Research and Reports Week 7

Name: Bingying Liang

ID: 48999397

CS7346 Cloud Computing

July 17 2023

Analyze how the six attack surfaces discussed in Section 8.2 and illustrated in Fig. 8.1 apply to the SaaS, PaaS, and IaaS cloud delivery models.

Cloud computing has revolutionized the way businesses operate, with Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) models offering flexibility, scalability, and cost savings[3]. However, these benefits also come with unique security challenges, including several attack surfaces that cybercriminals can exploit.

In the following, analyze each attack surface and illustrate how they apply to SaaS, PaaS, and IaaS models.

1. Data Breaches:

   This involves unauthorized access to data in a system. The most damaging breaches concern sensitive data, including financial and health information, trade secrets, and intellectual property. The ultimate responsibility rests with the organizations maintaining data on the cloud, and CSA recommends that organizations use multifactor authentication and encryption to protect against data breaches[2]. Multifactor authentication, such as one-time passwords, phone-based authentication, and smart card protection, make it harder for attackers to use stolen credentials[4].

   SaaS: Since data is stored on remote servers managed by the provider, vulnerabilities in the provider's security could expose user data[7].

   PaaS: The platform may be secure, but developers can introduce vulnerabilities into their applications, risking data breaches.

   IaaS: Users have the responsibility of securing their data and operating systems, [8]so breaches can occur if these aren't properly protected.

2. Compromised Credentials and Broken Authentication:

   This refers to unauthorized entities gaining access via stolen credentials or exploiting weak authentication processes. Such attacks are due to lax authentication, weak passwords, and poor key and/or certificate management[4].

   SaaS: The service may be accessed from anywhere; if users' credentials are stolen or the service has weak authentication processes, unauthorized access can occur.

   PaaS: Developers and users access the platform with their credentials, so stolen or weak credentials pose a threat here as well.

   IaaS: As users have complete control of the infrastructure, they are responsible for managing and securing their authentication processes.[9]

3. Hacked Interfaces and APIs:

   Almost all interactions with cloud services are done through APIs, and they can be exploited if not properly secured. Cloud security and service availability can be compromised by a weak API.[4] When third parties rely on APIs, more services and credentials are exposed.

   SaaS: Users interact with the service mainly via the provided interface and API; hence, any vulnerability can be exploited to gain unauthorized access.

   PaaS: Developers use APIs to manage and interact with their applications; thus, weak API security could lead to unauthorized access or manipulation.

   IaaS: Users interact with their virtual machines and storage through APIs[5]; hence, vulnerabilities can lead to unauthorized access or control.

4. Exploited System Vulnerabilities:

   These are weak points in a system that attackers can take advantage of to infiltrate or disrupt the system[4]. Resource sharing and multitenancy create new attack surfaces, but the cost to discover and repair vulnerabilities is small compared to the potential damage.

   SaaS: Users rely on the provider to keep the software updated and secure, but any neglected vulnerabilities can be exploited[6].

   PaaS: Even though the platform is maintained by the provider, vulnerabilities in the apps developed by users can be exploited.

   IaaS: As users control the system from the operating system upwards, they must ensure all their software is secure and up-to-date.

5. Account Hijacking:

   This refers to situations where an attacker gains control of a user's account. All accounts should be monitored so that every transaction can be traced to the individual requesting it[4]. **SaaS, PaaS, and IaaS:** All are at risk of account hijacking, especially if strong authentication measures are not in place[1]. The impact varies depending on the control and access the hijacked account has.

6. Malicious Insiders:

   These are individuals within an organization who have authorized access but use it to carry out harmful activities. This threat can be difficult to detect, and system administrator errors could sometimes be falsely diagnosed as threats. A good policy is to segregate duties and

enforce activities, such as logging, monitoring, and auditing administrator activities[4].

SaaS: Provider's employees might have access to sensitive user data and can misuse it.

PaaS: If a developer becomes malicious, they can potentially inject harmful code or access sensitive data.

IaaS: Since an organization has control over the infrastructure, a malicious employee could cause substantial damage.

To summarize, while cloud computing offers numerous benefits, it also exposes users to various attack surfaces. It is crucial for users to understand these risks and put robust security measures in place, particularly for IaaS where users have the most control and responsibility. Cloud providers also have a crucial role in securing their services and educating users about best security practices.

References

[1] Natalie Boyd. *Cloud Computing Security Architecture for IaaS, SaaS, and PaaS*. URL: https://www.sdxcentral.com/security/definitions/cloud-security-basics-definition/cloud-computing-security-architecture/. (accessed: 07.16.2023).

[2] Michael X. Heiligenstein. *Amazon Data Breaches: Full Timeline Through 202*. URL: https://firewalltimes.com/amazon-data-breach-timeline/. (accessed: 07.16.2023).

[3] IBM. *What are Iaas, Paas and Saas?* URL: https://www.ibm.com/topics/iaas-paas-saas. (accessed: 07.16.2023).

[4] Dan C Marinescu. *Cloud Computing: Theory and Practice. Third edition*. Cambridge, MA: Morgan Kaufmann is an imprint of Elsevier, 2023.

[5] Vordel Mark O'Neill. *A security checklist for SaaS, PaaS and IaaS cloud models*. URL: https://www.csoonline.com/article/528248/saas-paas-and-iaas-a-security-checklist-for-cloud-models.html. (accessed: 07.16.2023).

[6] TIMOTHY MORROW. *12 Risks, Threats, Vulnerabilities in Moving to the Cloud*. URL: https://insights.sei.cmu.edu/blog/12-risks-threats-vulnerabilities-in-moving-to-the-cloud/. (accessed: 07.16.2023).

[7] The Hacker News. *Study: 84% of Companies Use Breached SaaS Applications - Here's How to Fix it for Free!* URL: https://thehackernews.com/2023/04/study-84-of-companies-use-breached-saas.html. (accessed: 07.16.2023).

[8] Xavier Santolaria Sambit Misra. *Is Your Critical SaaS Data Secure?* URL: https://securityintelligence.com/posts/is-your-critical-saas-data-secure/. (accessed: 07.16.2023).

[9] Alexey Semeney. *What are the Top Cloud Computing Security Issues for Businesses*. URL: https://www.devteam.space/blog/what-are-the-top-cloud-computing-security-issues-for-businesses/. (accessed: 07.16.2023).