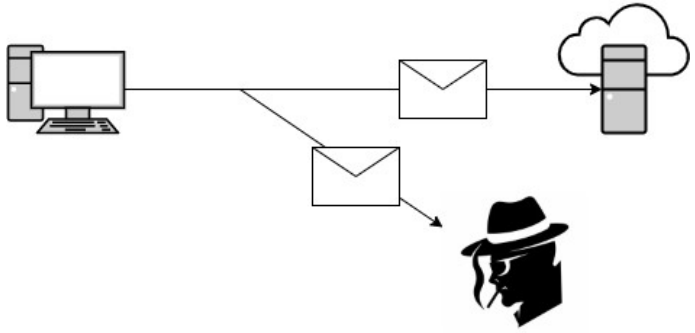
CS4650 Topic 20: Fundamental Cloud Security

Basic Security Terms and Concepts

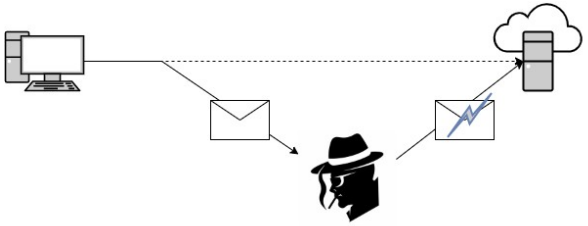
- Confidentiality
- Integrity
- Authenticity
- Availability
- Threat
- Vulnerability
- Risk
- Security Controls
- Security Mechanisms
- Security Policies

Confidentiality



- *Confidentiality* is the characteristic of something being accessible only to authorized parties.
- A major point of failure is in the network, where a third party could see the traffic, and possibly understand the message.
- If the message is incomprehensible, then the communication is confidential (unless you don't want third parties to even know that you communicated).
- Other weaknesses are in the cloud-based IT devices themselves.

Integrity



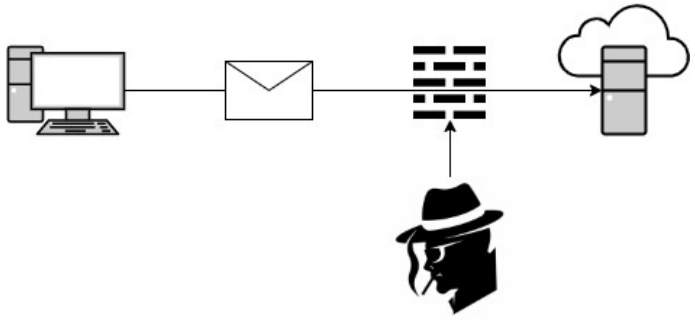
- *Integrity* is the characteristic of not being altered by an unauthorized party.
- In this example, a third party has intercepted and altered the message, so the cloud service receives altered data (either changing the values or mangling the values).
- Integrity can also extend to how the data is stored, processed, and retrieved.

Authenticity

- *Authenticity* is the characteristic of something having been provided by an authorized source.
- In this example, the third party has sent a message, but spoofed the service into thinking the message came from the authorized customer.
- Associated with authenticity is non-repudiation, which is the inability of a party to deny or challenge the authentication of an interaction.

Availability

- *Availability* is the characteristic of being accessible and usable during a specified time period.
- In this example, a third party can block the customer from accessing the service.
- In typical cloud environments, the responsibility for availability is shared between the cloud provider and cloud consumer.



Threat

- A *threat* is a potential security violation that can challenge defenses in an attempt to breach privacy and/or cause harm.
- Both manually and automatically instigated threats are designed to exploit known weaknesses.
- A threat that is carried out results in an *attack*.

Vulnerability

- A *vulnerability* is a weakness that can be exploited:
  - The protection might have insufficient security controls, or
  - Because existing security controls are overcome by an attack.
- IT resource vulnerabilities can have a range of causes:
  - Configuration deficiencies
  - Security policy weaknesses
  - User errors
  - Hardware or firmware flaws
  - Software bugs
  - Poor security architecture.

Risk

- *Risk* is the possibility of loss or harm arising from performing an activity.
- Risk is typically measured according to the threat level and the number of possible or know vulnerabilities.
- There are two useful metrics:
  - The probability of a threat occurring.
  - The expectation of loss due to the threat.

Security Controls

- Security controls are countermeasures used to prevent or respond to security threats.
- These reduce or avoid risk.
- Details on how to use security countermeasures are typically outlined in the security policy.
- This depends upon:
  - Correct and sufficient countermeasures.
  - Actually applying these countermeasures.

Security Mechanisms

- Countermeasures are typically described in terms of security mechanisms.
- These comprise the defensive framework that protects the IT resources.

Security Policies

- A security policy establishes a set of security rules and regulations.
- Often these policies also define how these rules and regulations are implemented and enforced.

Summary of Key Points

- Confidentiality, integrity, authenticity, and availability are characteristics that give a measure of security.
- Threats, vulnerabilities, and risks give a measure of insecurity, or lack of security.
- Security controls, mechanisms, and policies establish countermeasures and safeguards that improve security.

Threat Agents

- A *threat agent* is an entity that poses a threat because it is capable of exploiting a vulnerability which would be carrying out an attack.
- Cloud security threats can originate either internally or externally, from humans or from software programs.
- Technically, threats could also come from hardware failures or software bugs, with no particular agent or malicious intent.
- Let's consider some classes of threat agents.

Anonymous Attacker

- An *anonymous attacker* is a non-trusted cloud service consumer without permissions in the cloud.
- A typical example is an external software program that launches network-level attacks through public networks.
- From the attacker's point of view, ideally they have some inside knowledge of the security policies and defenses, and so can plan an effective attack.
- More likely they don't have this information, so alternative approaches are to bypass user accounts or stealing user credentials.

Malicious Service Agent

- A *malicious service agent* is able to intercept and forward the network traffic that flows within a cloud.
  - Actually, these agents can work in the Internet, performing their dastardly deeds before the traffic gets to the cloud.
- These agents typically exist as a compromised service agent, or a program pretending to be one of these agents.
- The goal might be to corrupt a message's contents:
  - Either to destroy the message, making it incomprehensible, or
  - Modifying the message so that the final online service thinks the message is legitimate, but is tricked into performing the wrong actions.

Trusted Attacker

- A *trusted attacker* shares IT resources in the same cloud environment as the cloud consumer.
- The attacker attempts to exploit legitimate credentials to attack cloud providers or cloud tenants.
- These attackers can launch their attacks from within the cloud's trust boundaries.

Malicious Insider

- *Malicious Insiders* are human threat agents acting on behalf of or in relation to the cloud provider.
- They are typically current or former employees, or third parties with access to the cloud provider's premises.
- This type of threat agent has tremendous damage potential, as they may have administrative privileges for accessing the IT resources.

Cloud Security Threats

- There are several common threats and vulnerabilities in cloud-based environments.
- We will look at a few of these.

Traffic Eavesdropping

- *Traffic Eavesdropping* occurs when data is being transferred to or from the cloud resource.
- The data is passively intercepted, so that the data reaches the original destinate with no trace that the data was also sent to a third party.
- The aim is to directly compromise the confidentiality of the data.
- What is also compromised is the relationship between the cloud consumer and cloud provider (the threat agent may not discover the *contents* of the message, but does discover that there was indeed a message).
- These attacks can go undetected for an extended period of time.

Malicious Intermediary

- The *malicious intermediary* threat arises when message are intercepted and altered by a malicious service agent.
- This is compromising the message's integrity.
- It may also insert harmful data into the message before forwarding.
- It is also possible that harmful programs such as viruses or other malware can be inserted (due to what is assumed to be a safe transmission protocol, checks for these types of insertions may be minimal or neglected).

Denial of Service

- The objective of a Denial of Service (DoS) attack is to overload IT resources to the point where they cannot function properly.
- These attacks are commonly launched in these ways:
  - The workload on the IT resource is artificially increased with imitation messages or repeated communication requests.
  - The network is overloaded with traffic to reduce its responsiveness and cripple its performance.
  - Multiple cloud service requests are sent, each of which is designed to consume excessive memory and processing resources.

Insufficient Authorization

- The *insufficient authorization* attack occurs when access is granted to an attacker erroneously or too broadly.
- The attacker then receives access to resources that are normally protected.
- Some on-line resources are designed to operate under the assumption that all requests are valid, coming from trusted consumer programs, so authentication and verification security may be weak or non-existent.
- The *weak authentication* attack is a variation where weak passwords or shared accounts are used to protect IT resources.

Virtualization Attack

- Virtualization provides multiple cloud consumers access to IT resources that share underlying hardware but which are logically isolated from each other.
- Because cloud providers grant cloud consumers some administrative access to virtualized resources, there is an inherent risk that cloud consumers could abuse this access to attack the underlying physical resources.

Overlapping Trust Boundaries

- When physical IT resources are shared by different cloud consumers, these consumers have overlapping trust boundaries.
- Because these IT resources are within the trust boundaries, consumers may place sensitive information on these resources.
- Also because these resources are within trust boundaries, other consumers may have more access to these resources.

Additional Considerations

- We have considered various threat actors that intentionally attempt to cause attacks.
- We have also considered the methods by which these attack frequently take place.
- We now consider some additional security threats that might not be sourced by a threat actor.

Flawed Implementations

- The hardware and the software used to build the cloud is not perfect.
- Flaws in these systems can cause the same damage as a direct attack by a threat agent.
- Since resources are shared, there is also a domino effect:
  - Cloud Consumer A may be using a service that encounters a software or hardware bug.
  - This may cause the physical server to crash.
  - This will then crash the virtual services run by other consumers on that same physical server.
- Note that this same behaviour can also be caused by an attacker that is aware of this flaw.

Security Policy Disparity

- A particular cloud consumer may have a very well thought out and comprehensive security policy, which covers all data and processes within that corporation.
- A cloud service may have a significantly different security policy, which may be a reasonable policy.
- However, the interaction of these two separate policies may have loopholes which can be exploited. The *interface* between separate security policies may not be as rigorous as either of the two policies.
- Actually, with a separate cloud provider and cloud service provider, there may be *three* security policies to be reconciled.

Contracts

- Cloud consumers need to carefully examine contracts and SLAs put forth by cloud providers.
- These contracts are much more complex when a cloud consumer deploys some of its own solutions upon the infrastructure of the cloud provider.
    - If there is a mismatch between the cloud service and the cloud infrastructure, how is the blame apportioned between the cloud consumer and cloud provider?
    - In this same situation, suppose the cloud consumer wants to impose a security policy on its owned cloud resource that is incompatible with the security policies of the cloud provider?

Wrap Up

- We have covered a lot of issues, but not dug too deeply.
- In the next lecture we will discuss some approaches to security implementations.