VM Escape, VM Sprawling, Malware Infection, Attacks on web applications hosted on VM
Virtual Machine Monitor	VMM DoS, VMM Malware injection, VMM Hyperjacking, VMM Backdoor
Hardware	DMA Attack, BIOS and SMM Atack
Storage	Data Ramanence, Data Leakage, Dumpster diving, Hash Value Manipulation
Network	VM Traffic spoofing, VM Port scanning, DoS, VM Traffic sniffing

- Virtual Machine - 클라우드 서비스 사용자라면 누구나 쉽게 접근할 수 있기 때문에 클라우드 환경의 공격 표적으로써 취약한 부분이다. 악의적인 의도를 가진 클라우드 서비스 사용자나 관리자는 위와 같은 공격을 수행할 수도 있다.
- Virtual Machine Monitor - 해커가 VMM에 있는 프로그램 코드의 취약성을 악용하여 제어중인 VM을 손상시킬 수 있다. 수행할 수 있는 일부 공격에 대한 내용은 위와 같다.
- Hardware - 권한이 없는 사용자가 호스트 시스템에 대한 물리적 접근 권한을 얻는다면, 하드웨어에서 위협이 발생할 수 있다. 위에서는 클라우드의 하드웨어 계층을 대상으로 하드웨어 보안을 침해하고 사용자의 VM 데이터의 무결성 및 개인 정보를 손상시키는 공격이 가능하다.
- Storage - 클라우드 서비스 사용자는 동일한 물리적 스토리지를 공유하고 사용 가능한 스토리지를 용량에 따라 논리적 단위로

할당받는다. 이러한 클라우드의 멀티 테넌시 특징은 클라우드 환경의 스토리지 계층에서 위와 같은 주요 공격을 발생시킬 수 있다.

- Network – 클라우드 사용자의 네트워크에 대한 공격을 주로 고려하여, 네트워크 계층에서의 취약성을 이용한 공격 유형들로 분류하였다.

2.1.3 위협 요소 분류

[표 2]는 CSA에서 발표된 클라우드 위협 보고서로서, 기술적인 부분과 함께 외부 환경적인 요인들까지 포괄한 보안 위협을 분류한다. 이를 통해 내부 인력에 의한 의도적인 보안 위협에 대한 분류도 가능하다.

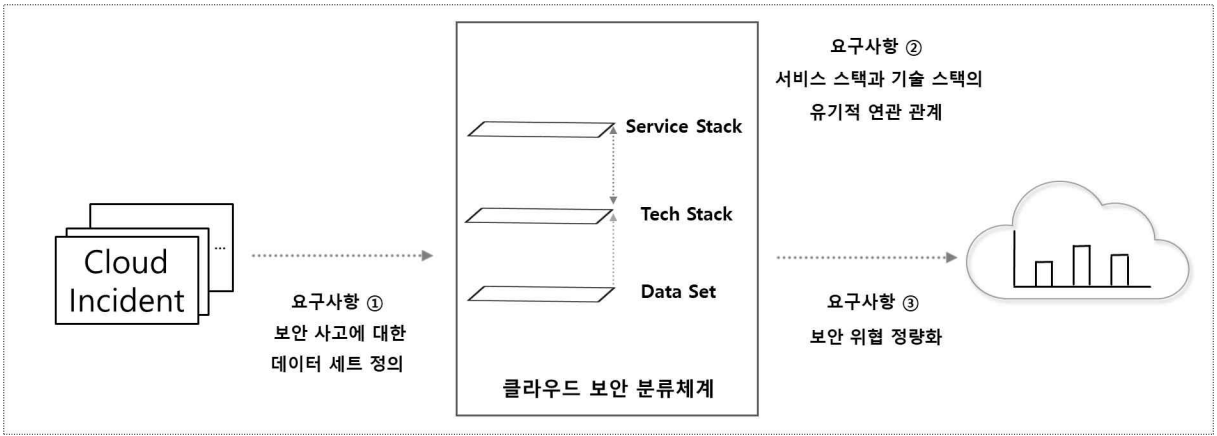
[표 2] 클라우드 환경에서의 보안 위협 분류

보안 위협	설명
데이터 유출	개인 정보를 저장하는 데이터베이스나 스토리지가 외부에 직접 노출되거나 애플리케이션 취약점으로 공격받아 노출되는 사례
잘못된 구성 및 부적절한 변경 제어	관리자의 잘못된 설정으로 인한 과도한 권한 상승, 표준 보안 제어 비활성화, 보안되지 않은 스토리지 및 컨테이너와 같은 경우
클라우드 보안 아키텍처 및 전략 부족	CSP가 제공하는 기능, 서비스에 대한 실제적인 검증을 철저히 하지 않아 클라우드 시스템의 취약점을 초래하는 경우
불충분한 ID, 자격증명 및 접근 관리	중요 권한을 가진 사용자의 계정을 공유하거나 쉬운 패스워드 사용 및 노출 등으로 인해 무단 접속을 허용하는 사례
안전하지 않은 인터페이스와 API	CSP가 관리하는 인터페이스나 API 프로그램 자체에 보안 취약점이 존재하는 경우
계정 도용	해커가 불법적으로 획득한 사용자 계정을 통해 클라우드 시스템에 접속을 시도하는 경우
내부자 위협	중요 시스템의 관리자가 의도하거나 의도치 않은 방식으로 중요 정보를 탈취하거나 침해를 하는 경우
데이터 손실	관리자의 실수로 데이터가 삭제되거나 물리적인 재해로 인해 데이터 센터의 정보 손실이 발생하는 경우
메타 구조 및 응용 구조의 구현 실패	CSP가 잘못 구현한 애플리케이션으로 인한 서비스의 기밀성, 무결성, 가용성이 침해된 경우
클라우드 서비스 남용과 악의적인 사용	자원의 확장이 쉬운 클라우드의 특성을 이용하여 취약한 클라우드 서비스를 이용하여 해킹 도구로 이용하는 경우
약한 제어 영역	CSP의 데이터 안정성과 런타임을 제공하는 데이터 영역을 보완하는 역할이 실패하는 경우
제한된 클라우드 사용 가시성	클라우드 서비스 사용자가 서비스를 제대로 활용할 능력이 없어 관리 능력 부족으로 발생하는 사고의 경우
공유 기술 취약점	가상화 기술을 활용하여 다양한 사용자가 함께 사용하는 클라우드 서비스에 격리가 안전하게 설계되지 않아 다른 사용자의 정보가 노출되는 경우

2.2 보안 사고의 정의 도출

[표 3] 보안 사고 정의를 위한 연구 분류

	인적요소 분류	표적요소 분류	위협요소 분류
Who	○	×	△
When	×	×	×
Where	×	○	△
What	×	○	○
How	×	△	△
Why	×	×	○



[그림 1] 클라우드 보안 분류체계 요구사항

[표 3]은 하나의 보안 사고를, 육하 원칙에 따른, 분류를 통해 정의하기 위한 관련 연구의 커버리지이다.

- Who - 보안 사고가 발생한 원인을 제공한 자이거나 침해를 받은 자를 '인적 요소 분류'를 통해 정의한다. 이는 '위협 요소 분류'를 통해 정의할 수도 있다.
- When - 보안 사고가 발생한 시점에 대해 분류하는 것은 고려하지 않았다.
- Where - 보안 사고가 발생한 지점에 대해선 '표적 요소 분류'에 해당되는 내용이라면, 해당되는 클라우드의 구성 요소로서 정의할 수 있다. 이는 '위협 요소 분류'를 통해 정의할 수도 있다.
- What - 보안 사고의 주된 요인이 무엇이었는지 '표적 요소 분류'에 해당되는 내용이라면, 해당되는 공격 유형으로서 정의할 수 있다, 또한 이는 '위협 요소 분류'를 통해 정의할 수 있다.
- How - 보안 사고가 어떻게 발생하였는지 '표적 요소 분류'와 '위협 요소 분류'를 통해 정의할 수 있다.
- Why - 보안 사고가 발생한 이유에 대해선 '위협 요소 분류'를 통해 정의할 수 있다.

III. 클라우드 보안 분류체계 설계를 위한 요구사항

본 장에서는 2장에서 분석한 클라우드 환경에서 발생 가능한, 분류된 보안 위협들을 기반으로 클라우드 보안 분류체계의 설계를 위한 요구사항을 알아본다.

3.1 보안 사고에 대한 데이터 세트 정의

클라우드 환경에서 발생한 보안 사고를 2장에서 분석한 관련 연구 내용을 기반으로 육하원칙을 통해 하나의 데이터 세트를 정의할 수 있어야 한다. 이를 통해 도출된 하나의 보안 사고에 대한 데이터 세트는 클라우드 보안 분류체계를 통해 표식 및 분류가 가능하다.

3.2 서비스 스택과 기술 스택의 유기적 연관 관계

3.1을 통해 도출된 보안 사고에 대한 데이터 세트를 기반으로 클라우드 보안 분류체계의 설계도 위에 표식이 가능할 수 있어야 한다. 표식이 가능하기 위한 클라우드 보안 분류체계는 클라우드 서비스 표면을 나타내는 서비스 스택과 이러한 서비스들을 구성하고 있는 기술 스택으로 이루어져 있으며 유기적인 연관 관계에 대한 정의가 이루어져야 한다. 이에 따라 앞으로 두 스택 간의 유기적 연관 관계와 가공된 보안 위협 데이터 세트를 상호 대응시키기 위한 연구가 이루어져야 한다.

3.3 보안 위협 정량화

클라우드 보안 분류체계를 통해, 클라우드 환경에서 발생한 다양한 보안 사고들에 대한 데이터를 정형화하여 체계적으로 통계 분석과 같은 결과물을 도출할 수 있다. 이를 통해 클라우드

보안 분류체계의 설계도에서 클라우드 환경을 구성하는 요소 중 어느 곳이 가장 보안 위협에 취약한지 중요도를 파악할 수 있어야 한다.

IV. 결론 및 향후 연구과제

클라우드 환경에서 발생 가능한 보안 사고를 클라우드 아키텍처와 연관분석을 통해 파악할 수 있다면 보안 위협에 대한 가시성을 확보할 수 있다. 본 논문에서는 이를 위해 제안하는 클라우드 보안 분류체계의 설계로서, 기존의 발생 가능한 보안 사고들을 체계적으로 분류한 논문들을 분석하고, 이를 통해 하나의 보안 사고를 육하원칙에 따른 데이터 세트 정의를 도출하기 위해 분류하였다. 이를 토대로 '보안 사고에 대한 데이터 세트 정의', '서비스 스택과 기술 스택의 유기적 연관 관계', '보안 위협 정량화'와 같은 요구사항들을 도출하였다. 추후 연구에서는 클라우드 보안 분류체계를 구성하는 서비스 스택과 기술 스택 간의 유기적 연관 관계에 대한 정의가 이루어지고 이를 통해 가공된 보안 위협 데이터 세트를 삽입하여 설계도에서 클라우드 환경을 구성하는 요소 중 어느 곳이 가장 보안 위협에 취약한지 중요도를 정량화하여 나타낼 수 있는 프레임 워크를 개발할 계획이다.

[참고문헌]

[1] 한국 클라우드 컴퓨팅 연구 조합, 클라우드 컴퓨팅 기술 스택 v3.0, http://cccr.or.kr/home/, 2017

[2] Hamed Tabrizchi and Marjan Kuchaki Rafsanjani, A survey on security challenges in cloud computing: issues, threats, and solutions, The Jounal of Supercomputing, 2020

[3] Preeti Mishra, Emmanuel S. Pilli, Vijay Varadharajan and Udaya Tupakula, Intrusion detection techniques in cloud environment: A survey, Journal of Network and Computer Applications, 2017

[4] CSA, The Treacherous 12 Cloud Computing Top Threats in 2016, February 2016

[5] CSA, Top Threats to Cloud Computing The Egregious 11, April 2020