Security Issues in Cloud Services

Shaikh Ashapakh Sattar

***Abstract*—Cloud Computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. However, cloud Computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. Cloud Computing leverages many technologies (SOA, virtualization, Web 2.0); it also inherits their security issues. The most important threats found in the literature related to Cloud Computing and its environment as well as to identify and relate vulnerabilities and threats with possible solutions.**

***Index Terms*— Cloud computing Security, API model, Vulnerabilities Threats Counter measures.**

I. Introduction

Enterprises are no longer sitting on their hands, wondering if they should risk migrating applications and data to the cloud. They're doing it - but security remains a serious concern. The first step in minimizing risk in the cloud is to identify the top security threats.

The shared, on-demand nature of cloud computing introduces the possibility of new security breaches that can erase any gains made by the switch to cloud technology. As noted in a CSA (Cloud Security Alliance) reports, cloud services by nature enable users to bypass organization-wide security policies and set up their own accounts in the service of shadow IT projects. New controls must be put in place.

“The 2016 Top Threats release mirrors the shifting ramification of poor cloud computing decisions up through the managerial ranks,” said J.R. Santos, executive vice president of research for the CSA.

II. IMPORTANT SECURITY THREAD

A. Data breaches

Cloud environments face many of the same threats as traditional corporate networks, but due to the vast amount of data stored on cloud servers, providers become an attractive target. The severity of potential damage tends to depend on the sensitivity of the data exposed. Exposed personal financial information tends to get the headlines, but breaches involving health information, trade secrets, and intellectual property can be more devastating.

When a data breach occurs, companies may incur fines, or they may face lawsuits or criminal charges. Breach investigations and customer notifications can rack up significant costs. Indirect effects, such as brand damage and loss of business, can impact organizations for years.

B. Compromised credentials and broken authentication

Data breaches and other attacks frequently result from lax authentication, weak passwords, and poor key or certificate management. Organizations often struggle with identity management as they try to allocate permissions appropriate to the user’s job role. More important, they sometimes forget to remove user access when a job function changes or a user leaves the organization.

Multifactor authentication systems such as one-time passwords, phone-based authentication, and smartcards protect cloud services because they make it harder for attackers to log in with stolen passwords. The Anthem breach, which exposed more than 80 million customer records, was the result of stolen user credentials.

Many developers make the mistake of embedding credentials and cryptographic keys in source code and leaving them in public-facing repositories such as GitHub. Keys need to be appropriately protected, and a well-secured public key infrastructure is necessary. They also need to be rotated periodically to make it harder for attackers to use keys they’ve obtained without authorization.

Organizations planning to federate identity with a cloud provider need to understand the security measures the provider uses to protect the identity platform. Centralizing identity into a single repository has its risks. Organizations need to weigh the trade-off of the convenience of centralizing identity against the risk of having that repository become an extremely high-value target for attackers.

C. Hacked interfaces and APIs

Practically every cloud service and application now offers APIs. IT teams use interfaces and APIs to manage and interact with cloud services, including those that offer cloud provisioning, management, orchestration, and monitoring.

The security and availability of cloud services - from authentication and access control to encryption and activity monitoring - depend on the security of the API. Risk increases with third parties that rely on APIs and build on these interfaces, as organizations may need to expose more services and credentials. Weak interfaces and APIs expose organizations to security issues related to confidentiality, integrity, availability, and accountability.

APIs and interfaces tend to be the most exposed part of a system because they're usually accessible from the open Internet. It is recommends adequate controls as the “first line of defense and detection.” Threat modeling applications and systems, including data flows and architecture/design, become important parts of the development lifecycle. It is also recommends security-focused code reviews and rigorous penetration testing.

Shaikh Ashapakh Sattar, Research Scholar, Dr. Babasaheb Ambedkar Marathwada University Aurangabad

D. Exploited system vulnerabilities

System vulnerabilities, or exploitable bugs in programs, are not new, but they've become a bigger problem with the advent of multi-tenancy in cloud computing. Organizations share memory, databases, and other resources in close proximity to one another, creating new attack surfaces.

Fortunately, attacks on system vulnerabilities can be mitigated with “basic IT processes”. Best practices include regular vulnerability scanning, prompt patch management, and quick follow-up on reported system threats.

The costs of mitigating system vulnerabilities “are relatively small compared to other IT expenditures.” The expense of putting IT processes in place to discover and repair vulnerabilities is small compared to the potential damage. Regulated industries need to patch as quickly as possible, preferably as part of an automated and recurring process. Change control processes that address emergency patching ensure that remediation activities are properly documented and reviewed by technical teams.

E. Account hijacking

Phishing, fraud, and software exploits are still successful, and cloud services add a new dimension to the threat because attackers can eavesdrop on activities, manipulate transactions, and modify data. Attackers may also be able to use the cloud application to launch other attacks.

Common defense-in-depth protection strategies can contain the damage incurred by a breach. Organizations should prohibit the sharing of account credentials between users and services, as well as enable multifactor authentication schemes where available. Accounts, even service accounts, should be monitored so that every transaction can be traced to a human owner. The key is to protect account credentials from being stolen.

F. Malicious insiders

The insider threat has many faces: a current or former employee, a system administrator, a contractor, or a business partner. The malicious agenda ranges from data theft to revenge. In a cloud scenario, a hell bent insider can destroy whole infrastructures or manipulate data. Systems that depend solely on the cloud service provider for security, such as encryption, are at greatest risk.

It is recommends that organizations control the encryption process and keys, segregating duties and minimizing access given to users. Effective logging, monitoring, and auditing administrator activities are also critical.

It's easy to misconstrue a bungling attempt to perform a routine job as "malicious" insider activity. An example would be an administrator who accidentally copies a sensitive customer database to a publicly accessible server. Proper training and management to prevent such mistakes becomes more critical in the cloud, due to greater potential exposure.

G. The APT parasite

It is advanced persistent threats (APTs) “parasitical” forms of attack. APTs infiltrate systems to establish a foothold, then stealthily exfiltrate data and intellectual property over an extended period of time.

APTs typically move laterally through the network and blend in with normal traffic, so they're difficult to detect. The major cloud providers apply advanced techniques to prevent APTs from infiltrating their infrastructure, but customers need to be as diligent in detecting APT compromises in cloud accounts as they would in on-premises systems.

Common points of entry include spear phishing; direct attacks, USB drives preloaded with malware, and compromised third-party networks. In particular, recommends training users to recognize phishing techniques.

Regularly reinforced awareness programs keep users alert and less likely to be tricked into letting an APT into the network -- and IT departments need to stay informed of the latest advanced attacks. Advanced security controls, process management, incident response plans, and IT staff training all lead to increased security budgets. Organizations should weigh these costs against the potential economic damage inflicted by successful APT attacks.

H. Permanent data loss

As the cloud has matured, reports of permanent data loss due to provider error have become extremely rare. But malicious hackers have been known to permanently delete cloud data to harm businesses, and cloud data centers are as vulnerable to natural disasters as any facility.

Cloud providers recommend distributing data and applications across multiple zones for added protection. Adequate data backup measures are essential, as well as adhering to best practices in business continuity and disaster recovery. Daily data backup and off-site storage remain important with cloud environments.

The burden of preventing data loss is not all on the cloud service provider. If a customer encrypts data before uploading it to the cloud, then that customer must be careful to protect the encryption key. Once the key is lost, so is the data.

Compliance policies often stipulate how long organizations must retain audit records and other documents. Losing such data may have serious regulatory consequences. The new EU data protection rules also treat data destruction and corruption of personal data as data breaches requiring appropriate notification. Know the rules to avoid getting in trouble.

I. Inadequate diligence

Organizations that embrace the cloud without fully understanding the environment and its associated risks may encounter a “myriad of commercial, financial, technical, legal, and compliance risks”. Due diligence applies whether the organization is trying to migrate to the cloud or merging (or working) with another company in the cloud. For example, organizations that fail to scrutinize a contract may not be aware of the provider’s liability in case of data loss or breach.

Operational and architectural issues arise if a company's development team lacks familiarity with cloud technologies as apps are deployed to a particular cloud. Organizations they must perform extensive due diligence to understand the risks they assume when they subscribe to each cloud service.

J. Cloud service abuses

Cloud services can be commandeered to support nefarious activities, such as using cloud computing resources to break an encryption key in order to launch an attack. Other examples including launching DDoS attacks, sending spam and phishing emails, and hosting malicious content.

Providers need to recognize types of abuse - such as scrutinizing traffic to recognize DDoS attacks - and offer tools for customers to monitor the health of their cloud environments. Customers should make sure providers offer a mechanism for reporting abuse. Although customers may not be direct prey for malicious actions, cloud service abuse can still result in service availability issues and data loss.

K. DoS attacks

DoS attacks have been around for years, but they have gained prominence again thanks to cloud computing because they often affect availability. Systems may slow to a crawl or simply time out. “Experiencing a denial-of-service attack is like being caught in rush-hour traffic gridlock; there is one way to get to your destination and there is nothing you can do about it except sit and wait,” the report said.

DoS attacks consume large amounts of processing power, a bill the customer may ultimately have to pay. While high-volume DDoS attacks are very common, organizations should be aware of asymmetric, application-level DoS attacks, which target Web server and database vulnerabilities. Cloud providers tend to be better poised to handle DoS attacks than their customers. The key is to have a plan to mitigate the attack before it occurs, so administrators have access to those resources when they need them.

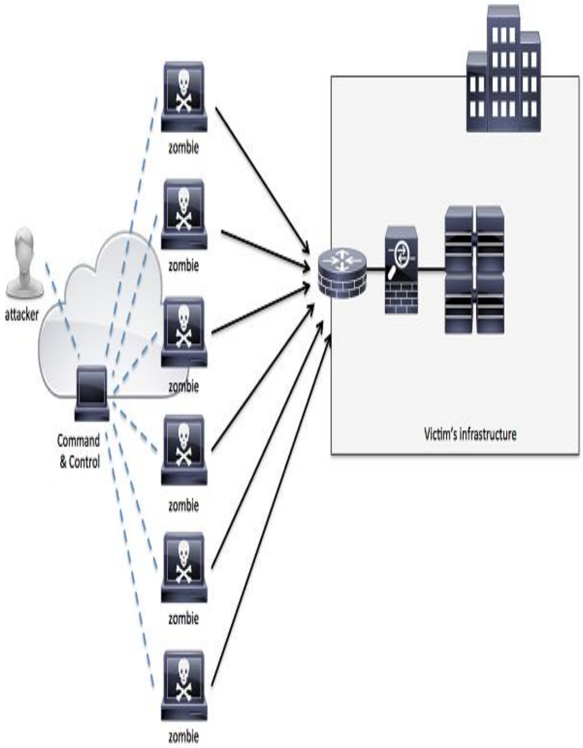

Fig 1: DoS attack

L. Shared technology, shared dangers

Vulnerabilities in shared technology pose a significant threat to cloud computing. Cloud service providers share infrastructure, platforms, and applications, and if a vulnerability arises in any of these layers, it affects everyone. “A single vulnerability or mis-configuration can lead to a compromise across an entire provider’s cloud”.

If an integral component gets compromised - say, a hypervisor, a shared platform component, or an application - it exposes the entire environment to potential compromise and breach. It is recommended a defense-in-depth strategy, including multifactor authentication on all hosts, host-based and network-based intrusion detection systems, applying the concept of least privilege, network segmentation, and patching shared resources.

III. CONCLUSION

Cloud providers typically deploy security controls to protect their environments, but ultimately, organizations are responsible for protecting their own data in the cloud. It is recommended organizations use multifactor authentication and encryption to protect against data breaches.

Security services can be used in an enterprise-virtualized environment to establish protected zones in an otherwise open environment. This means that the virtual security gateway is used in an enterprise virtual datacenter in order to establish security zones for different areas of the virtual network, which contains information of different security classifications.

REFERENCES

[1] Cloud Security: A Comprehensive Guide to Secure Cloud Computing by - Ronald L. Krutz and Russell Dean Vines
[2] http://www.wikinvest.com/concept/Cloud_Computing
[3] http://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html