정 보 보 호 학 회 지
제27권 제6호, 2017. 12

이메일 클라우드 보안 서비스(E-mail SecaaS)의 기술적 보안위협 연구 - 위협모델링 기법을 중심으로 -

김 혜 원*, 유 호 준**, 이 재 우***

요 약

현재 클라우드 컴퓨팅 시장은 빠른 속도로 광범위해지고 있으며 몇몇 기업에서는 클라우드를 이용한 보안서비스를 제공하기 시작했다.그 중 이메일 클라우드 보안 서비스는 클라우드 컴퓨팅의 특징을 가지고 안전한 조직의 이메일 사용을 지원하고 있다. 여러 조직의 이메일 데이터가 한 곳으로 집중되는 만큼 서비스 공급자는 보다 안전하고 가용성 높은 서비스를 제공해야만 한다. 이를 위해 본 논문에서는 이메일 클라우드 보안 서비스 기본구조를 기반으로 STRIDE 위협모델링 분석을 통해 잠재적인 기술적 보안약점 및 위협을 살펴보고 공격트리를 구성하여 대응방안을 모색해보고자 한다.

Ⅰ. 서 론

클라우드 컴퓨팅이란 인터넷 기술을 활용하여 다수의 사용자에게 가상의 IT자원과 서비스를 제공하는 컴퓨팅[1]으로 아마존의 Amazon Web Service, IBM사의 IBM 클라우드, Microsoft사의 Azure 등 이미 많은 기업에서 클라우드 서비스를 제공하고 있다.

클라우드 서비스는 제공 형태에 따라 컴퓨팅 인프라를 제공하는 Infrastructure as a Service(IaaS), 플랫폼을 제공하는 Platform as a Service(PaaS) ,소프트웨어를 제공하는 Software as a Service (SaaS)로 나뉘고 SaaS에서 더 나아가 클라우드에서 보안기술을 제공하는 Security as a Service (SecaaS)가 등장했다.

클라우드 컴퓨팅에서의 보안 이슈를 해결하기 위한 단체인 Cloud Security Alliance(CSA)는 클라우드 기반 보안 서비스 구현 시에 고려 사항과 문제점들을 Identity and Access Management(IAM), Data Loss Prevention (DLP), Web Security, Email Security, Intrusion Management(IM), Security Assessments, Security Information and Event Management(SIEM), Encryption, Business Continuity and Disaster Recovery (BCDR),Network Security의 총 10개 항목으로 구분하여 설명하고 있다. [2]

이 중 이메일 클라우드 보안 서비스(Email SecaaS)는 악성코드 첨부메일, 스팸메일, 피싱 메일 등과 같은 보안 위협으로부터 이메일을 안전하게 보호하고 관리하는 서비스이다. 그러나 이 역시 클라우드를 기반으로 한 소프트웨어의 일종이므로 네트워크 및 어플리케이션 수준에서 보안 위협이 존재한다.

따라서 본 고에서는 이메일 클라우드 보안 서비스의 기본구조 모델을 바탕으로 Microsoft사에서 제공하는 STRIDE 기반의 위협모델링을 실시하여 해당 서비스에서 발생 가능한 기술적 취약점과 그에 대한 대응방안을 연구하고자 한다.

Ⅱ. 이메일 클라우드 보안 서비스

2.1. 서비스의 특징

이메일 클라우드 보안 서비스는 클라우드를 통해 서비스를 제공하는 형태이고 이 때문에 기존의 구축형 이메일 보안 장비와는 다른 특징을 가진다. 먼저 사용자는 서비스 공급자가 제공하는 보안기술을 이용해 안전한 환경을 이용할 수 있어 이메일 보안관리를 위해 추가 인력이나 장비를 구성해야 하는 노력이 절감된다.

* 동국대학교 국제정보보호대학원 사이버모바일보안학과 (khwcjswp@naver.com)
** 동국대학교 국제정보보호대학원 사이버모바일보안학과 (hjopy89@gmail.com)
*** 동국대학교 국제정보보호대학원 교수(@)

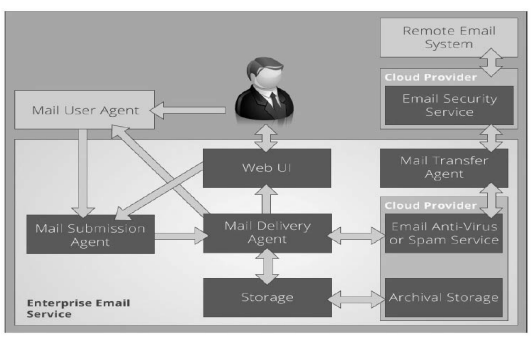
또한 지불한 요금만큼 사용하는 클라우드 서비스의 특성 상 메일서버의 용량과 네트워크 트래픽을 시간·계절 등에 따라 유동적으로 관리할 수 있어 경제적이기도 하다. 서비스를 업데이트하는 경우, 공급자의 한 번의 업데이트로 해당 서비스를 이용하는 모든 사용자가 개선된 기능을 사용할 수 있다. 그리고 서비스 공급자는 운영과정에서 다양한 조직의 이메일을 모니터링하면서 대량의 데이터를 얻을 수 있고 이메일 클라우드 보안에 대한 의미 있는 통계와 분석을 얻고 사용자로부터 피드백을 받아 다시 서비스에 반영할 수 있다.

그러나 위의 다양한 특징만큼 우려되는 측면 또한 존재한다. 조직 외부에 저장되어 있는 이메일 데이터를 어떻게 저장하고 보호할 것인지, 서비스 사용자와 공급자 사이의 전송구간 암호화와 접속 시 사용자의 인증은 어떤 방식을 취할 것인지, 웹 서비스 상의 사용자 편의성과 보안을 어떻게 구현할 것인지, 서비스 공급사의 서버에 아카이빙 되어 있는 저장 데이터를 어떻게 관리할 것인지, 접속로그와 변경사항 로그는 어떻게 저장할 것인지 등이 그것이다.

이처럼 이메일 클라우드 보안 서비스는 클라우드 컴퓨팅 기반의 웹 서비스이기 때문에 이메일에서 생길 수 있는 보안 위협뿐만 아니라 클라우드와 웹 서비스에서 발생할 수 있는 위협을 추가로 가지고 있다.

2.2. 서비스 구성

그림 1은 2012년 이 외 2인이 제시한 이메일 클라우드 보안 서비스의 기본구조로 기존의 이메일 서비스와 마찬가지로 이메일을 보내고 받고, 저장하는 기능이 있다. 사용자가 메일 사용자 에이전트(MUA)에서 이메일을 보내면 메일 호스팅 서비스에서 제공하는 메일 제출 에이전트(MSA)로 이동한다. 그 후 메일 전송 에이전트(MTA)가 메일을 전송한다. 이러한 구성요소는 이메일 클라우드 보안 서비스뿐만 아니라 모든 이메일 시스템에서 공통으로 사용되고 있다.[3]



〔그림 1〕 이메일 클라우드 보안 서비스 기본구조

Ⅲ. 분석

3.1. 위협모델링의 정의와 필요성

위협모델링은 소프트웨어 개발 생명주기(SDLC) 과정 중에 구현 전 단계에서 시스템 구성도, 네트워크 구성도, UI/UX 문서 등 소프트웨어 관련문서를 분석하고 이를 토대로 발생 가능한 잠재적인 취약점을 찾아 미리 대응할 수 있도록 하는 분석방법이다.

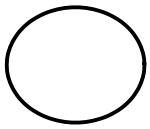
위협모델링을 통해 보안위협을 개발단계에서 대처함으로써 기술적 보안약점을 줄이고 개발 수정비용을 절감할 수 있다. 또한 서비스 운영과정에서 고려해야할 위협까지 미리 파악할 수 있는 장점이 있다.

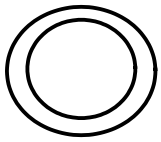
3.2. 위협모델링 분석방법

3.2.1. 데이터 흐름 다이어그램

표 1의 데이터 흐름 다이어그램(Data Flow Diagram, DFD)은 프로세스, 데이터 저장소, 데이터 흐름, 엔티티 등 구체적인 구성요소로 데이터 흐름을 나타낼 수 있기 때문에 대상의 기능과 전체적인 서비스 방식을 파악하기 용이하다. 그래서 데이터 흐름 다이어그램을 작성할 경우 보안위협을 파악하는데 도움을 줄 수 있다.

〔표 1〕 데이터 흐름 다이어그램 요소

구성요소	기호	설명
Entity		사용자 혹은 프로그램
Process		데이터를 처리하는 작업

구성요소	기호	설명
Multiple Process		다중 작업
Device		저장장치
Data Flow		요소 간 데이터 흐름
Trust Boundary		신뢰경계

3.2.2. STRIDE 분석

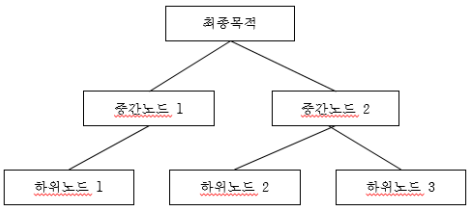
STRIDE분석은 시스템을 6가지 위험유형으로 분류하여 서비스의 취약성 및 잠재적 위협을 식별하기 위해 실시한다. 표 2에서와 같이 위장, 변조, 부인, 정보노출, 서비스 거부, 권한상승의 위험유형이 있으며 이 외에 존재하는 위협의 경우 추가적으로 고려해야 한다.

〔표 2〕 STRIDE 분석의 분류와 정의

분류	정의
위장 (Spoofing)	사람이나 시스템이 아닌 척 가장
변조 (Tempering)	악의적인 변경·수정을 목적으로 한 행위
부인 (Repudiation)	어떤 행위를 하지 않았다고 주장
정보노출 (Information Disclosure)	권한이 없는 사람 혹은 시스템에게 정보를 제공
서비스거부 (Denial of Service)	원활한 서비스 제공을 방해
권한상승 (Elevation of Privilege)	권한이 없는 사람이나 시스템에 권한을 부여하고 권한에 따른 행위가 가능

3.2.3. 공격트리 분석

공격트리는 네트워크 시스템을 대상으로 한 다양한 공격에 대해 보안 대책을 수립할 수 있도록 논리적이고



〔그림 2〕 공격트리의 기본 구조

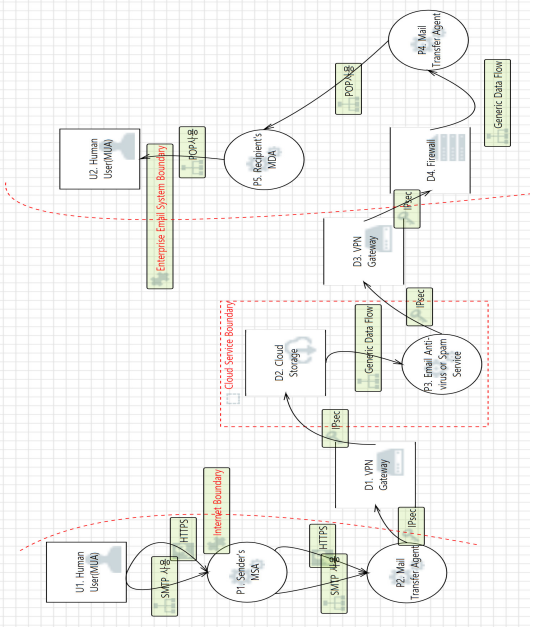
체계적인 이해를 돕는다.〔4〕 분석을 통해 공격자의 의도를 파악하고 대처하기가 용이하다는 장점이 있다. 또한 목적별 중복되는 공격기법을 찾아 하나의 대응책을 마련하는데 도움을 준다.

구조는 그림 2와 같이 최종 목적인 루트노드(Root Node)와 중간단계인 중간노드(Internal Node), 초기 공격인 최하위 노드(Leaf Node)가 있다.

3.3. 이메일 클라우드 보안 서비스 위협모델링 분석

3.3.1. 데이터 흐름 다이어그램

데이터 흐름 분석은 Microsoft사에서 제공하는 공개 소프트웨어인 Microsoft Threat Modeling Tool 2016을 사용하여 이메일 클라우드 보안 서비스의 기본 구조를



〔그림 3〕 이메일 클라우드 보안 서비스 DFD

바탕으로 작성하였다. 해당 DFD는 부록A에 별도 첨부하였다.

메일을 보내는 사용자가 이메일을 작성하면 Mail User Agent(U1)는 Simple Mail Transfer Protocol을 이용하여 이메일을 Mail Submission Agent(P1)로 이동시킵니다. 그 후 Mail Transfer Agent(P2)로 이동한 메시지는 네트워크(D1)를 통해 이메일 클라우드 서비스 공급사의 Cloud Storage(D2)에 저장됩니다.

메일을 받는 사용자가 서비스에 저장된 메일을 받아올 경우, Cloud Storage에서 받아온 이메일 데이터를 스팸분석 혹은 악성코드 포함여부 등을 분석하고(P3) 네트워크를 통해(D3) 사용자의 조직 네트워크로 전달됩니다. 그 후 Mail Transfer Agent(P4)와 Mail Delivery Agent(P5)를 거쳐 메일을 클라이언트의 컴퓨터에 저장하거나 웹 서비스 상에서 확인할 수 있게 된다.

〔표 3〕 이메일 클라우드 보안 서비스 DFD요소

Element	No	Name	Description
User	U1	클라이언트 사용자 ,MUA	고객 측 이메일 사용자
	U2	기업 사용자 ,MUA	기업 측 이메일 사용자
Process	P1	MSA	MUA로부터 이메일을 수신하고 MTA로 전달
	P2	MTA	이메일을 전달
	P3	Anti-virus & Spam Service	클라우드 상에서 이메일의 안티바이러스, 스팸필터 서비스 제공
	P4	MTA	이메일을 전달
Process	P5	MDA	MTA로부터 이메일을 받아 받는 사람의 MUA로 전달
Device	D1	VPN Gateway	VPN 통신을 할 수 있도록 하는 장치
	D2	Cloud Storage	클라우드 이메일 보안서비스를 위한 저장장치
	D3	VPN Gateway	VPN 통신을 할수 있도록 하는 장치
	D4	Firewall	방화벽

표 3은 위의 DFD의 요소를 정리한 것이다.

3.3.2. STRIDE 분석

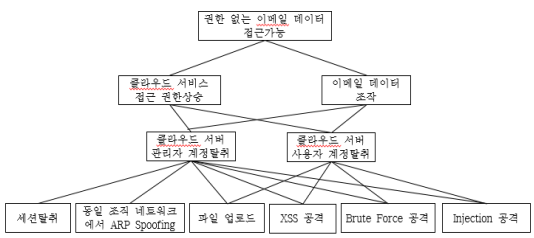
데이터 흐름 다이어그램을 이용하여 STRIDE의 6가지 보안위협을 식별해 보았다. 그 결과 표 4와 같이 총 24개의 보안 위협을 도출하였다.

Spoofing 위협이 7가지, Tempering 위협이 2가지, Repudiation 위협은 4가지, Information Disclosure 위협이 2가지, Denial of Service위협이 6가지, Elevation of Privilege 위협이 3가지가 확인되었다.

3.3.3. 공격트리 분석

STRIDE 분석을 통해 24개의 위협이 식별되었지만 이는 각 Element에서 단순한 보안위협을 열거한 것에 불과하다. 따라서 식별한 보안위협이 앞서 설정한 공격자의 공격목표를 달성하는데 어떻게 적용이 될 수 있는지 체계화 시켜야 한다. 따라서 공격트리를 이용하여 식별한 보안위협을 체계화하여 공격 목표 달성을 위한 여러 가지 방법을 식별해 보았다.

총 파악한 공격트리는 3가지이다. 권한이 없는 이메일 데이터에 접근하는 방법을 나타내는 그림 4의 공격트리를 살펴보면 총 3가지의 공격루트를 파악할 수 있다. 조직 외·내부자가 세션을 탈취하거나 Brute Force 공격, Injection공격, 조직의 동일 네트워크에서 ARP Spoofing, 파일업로드 공격, 크로스사이트 스크립트 공격을 통해 이메일 클라우드 보안 서비스의 관리자 계정을 탈취하여 본인의 권한보다 높은 권한으로 권한이 없는 이메일 데이터에 접근가능하다는 첫 번째 공격루트와 마찬가지로 Brute Force 공격, Injection공격, 파일업로드 공격, 크로스사이트 스크립트 공격으로 서비스의 다른 사용자 계정을 탈취하여 권한이 없는 데이터에 접



〔그림 4〕 공격트리 1

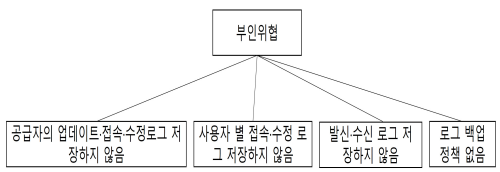
〔표 4〕 Email SecaaS DFD에 대한 STRIDE 분석결과

Element	No	Name	STRIDE	Description
User	U1	클라이언트 사용자 (MUA)	S	사용자가 아닌 사람이 사용자로 속이고 접근가능
	U2	기업 사용자 (MUA)	S	사용자가 아닌 사람이 사용자로 속이고 접근가능
Process	P1	MSA	E	사용자가 아닌 사람이 스푸핑으로 추가권한을 획득
	P2	MTA	E	사용자가 아닌 사람이 스푸핑으로 추가권한을 획득
			D	방대한 리소스를 처리하기 위한 제어 필요
	P3	Anti-virus & Spam Service	R	프로세스에 대한 기록이 필수적으로 필요
			D	방대한 리소스를 처리하기 위한 제어 필요
	P4	MTA	S	사용자가 아닌 사람이 사용자로 속이고 접근가능
	P5	MDA	E	사용자가 아닌 사람이 스푸핑으로 추가권한을 획득
Device	D1	VPN Gateway	S	사용자가 아닌 사람이 스푸핑으로 추가권한을 획득
			T	IPsec을 통해 흐르는 데이터는 침입자의 의해 변조가능
			R	프로세스에 대한 기록이 필수적으로 필요
			D	방대한 리소스를 처리하기 위한 제어 필요
	D2	Cloud Storage	S	사용자가 아닌 사람이 사용자로 속이고 접근가능
			I	부적절한 데이터 보호로 인해 공격자가 공개되지 않은 정보를 획득가능
			R	프로세스에 대한 기록이 필수적으로 필요
			D	방대한 리소스를 처리하기 위한 제어 필요
	D3	VPN Gateway	S	사용자가 아닌 사람이 스푸핑으로 추가권한을 획득
			T	IPsec을 통해 흐르는 데이터는 침입자의 의해 변조가능
			D	방대한 리소스를 처리하기 위한 제어 필요
	D4	Firewall	S	사용자가 아닌 사람이 스푸핑으로 추가권한을 획득
			I	부적절한 데이터 보호로 인해 공격자가 공개되지 않은 정보를 획득가능
			R	프로세스에 대한 기록이 필수적으로 필요
			D	방대한 리소스를 처리하기 위한 제어 필요

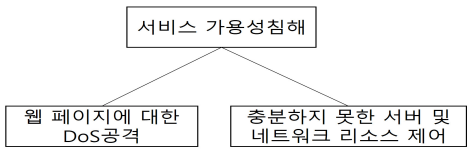
근가능하다는 두 번째 공격루트를 도출했다. 마지막으로 앞서 언급한 공격을 통해 이메일 데이터 변조가 가능하다는 세 번째 위협이 존재한다.

그림 5는 서비스 공급자, 사용자 혹은 외부자의 이메일 전송이나 수신, 접속기록, 수정기록 등에 대한 부인 가능성을 최종 목적으로 설정하고 공격루트를 살펴본 결과이다. 서비스 공급자가 서비스를 업데이트한 내용, 관리를 위해 접속·수정한 내용의 로그를 저장하지 않는 경우와 서비스 사용자 별 접속·수정로그를 저장하지 않는 경우, 사용자의 이메일 발신·수신 로그를 저장하지 않는 경우, 시스템 접근 및 이용에 대한 부인 위협이 생길 수 있다. 또한 로그를 완전하게 백업하지 못할 경우, 서비스의 무결성 유지와 부인방지에 위협이 될 것으로 판단하였다.

그림 6은 이메일 클라우드 보안 서비스의 가용성 침해에 대한 공격트리이다. 해당 서비스를 제공하는 웹 페이지에 대하여 DoS 공격이 이루어질 경우 서비스 접속



〔그림 5〕 공격트리 2



〔그림 6〕 공격트리 3

지연, 이메일 발신·수신 실패, 웹 서비스 접속 거부 등의 가용성 침해 형태의 공격이 이루어질 수 있다고 판단하였다. 그리고 DoS공격을 포함하여 다양한 이유로 클라우드 이메일 보안 서비스 공급자가 서버와 리소스 제어에 실패할 경우에도 같은 결과가 있을 수 있다.

3.3.4. 대응책

공격트리 분석에서 도출된 하위노드를 토대로 클라우드 이메일 보안 서비스의 보안위협에 대한 대응방안을 살펴보았다.

〔표 5〕 공격트리에 대한 대응방안

보안위협	대응책
세션 탈취	VPN 상에서 OpenSSL을 사용할 경우 Heart Bleed 취약점을 이용하여 세션 탈취가 가능하므로 1. 시스템 측면 대응책 → OpenSSL 버전 업데이트 heartbeat 사용 하지 않음 → 쿠키의 만료시간을 세션의 지속시간을 고려하여 최소한으로 설정 → 싱글세션 구현 2. 네트워크 측면 대응책 → 보안 장비에 공격 탐지 패턴과 차단 패턴 적용 3. 서비스 관리 측면 대응책 → 서버 측 SSL 비밀키가 유출 되었을 가능성을 배제할 수 없기 때문에 인증서를 재발급 받는 것을 주기적으로 검토
동일 조직 네트워크에서 ARP Spoofing	1. 패킷 감지 프로그램을 사용하여 ARP 신호를 보내는 패킷을 확인 2. ARP 테이블을 정적으로 관리 3. ARP 스푸핑 감지 소프트웨어 사용 4. 네트워크 장비에서 서로 다른 ip에 동일한 mac 주소가 매핑 되어 있는지 확인
Brute Force	외부에서 Brute Force를 실행 하게 되면 특정 포트에 대하여 진행하므로 1. Brute Force시 해당 포트를 변경 2. Tcp wrapper를 통해 방어 3. IP Table 규칙을 설정하여 방어 4. 로그인 페이지는 로그인 횟수 시도 제한정책을 적용 5. 취약한 비밀번호를 허용하지 않는 정책 적용
파일업로드	1. White list방식으로 안전한 확장자만 허용
크로스 사이트 스크립트	1. 외부 입력 값에 대해 문자변환 함수나 매서드를 사용하여 안전한 형태로 치환 2. HTML태그를 허용하는 경우 태그를 White list로 만들어 지원
Injection 공격	1. SQL Injection공격을 방지하기 위하여 외부 입력 값에 대한 특수문자 필터링 2. 에러 기반 Injection공격을 방지하기 위하여 미리 정의된 메시지만을 제공하며 민감한 정보를 노출하지 않도록 조치 3. 값을 반환하는 모든 함수의 결과 값을 검사하고 구체적인 예외처리 수행 4. 웹 방화벽과 같은 보안 솔루션을 사용
DoS 공격	1. 탐지 시스템을 구축 2. Flow 기반 탐지 시스템과 Inline/Mirroring 기반 탐지 시스템의 특징을 파악하여 기업에 맞는 시스템을 구축
충분하지 못한 서버 및 네트워크 리소스 제어	1. 서버, 네트워크의 보안 장비의 특정 옵션을 기업에 맞게 조정한 후, 트래픽, 액세스 등 리소스 제어를 실시
부인위협	1. 로그에 관한 기업의 정책이 존재하지 않는다면 정책수정 2. 부인방지 솔루션을 조직에 맞게 선정하여 운영

Ⅳ. 결 론

클라우드 서비스가 점점 발전해 하면서 여러 기업들은 SecaaS를 제공하는 단계에 이르렀다. 사용자들은 자신에게 적합한 클라우드 기반의 보안 서비스를 찾아 편리하게 사용하고 있지만 적절한 보안을 적용하지 않는다면 큰 위험을 초래할 수 있기 때문에 클라우드 보안 서비스의 위협모델링 연구를 진행하였다.

이메일 클라우드 보안 서비스의 데이터 흐름 분석, STRIDE 분석, 공격트리 분석의 순서로 연구하였다. 기본모델을 바탕으로 요소 간의 데이터 흐름을 분석하고 위장 7가지, 변조 2가지, 부인위협 4가지, 정보유출 2가지, 서비스 거부 6가지, 권한상승 3가지의 위협을 파악하였다. 그 다음 공격루트를 파악하고 공격루트의 하위

노드에 대한 대응책을 알아보았다. 네트워크 관련 취약점, 부인 가능성, 어플리케이션의 보안약점 등 보편적 보안위협이 확인되었고 이를 이용해 해당 서비스의 보안기능 요구사항 정의서 작성에 활용 가능할 것이라 생각된다.

하지만 본 논문은 기술적 취약점 설명에 국한되어있고, 이메일 클라우드 보안 서비스 기본모델로 가정하여 연구하였기 때문에 실제적 적용에 있어서는 한계점이 존재한다. 그렇기 때문에 클라우드 보안 서비스에 대한 위협모델링을 수행하고자 한다면 대상 서비스에 대한 이해를 바탕으로 맞춤형 위협모델링을 수행해야 하고 서비스를 하는 조직과 서비스 사용자의 관리적 취약점도 함께 고려해야 할 것이다.

참 고 문 헌

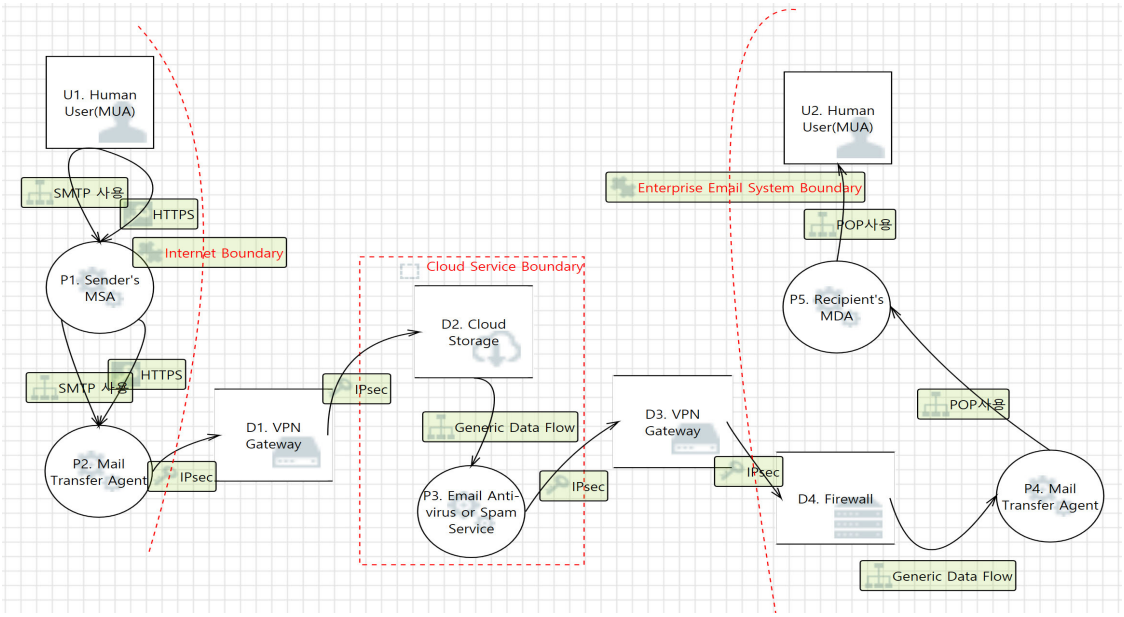
[1] 민옥기, 김학영, 남궁한, “클라우드 컴퓨팅 기술 동향”, *전자통신동향분석* 24(4), pp.1-13, 1997

[2] 정수환, “클라우드 기반 보안서비스 기술 동향”, *정자공학회지*, 40(10), pp.972-977.

[3] 이종훈, 정승욱, 정수환, “Security as a Service동향”, *정보보호학회지* 22(7), pp.54-61, 2012

[4] 엄정호, “능동적인 사이버 공격 트리 설계 : 애트리뷰트 접근”, *정보보호학회지* 21(3), pp.67-74, 2011

부록 A.



〔그림 3〕 이메일 클라우드 보안 서비스 DFD

〈저 자 소 개〉

김 혜 원 (Hye-Won KIM)
학생회원

2014년 8월 : 충남대학교 해양 환경과학과 졸업
2016년 3월~현재 : 동국대학교 국제정보보호대학원 사이버모바일 보안학과 석사과정
<관심분야> 정보보호, 정보보호 관리체계 인증, 클라우드 컴퓨팅

유 호 준 (Ho-Jun Yu)
학생회원

2015년 8월 : 동국대학교 컴퓨터 공학과 졸업
2016년 3월~현재 : 동국대학교 국제정보보호대학원 사이버모바일 보안학과 석사과정
<관심분야> 컴퓨터공학, 정보보호

이 재 우 (Jae-Woo Lee)
명예회원

동국대학교 국제정보보호대학원 석좌교수(현)
한국포렌식조사전문가협회 회장 (현)
ISC2 Fellow, Asia Board 의장 (현)
한국정보보호진흥원 초대 원장