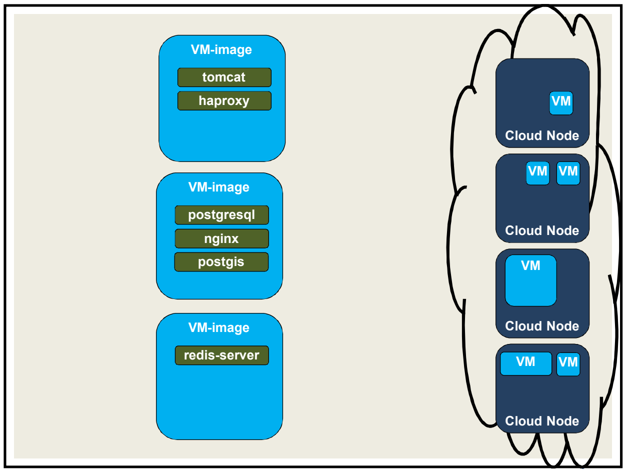
TCSS 562: SOFTWARE ENGINEERING FOR CLOUD COMPUTING

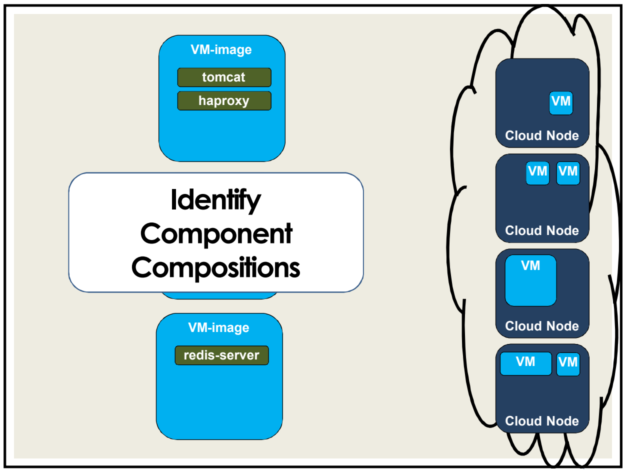
Cloud Security

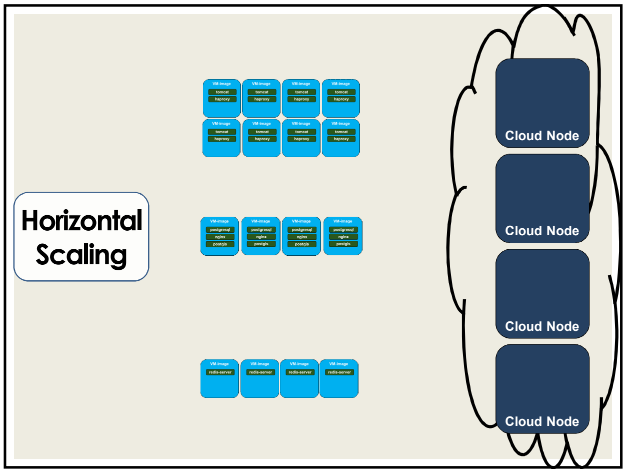
Wes J. Lloyd
Institute of Technology
University of Washington - Tacoma

FEEDBACK – 4/20

- Point(s) that are unclear:
  - Virtual machine servers: physical servers that host VMs
  - Docker
    - (Linux) operating system containers
  - Service load balancing architecture
    - Same as workload distribution architecture
    - Specialized to hosting web/cloud services
  - What does high availability mean? Does it mean the same data has been duplicated and stored in multiple places?
    - Yes and more, it also means there is redundant virtual infrastructure to step in, in case of failure
  - Horizontal scaling . . . (graphic)

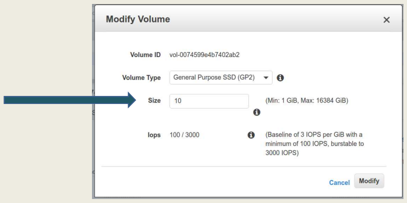






FEEDBACK - 2

- Example if elastic disk provisioning
- Amazon Elastic Block Storage
- Can resize existing volumes on demand:



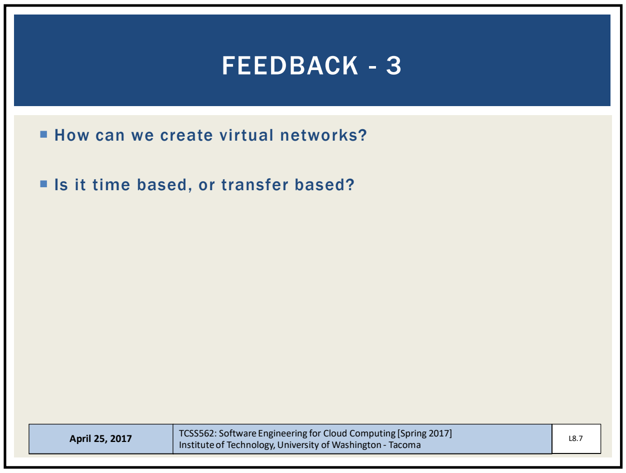
Modify Volume ×

Volume ID vol-0074599e4b7402ab2

Volume Type General Purpose SSD (GP2)

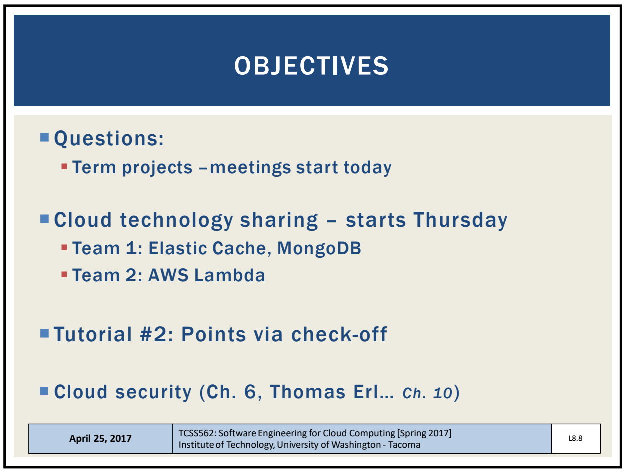
Size 10 (Min: 1 GiB, Max: 16384 GiB)

Iops 100 / 3000 (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)



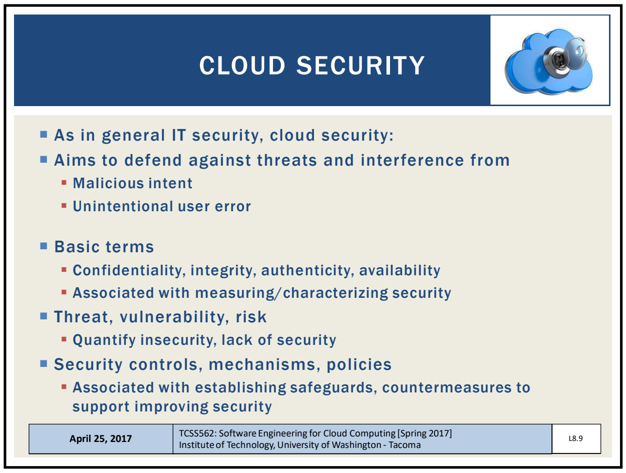
FEEDBACK - 3

- How can we create virtual networks?
- Is it time based, or transfer based?



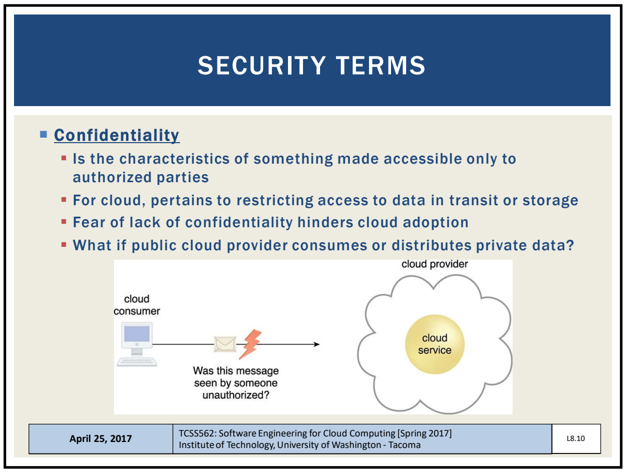
OBJECTIVES

- Questions:
  - Term projects –meetings start today
- Cloud technology sharing – starts Thursday
  - Team 1: Elastic Cache, MongoDB
  - Team 2: AWS Lambda
- Tutorial #2: Points via check-off
- Cloud security (Ch. 6, Thomas Erl… *Ch. 10*)



CLOUD SECURITY

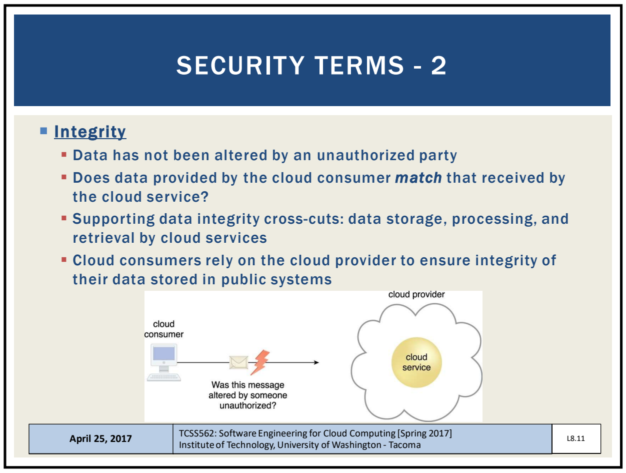
- As in general IT security, cloud security:
- Aims to defend against threats and interference from
  - Malicious intent
  - Unintentional user error
- Basic terms
  - Confidentiality, integrity, authenticity, availability
  - Associated with measuring/characterizing security
- Threat, vulnerability, risk
  - Quantify insecurity, lack of security
- Security controls, mechanisms, policies
  - Associated with establishing safeguards, countermeasures to support improving security



SECURITY TERMS

- **Confidentiality**
  - Is the characteristics of something made accessible only to authorized parties
  - For cloud, pertains to restricting access to data in transit or storage
  - Fear of lack of confidentiality hinders cloud adoption
  - What if public cloud provider consumes or distributes private data?

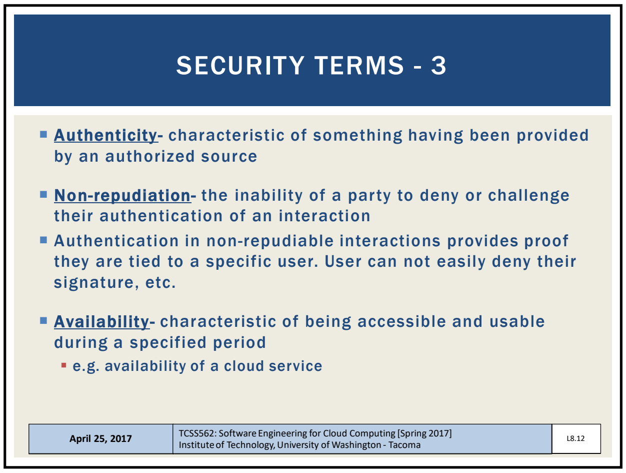
cloud provider
cloud consumer
Was this message seen by someone unauthorized?
cloud service



SECURITY TERMS - 2

- **Integrity**
  - Data has not been altered by an unauthorized party
  - Does data provided by the cloud consumer ***match*** that received by the cloud service?
  - Supporting data integrity cross-cuts: data storage, processing, and retrieval by cloud services
  - Cloud consumers rely on the cloud provider to ensure integrity of their data stored in public systems

cloud provider
cloud consumer
Was this message altered by someone unauthorized?
cloud service



SECURITY TERMS - 3

- **Authenticity**- characteristic of something having been provided by an authorized source
- **Non-repudiation**- the inability of a party to deny or challenge their authentication of an interaction
- Authentication in non-repudiable interactions provides proof they are tied to a specific user. User can not easily deny their signature, etc.
- **Availability**- characteristic of being accessible and usable during a specified period
  - e.g. availability of a cloud service

SECURITY TERMS - 4

- **Threat**- potential security violation that can challenge defense in an attempt to breach privacy and/or cause harm
- **Vulnerability**- weakness that can be exploited because it is protected by insufficient security controls, or because existing security controls are overcome by attack
- **Risk**- possibility of loss or harm from performing an activity
- Risk Measures
  - Probability of a threat occurring
  - Expectation of loss if resource is compromised

CLOUD SECURITY QUESTIONS

- Threat, vulnerability, or risk?
- Accidentally publishing ssh key and connection information to access an important cloud VM in a public repository
  - Risk: represents accidental disclosure of information which increases risk
- Opening port 22 (SSH) for world access? CIDR block of 0.0.0.0/0
  - Vulnerability: resource is more easily accessed
- Using passwords to access virtual machines as opposed to SSH keys
  - Vulnerability: passwords can be cracked more easily than ssh keys (but ssh keys can be misplaced… tradeoff?)

CLOUD SECURITY QUESTIONS - 2

- Threat, vulnerability, risk?
- A public cloud hosted webservice deployed using PaaS goes down due to external denial-of-service attack against the cloud provider
  - Threat
- Hacker harnesses free PaaS service to horizontally scale distributed password cracking code
  - Threat

SECURITY TERMS - 5

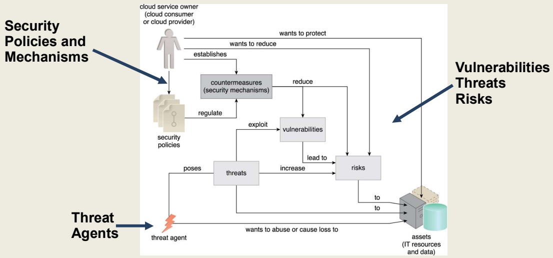
- **Security controls**- Countermeasures to prevent or respond to security threats to reduce and/or avoid risk
- **Security mechanisms**- components compromising defensive framework that protects IT resources, information, and services
- **Security policies**- establishes security rules and regulations

THREAT AGENTS

- Entity that poses a threat because it is capable of carrying out an attack.
  - Can originate internally or externally
  - From humans or software programs
- Trusted attackers, and malicious insiders have the highest damage potential

CLOUD SECURITY

- Security policies and mechanisms are used to counter threats, vulnerabilities, and risks caused by threat agents


Security Policies and Mechanisms
cloud service owner (cloud consumer or cloud provider)
wants to protect
wants to reduce
establishes
countermeasures (security mechanisms)
reduce
regulate
security policies
exploit
vulnerabilities
lead to
poses
threats
increase
risks
to
to
Vulnerabilities
Threats
Risks
Threat Agents
threat agent
wants to abuse or cause loss to
assets (IT resources and data)

THREAT AGENTS

- **Anonymous attacker**: non-trusted cloud service consumer without cloud permissions
  - Network level attacks on public networks
  - Attacks may be ineffective
  - May require substantial resources for attack (DoS)
- **Malicious service agent**: able to intercept and forward network traffic within a cloud
  - Service agent with compromised or malicious logic
  - Or an external program that remotely intercepts and corrupts message content bound for cloud services

THREAT AGENTS - 2

- **Trusted attacker**- shared IT resources in cloud with cloud consumers. Attempts to exploit credentials to target cloud providers and cloud tenants
- Attacks launched from within a cloud's trust boundaries
- May abuse legitimate credentials
- Also known as ***malicious tenants***
- May use cloud-based IT resources for:
- Hacking weak authentication processes, breaking encryption, generating spam email, launching common attacks, denial of service campaigns

THREAT AGENTS - 3

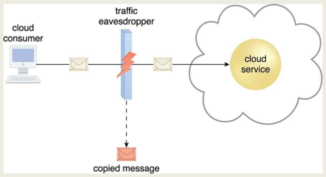
- **Malicious insider**- human threat agents acting on behalf or in relation to the cloud providers
- Current or former employees, or third parties with access to cloud provider premises
- Tremendous damage potential
- May have administrative privileges

THREAT AGENT QUESTIONS

- Compared to on-premise IT, what is different about potential threat agents?
  - ***What is different about . . .*** anonymous attacker threats?
    - Potentially more anonymous attackers, from more diverse user pool
  - **. . . malicious service agent threats?**
    - What vulnerabilities are needed for a malicious service agent to be deployed to on-premise IT?
    - To a public cloud?
    - Is there a large change in threat?
  - **. . . trusted attackers (malicious tenants)?**
    - Trusted attackers could be from external organizations
    - Potentially more malicious tenants from a more diverse user pool – *the cloud provider*
  - **. . . malicious insiders?**

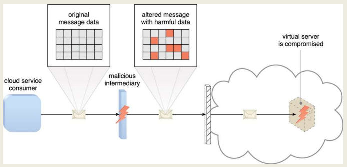
CLOUD SECURITY THREATS

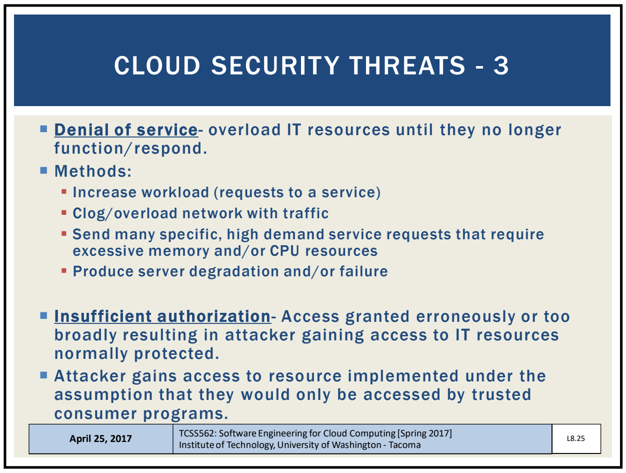
- **Traffic eavesdropping**- when data transferred to or within a cloud is passively intercepted by a malicious service agent for illegitimate information gathering purposes
- Directly compromises data confidentiality, and the confidentiality relationship between the cloud consumer and provider
- Due to passive nature, can go undetected for a long time



CLOUD SECURITY THREATS - 2

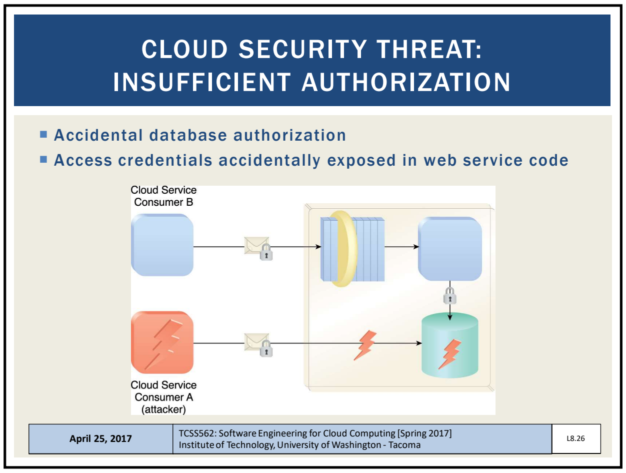
- **Malicious intermediary**- threat arises when messages from cloud consumer are intercepted enroute to cloud provider and altered by a malicious service agent
- Can compromise confidentiality and/or integrity
- May insert harmful data into message before it is forwarded to a destination (e.g. malware, virus)
- Can be carried out by a malicious cloud service consumer program





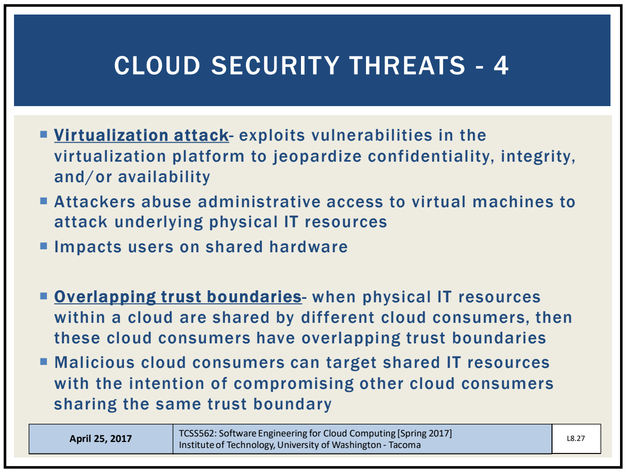
CLOUD SECURITY THREATS - 3

- **Denial of service**- overload IT resources until they no longer function/respond.
- Methods:
  - Increase workload (requests to a service)
  - Clog/overload network with traffic
  - Send many specific, high demand service requests that require excessive memory and/or CPU resources
  - Produce server degradation and/or failure
- **Insufficient authorization**- Access granted erroneously or too broadly resulting in attacker gaining access to IT resources normally protected.
- Attacker gains access to resource implemented under the assumption that they would only be accessed by trusted consumer programs.



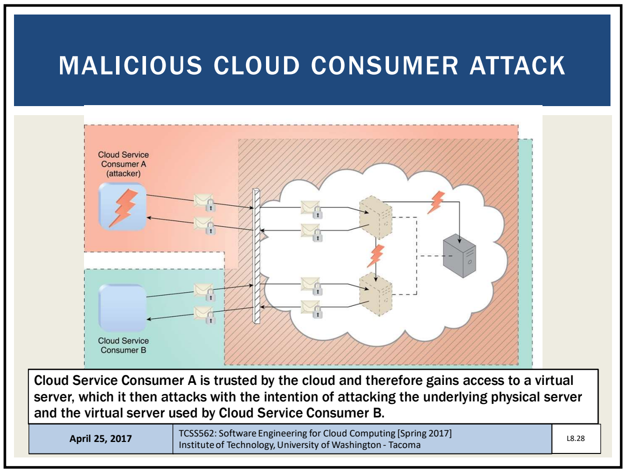
CLOUD SECURITY THREAT: INSUFFICIENT AUTHORIZATION

- Accidental database authorization
- Access credentials accidentally exposed in web service code



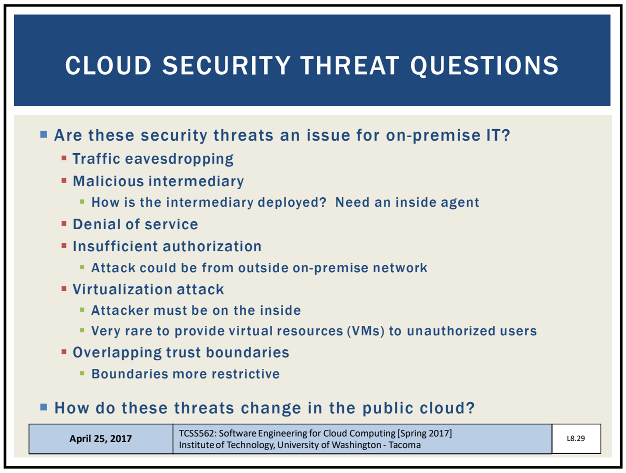
CLOUD SECURITY THREATS - 4

- **Virtualization attack**- exploits vulnerabilities in the virtualization platform to jeopardize confidentiality, integrity, and/or availability
- Attackers abuse administrative access to virtual machines to attack underlying physical IT resources
- Impacts users on shared hardware
- **Overlapping trust boundaries**- when physical IT resources within a cloud are shared by different cloud consumers, then these cloud consumers have overlapping trust boundaries
- Malicious cloud consumers can target shared IT resources with the intention of compromising other cloud consumers sharing the same trust boundary



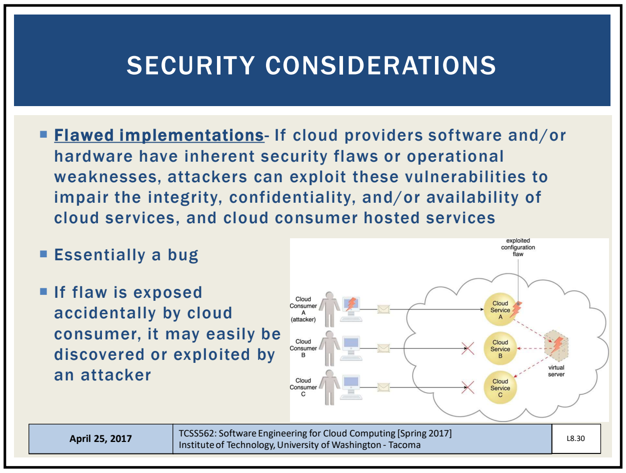
MALICIOUS CLOUD CONSUMER ATTACK

Cloud Service Consumer A is trusted by the cloud and therefore gains access to a virtual server, which it then attacks with the intention of attacking the underlying physical server and the virtual server used by Cloud Service Consumer B.



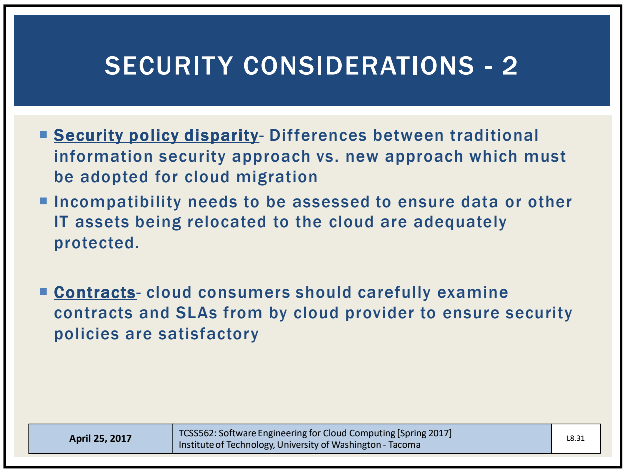
CLOUD SECURITY THREAT QUESTIONS

- Are these security threats an issue for on-premise IT?
  - Traffic eavesdropping
  - Malicious intermediary
    - How is the intermediary deployed? Need an inside agent
  - Denial of service
  - Insufficient authorization
    - Attack could be from outside on-premise network
  - Virtualization attack
    - Attacker must be on the inside
    - Very rare to provide virtual resources (VMs) to unauthorized users
  - Overlapping trust boundaries
    - Boundaries more restrictive
- How do these threats change in the public cloud?



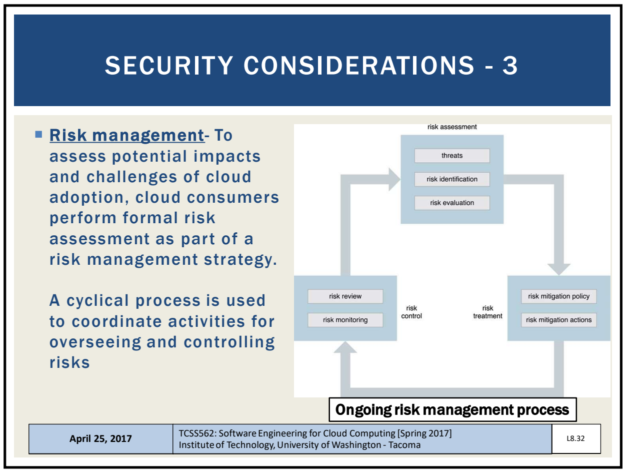
SECURITY CONSIDERATIONS

- **Flawed implementations**- If cloud providers software and/or hardware have inherent security flaws or operational weaknesses, attackers can exploit these vulnerabilities to impair the integrity, confidentiality, and/or availability of cloud services, and cloud consumer hosted services
- Essentially a bug
- If flaw is exposed accidentally by cloud consumer, it may easily be discovered or exploited by an attacker



SECURITY CONSIDERATIONS - 2

- **Security policy disparity**- Differences between traditional information security approach vs. new approach which must be adopted for cloud migration
- Incompatibility needs to be assessed to ensure data or other IT assets being relocated to the cloud are adequately protected.
- **Contracts**- cloud consumers should carefully examine contracts and SLAs from by cloud provider to ensure security policies are satisfactory

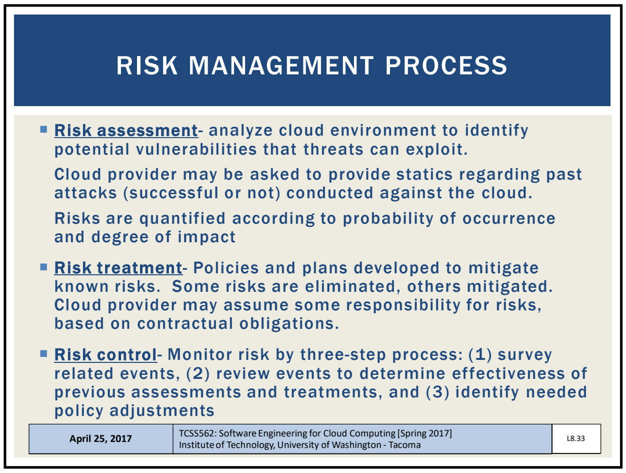


SECURITY CONSIDERATIONS - 3

- **Risk management**- To assess potential impacts and challenges of cloud adoption, cloud consumers perform formal risk assessment as part of a risk management strategy.

  A cyclical process is used to coordinate activities for overseeing and controlling risks

Ongoing risk management process

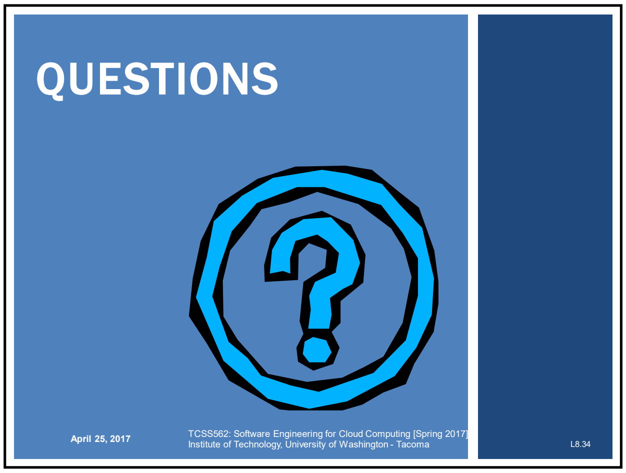


RISK MANAGEMENT PROCESS

- **Risk assessment**- analyze cloud environment to identify potential vulnerabilities that threats can exploit.

  Cloud provider may be asked to provide statics regarding past attacks (successful or not) conducted against the cloud.

  Risks are quantified according to probability of occurrence and degree of impact
- **Risk treatment**- Policies and plans developed to mitigate known risks. Some risks are eliminated, others mitigated. Cloud provider may assume some responsibility for risks, based on contractual obligations.
- **Risk control**- Monitor risk by three-step process: (1) survey related events, (2) review events to determine effectiveness of previous assessments and treatments, and (3) identify needed policy adjustments



QUESTIONS