KIPS Trans. Comp. and Comm. Sys.
Vol.10, No.5 pp.145~154
ISSN: 2287-5891 (Print), ISSN 2734-049X (Online)

https://doi.org/10.3745/KTCCS.2021.10.5.145

Derivation of Security Requirements for Cloud Managing Security Services System by Threat Modeling Analysis

Jang Hwan†

ABSTRACT

Recently, the introduction of Cloud Managing Security Services System to respond to security threats in cloud computing environments is increasing. Accordingly, it is necessary to analyze the security requirements for the Cloud Managing Security Services System. However, the existing research has a problem that does not reflect the virtual environment of the cloud and the data flow of the Cloud Managing Security Services System in the process of deriving the requirements. To solve this problem, it is necessary to identify the information assets of the Cloud Managing Security Services System in the process of threat modeling analysis, visualize and display detailed components of the cloud virtual environment, and analyze the security threat by reflecting the data flow. Therefore, this paper intends to derive the security requirements of the Cloud Managing Security Services System through threat modeling analysis that is an improved existing research.

Keywords : Cloud Managing Security Services System, Threat Modeling Analysis, Security Function Requirements

위협 모델링 분석에 의한 클라우드 보안관제시스템 보안요구사항 도출

장 환†

요 약

최근 클라우드 컴퓨팅 환경의 보안 위협에 대응하기 위한 클라우드 보안관제시스템 도입이 증가하고 있다. 이에 따라 클라우드 보안관제시스템에 대한 보안 요구 사항 분석이 필요하다. 하지만 기존의 연구는 요구사항을 도출하는 과정에서 클라우드의 가상환경과 보안관제시스템의 데이터 흐름 등을 반영하지 못한 문제점이 있다. 이를 해결하기 위해, 위협 모델링 분석과정에서 클라우드 보안관제시스템의 정보자산을 식별하여 클라우드 가상환경의 세부적인 구성요소를 시각화하고, 데이터 흐름을 반영하여 보안 위협을 분석하는 과정이 필요하다. 따라서 본 논문은 기존의 연구를 개선한 위협 모델링 분석을 통해, 클라우드 보안관제시스템의 보안 요구 사항을 도출한다.

키워드 : 클라우드 보안관제시스템, 위협모델링 분석, 보안 요구 사항

1. 서 론

미국 국립표준기술연구소 NIST(National Institutes of Standards and Technology)는 클라우드 컴퓨팅을 “최소한의 관리 노력으로 신속하게 공급 및 배포할 수 있는 컴퓨팅 자원의 공유 환경에 대한 주문형 네트워크를 언제 어디서나 편리하게 접근할 수 있는 모델”로 정의한다. 언제 어디서나 편리하게 이용할 수 있는 이점이 있어서 클라우드 컴퓨팅 환경의 서비스에 대한 도입이 증가하고 있다[1]. 클라우드 컴퓨팅 환경의 서비스 증가로 보안 이슈도 발생하고 있다. 클라우드 보안 협회 CSA(Cloud Security Alliance)는 클라우드 보안 이슈를 해결하기 위해 SecaaS를 Table 1과 같이 정의하고 있다[2].

Table 1. CSA SecaaS [2]

12 SecaaS categories selected by CSA	
Network Security	Vulnerability Scanning
Web Security	Email Security
Identity and Access Management	Encryption
Intrusion Management	Data Loss Prevention
Security Information and Event Manager	Business Continuity and Disaster Recovery
Continuous Monitoring	Security Assessment

† 준 회 원 : 한국방송통신대학교 정보과학과 석사과정
Manuscript Received : July 3, 2020
Accepted : August 11, 2020
* Corresponding Author : Hwan Jang(jangh1220@knou.ac.kr)

따라서 클라우드 컴퓨팅 환경의 보안 위협에 대응하기 위해 SecaaS 목록에 해당하는 보안 서비스 구현이 증가하고 있다[6]. SecaaS 목록 중에서 Security Information and Event Manager는 클라우드 컴퓨팅 환경에서 보안정보 및 이벤트 로그를 실시간으로 수집하고 각 정보의 상관관계를 분석할 수 있는 서비스가 요구된다. 이에 해당하는 SIEM은 클라우드 보안장비의 보안 로그와 서버/스토리지의 이벤트 로그를 통합 수집하여 분석 및 대응할 수 있는 보안관제시스템의 구성요소이다. Intrusion Management는 패턴 매칭과 통계적 임계치값을 통해 비정상 이벤트를 감지하고, 침입시도를 탐지 및 대응할 수 있는 서비스가 요구된다. 이에 해당하는 TMS는 정보자산에 대한 위협 트래픽을 시그니처 기반의 탐지룰과 Threshold를 통해 탐지 및 수집하고, 분석 및 대응할 수 있는 보안관제시스템의 구성요소이다. 클라우드 보안관제센터에서 SIEM과 TMS의 도입이 필요하지만, 기존의 연구는 보안 요구사항을 도출하는 과정에서 클라우드의 가상환경과 보안관제시스템의 데이터 흐름 등을 반영하지 못한 문제점이 있다[3,4]. 이러한 문제점을 해결하기 위해, 본 논문은 데이터 흐름 다이어그램에 클라우드 보안관제시스템의 데이터 흐름과 클라우드 가상환경을 반영한다. 도출된 데이터 흐름 다이어그램을 토대로 STRIDE 위협 분석을 수행한다. STRIDE 위협 분석결과에 따라 클라우드 보안관제시스템에 내재된 OWASP 취약점 리스트에 대한 외부의 위협을 공격 시나리오로 구성하여 Attack Tree 분석을 수행한다. 마지막으로, Attack Tree 분석 결과를 Category, Sub Category, Primary Category로 분류 및 맵핑하여 보안 요구 사항을 도출한다.

2. 관련 연구

2.1 보안관제시스템의 보안 요구 사항 도출

[3]에서는, 보안 문제와 보안목적을 정의하여, 보안 요구 사항을 도출하였다. 하지만 보안관제시스템의 데이터 흐름을 고려하지 못한 문제점이 있다. 이를 해결하기 위해, 보안관제시스템의 데이터 흐름을 분석하여 다이어그램을 작성하고, 위협 모델링 분석을 통해 보안 요구사항을 도출하는 과정이 필요하다.

2.2 위협 모델링 분석에 의한 클라우드 보안서비스

[4]에서는, 이메일 클라우드 보안 서비스에 대한 데이터 흐름 다이어그램 작성을 통해 위협 모델링 분석을 수행하였다. 하지만 클라우드 스토리지의 가상환경을 데이터 흐름 다이어그램에 반영하지 못한 문제점이 있다. 이를 해결하기 위해, 가상환경의 반영이 필요하다.

3. 위협모델링 분석

위협모델링 분석이란 Software Development Life Cycle의 구현 전 단계에서 임의의 공격자 관점으로 분석대상의 위협을 식별 및 분석하는 방법론이다[4,5].

본 논문에서는 Microsoft에서 제공하는 Threat modeling tool을 사용하여 클라우드 보안관제시스템에 대해 위협모델링 분석을 수행하였다. 위협모델링 분석은 정보자산 식별 → 데이터 흐름 다이어그램 도출 → STRIDE 위협 분석 → Attack Tree 분석 순서로 진행하였다[4,5].

3.1 위협 모델링 분석 사례

[8]에서는, Microsoft에서 개발한 STRIDE 분석 방법론을 사용하여, 스마트시티에 대한 위협모델링 분석을 수행하였다. 시스템을 구성 요소로 분해하고, 각 구성 요소에 대한 데이터 흐름 다이어그램을 스케치하였으며, 데이터 흐름 다이어 그램의 각 요소에 대해 위협을 식별하고, 분류하여 대응책을 제시하였다.

[9]에서는, 스마트 TV를 대상으로 위협 모델링 분석을 수행하였다. 수집한 공격 라이브러리를 기반으로 데이터 흐름도를 도출하고 STRIDE 위협을 분석하였다. 식별된 위협을 바탕으로 Attack Tree를 작성하여 스마트 TV 모의해킹 시나리오를 제시하고, 취약점 점검 리스트를 도출하여 검증한 것이 특징이다.

3.2 정보자산 식별

기업이 서비스를 개발 및 운영하기 위해서는 인프라 즉, 데이터베이스, 시스템, 네트워크 등의 정보자산이 필요하며, 정보 보안의 관점에서 Cloud Service Provider Boundary와 Cloud Service Consumer Boundary 내 모든 정보자산이 위협으로부터 보호해야 할 대상이 된다. 이를 관리하기 위해 정보자산을 식별하고 위협을 분석하여, 보안요구사항을 도출할 필요가 있다. 따라서 클라우드 보안관제시스템의 정보자산을 Table 2와 같이 식별하여 정보자산 목록을 작성하였다.

Table 2. List of Information Assets

Location	Category	Assets No.	Assets	Levels
Cloud Service Provider Boundary	Storage	ST-01	Physical Storage	High
	Network	NW-01	Physical Router	High
	Security equipment	SE-01	Physical FW	High
		SE-02	Physical IPS	High
		SE-03	Physical WAF	High
		SE-04	TMS Sensor	High
		SE-05	TMS	High
		SE-06	SIEM	High
	Software	SW-01	Hypervisor	High
Cloud Service Consumer Boundary	Server	SV-01	Virtual Machine	High
	Network	NW-02	Virtual Router	High
	Security equipment	SE-07	Virtual FW	High
		SE-08	Virtual IPS	High
		SE-9	Virtual WAF	High
		SE-10	TMS Sensor	High
		SE-11	Cloud TMS Application	High
		SE-12	Cloud SIEM Application	High
	Software	SW-02	OS	High

Table 3. Data Flow Diagram Component

Element	Shape	Description
Entity		Generate data input/output
Device		Temporary / permanent data storage
Process		Data input/output processing
Data Flow		Data movement
Trust Boundary		Change of authority level

3.3 데이터 흐름 다이어그램 도출

DFD(Data Flow Diagram)는 시스템 구성요소 간의 데이터 흐름을 시각화하여 나타낸 그림이다. DFD의 구성요소는 Table 3과 같다[4,5]. 이를 활용하여 클라우드 보안관제시스템의 DFD를 도출한다.

1) 클라우드 보안관제시스템 DFD 구조 및 설명

클라우드 보안관제시스템은 클라우드 환경에서 보안관제를 위해 보안관제센터에서 운영하는 시스템이다[3]. 따라서 클라우드 보안관제시스템에서 보안장비의 보안정보와 서버/스토리지의 이벤트 로그를 수집하는 구조로 DFD를 Fig. 1과 같이 작성하였고, Table 1의 SecaaS를 반영하여 SIEM과 TMS를 클라우드 보안관제시스템의 구성요소에 포함하였다. 클라우드 보안관제시스템 DFD의 구조 및 설명은 아래와 같다[20].

a) User : 클라우드 컴퓨팅 환경의 이용자 혹은 관리자
b) Physical Router : 물리적으로 서로 다른 네트워크의 거점에 설치되어 수신한 패킷을 라우팅 테이블의 정보에 따라 적절한 경로로 목적지에 전송하는 기능을 갖춘 네트워크 장비
c) Virtual Router : 가상환경에서 서로 다른 네트워크의 거점에 수신된 패킷을 라우팅 테이블의 정보에 따라 적절한 경로로 목적지에 전송하는 기능을 갖춘 네트워크 장비
d) Physical FW : 물리적 환경에 설치되어 In-Out Bound 전송 트래픽을 IP, Port 기반 허용/차단 정책에 따라 처리하는 기능을 갖춘 보안장비
e) Virtual FW : 가상의 환경에 설치되어 In-Out Bound 전송 트래픽을 IP, Port 기반 허용/차단 정책에 따라 처리하는 기능을 갖춘 보안장비
f) TMS Sensor : 물리/가상의 환경에 설치되어 미러링 된 In-Out Bound 전송 트래픽을 탐지룰에 따라 실시간으로 수집하고 TMS Manager Server에 전송하는 기능을 갖춘 보안장비
g) Physical IPS : 물리적 환경에 설치되어 In-Out Bound 전송 트래픽을 탐지룰 및 임계치 값에 따라 실시간으로 분석하고 비정상 패킷을 탐지 및 차단하는 기능을 갖춘 보안장비
h) Virtual IPS : 가상환경에 설치되어 In-Out Bound 전송 트래픽을 탐지룰 및 임계치 값에 따라 실시간으로 분석하고 비정상 패킷을 탐지 및 차단하는 기능을 갖춘 보안장비
l) Physical WAF : 물리적 환경에 설치되어 Web Application 계층의 In-Out Bound 전송 트래픽을 탐지룰 및 임계치값에 따라 실시간으로 해독 및 분석하고 비정상 패킷을 탐지 및 차단하는 기능을 갖춘 보안장비
j) Virtual WAF : 가상환경에 설치되어 Web Application 계층의 In-Out Bound 전송 트래픽을 탐지룰 및 임계치값에 따라 실시간으로 해독 및 분석하고 비정상 패킷을 탐지 및 차단하는 기능을 갖춘 보안장비
k) TMS : Threat Management System의 약자이며, 클라우드 컴퓨팅 환경에서 서로 다른 위치에 설치된 TMS Sensor로부터 위협 트래픽을 수집하고 분석하여 침해사고에 대응할 수 있는 기능을 갖춘 보안장비
l) SIEM : Security Information and Event Management의 약자이며, 클라우드 컴퓨팅 환경에서 보안장비에 저장된 로그와 서버/스토리지의 이벤트로그를 수집하여, 통합적으로 로그를 분석 및 관리할 수 있는 기능을 갖춘 보안장비
m) Cloud Service Provider's CERT : Cloud Service Provi der Boundary에서 TMS와 SIEM 등의 클라우드 보안관제시스템을 이용하여 공격을 탐지 및 분석하고 침해사고에 대응하는 그룹
n) Physical Storage : CSC에게 클라우드 컴퓨팅 환경을 제공하기 위해 CSP가 보유하고 있는 물리적인 저장소
o) Hypervisor : 스토리지에서 다수의 Virtual Machine을 실행하고 제어하는 플랫폼
p) Virtual Machine : CPU, Memory, Disk, NIC 등 HW 자원이 에뮬레이트된 가상의 컴퓨터
q) OS : Virtual Machine에 설치된 운영체제
r) Cloud Web Server Application : 가상환경의 OS에 설치되어 Application 계층에서 Web Service를 User에게 제공하는 서버 응용 프로그램
s) Cloud TMS Application : 가상환경의 OS에 설치되어 Application 계층에서 TMS Service를 SaaS 형태로 CERT에게 제공하는 응용 프로그램
t) Cloud SIEM Application : 가상환경의 OS에 설치되어 Application 계층에서 SIEM Service를 SaaS 형태로 CERT에게 제공하는 응용 프로그램
u) Cloud Service Consumer's CERT : Cloud Service Co nsumer Boundary에서 Cloud TMS Application과 Cloud SIEM Application 등의 클라우드 보안관제시스템을 이용하여 공격을 탐지 및 분석하고 침해사고에 대응하는 그룹

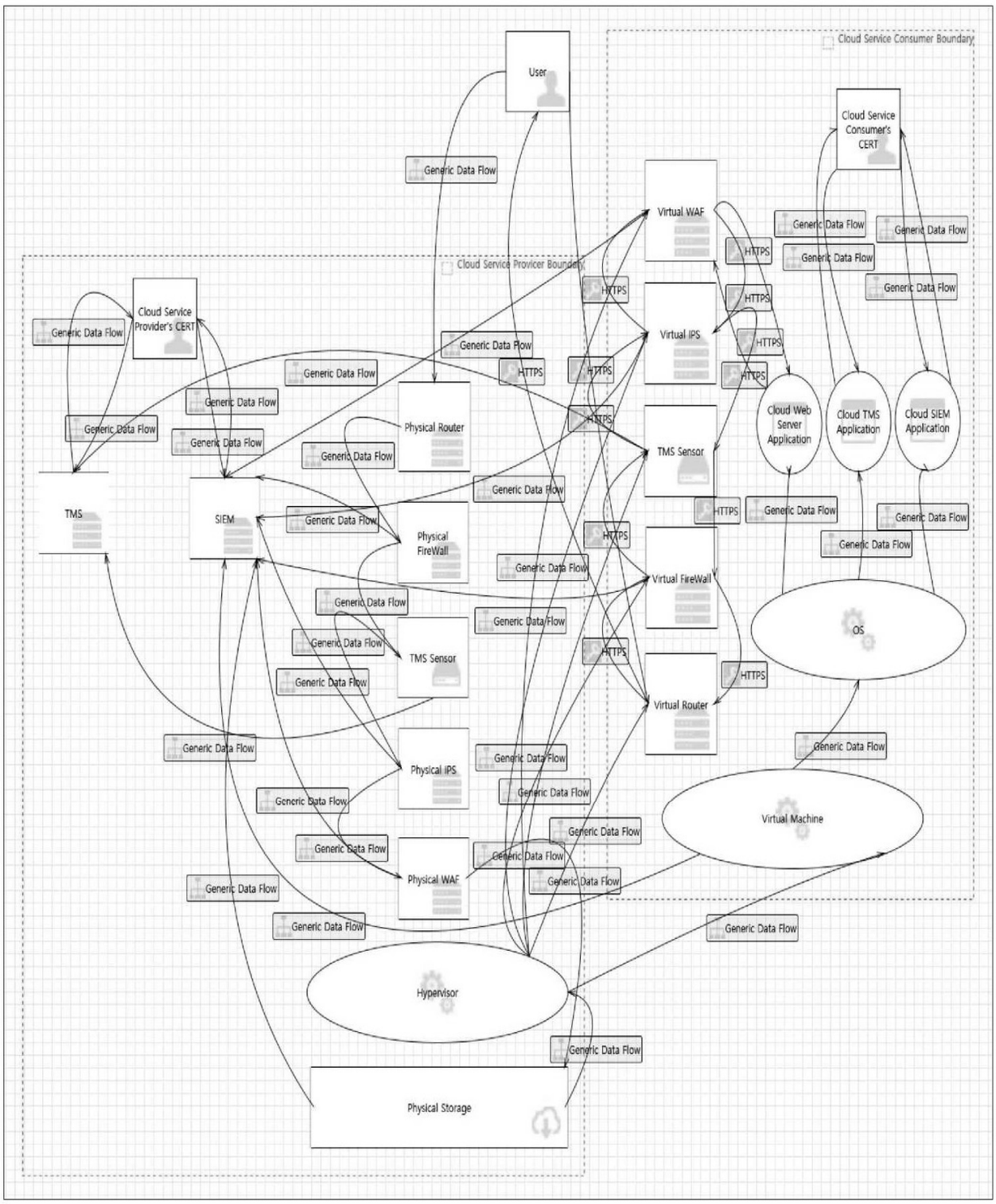

Fig. 1. Cloud Managing Security Services System Data Flow Diagram

2) 클라우드 보안관제시스템 데이터 흐름도

CSP(Cloud Service Provider)의 영역인 물리적 환경의 경계와 CSC(Cloud Service Consumer)의 영역인 가상환경의 경계를 구분하고, Cloud Service Consumer Boundary와 Cloud Service Provider Boundary를 모두 보호하기 위한 데이터 흐름을 반영하여 클라우드 보안관제시스템의 Data Flow Diagram을 도출하였다[4,5,7]. 데이터 흐름도에 대한 설명은 아래와 같다.

a) Cloud Service Provider Boundary에 있는 Physical Storage에서 Hypervisor가 실행된다. Hypervisor에서 Cloud Service Consumer Boundary의 Virtual Machine이 실행되고, Virtual Machine에서 OS가 실행된다. OS에서는 Cloud Web Server Application, Cloud SIEM Application, Cloud TMS Application 등의 Application이 실행되고 User와 Cert에게 각 서비스가 제공된다.

b) Hypervisor에 Virtual Router, Virtual FireWall, TMS Sensor, Virtual IPS, Virtual WAF 등 가상의 네트워크 장비 및 보안장비와 Virtual Machine이 실행되어 운영된다.

c) 클라우드 컴퓨팅 환경에서 인프라를 관리하는 User가 Cloud Service Provider Boundary에 있는 Physical Storage에 접근하면, Physical Router를 통해 Physical FireWall, TMS Sensor, Physical IPS, Physical WAF를 경유한다.

d) 클라우드 컴퓨팅 환경에서 클라우드 서비스를 이용하는 User가 Cloud Service Consumer Boundary의 Virtual Machine에 웹 서비스를 요청하면 Virtual Router를 통해 Virtual FireWall, TMS Sensor, Virtual IPS, Virtual WAF를 경유한다.

e) User로부터 웹 서비스 요청을 수신한 Cloud Service Consumer Boundary의 Virtual Machine은 Cloud Web Server Application을 통해 처리된 응답을 제공한다.

f) TMS는 User가 Cloud Service Provider Boundary 및 Cloud Service Consumer Boundary에서 데이터를 송수신할 때, TMS Sensor로부터 위협 트래픽을 수집하고, 로그를 분석 및 위협에 대응한다.

g) SIEM은 Cloud Service Provider Boundary에서 Physical FireWall, Physical IPS, Physical WAF에 수집된 보안정보와 Physical Storage에서 실시간으로 발생하는 이벤트 로그를 수집하고, Cloud Service Consumer Boundary에서 Virtual FireWall, Virtual IPS, Virtual WAF에 수집된 보안정보와 Virtual Machine에서 발생하는 이벤트 로그를 수집하여, 분석 및 위협에 대응한다.

h) Cloud Service Provider's CERT는 TMS와 SIEM을 통해 클라우드 보안관제를 수행한다.

I) Cloud Service Consumer's CERT는 Cloud SIEM Application, Cloud TMS Application을 통해 클라우드 보안관제를 수행한다.

3.3 STRIDE 위협 분석 수행

STRIDE 위협분석은 Spoofing, Tempering, Repudiation, Information Disclosure, Denial of service, Elevation of Privilege의 6가지 카테고리로 분류하여 위협을 분석한다. 6가지 카테고리로 분류된 위협으로부터 정보자산을 보호하기 위한 정보 보안의 6가지 요소는 Table 4와 같다. 따라서 STRIDE 위협분석은 클라우드 보안관제시스템의 6가지 정보 보안 요소에 대한 위협을 식별할 목적으로 수행한다.

데이터 흐름 다이어그램을 토대로 STRIDE 위협 분석을 수행하면 데이터 흐름 다이어그램의 각 시스템 구성요소에 내재된 취약점에 대한 STRIDE 위협과 시스템 구성요소 간 데이터 흐름에서 발생하는 STRIDE 위협을 식별할 수 있다. 도출된 데이터 흐름 다이어그램을 토대로 클라우드 보안관제시스템의 STRIDE 위협 분석을 수행한 결과에서 Table 2의 클라우드 보안관제시스템 정보자산과 데이터 흐름에 대한 STRIDE 위협을 분석한 결과는 Table 5와 같이 Spoofing 46개, Tempering 15개, Repudiation 10개, Information Disclosure 5개, Denial of service 9개, Elevation of Privilege 6개로 총 91개의 위협이 분석되었다[4,5]. 클라우드 보안관제시스템의 정보자산에 대한 STRIDE 위협 분석을 수행한 결과는 Table 6과 같다.

3.4 Attack Tree 분석

Attack Tree는 Target System에 대한 공격 시나리오를

Table 4. The Six Property of Information Security

STRIDE	Security Property	Description
S	Authentication	Being able to verify the identity of the entity
T	Integrity	Preventing unauthorized users or objects from tampering with information
R	Non-Repudiation	Failure to deny that the recipient has received the information
I	Confidentiality	Preventing unauthorized users or objects from knowing the content of the information
D	Availability	To ensure that when unauthorized users or objects try to access information, this is not disturbed
E	Authorization	To be able to trust the behavior of an entity

Table 5. STRIDE Threat Analysis Results

Category	Description	Analysis
Spoofing	Sending malicious data in disguise	46
Tempering	Improper security settings and tampering	15
Repudiation	Denial of data reception from external boundaries	10
Information Disclosure	Exposing private documents to unauthorized persons	5
Denial of service	Service crashes, freezes, or runs slowly	9
Elevation of Privilege	Elevation of privilege through malicious attack on the target	6

Table 6. STRIDE Threat Analysis on Cloud Managing Security Services System Information Assets

Location	Assets	STRIDE	Description	Priority
Cloud Service Provider Boundary	Physical Storage	S	Attackers may spoof data flows between Physical Storage and hypervisor.	High
		S	Attackers may send data to another destination by spoofing data flows from Physical Storage.	High
		S	Attackers may spoof data flows between Physical Storage and SIEM.	High
		I	Attackers may be able to read non-public information on Physical Storage.	High
	Physical Router	S	Attackers may send data to another destination by spoofing data flows from Physical Router.	High
		S	Attackers may spoof data flows between Physical Router and Physical FireWall.	High
		T	Attackers may alter the data transmitted to the Physical Router.	High
		R	Physical Router may deny data received from the outer boundary.	High
	Physical FW	S	Attackers may spoof data flows between Physical FireWall and SIEM.	High
		S	Attackers may spoof data flows between Physical FireWall and TMS Sensor.	High
		S	Attackers may send data to another destination by spoofing data flows from Physical FireWall.	High
	Physical IPS	S	Attackers may spoof data flows between Physical IPS and Physical WAF.	High
		S	Attackers may send data to another destination by spoofing data flows from Physical IPS.	High
		S	Attackers may spoof data flows between Physical IPS and SIEM.	High
	Physical WAF	S	Attackers may send data to another destination by spoofing data flows from Physical WAF.	High
		S	Attackers may spoof data flows between Physical WAF and Physical Storage.	High
		S	Attackers may spoof data flows between Physical WAF and SIEM.	High
	TMS Sensor	S	Attackers may spoof data flows between TMS Sensor and Physical IPS.	High
		S	Attackers may spoof data flows between TMS Sensor and TMS.	High
		S	Attackers may send data to another destination by spoofing data flows from TMS Sensor.	High
		T	Attackers may alter the data transmitted to the TMS Sensor.	High
		R	TMS Sensor may deny data received from the outer boundary.	High
		D	Attackers may exhaust the resources of the TMS sensor.	High
	TMS	S	Attackers may send data to another destination by spoofing data flows from TMS.	High
		S	Attackers may spoof data flows between TMS and Cloud Service Provider's CERT.	High
		R	TMS may deny data received from the outer boundary.	High
		I	Attackers may be able to read non-public information on TMS.	High
	SIEM	S	Attackers may send data to another destination by spoofing data flows from SIEM.	High
		S	Attackers may spoof data flows between SIEM and Cloud Service Provider's CERT.	High
		T	Attackers may alter the data transmitted to the SIEM.	High
		R	SIEM may deny data received from the outer boundary.	High
		I	Attackers may be able to read non-public information on SIEM.	High
		D	Attackers may exhaust the resources of the SIEM.	High
	Hypervisor	S	Attackers may spoof data flows between Hypervisor and Virtual Machine.	High
		S	Attackers may spoof data flows between Hypervisor and TMS Sensor.	High
		S	Attackers may spoof data flows between Hypervisor and Virtual FireWall.	High
		S	Attackers may spoof data flows between Hypervisor and Virtual Router.	High
		S	Attackers may spoof data flows between Hypervisor and Virtual IPS.	High
		S	Attackers may spoof data flows between Hypervisor and Virtual WAF.	High
		D	Attackers may exhaust the resources of the Hypervisor.	High
		E	Attackers may perform an elevation of privilege attack through a vulnerability in the Hypervisor.	High
Cloud Service Consumer Boundary	Virtual Machine	S	Attackers may spoof data flows between Virtual Machine and Hypervisor.	High
		S	Attackers may spoof data flows between Virtual Machine and SIEM.	High
		T	Attackers may alter the data transmitted to the Virtual Machine.	High
		R	Virtual Machine may deny data received from the outer boundary.	High
		D	The availability of the virtual machine may be violated by a DoS attack.	High
		D	Attackers may exhaust the resources of the Virtual Machine.	High
		E	Attackers may perform a privilege escalation attack on the Virtual Machine to gain additional privileges.	High
	Virtual Router	E	Attackers may perform a privilege escalation attack to change the data flow of the virtual machine.	High
		S	Attackers may send data to another destination by spoofing data flows from Virtual Router.	High

Location	Assets	STRIDE	Description	Priority
Cloud Service Consumer Boundary		S	Attackers may spoof data flows between Virtual Router and Virtual FireWall.	High
		S	Attackers may spoof data flows between Virtual Router and User.	High
		T	Attackers may alter the data transmitted to the Virtual Router.	High
		T	Attackers may be able to tamper with the data transmitted by https to the Virtual router.	High
		R	Virtual Router may deny data received from the outer boundary.	High
		I	Attackers may be able to read non-public information on Virtual Router.	High
		D	Attackers may exhaust the resources of the Virtual Router.	High
	Virtual FW	S	Attackers may spoof data flows between Virtual FireWall and SIEM.	High
		S	Attackers may send data to another destination by spoofing data flows from Virtual FireWall.	High
		S	Attackers may spoof data flows between Virtual FireWall and TMS Sensor.	High
		S	Attackers may spoof data flows between Virtual FireWall and Virtual Router.	High
		T	Attackers may alter the data transmitted to the Virtual FireWall.	High
		R	Virtual FireWall may deny data received from the outer boundary.	High
		D	Attackers may exhaust the resources of the Virtual FireWall.	High
	Virtual IPS	S	Attackers may spoof data flows between Virtual IPS and SIEM.	High
		S	Attackers may send data to another destination by spoofing data flows from Virtual IPS.	High
		S	Attackers may spoof data flows between Virtual IPS and Virtual WAF.	High
		S	Attackers may spoof data flows between Virtual IPS and TMS Sensor.	High
		T	Attackers may alter the data transmitted to the Virtual IPS.	High
		R	Virtual IPS may deny data received from the outer boundary.	High
		D	Attackers may exhaust the resources of the Virtual IPS.	High
	Virtual WAF	S	Attackers may spoof data flows between Virtual WAF and SIEM.	High
		S	Attackers may send data to another destination by spoofing data flows from Virtual WAF.	High
		S	Attackers may spoof data flows between Virtual WAF and Cloud Web Server Application.	High
		S	Attackers may spoof data flows between Virtual WAF and Virtual IPS.	High
		T	Attackers may alter the data transmitted to the Virtual WAF.	High
		R	Virtual WAF may deny data received from the outer boundary.	High
		I	Attackers may be able to read non-public information on Virtual WAF.	High
		D	Attackers may exhaust the resources of the Virtual WAF.	High
	TMS Sensor	S	Attackers may send data to another destination by spoofing data flows from TMS Sensor.	High
		S	Attackers may spoof data flows between TMS Sensor and Virtual FireWall.	High
		T	Attackers may alter the data transmitted to the TMS Sensor.	High
		R	TMS Sensor may deny data received from the outer boundary.	High
	Cloud TMS Application	T	Attackers may perform a tampering attack on the Cloud TMS Application by not verifying the input value.	High
		E	Attackers may perform a privilege escalation attack on the Cloud TMS Application to gain additional privileges.	High
	Cloud SIEM Application	T	Attackers may perform a tampering attack on the Cloud SIEM Application by not verifying the input value.	High
		E	Attackers may perform a privilege escalation attack on the Cloud SIEM Application to gain additional privileges.	High
	OS	T	Attackers may perform a tampering attack on the Cloud Web Server Application through the vulnerability of the OS.	High
		T	Attackers may perform a tampering attack on the Cloud SIEM Application through the vulnerability of the OS.	High
		T	Attackers may perform a tampering attack on the Cloud TMS Application through the vulnerability of the OS.	High
		E	Attackers may perform a privilege escalation attack on the OS to gain additional privileges.	High

Fig. 2와 같이 상향식 트리 형식으로 가시화하여 나타낸 개념도 이다[4,5].

STRIDE 위협 분석 결과에 따라 Table 7의 OWASP 취약점 리스트를 참조하여 클라우드 보안관제시스템의 Attack Tree 분석을 수행하였다[19].

Spoofing 공격 시나리오에 따라 Fig. 3의 Attack Tree 분석을 수행하였다.

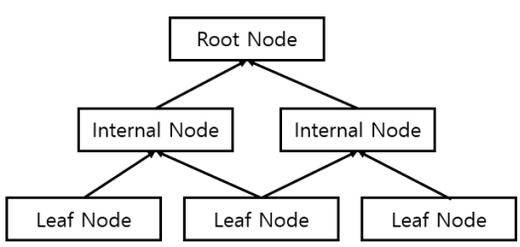

Fig. 2. Attack Tree Analysis

Table 7. The Top 10 OWASP Vulnerabilities [19]

The Top 10 OWASP Vulnerabilities in 2020
1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access control
6. Security misconfigurations
7. Cross Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with known vulnerabilities
10. Insufficient logging and monitoring

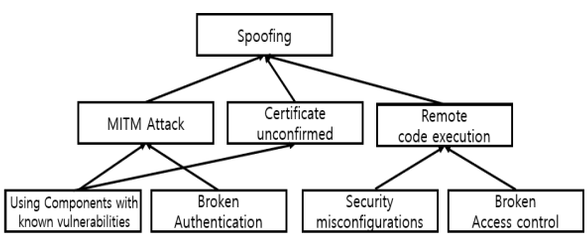

Fig. 3. Spoofing Attack Tree Analysis

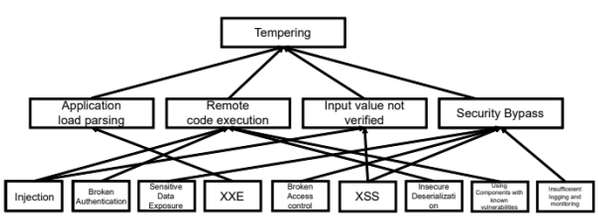

Fig. 4. Tempering Attack Tree Analysis

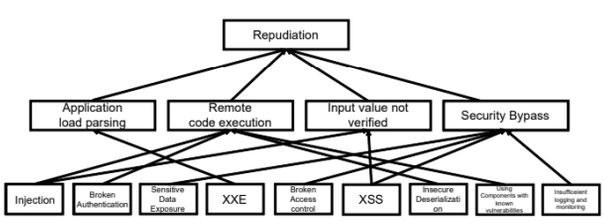

Fig. 5. Repudiation Attack Tree Analysis

Tempering 공격 시나리오에 따라 Fig. 4의 Attack Tree 분석을 수행하였다.

Repudiation 공격 시나리오에 따라 Fig. 5의 Attack Tree 분석을 수행하였다.

Information Disclosure 공격 시나리오에 따라 Fig. 6의 Attack Tree 분석을 수행하였다.

Denial of service 공격 시나리오에 따라 Fig. 7의 Attack Tree 분석을 수행하였다.

Elevation of Privilege 공격 시나리오에 따라 Fig. 8의 Attack Tree 분석을 수행하였다.

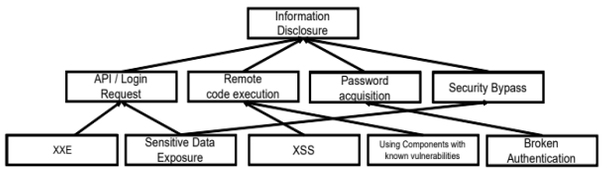

Fig. 6. Information Disclosure Attack Tree Analysis

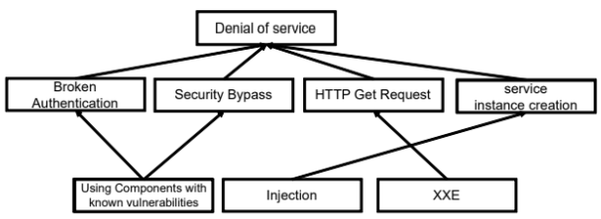

Fig. 7. Denial of service Attack Tree Analysis

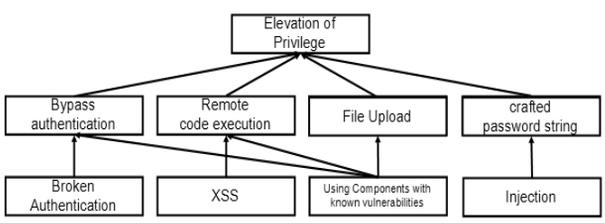

Fig. 8. Elevation of Privilege Attack Tree Analysis

Spoofing, Tempering, Repudiation, Information Disclosure, Denial of service, Elevation of Privilege의 공격 시나리오를 구성하고, 상향식 트리 형식으로 가시화하였다. Leaf Node는 클라우드 보안관제시스템의 정보자산과 정보자산의 데이터 흐름에 내재된 OWASP 취약점이며, Internal Node의 외부 위협이 발생하여, Root Node의 공격에 성공한 것을 알 수 있다. 따라서 이에 대응하는 보안 요구 사항이 필요하다.

4. 보안 요구 사항 도출

정보자산 식별, Data Flow Diagram 도출, STRIDE 위협 분석, Attack Tree 분석에 따라 Table 8과 같이 클라우드 보안관제시스템의 보안 요구 사항을 도출하였다. Category는 Attack Tree 분석의 Root Node에 맵핑되는 공격이며, Sub Category는 Leaf Node에 맵핑되는 OWASP 취약점 리스트이다. Primary Category는 Internal Node에 맵핑되는 외부 위협과 Sub Category의 취약점에 대응하기 위한 보안 요구 사항이다. 이러한, 위협모델링 분석에 의한 보안 요구 사항 도출은 Reference의 다양한 논문에서 활용하고 있고, 검증된 방법이다[4-17].

Table 8. Security Function Requirements of Cloud Managing Security Services System

Category	Sub Category	Primary Category
Spoofing	Using Components with known vulnerabilities	In order to defend against spoofing attacks, security functions corresponding to Sub Category and MITM Attack, Certificate unconfirmed, and Remote code execution are required.
	Broken Authentication	
	Security misconfigurations	
	Broken Access control	
Tempering	Injection	In order to defend against tempering attacks, security functions corresponding to sub categories and application load parsing, remote code execution, input value not verified, and security bypass are required.
	BrokenAuthentication	
	Sensitive Data Exposure	
	XXE	
	Broken Access control	
	Security misconfigurations	
	XSS	
	Insecure Deserialization	
	Using Components with known vulnerabilities	
	Insufficeient logging and monitoring	
Repudiation	Injection	In order to protect against repudiation attacks, security functions corresponding to Sub Category and Application load parsing, Remote code execution, Input value not verified, and Security Bypass are required.
	BrokenAuthentication	
	Sensitive Data Exposure	
	XXE	
	Broken Access control	
	Security misconfigurations	
	XSS	
	Insecure Deserialization	
	Using Components with known vulnerabilities	
	Insufficeient logging and monitoring	
Information Disclosure	XXE	To defend against Information Disclosure attacks, security functions corresponding to Sub Category and API / Login Request, Remote code execution, Password acquisition, and Security Bypass are required.
	Sensitive Data Exposure	
	XSS	
	Using Components with known vulnerabilities	
	Broken Authentication	
Denial of service	Using Components with known vulnerabilities	In order to defend against denial of service attacks, security functions corresponding to Sub Category and Broken Authentication, Security Bypass, Http Get Request, and Service instance creation are required.
	Injection	
	XXE	
Elevation of Privilege	Broken Authentication	To defend against the Elevation of Privilege attack, security functions corresponding to Sub Category and Bypass authentication, Remote code execution, File Upload, and Crafted password string are required.
	XSS	
	Using Components with known vulnerabilities	
	Injection	

5. 결 론

본 논문은 클라우드의 가상환경 구성과 클라우드 보안관제시스템의 데이터 흐름을 위협 모델링 분석에 반영하여, 보안 요구 사항을 도출하였다. 정보자산을 식별하고, 데이터 흐름도에 클라우드 가상환경의 세부 프로세스를 배치하여, STRIDE 위협 분석을 수행하였다. 따라서 클라우드 보안관제시스템의 기밀성, 무결성, 가용성, 인증, 부인방지, 권한 부여의 정보 보안 목표를 달성하는데 유용하다. 또한, 도출된 클라우드 보안관제시스템 보안 요구 사항을 통해 SIEM과 TMS를 개발하는 보안업체는 기본 탐지룰을 설정하고, 침해대응을 수행하는 CERT는 취약점 진단 및 추가 탐지룰을 설정한다. 보안 엔지니어는 해당되는 취약점을 제거하여 클라우드 보안 실무에 활용한다.

References

[1] National Institutes of Standards and Technology, “NIST Cloud Computing Standards Roadmap,” Jul. 2013.

[2] Cloud Security Alliance, “Defined Categories of Security as a Service,” 2016.

[3] Seung-Wan Son, Kwang-Seok Kim, Jung-Won Choi, and Gang-Soo Le, "Development of Managing Security Services System Protection Profile," *Journal of Digital Contents Society*, Vol.16 No.2, pp.345-353, 2015.

[4] Hye-Won KIM, Ho-Jun Yu, and Jae-Woo Lee, "Research on technical security threats of email cloud security service (E-mail SecaaS) Focusing on threat modeling techniques," *Korea Institute of Information Security And Cryptology*, pp.57-64(8). 2017.

[5] Jisoo Park and Seungjoo Kim, "Security Requirements Analysis on IP Camera via Threat Modeling and Common Criteria," *Korea Information Processing Society,* Vol.6, No.3 121-123. 2017.

[6] Korea Internet & Security Agency, "Casebook of Cloud Security Support Project," 2019.

[7] Jang Hwan, "Cloud SOC's forensic compliance reflects the shared responsibility model". *Proc. Conference on Information Security and Cryptography*, pp.41-44, 2020.

[8] Malik Nadeem Anwar, Mohammed Nazir, Adeeb, and Mansoor Ansari, "Modeling Security Threats for Smart Cities: A STRIDE-Based Approach," *Proc. Smart Cities—Opportunities and Challenges*, pp.387-396, 2020.

[9] In-Kyung Oh, Jae-Wan Seo, Min-Kyu Lee, Tae-Hoon Lee, Yu-Na Han, Ui-Seong Park, Han-Byeol Ji, Jong-Ho Lee, Kyu-Hyung Cho, and Kyounggon Kim, "Derivation of Security Requirements of Smart TV Based on STRIDE Threat Modeling," *Journal of The Korea Institute of Information Security & Cryptology*, Vol.30, No.2, pp.213-230, 2020.

[10] Eun-ju Park, Seung-joo Kim, "Derivation of Security Requirements of Smart Factory Based on STRIDE Threat Modeling," *Journal of The Korea Institute of Information Security & Cryptology*, Vol.27, No.6, pp.1467-1482, Dec. 2017.

[11] Soo-young Kang and Seung-joo Kim, "Analysis of Security Requirements for Secure Update of IVI(In-Vehicle -Infotainment) Using Threat Modeling and Common Criteria," *Journal of The Korea Institute of Information Security & Cryptology*, Vol.29, No.3, pp.613-628, Jun. 2019.

[12] Jae-Ki Kim, Jeong-Hoon Shin, and Seung-Joo Kim, "Study on the Femtocell Vulnerability Analysis Using Threat Modeling," *KIPS Transactions on Computer and Communication Systems*, Vol.5, No.8 pp.197-210, Aug. 2016.

[13] Ye-Seul Cha and Seung-joo Kim, "A Study on Security Requirements of Electric Vehicle Charging Infrastructure Using Threat Modeling," *Journal of The Korea Institute of Information Security & Cryptology*, Vol.27, No.6, pp.1441-1455, Dec. 2017.

[14] Hong Paul, Lee Sangmin, Park Minsu, and Kim Seungjoo, "Threat-Based Security Analysis for the Domestic Smart Home Appliance," *KIPS Transactions on Computer and Communication Systems*, Vol.6, No.3, pp.143-158, Mar. 2017.

[15] Tong Xin and Ban Xiaofang, "Online Banking Security Analysis based on STRIDE Threat Model," *International Journal of Security and Its Applications*, Vol.8, No.2, pp.271-282, 2014.

[16] Seung-young Ma, Jung-ho Ju, and Jong-sub Moon, "The security requirements suggestion based on cloud computing security threats for server virtualization system," *Journal of The Korea Institute of Information Security & Cryptology*, Vol.25, No.1, pp.95-105, Feb. 2015.

[17] James Sanfilippo, Tamirat Abegaz, Bryson Payne, and Abi Salimi, "STRIDE-Based Threat Modeling for MySQL Databases," *Proceedings of the Future Technologies Conference*, pp.368-378, 2019.

[18] Jeong-Seok Jo and Jin Kwak, "STRIDE and HARM Based Cloud Network Vulnerability Detection Scheme," *Journal of The Korea Institute of Information Security & Cryptology*, VOL.29, NO.3, pp.599-612, Jun. 2019.

[19] The Open Web Application Security Project, "OWASP Top Ten Web Application Security Risks | OWASP" [Internet], https://owasp.org/www-project-top-ten.

[20] Telecommunications Technology Association, "TTA Inf ormation and Communication Glossary" [Internet], https: //terms.tta.or.kr/main.do.

장 환

https://orcid.org/0000-0003-3441-5549

e-mail : jangh1220@knou.ac.kr

2020년 ~ 현 재 한국방송통신대학교 정보과학과 석사과정

관심분야 : Cloud SOC, A.I, Cryptography