Richard Nelson

Ragib Hasan

CS 643

September 20, 2020

Assignment 1

(Please type your answers and submit the pdf file via canvas file upload)

1. What are the things that differentiate cloud security from traditional security? Explain each of the items briefly (4 points).

In traditional security the main issue is usually keeping bad guys out. Also, in traditional security there is not much plausible reason for the owner to ever attack, steal data, or tamper with his/her own system. In cloud security there can be several users who can all share the same physical infrastructure. This would mean that you can potentially have an attacker be in the same physical machine they are trying to target. Having access to a machine makes it easier to plan attacks. Clouds also have more areas for attacks to be conducted. At any given point, it's possible for the client, the service, or the cloud itself to be attacked. Any single one of these three pieces being compromised could pose risk for the other two. In traditional security you would only have to worry about not letting yourself or your system get compromised. In cloud computing you have to worry about that same thing and additionally, you have to worry about the cloud service and cloud itself being compromised.

2. In the threat model for a cloud-based system, can the cloud service provider be considered as malicious? What are the arguments for and against considering the cloud service provider malicious? (2+2 = 4)

Yes, a cloud service provider can be listed as malicious in the threat model for a cloud based- system. With any threat model it is paramount to list all potential threats. While ideally, this should never be a problem, it's best to be prepared for any scenario. The entire staff that provides the cloud service doesn't have to be malicious, but even if one member had bad intentions, he/she could do some damage. It can be hard to be assured confidentially, integrity, and availability depending on your level of access to a cloud facility. Some potential reasons that a cloud service provider might have malicious intentions include: financial gain and/or intellectual gain. For instance, a cloud service provider can charge a company X amount of dollars to use their service per year, but if the company uses more services then they must pay more. The cloud server could send traffic to the company to make it seem like they are using more of the services then they actually are, which would allow the cloud service provider to receive more money from the company. The service provider can also be motivated by intellectual gain. If an employee with access to the server wanted to know something about the company that is buying the service, he/she could peek through that companies data. If that company doesn't have good cloud security measures emplace like TMPs then they

won’t even know their confidentiality and integrity were breached. On the other hand, there is reason to justify that a cloud service provider shouldn’t be listed in a threat model. A simple reason is that if you have reasonable suspicion about a cloud service provider you probably shouldn’t use them in the first place. Another reason is that even if you make a threat model you can’t foresee the malicious methods the cloud service provider will use. And any tools you use to try to assure confidentially and integrity will also be known by the service provider so they can find ways around it. Also, if you keep a threat model in the cloud and include the cloud service provider in the threat model, then they might have even more incentive to perform malicious actions against you.

3. What are the security advantages of using a cloud over a local data center? (2)

Cloud servers are usually spread out in different areas. This could make it harder for someone to physically disrupt the cloud servers. Additionally, cloud servers usually have methods in place just in case something goes wrong. Having an assured cloud fall back method in tandem with having a backup somewhere else could prove to be safer than just having your own local data center with a backup probably somewhere in that same local data center. Cloud service providers have to continuously update their services so there is a good chance you won’t have to worry about old vulnerabilities taking out your infrastructure. Cloud service providers usually have a large budget which enables them to have more cybersecurity specialists. This could mean you have more people trying to prevent your stuff from being breached than if it was just a staff of a local company. Also, cloud servers haven’t been around as long as traditional local servers. Just in terms of recency there would be less documented vulnerabilities to cloud servers than traditional local data centers because cloud servers haven’t been a thing for as long.

If you are an MS **student, please answer the following additional question. (BS and** PhD **students do not need to answer this question)**

4-MS: Write a threat model for a cloud-based database service (here the database is hosted in the cloud, and the users manage it through a web interface and can query it via the web interface). (the threat model should include the following: a) List of Assets b) List of Entry points c) Attacker model, with attacker capabilities and motivation, and d) Vulnerabilities and mitigation strategies. (5 points)

Assets
1. Company Files
2. Employee Credentials
3. Information on other companies

Entry Points
1. Local / user end
a. Cloud login
b. Web interface
c. Local servers
2. Cloud service
a. Cloud login/logout
b. Web interface for management
c. Web interface for querying information
d. Cloud servers
3. Cloud
a. Cloud server
b. Person on inside already

Attacker Model for Threat Actor Outside the Cloud	
Attacker capabilities	Attacker motivations
SQL inject	• Gain credentials • Gain some type of information
Buffer Overflow	• Render services unusable thwarting company production • Write malicious code into memory
Privilege Elevation	• Access documents that would be access controlled • Run malware under admin for better exploits • Run ransomware • Reconfigure system settings
SSL certificate spoofing	• Gain credentials
phishing	• Gain credentials • Gain access to server • Drop malware onto server that infects cloud service or local server
Resource exhaustion	• Force company to buy more resources • Render services unusable thwarting company production
Denial of Service (DOS)	• Render services unusable thwarting company production
Privacy, integrity, and/or confidentiality attack	• Attain sensitive data • Planning to use sensitive data for financial or social exploit
Physical destruction of local or cloud servers	• Render services unusable thwarting company production

Attacker Model for Threat Actor Inside the Cloud	
Attacker Capabilities	• Attacker Motivations
Access Company Data with Admin privileges	• Gain sensitive information • Financial gain by exploiting information discovered • Reconfiguring companies' system to force them to use more of a service (more money)
Increase in services provided	• Financial gain
Physical disruption of server	• Render services unusable thwarting company production

Vulnerabilities and Mitigation Strategies for Threat Actor Outside the Cloud	
Vulnerabilities	Mitigation strategies
SQL inject	
Buffer Overflow	• Use cloud servers written in languages that don't really have as many memory vulnerabilities.
Privilege Elevated	• This would largely be accomplished via other exploits. In the case it happens you can set it up to where an alert is raised whenever someone privileges our elevated
SSL certificate spoofing	Disable puny code display in support browser
phishing	• open attachments from email in notepad or don't open them at all (if they look suspicious) • enable antivirus software (will warn about files or redirects being malicious)
Resource exhaustion	
Denial of Service (DOS)	• Should be intrinsically made safe or at least less likely by using cloud service • Form a load balance plan that includes adjusting firewalls and blocking blacklisted IPs
Physical destruction of local or cloud servers	• Increase physical security measures at local servers • Make sure the cloud service we purchase has sufficient physical security implemented

Vulnerabilities and Mitigation Strategies for Threat Actor Inside the Cloud	
Vulnerabilities	Mitigation strategies

Access Company Data with Admin privileges	• Use TMPs • Audit with third party
Increase in services provided	• Ask for copy of services used • Keep a log of services used
Physical disruption of server	• Should be recompensated if this happens