Asset Matrix Case Study

CS 573 A - Introduction to Cyber Security

Spring 2022

By

Omkar Sinha

CWID: 10468301

Dept. Computer Science

Stevens Institute of Technology

Under Guidance of

Prof. Dr. Edward G. Amoroso

Description:

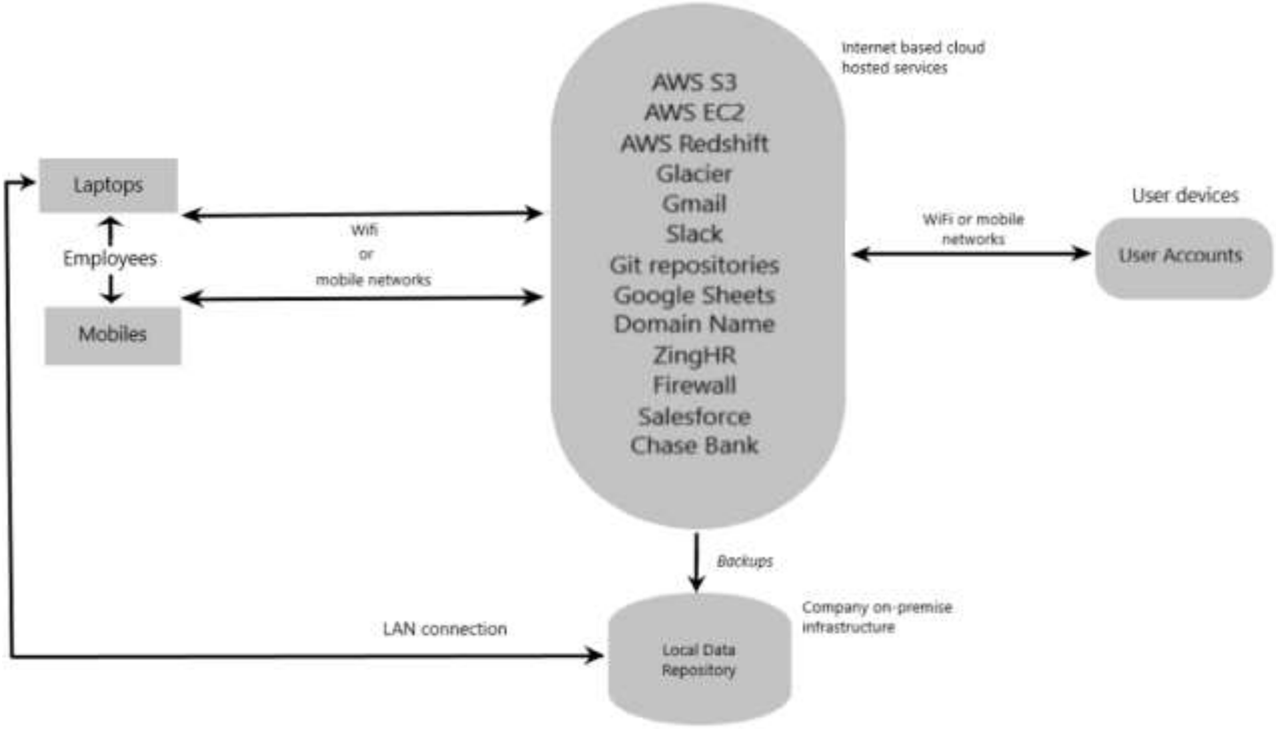
We assume the network of a company, known as "JustPost", that runs a social media application similar to Twitter, Instagram or Facebook for the general public to post. This fictious application is hosted and deployed on Amazon Web services (AWS).

The assets for this company are listed and described as follows:-

1) **AWS S3** : The data of the application which includes all the posts made by the users (text, media, video, etc) are stored on the S3 buckets.
2) **AWS EC2** : The application is deployed using Elastic Compute Cloud (EC2) instances as the servers. Elasticity load balancing service of AWS, automatically scales the number of instances as the need arises.
3) **AWS Redshift** : Redshift is used for analytics and warehousing of large petabyte-sized data that is generated dynamically on the system.
4) **Glacier** : application data(user posts) stored on S3 will routinely be transferred to glacier after a stipulated time period since their generation.
5) **Gmail** : The company's email domain for its employees, management, partners and clients. Employees will have their own google account within the company's domain.
6) **Slack** : employees, like developers, can collaborate in team using slack channels on their workplace or remotely.
7) **Git repositories** : developers working in the company will use git tools to coordinate their work before the software goes into production. It is stored locally as in most companies.
8) **Google Sheets** : google sheets are a very handy tool for preparing and collaborating on spreadsheet-related work. It comes with the G suite account for each user.
9) **Domain Name**: the web domain name to access the application from browser (*justpost.com*).
10) **ZingHR** : ZingHR is an HR management software. It is used for processing payrolls, keeping employee records (like leaves, designation , etc) and processing employee application for leaves, resignation, compensation, etc.
11) **Firewalls** : firewall is user as a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
12) **Salesforce** : is a merchant software to manage client relationship data.
13) **Chase Bank** : bank service for payroll and other financial transactional purposes and to store money securely.
14) **Employee laptops** : As most IT companies, 'JustPost' will provide its employees with a company laptop (Mac in this case). Inevitable, important code, data and email communication will be present on it.
15) **Employee mobile devices** : Employees will configure their emails on their personal/work mobile devices as well as probably the slack channel for faster communication.
16) **Local Data storage** : a repository for the data stored on cloud will also be stored on local on-premise data storage as a backup. Local data backups are taken from cloud for both data security and experimentation purposes.
17) **User accounts** : the users who post on 'JustPost' will create accounts to access the application from their devices, just like in other social media applications. These accounts will authenticate them before they can access it.

Diagrammatic Representation:

The diagrammatic representation of the above describes architecture is as follows:



The threats faced by the assets of this system fall mainly in 4 categories: (i) Confidentiality, (ii) Integrity, (iii) Availability and (iv) fraud/theft.

Threat-Asset matrix:

The threat-Asset matric for the above describe system is as follow:

Assets/Threats	Confidentiality	Integrity	Availability	Theft/Fraud
AWS S3	P = 2 C = 3 | R = 6	P = 2 C = 3 | R = 6	P = 1 C = 2 | R = 2	P = 2 C = 3 | R = 6
AWS EC2	P = 2 C = 3 | R = 6	P = 2 C = 2 | R = 4	P = 2 C = 1 | R = 2	P = 1 C = 1 | R = 1
AWS Redshift	P = 2 C = 3 | R = 6	P = 2 C = 2 | R = 4	P = 2 C = 2 | R = 4	P = 2 C = 3 | R = 6
Glacier	P = 1 C = 3 | R = 3	P = 2 C = 2 | R = 4	P = 1 C = 1 | R = 1	P = 2 C = 3 | R = 6
Gmail	P = 2 C = 3 | R = 6	P = 1 C = 2 | R = 2	P = 1 C = 1 | R = 1	P = 2 C = 2 | R = 4
Slack	P = 2 C = 2 | R = 4	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1	P = 2 C = 1 | R = 2
Git repositories	P = 2 C = 3 | R = 6	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1	P = 2 C = 3 | R = 6
Google Sheets	P = 2 C = 2 | R = 4	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1	P = 2 C = 1 | R = 2
Domain Name	P = 1 C = 3 | R = 3	P = 1 C = 3 | R = 3	P = 1 C = 3 | R = 3	P = 1 C = 3 | R = 3
ZingHR	P = 1 C = 2 | R = 2	P = 1 C = 2 | R = 2	P = 1 C = 1 | R = 1	P = 1 C = 2 | R = 2
Firewall	P = 2 C = 3 | R = 6	P = 2 C = 3 | R = 6	P = 1 C = 3 | R = 3	P = 1 C = 1 | R = 1
Salesforce	P = 2 C = 2 | R = 4	P = 2 C = 2 | R = 4	P = 1 C = 2 | R = 2	P = 1 C = 1 | R = 1

Chase Bank	P = 2 C = 3 | R = 6	P = 2 C = 2 | R = 4	P = 1 C = 1 | R = 1	P = 2 C = 2 | R = 4
Employee laptops	P = 2 C = 3 | R = 6	P = 1 C = 1 | R = 1	P = 1 C = 2 | R = 2	P = 2 C = 3 | R = 6
Employee mobiles	P = 2 C = 2 | R = 4	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1	P = 1 C = 2 | R = 2
Local Data storage	P = 3 C = 3 | R = 9	P = 2 C = 2 | R = 4	P = 1 C = 1 | R = 1	P = 3 C = 3 | R = 9
User accounts	P = 2 C = 3 | R = 6	P = 2 C = 3 | R = 6	P = 1 C = 1 | R = 1	P = 2 C = 3 | R = 6

1) AWS S3 :-

(i) **Confidentiality**: Since AWS is a major cloud provider, probability of attempts to attack are very significant. While S3 has encryption options, given its storage of vast amounts of user data (including private posts and other sensitive user information), consequences of a chance hack can be severe.

(ii) **Integrity:** S3 has a somewhat strong backup and recovery system. This reduces probability of attacks succeeding. However, the consequences of corruption of data will be serious; given that undermining user data integrity will amount to breach of trust on the part of the company.

(iii) **Availability:** Since S3 is only flat files DDoS attacks are not very likely; though consequences of the denial of service will be somewhat inconvenient despite not being critical.

(iv) **Theft/fraud:** Stealing user data will be useful for malicious actors, for purposes of data mining and even in cases of doxing on a large scale. This will have very serious consequences for the company’s reputation.

2) AWS EC2 :-

(i) **Confidentiality:** EC2 deploys the application software using the executable(.exe) file. Being a public cloud it is often attacked by malicious actors but reverse-engineering the code is extremely hard, hence there is not a very high confidentiality threat.

(ii) **Integrity:** An integrity compromising attack seeks to alter the application software in production. While motivations for such an attack exist, the EC2 is generally secure and in the worst case is backed up by replication and can be scaled to exclude the hacked instances.

(iii) **Availability:** Possibility of a DDoS attack originating from hacked user accounts, employee accounts or corrupted software is present but is not likely to work due to elastic load balancing feature of AWS, which will expand the capacity of the compute.

(iv) **Theft/Fraud:** Stealing of compute will not have any impact due to the elasticity of EC2 and in any case will be a liability of the cloud vendor rather than the company.

3) AWS Redshift :-

(i) **Confidentiality:** While Redshift has encryption options like S3, the consequences of a chance hack can be really serious due to the user data that is warehoused.

(ii) **Integrity:** Corruption of the data warehouse hosted on the redshift will constitute an integrity attack. Redshift is backed up and hence relatively secure.

(iii) **Availability:** Since redshift is dynamic its availability can be compromised by attacks, though it has safety mechanisms.

(iv) **Theft/fraud:** similar to S3, possibility on stolen data being sold to unauthorized parties is a serious threat.

4) Glacier :-

(i) **Confidentiality:** AWS glacier is less regularly used than S3, but does contain sensitive data, that if leaked, will constitute a breach of trust on part of company.

(ii) **Integrity:** Like in S3, data here on encrypted but a chance hit will be less consequential since the data is less frequently accessed giving the system more time to remedy the breach.

(iii) **Availability:** a DDoS attack is less effective since glacier data is of an archival nature.

(iv) **Theft/fraud:** probability of a theft remains significant due to the high rate of possible attacks and the presence of sensitive user data. Especially as data in present times is referred to as new oil.

5) Gmail :-

(i) **Confidentiality:** the email data consist of highly important information with a high value for competitors and fraudsters. It's security depends on general email account authentication aided by the company's firewall.

(ii) **Integrity:** system is reasonably secured against illicit access due to authentication protocols and firewall. Any attack on the integrity of the data can be mostly remedied easily without long lasting effects.

(iii) **Availability:** denial-of-service attacks on the company's Gmail domain space is possible (if hacker finds way to get past authentication and firewalls). While this will cause inconveniences to employees/management, it's not critical.

(iv) **Theft/fraud:** generally, there is not much of company's purchase-able service and data on Gmail to motivate attackers looking to steal. However certain valuable and confidential business plans maybe of interest to hackers.

6) Slack :-

(i) **Confidentiality:** slack security depends mostly on the platform and its own security protocols. This leads to delegation of control for the company and an outlet for attackers to eavesdrop.

(ii) **Integrity:** much of the communication over slack is trivial and corrupting it's integrity will serve little purpose for the malicious actors.

(iii) **Availability:** since slack channels are used internally by the company's workforce to communicate; other forms of communication can be employed while it's remedied.

(iv) **Theft/fraud:** while occasionally confidential information is shared over slack channels, like Gmail, there is little directly purchase-able value to it and the implications are covered in the preceding 3 threats.

7) Git repositories :-

(i) **Confidentiality:** git repositories contain the code base for the whole software and is of critical importance. It can be stored locally and hence is mostly secure but a chance hit will have very serious consequences as the code is the core intellectual property for the company.

(ii) **Integrity:** Since the code in rigorously tested before going into production and backed up for security, any change to it will be easily detected and remedied.

(iii) **Availability:** Since the git is used to collaborate development before the production phase, it is not a candidate for DDoS attack.

(iv) **Fraud/theft:** if a hacker manages to breach the authentication and firewall security of the company or use some kind of phishing attack to compromise the account of employees; and reach the locally stored git repositories, this will be a serious loss to the company, and big asset for hackers.

8) Google Sheets :-

(i) **Confidentiality:** google sheets are used for representing analytic information, especially with multiple people working as a team. It can occasionally contain sensitive data use in internal and external meetings.

(ii) **Integrity:** the scope for an integrity attack on these internal documents is not there.

(iii) **Availability:** These documents are backed up and any DDoS attack on google sheets will be remedied soon by google. Also alternatives to google sheets exist(such as excel), if need arise.

(iv) **Fraud/theft:** google sheets are not a service offered by the company to consumers. There is also not much scope for selling information stolen from company's google sheets, except in certain coordinated attack to benefit competitors with malicious motives.

9) Domain Name :-

(i) **Confidentiality:** domain name hijackers use identity theft or phishing. Once they hijack the domain name, they have also gained control of its email accounts, leading to major confidentiality consequences. But these attacks are relatively simple to defend against if one is careful to enable 2-factor authentication and choose a reputable domain registrar company.

(ii) **Integrity:** Once domain name is hijacked, the attackers can install malware or use social engineering attacks using hijacked domain website and email accounts. But as noted, the probability of success of this attack is decidedly low.

(iii) **Availability:** The primary motivation for a Domain Name hijacking attack is to steal a popular domain name and use it for their own website. This leads to significant denial of service consequences to legitimate users who access the application via web.

(iv) **Theft/fraud:** after hijacking the domain name, the attackers can bait unsuspecting users to enter their password and other personally identifiable information(PII), on the hijacked website. This way great deal of data maybe stolen in the unlikely case of a successful attack.

10) ZingHR :-

(i) **Confidentiality:** ZingHR contains confidential information of the company's employees, which can potentially be sold on the dark web. The application is password protected with role-based access to authorized users and uses AES 256 bit encryption and TLS 1.2 protocol. It is considered well secured. Also it does not directly affect the company's system and can be altogether considered low risk.

(ii) **Integrity:** an attempt to alter the transactions and/or records on the site. As noted, ZingHR is generally secure, but chance successful attack(possibly by an employee) can lead to fraudulent payments and corruption of existing records.

(iii) **Availability:** HR and payroll sites like ZingHR are fairly consistent.

(iv) **Fraud/theft:** HR and Payroll service is owned by an entirely different entity and is not a service provided by the company. However stolen user data can fetch value on dark web.

11) Firewall :-

(i) **Confidentiality:** since the firewall is the first line of defence against many cyber attacks it, it is often affected. This can have implications to security leaving the assets vulnerable.

(ii) **Integrity:** data packets that disguise as actual packets have a high chance of beating the firewall. These packets can corrupt the system.

(iii) **Availability:** systems generally possess backup firewalls to replace damaged ones.

12) Salesforce :-

(i) **Confidentiality:** CRM data usually sees high probability of attacks because it includes user data.

(ii) **Integrity:** hackers who gain access to CRM can corrupt website trends and confidential user data.

(iii) **Availability:** CRM data is owned by Salesforce and is available as long there is a contract with the salesforce.

13) Chase Bank :-

(i) **Confidentiality:** highly confidential as the bank processing and transaction take place here. Banking system are very highly secured but are also regularly attacked to carry out illegal transactions.

(ii) **Integrity:** Information stored in the bank records can be altered by attackers if they get access.

(iii) **Availability:** Banking services are always available since no one has anything to gain from shutting it down.

(iv) **Theft/fraud:** Credit/debit card fraud happen occasionally in banking systems.

14) Employee laptops :-

(i) **Confidentiality:** developer laptops contain important code as well as email information – which is of value to competitors. However, Macs are well protected against malware.

(ii) **Integrity:** companies typically ensure strong policies of code backup, leading to little worry of any integrity attack.

(iii) **Availability:** employee laptops, especially those involved closely with support and maintenance of deployed software are important, but companies can use ad-hoc solutions like providing another laptop, or logging in from colleague’s device - should an employee laptop go out of service. Also, there is no strong motivation on part of hackers to target employee laptops with DDoS attacks.

(iv) **Theft/fraud:** since source code is of significant value to competitors, attempts of theft maybe made upon employee laptops.

15) Employee mobile devices :-

(i) **Confidentiality:** email information and slack channels are typically present on the mobile devices of employees, but not anything more critical. Most phones like iphones have biometric protection. However, this is not always a guarantee in our case since phones unlike laptops are not provided by companies and are personal.

(ii) **Integrity:** employee phones are not providing any major service to company and hence threat of integrity here in trivial.

(iii) **Availability:** employees can switch to using laptops in case their mobiles are out of service.

(iv) **Theft/fraud:** while email information and contact have some value to competitors, they are not of a critical nature and generally secured by biometric or 2-factor authentication.

16) Local data backup :-

(i) **Confidentiality:** data backups are connected to cloud by the company's wifi network to take backups and are vulnerable to attacks on internet. They are also connected to developer systems to work on it.

(ii) **Integrity:** Since these data backups are not part of the deployed system and hence not obvious targets for integrity attacks, they can be used as a route for malware. For eg., malware from an employee device can be infected into local data repository from which it affects the cloud deployed infrastructure.

(iii) **Availability:** Since the backups are not a service provided by the company, they are not targets for denial-of-service attack.

(iv) **Theft/fraud:** stolen data can be a sold for profits

17) User accounts :-

(i) **Confidentiality:** User accounts can be hacked by unveiling the password which will lead to loss of the particular user's personal data. While authentication using passwords in generally secure; phishing and social engineering can be used to obtain the password from the user or on a larger scale, server systems may be hacked to reveal the password on multiple users. Social engineering on employees can also be used or hacking of their systems can also be used.

(ii) **Integrity:** Often malicious actors seek to take control on user accounts, by getting hold of their passwords. Password authentication which is common in social media application is a weak link. Personal data of user can be disclose and sold on dark web.

(iii) **Availability:** Since the users are the consumers of the service directing DDoS attacks on them does not make sense.

(iv) **Theft/Fraud:** user data is considered valuable. On a large scale, data of vast numbers of users is of value to competitors for data analysis and consumer profiling. On a small scale, a single user maybe targeted to disclose confidential information about them, that is of interest to someone.