Network Security
Professor Gaurav S. Kasbekar
Department of Electrical Engineering
Indian Institute of Technology, Bombay
Week - 12
Lecture - 69
Cloud Security: Part 3

Hello, recall that in the previous two lectures, we discussed the basics of cloud computing. In this lecture, we will discuss the security aspects of cloud computing. So, in particular, we will discuss cloud security risks and the corresponding countermeasures that can be taken to defend against these risks. This slide lists the different cloud-specific security threats. There are these 12 security threats which are cloud-specific.

Many of these are also present in other contexts, but we will discuss all these threats in the context of cloud. In the next several slides, we will discuss all of these 12 security threats and the corresponding countermeasures in detail. So, we start with the first one, that is, Data Breaches. Data breaches, as the name suggests, it is an incident in which sensitive, protected, or confidential information is released, viewed, stored, or used by an individual who is not authorized to do so. So, some individual accesses data to which that individual actually does not have privileges.

Another example of a data breach is the deletion or alteration of records without a backup of the original content. So, this is another example of a data breach. Another example is that unlinking a record from a larger context may render it unrecoverable. And another example is storage on unreliable media. So, by the first one, I mean that there is a large file, for example, and there is a part of that file, and if this part of the file gets disconnected from the rest of the file, then that may make it unrecoverable.

And if some information is stored on unreliable media and there is some corruption of that medium, then the data may be lost. So, these are examples of data breaches. Then another example is some data is encrypted and stored, but then the encryption key used for encryption is lost. In that case, the data is not useful. It cannot be read, so it is as good as destroyed.

The threat of data compromise increases in the cloud compared to traditional systems. In traditional systems, the data is stored in proximity to the users themselves, so it is better protected. In contrast, in the case of the cloud, there is a greater possibility of data breaches. What are some countermeasures that can be taken to defend against all these possible security risks? One countermeasure is that the client can employ encryption to protect data in transit.

We have discussed encryption in detail in this course. The client can encrypt data before transmitting it. So, data in transit refers to data that has been transmitted by some party and is being transferred over some communication link. So, if it is encrypted, then it cannot be read by intruders. So, that helps in defending against data breaches.

Another countermeasure is that the client can enforce access control techniques. So, it can ensure that only a party that has access to a particular piece of data can read that data or write to that data, and so on. So, access control techniques can be enforced to defend against data breaches. In the case of data at rest, which means data that is just stored, the client can encrypt the database and only store the encrypted data in the cloud, with the cloud service provider having no access to the encryption key. So, even though the data is stored in the resources of the cloud, it is in an encrypted form. Hence, the cloud service provider cannot read the data.

The encryption key is not provided to the cloud service provider. So, even if the cloud service provider is dishonest in this case, they are not able to read the data that is stored by the consumer. So, these are some countermeasures that can be taken to defend against the first kind of security risk in clouds, that is, data breaches. Then, we discuss the next example of security risk, that is, weak identity, credential, and access management. So, identity and access management includes people, processes, and systems used to manage access to enterprise resources by ensuring that the identity of an entity is verified and then granting the correct level of access based on this verified identity.

In this course, we have discussed authentication in detail. Authentication techniques can be used to verify the identity of an entity. For example, password-based authentication or biometric-based authentication, mobile authentication, such as having to enter some one-time password. So, these are some techniques that can be used to verify the identity of an entity. And once the identity is verified, one should grant only the correct level of access based on the assured identity.

For example, a particular party, say Alice, may be only authorized to read data but not right to that resource. Bob may have read and write privileges for the same data, and so on. So, the correct level of access is provided based on the identified identity of the user. The cloud service provider must be able to authenticate users in a trustworthy manner. So, this can be done using the different techniques for authentication that we discussed in this course.

User profile and policy information must be used to control access within the cloud service. So, the user profile includes information about what privileges the user has for a particular data set. And the policy information can be used to control access within the cloud service. So, this concludes our brief discussion of weak identity, credential, and access management. So, that's a security risk, and authentication techniques are one countermeasure that can be taken to defend against this risk.

Then another security risk is insecure APIs, or Application Programming Interfaces. CSPs expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. The security of cloud services are dependent upon the security of these basic APIs. So, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy via authentication, access control, encryption, and activity monitoring. So, authentication is a measure that must be included within the APIs.

For example, the API may include login and password fields where the user has to type their login name and password. And also, access control is included in the APIs. So, whenever the user is identified, that user is provided access only to the resources to which that user has legitimate access. The APIs transfer only encrypted data, and the activity of users using that API is monitored. So, this concludes our discussion of this security risk that is insecure APIs.

Next, we discuss system vulnerabilities. These are vulnerabilities within the operating system or other system software. These are exploitable bugs or weaknesses in the operating system and other system software on platforms that constitute the cloud infrastructure. These vulnerabilities can be exploited by hackers and malicious software. In our discussion of different types of attacks on networks, we discussed, for example, buffer overflow kind of attacks and also denial-of-service attacks, which exploit vulnerabilities in operating systems. Hence, these vulnerabilities, bugs, or weaknesses can be exploited by hackers and malicious software. What are some countermeasures that can be taken to defend against these? Regular vulnerability detection is one countermeasure that can be taken. Some security experts can try and detect vulnerabilities that are present in the operating systems and other systems software.

Patch management is another key. So, if some vulnerability is detected, then a patch must be deployed to fix that vulnerability as soon as possible then IT staff training, so the staff can be trained to, so that they avoid vulnerabilities in operating systems and system software. We now discuss the next security risk that is account hijacking. So, this is usually done using stolen credentials. For example, Alice is authorized to access some cloud resources, but Bob steals the credentials of Alice.

In that case, Bob logs in as Alice and accesses the resources of the cloud. So, this account hijacking is typically done using stolen credentials, as in this example. With stolen credentials, the attackers can access critical areas of the deployed cloud computing services. This allows the attackers to compromise the confidentiality, integrity, and availability of those services. What are some countermeasures that can be taken to defend against account hijacking?

So, one countermeasure is we prohibit the sharing of account credentials between users and services. And also, we used strong two-factor authentication techniques where possible. So, examples of two-factor authentication techniques are the case where a user has to type a password as well as type in a one-time password from a mobile device. So, that's two-factor authentication, where the user has to provide a password as well as a one-time password from the mobile device. There can also be three-factor authentication techniques where, in addition to password and one-time password from the mobile, a user also has to provide biometric information.

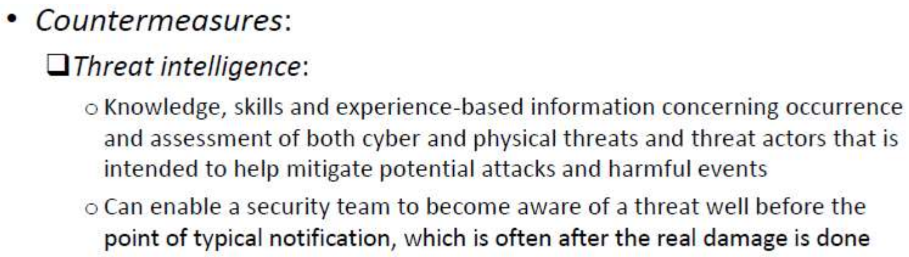
So, that is a three-factor authentication technique. So, such strong authentication techniques can be used to defend against account hijacking. Another countermeasure is, we employ proactive monitoring to detect unauthorized activity. Then another security risk in the context of cloud is malicious insiders. Malicious insider activity in the cloud service provider is a concern.

So, some of the employees of the cloud service provider themselves can be malicious, and they can introduce some unwanted effects. For example, by CSP system administrators and managed security service providers, there can be some malicious activity. Some countermeasures are a cloud service consumer conducts a comprehensive cloud service supplier assessment. That is, carefully checks the history and background of a cloud service provider before selecting that cloud service provider. The next security risk we discuss is Advanced Persistent Threats (APT).

So, this is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. So, a person gains access to the resources of a particular network but then does not immediately launch attacks on the network, but it stays there undetected for a long period of time. For example, six months or one year, and so on. So, the cloud service on which this intrusion is performed is not aware of this unauthorized access. So, the term persistent refers to such a stay for a long period of time.

That is, the access to the network is there for a long period of time. That is what is denoted by the term 'persistent.' The attacker may steal data from the network. Advanced persistent threats attack target organizations in sectors with high-value information, such as national defense, manufacturing, and financial industry. What are some countermeasures that can be taken to defend against APTs?

So, one important countermeasure is threat intelligence. Threat intelligence refers to knowledge, skills, and experience-based information concerning the occurrence and assessment of both cyber and physical threats and threat actors that is intended to help mitigate potential attacks and harmful events. So, this is some intelligence based on knowledge, skills, and experience which can help to mitigate cyber and physical threats. And these can help detect these threats well in advance. So, this time factor is the major advantage provided by threat intelligence.



- *Countermeasures*:
  - ❑ *Threat intelligence*:
    - ○ Knowledge, skills and experience-based information concerning occurrence and assessment of both cyber and physical threats and threat actors that is intended to help mitigate potential attacks and harmful events
    - ○ Can enable a security team to become aware of a threat well before the point of typical notification, which is often after the real damage is done

It can enable a security team to become aware of a threat well before the point of typical notification, which is often after the real damage is done. So, if an unauthorized person gains access to a network for a long period of time—for example, one year—and this threat is detected after a long time, for example, after one year has elapsed, in that case, the damage to the organization has already been done. Hence, this detection is too late. But with the help of threat intelligence, knowledge, skills, and experience can be applied, and these threats can be detected well in advance. So that before the damage is done, these intruders can be detected.

Then another example of a security risk is data loss. Permanent loss of cloud service consumer data that are stored in the cloud through accidental or malicious detection of data and deletion of data and backup copies from cloud storage. So, that's data loss. What are some countermeasures that can be taken? The cloud service consumer should be assured that the cloud service provider has a thorough redundancy scheme with regular backups, including geographic redundancy.

So, each piece of data is stored not only at one server but also at, but in fact at, multiple servers at different locations which are geographically separated from each other. So, even if one of the servers crashes, the data is still available on the other servers. And this geographic redundancy is important because, for example, if there is some power failure or other catastrophic event at one location, then the data is still available at other locations. Another countermeasure that can be taken is this backup can be supplemented by cloud-to-premise backup so that recent copy is available at the customer's side. So, the customer uses cloud computing, and it uses the resources of the cloud.

But the data from the cloud is periodically backed up to a location which is within the premises of the organization that is using the cloud services. So, a recent copy is available to the cloud service consumer on the customer side. Then another security risk is insufficient due diligence. This refers to the due diligence that should be performed by a cloud service consumer before choosing a particular CSP. If the cloud service consumer does not perform due diligence and does not choose the cloud provider carefully, in that case, it can suffer from various risks such as data loss and other attacks, which we discussed earlier.

Some countermeasures are, first of all, the enterprise needs to analyze the risks involved in moving to a cloud-based solution. Also, the choice of the cloud service provider and contractual terms with that CSP must be scrutinized carefully to minimize risk. So, that is, obviously, due diligence should be performed carefully while selecting the CSP and the contractual terms with the CSP. And also, in the first place, should a cloud-based solution be used, or should the data and processing be done locally? So, that needs to be analyzed.

Then another security risk is the abuse and nefarious use of cloud services. For many cloud service providers, it is relatively easy for a cloud service consumer to register and begin using cloud services. That's because some cloud service providers offer free limited trial periods. So, anyone can start using cloud services without having to pay any charges. This enables attackers to get inside the cloud to conduct various attacks.

For example, spamming. They can send out spam email. Malicious code attacks, they can infect the cloud resources with malicious code. And denial-of-service attacks can be launched by these attackers once they get inside the cloud. So, what are the countermeasures that can be taken to defend against this security risk? We can impose stricter initial registration and validation processes so that it becomes difficult for an attacker to start using the cloud services.

Another countermeasure is the cloud service providers must monitor activity with respect to their data and resources to detect any malicious behavior. The next security risk we will discuss is denial-of-service. By the nature of the service it provides, a public cloud service provider has to be exposed to the internet and other public networks. Only then will cloud service consumers be able to use the resources of the cloud service provider. The presence of the CSP has to be advertised, and its interface is very different.

These factors make it vulnerable to denial-of-service attacks. All these factors make cloud service providers a logical target for denial-of-service attacks. Such attacks can prevent a cloud service consumer from accessing their data or applications for some time. For example, we have discussed denial-of-service attacks in detail in this course. As an example, some malicious users may send a lot of data and clog the access link of the cloud service provider.

That is an example of a denial-of-service attack. Some countermeasures are the following. The cloud service provider must perform ongoing threat intelligence to be aware of the nature of potential threats and potential vulnerabilities in their cloud. We discussed threat intelligence earlier in the context of defending against APTs. Threat intelligence is also useful to defend against denial-of-service attacks.

Another countermeasure is to deploy automated tools to spot and defend core cloud services from such denial-of-service attacks. Then, another security risk is shared technology vulnerabilities. So, we recall that we discussed three service models: one is Platform as a Service, Software as a Service, and Infrastructure as a Service. So, in the case of Infrastructure as a Service, vendors can deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure, such as CPU caches and graphics processing units, were not designed to offer strong isolation properties for a multi-tenant architecture.

What are some countermeasures that can be taken to defend against these vulnerabilities? One countermeasure is that CSPs can use isolated virtual machines for individual clients. So, virtual machines—different virtual machines—use the same physical hardware, but isolation is provided between the virtual machines that are used by different users. So, a countermeasure against shared technology vulnerabilities is that CSPs can use isolated virtual machines for individual clients. Also, CSPs can promote strong authentication and access control for administrative access and operations.

So, we discussed authentication earlier in the context of other security risks. Authentication can be used to defend against this risk, as well as access control for administrative access and operations. That's another countermeasure. Another countermeasure is that CSPs can conduct vulnerability scanning and configuration audits. So, in summary, we discussed different security risks which are present in the context of cloud computing.

And we discussed different countermeasures that can be taken to defend against these different risks. We'll continue our discussion on cloud security in the next lecture. Thank you.