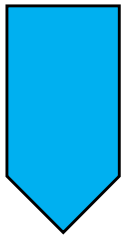
클라우드컴퓨팅

김태운



클라우드 보안 (기초)

클라우드 보안: 기본 용어와 개념

- 기밀성 (confidentiality)
  - 권한이 부여된 자만 접근을 허용하는 특징
  - 클라우드 환경에서 기밀성을 보장하기 위해, 전송 중인 데이터에 접근을 제한함
- 무결성 (integrity)
  - 권한이 없는 사용자가 정보를 함수로 수정할 수 없는 특징
  - 클라우드 환경에서, 클라우드 소비자가 보낸 데이터와 클라우드 서비스가 받은 데이터가 서로 일치하는 지(= 수정되지 않았는지)를 보증하는 것이 중요
- 신뢰성 (authenticity, 진정성)
  - 인증된 출처에서 제공 되었는지를 보장하는 특징
  - 둘 간에 정보를 교환할 경우, 이를 부정하거나 반박할 수 없는 부인 방지를 포함

클라우드 보안: 기본 용어와 개념

- 가용성 (availability)
  - 사용이 허가된 지정 시간 동안 접속 및 사용이 가능한 특징
  - 클라우드 환경에서 클라우드 서비스의 가용성을 보장하는 것에 대한 책임은 클라우드 제공자와 클라우드 전달자에 있음
    - 클라우드 전달자(Cloud Carrier) : 클라우드 제공자와 클라우드 소비자 사이에서 서비스의 연결과 전달을 제공하는 중간자 = 통신/네트워크 제공 업체 (예: SKT, LG U+, KT 등)

- 위협 (threat)
  - 프라이버시를 침해하거나 손상하려는 보안 침해, 정보 자산의 보안에 부정적 영향을 줄 수 있는 행위를 의미
  - 위협은 보안 취약성을 타겟으로 하며, 위협이 수행되면 공격이라 함

클라우드 보안: 기본 용어와 개념

- 취약성 (vulnerability)
  - 불충분한 보안 통제로 인해, 자원/데이터 보호나 기존 보안 통제를 능가하는 공격에 침해될 수 있는 '약점'을 의미
  - IT 자원의 취약성 예:
    - 보안 정책의 약점, 사용자 실수, 하드웨어나 펌웨어의 약점, SW 버그 등

- 위험 (risk)
  - 어떤 행위가 야기할 수 있는 손실이나 손상 가능성
  - 위험은 위협 수준 및 알려진 취약성의 수를 기준으로 측정됨
  - IT 자원에 대한 위협을 측정하는 데 사용하는 두 가지 지표:
    - (IT 자원의 취약성을 파고드는) 위협이 발생할 확률
    - (보안 공격이 성공했을 경우) 예상되는 IT 자원 손실 량

클라우드 보안: 기본 용어와 개념

- 보안 통제 (security control)
  - 보안 위협을 예방하거나 대응하고, 위험을 줄이거나 피하기 위해 사용하는 대책
- 보안 매커니즘 (security mechanism)
  - 위협에 대응하기위한 '대책'은 대개 IT 자원, 정보, 서비스를 보호하는 방어 프레임워크를 구성하는 컴포넌트인 보안 매커니즘으로 만들어짐
- 보안 정책 (security policy)
  - 일련의 보안 규칙과 규제를 정하고, 이를 어떻게 구현하고 강화할지를 결정함

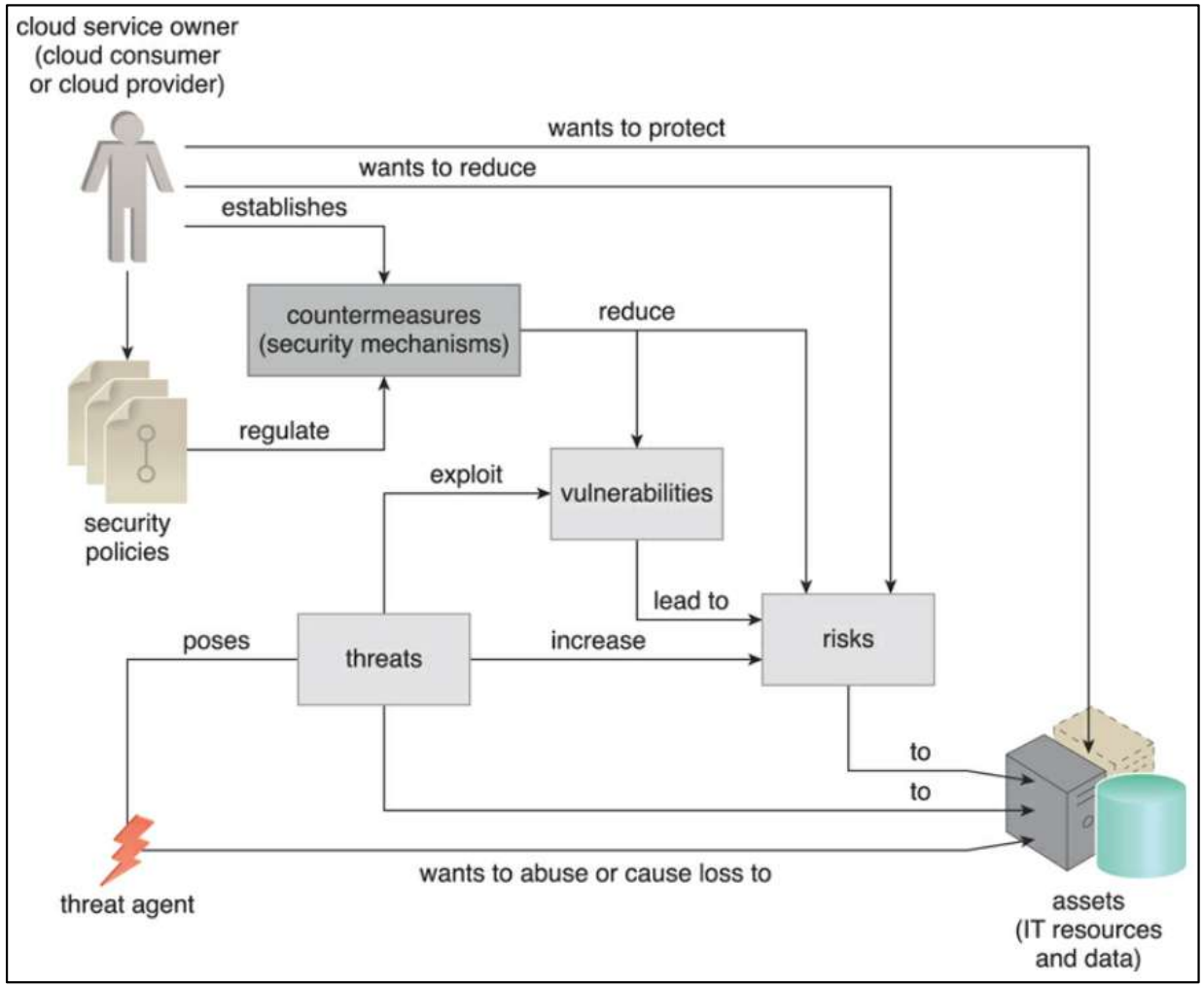
클라우드 보안: 기본 용어와 개념

- 요약(summary)
  - 기밀성, 무결성, 신뢰성(진정성), 가용성은 보안을 판단하기 위한 특징
  - 위협, 취약성, 위험은 보안의 부족이나 불안을 측정하고 평가하기 위한 특징
  - 보안 통제, 보안 매커니즘, 보안 정책은 보안 향상을 지원하는 대책, 그리고 안전 장치 구축과 관련된 특징

클라우드 보안: 위협 에이전트

참고) "Zero Trust"
- 네트워크 경계와 관계없이 그 누구도, 그리고 어떠한 활동이든 기본적으로 '신뢰하지 않는' 것에 바탕을 둔 보안 개념으로,
- 기존의 암묵적인 신뢰를 제거하고 모든 사용자와 기기를 검증하는 방식을 기반으로 함

- 위협 에이전트
  - 공격을 수행하는 능력이 있고, 위협을 가하는 개체
  - 클라우드 보안 위협은 내부적 또는 외부적으로, 사람이나 SW 프로그램에 의해 발생할 수 있음



- 위협 에이전트가 야기할 수 있는 위협과 취약성에 대한 다이어그램
- 위험에 대응하기 위해 보안 정책과 보안 매커니즘을 사용하는 방법에 대한 다이어그램

클라우드 보안: 위협 에이전트

- 위협 에이전트 : 관련 용어/개념
  - 익명 공격자
    - 클라우드의 허가를 받지 않은, 신뢰할 수 없는 클라우드 서비스 소비자
    - 일반적으로, 퍼블릭 네트워크를 이용해 네트워크 수준의 공격을 하는 외부 SW 프로그램의 형태로 존재함
  - 악성 서비스 에이전트
    - 클라우드 내에 오가는 네트워크 트래픽을 허가 받지 않은 에이전트가 가로챌 수 있음
    - 일반적으로, 손상을 가할 수 있거나 악의적인 로직을 보유한 서비스 에이전트 형태로 존재
    - 메시지 내용을 원격에서 가로채는 외부 프로그램 형태로 존재할 수도 있음

클라우드 보안: 위협 에이전트

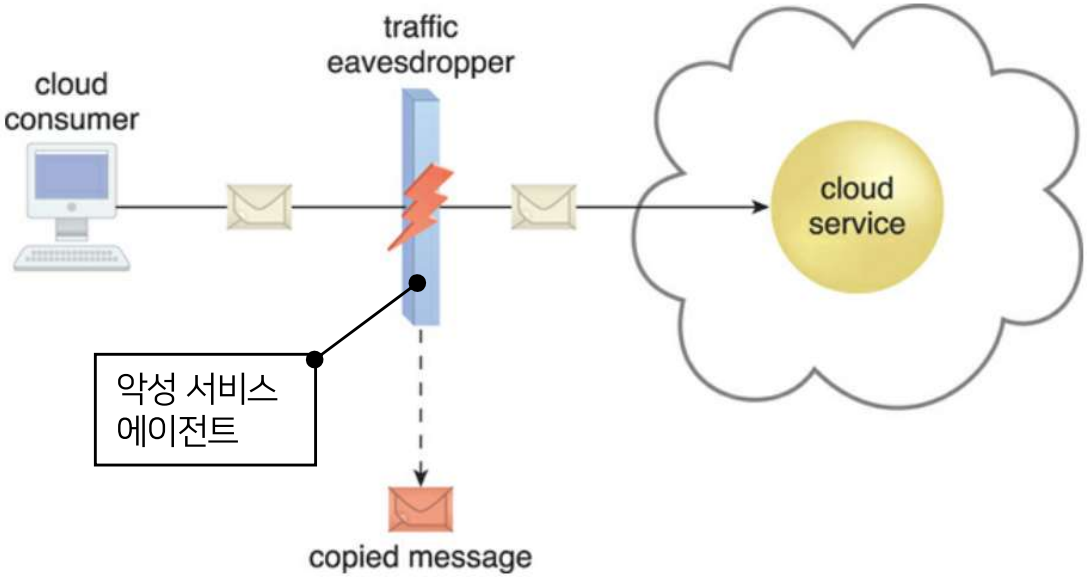
- 위협 에이전트 : 관련 용어/개념
  - 신뢰할 수 있는 공격자...??
    - 클라우드 소비자로서, 동일 클라우드 환경에 있는 IT 자원을 공유하고, IT 자원을 공유하는 클라우드 제공자와 클라우드 사용자를 목표로 부당한 IT 자원 사용을 시도함
    - 익명 공격자와 달리 신뢰할 수 있는 공격자는 대개 합법적인 자격을 오용하거나 민감한 정보를 도용해서 클라우드 신뢰 경계 내에서 공격을 수행
    - 참고) 제로 트러스트(Zero Trust) :
      - 신뢰 경계와 관계없이 그 누구도, 그리고 어떠한 활동이든 기본적으로 '신뢰하지 않는' 것에 바탕을 둔 보안 개념
      - 아무것도 신뢰할 수 없다는 가정하에, 사용자 및 다양한 정보를 바탕으로 최소한의 권한과 세밀한 통제를 지속적으로 수행하는 보안 활동을 강조하는 개념
  - 악성 내부자
    - 클라우드 제공자처럼 행동하거나 클라우드 제공자와 관계가 있는 사람
    - 일반적으로, 현재 혹은 과거의 직원이거나 클라우드 제공자의 구역에 접근할 수 있는 제3자인 경우가 많음
    - 클라우드 소비자의 IT 자원에 접근할 수 있는 관리자 권한을 가질 수 있음

클라우드 보안: 위협 에이전트

- 위협 에이전트 : 관련 용어/개념 (정리)
  - 익명 공격자 : 신뢰할 수 없는 위협 에이전트로, 대개 클라우드 경계 밖에서 공격 시도
  - 악성 서비스 에이전트 : 네트워크 통신을 가로채 데이터의 악의적 사용을 시도
  - 신뢰할 수 있는 공격자 : 합법적인 자격을 가진 인증된 클라우드 서비스 소비자로, 클라우드 기반 IT 자원에 부당하게 접근을 시도
  - 악성 내부자 : 클라우드 구역에 접근할 수 있는 권한을 오용하려는 사람.

클라우드 보안: 보안 위협 및 취약성

- 트래픽 도청 (traffic eavesdropping)
  - 클라우드로 또는 클라우드 내에서 전달되는 데이터가 악성 서비스 에이전트에 의해 (수동적으로) 가로채기 당하는 것 (= 엿듣기)
  - 공격의 목표는 클라우드 소비자와 클라우드 제공자 사이 관계의 기밀성과 데이터의 기밀성을 누설하려는 목적
  - 수동적인 공격의 특성상, 악성 에이전트를 탐지해 내기 어려움

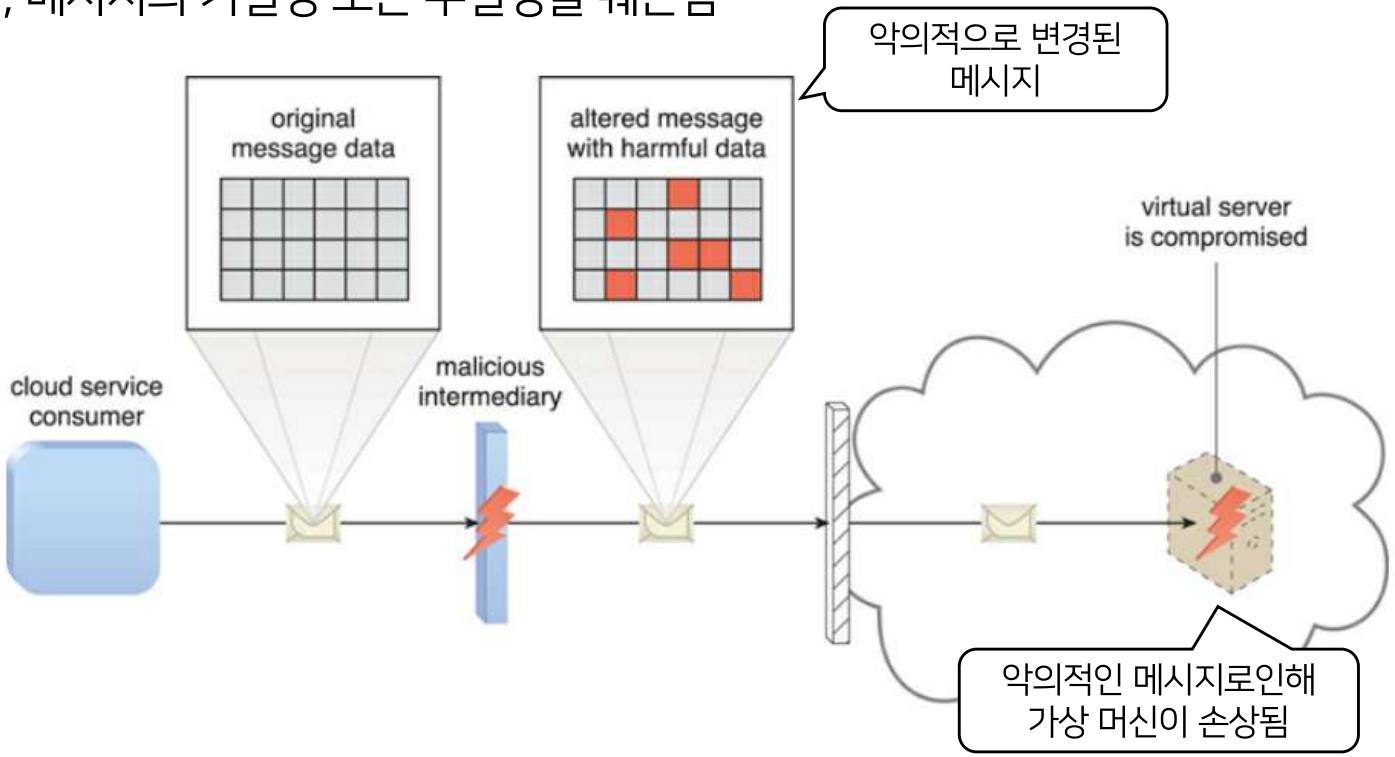


외부에 위치한 악성 서비스 에이전트는 클라우드 서비스 소비자가 클라우드 서비스에 보내는 메시지를 가로채서 트래픽 도청 공격을 수행한다. 이 과정에서, 비 인가된 메시지 복제본을 만든다.

클라우드 보안: 보안 위협 및 취약성

- 악성 중개자 (malicious intermediary)
  - 악성 서비스 에이전트는 클라우드 소비자와 서비스 간 전달되는 메시지를 가로채고 악의적인 목적으로 메시지 변경을 시도함
  - 이를 통해, 메시지의 기밀성 또는 무결성을 훼손함

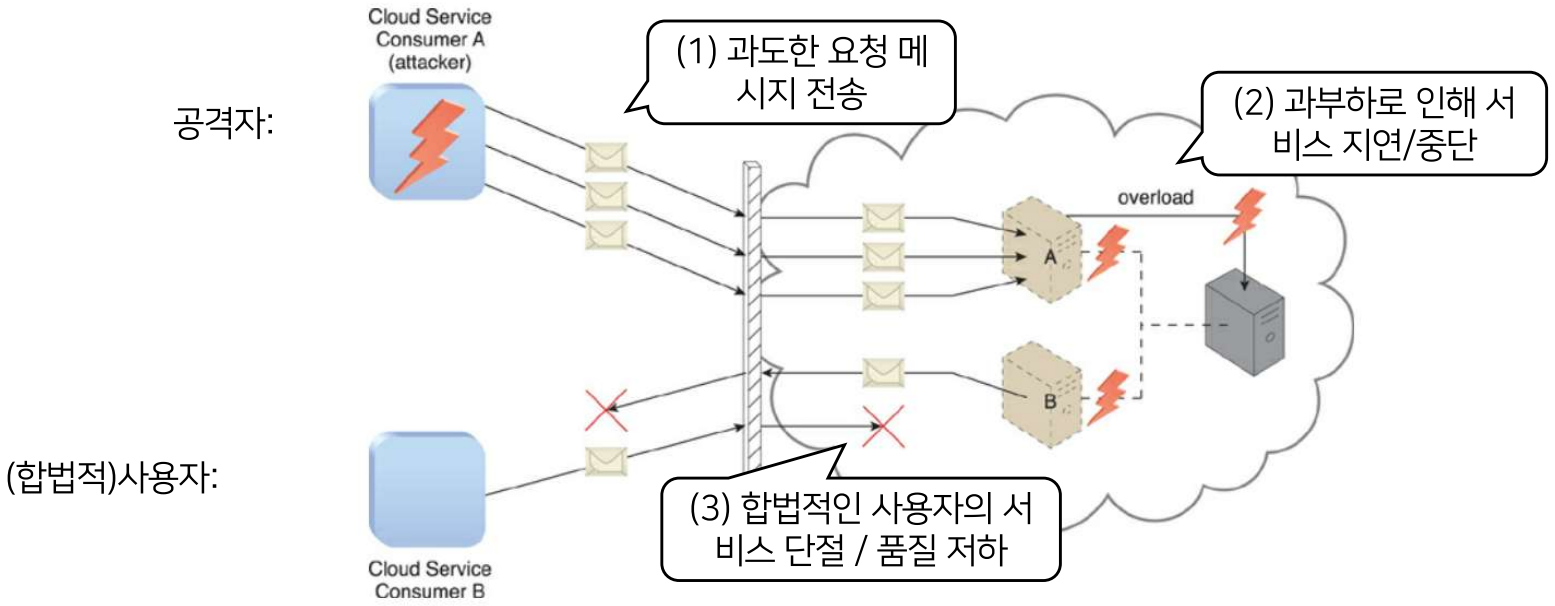
Example:



클라우드 보안: 보안 위협 및 취약성

참고.
DDoS 공격은 DoS 공격의 분산화 된 버전에 해당함

- 서비스 거부 공격 (DoS, Denial of Service)
  - 기능이 정상적으로 동작하지 못하도록(= 서비스 마비) IT 자원에 과부하를 일으키는 공격
  - 공격을 실행하는 일반적인 방법:
    - 복제된 메시지나 반복적인 통신 요청으로 클라우드 서비스의 작업 부하를 크게 높임
    - 과도한 메시지가 유입되어 네트워크에 과부하가 걸리고, 서비스 응답시간이 크게 늘어남
    - 과도한 CPU/MEM 자원을 사용하는 요청을 반복적으로 전송함



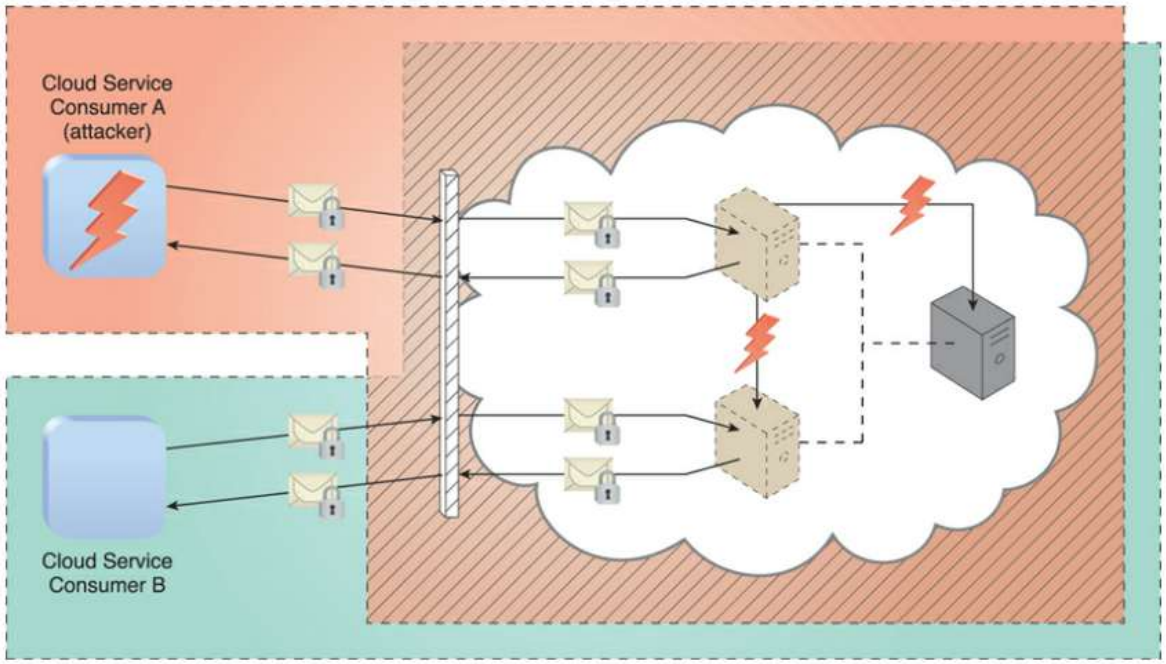
클라우드 보안: 보안 위협 및 취약성

- 불충분한 권한 부여 (또는, 잘못된 권한 부여)
  - 공격자에게 접근 권한이 잘못 주어지거나, 너무 넓은 범위의 주체/사람에게 접근 권한이 주어졌을 때 보안 위협이 증가
  - 공격자는 잘못 부여된 권한을 이용하여, 보호 되어야 할 자원에 접근함

- 가상화 공격
  - 가상화는 기반 하드웨어를 공유하지만 논리적으로는 각각 분리된 IT 자원을 사용할 수 있게함
  - 클라우드 제공자는 클라우드 소비자에게 가상화된 IT 자원에 대한 관리자 접근을 부여하고, 악의적인 사용자는 이를 이용해 물리 HW 자원을 공격할 수 있다

클라우드 보안: 보안 위협 및 취약성

- 신뢰 경계의 중첩
  - 클라우드 내의 물리적 IT 자원이 다른 클라우드 서비스 소비자에 의해 공유된다면, 이러한 환경을 사용하는 소비자들은 중첩된 신뢰 경계를 갖게 됨
  - 악성 클라우드 소비자는 다른 클라우드 소비자 또는 같은 신뢰 경계를 공유하는 다른 IT 자원을 손상시킬 의도로 공유된 IT 자원을 공격함
  - 그 결과, 동일한 신뢰 경계를 공유하는 다른 소비자들에게 피해를 줄 수 있음



- 클라우드 소비자 A와 B는 신뢰 경계를 공유함
- 악성 소비자 A에 의해 물리 HW 자원이 공격 당한 경우, 이로 인해 사용자 B도 영향을 받게 됨

끝