Security Threats in Cloud Computing - A survey

Boakye Dankwa
Computer and Information Science
Indiana University - Purdue University
Indianapolis, Indiana 46202
Email: bdankwa@iupui.edu

***Abstract*—TODO**

***Index Terms*—cloud computing; security threat; attack surface; Treacherous 12;**

I. Introduction

Cloud computing has created a paradigm shift from traditional IT systems and promises low cost, scalability, efficiency and advanced technology benefits to businesses and organizations. Its service models can be easily tailored to the needs of small to large businesses. Despite the benefits this paradigm shift brings, many businesses hesitate adopting cloud computing, perhaps due to the unknown security risks associated with migrating business data to outside the organization's security perimeter into the cloud. This uncertainty usually arise due to lack of fine grain visibility into the security vulnerabilities and controls of the cloud service provider.

This survey summarizes work done by reputable organizations and individuals to identify top security vulnerabilities in today's cloud computing. A description of the cloud service models and security goals for cloud computing are presented in section II. In section III, a description of the taxonomy proposed in [1] for classifying six attack surfaces in cloud systems is presented, and also the twelve most important security vulnerabilities in cloud computing reported in [2]. Section IV provides some defense strategies to address these threats. The survey is concluded in section V.

II. Security Goals for cloud computing

Cloud computing brings many benefits to businesses and organizations. Many businesses are migrating one way or the other to cloud computing due to the cost savings, efficiency, scale and advances in cloud technology. The cloud service models deliver enabling technologies to businesses than the traditional client - server model. These advances in technology comes with new security vulnerabilities and magnifies already existing ones [3]. Therefore the cloud service and deployment models should be well understood to appreciate the vulnerabilities they bring to an organization. This section describes the cloud service models and the fundamental security requirements in cloud computing.

A. Cloud Service Models

Figure 1 shows the three cloud service models: Infrastructure as a Service (IaaS), Platform as a Service (Paas) and Software as a Service (SaaS).

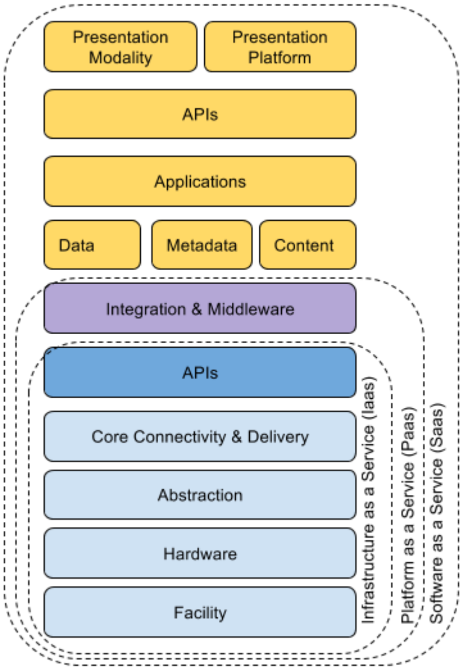

Fig. 1. Cloud service models

Infrastructure as a Service (IaaS): This delivery model delivers virtualized computer infrastructure, typically compute, storage and networking, as a service. Customers subscribe to this service as opposed to owning and maintaining their own computing infrastructure. They deploy their choice of operating system, middleware and applications and interact with the infrastructure with vendor provided API's.

Platform as a Service (PaaS): This is the delivery of a computing platform with solution stack on top as a service. Web applications and services are deployed without the cost of owing and maintaining the underlying hardware and software, including hosting of the applications and services. This service model provides the resources required to develop and deploy web applications and services entirely available from the Internet.

Software as a Service (SaaS): It's a software delivery model in which software and its associated data are hosted in the cloud over the Internet and accessed by customers via a thin client, usually the web browser.

B. Security Requirements

The requirements for securing a cloud system is not much different from securing a traditional IT system. However, due features such as high accessibility, co-tenancy and new technologies associated with the cloud service models, cloud computing faces different risks than traditional IT systems. Additionally, the responsibility of security controls is shared between the service provider and the customer, as opposed to sole responsibility in traditional IT systems. In the order of SaaS, PaaS and IaaS, service providers gradually release responsibility of security controls to customers.

In a IaaS offering, providers are typically responsible for security controls from physical security, to network security, to virtualization security. However, security controls for the operating system, applications and data are the responsibilities of the consumer of an IaaS offering. On the other hand, in a typical SaaS offering, the service provider must address the security controls for the infrastructure, the application and the data. In a PaaS offering, customers are typically responsible for application and data security.

To secure a cloud system, cloud service providers and consumers share the burden of providing security controls across the cloud architecture to ensure *confidentiality*, *integrity*, *access control*, *privacy*, *availability*, *authorization* and *accountability* of the system [4].

III. Vulnerabilities in cloud systems

Cloud systems share the same vulnerabilities as traditional IT systems in addition to new threats due to features such as high accessibility, co-tenancy and new enabling technologies. That is, cloud systems are exposed via several attack surfaces. This section describes such attack surfaces [1] and top security threats in cloud systems as described by the Cloud Security Alliance (CSA) [2].

A. Attack Surfaces

In a work in progress effort, the authors in [1] modeled cloud computing scenario as consisting of interaction of three entities: *users*, *services* and the *cloud* provider. For example, the cloud exposes the service-to-user surface to a user requesting a service or a user managing cloud storage infrastructure. Therefore there are six ways for these entities to interact, namely, *service-to-user*, *user-to-service*, *cloud-to-service*, *service-to-cloud*, *cloud-to-user* and *user-to-cloud* as shown in Figure 2.

The authors referred to these interfaces as attack surfaces in cloud computing. Some of these attack surfaces are not peculiar to cloud computing, for example SQL injection or cross-site scripting occurring across the *service-to-user* interface is no different from that occurring in a traditional client-server model. However, the inherent architecture and the service models of cloud computing subject it to additional attack surfaces.

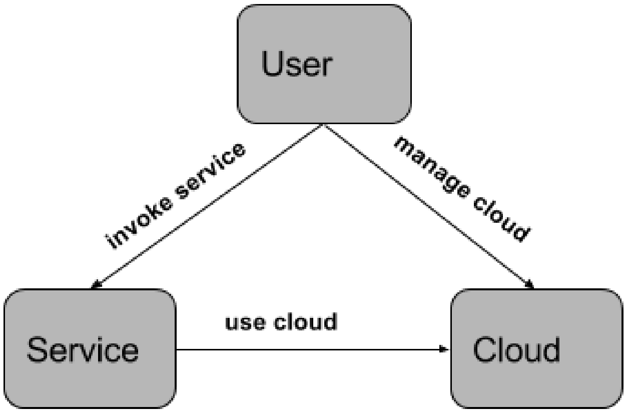

Fig. 2. The six attach surfaces in cloud computing

The *service-to-user* attach surface is the interface that the service instance provides towards the user. This attack interface is broader in a cloud system than the traditional client-server model as suggested by the authors. It is so because there are two additional service models (IaaS and Paas) besides SaaS (which can be approximated as a traditional client-server model) that a user can interact with. This leads to all vulnerabilities that exits in the client-server model such as code injection, buffer overflow, or escalation of privilege, as well as API exploits that users can leverage in an attack against the cloud infrastructure.

Similarly, *user-to-service* interface is the attack surface provisioned by the interface the user provides towards the service instance, also broader than the threats clients are exposed to from the server in the transitional client-server model. Attacks via this interface include Phishing attacks on email clients or SSL certificate spoofing.

The *cloud-to-service* attack surface classifies all attacks that the cloud service provider is exposed to from the service instance. A service instance can exploit vulnerabilities in the underlying cloud infrastructure to attack the cloud service provider. For instance, a PaaS service instance can maliciously allocate more infrastructure resources to itself.

Also, the *service-to-cloud* attack surface is the attack surface a service instance provides to the cloud system. This includes all attacks a cloud service provider can perform against a service instance. For example, an internal employee of the cloud provider with sufficient privileges can compromise the privacy and integrity of user's data, or accidentally or maliciously disrupt a service instance.

The fifth attack surface *cloud-to-user* is the attack surface the cloud infrastructure provides to the user. Users manage cloud services using provider supplied APIs. Malicious users can leverage insecurities in provider APIs to launch attacks on the cloud provider.

Finally, the *user-to-cloud* attack surface is the surface a user exposes to the cloud provider. This involves attacks originates from the cloud infrastructure and targets the user. For example, a malicious employee of the cloud provider can manipulate a vulnerable system to generate a bogus usage bill to a user.

Attackers can compromise the security of a cloud system by combining attacks across multiple attack surfaces depending on the complexity and the goal of the attack. The top security threats in cloud computing are a consequence of exploitation of these attach surfaces. The next section describes some of the top security vulnerabilities in modern cloud systems.

B. Treacherous 12

The CSA identifies the following as the twelve top security threats in cloud computing (ranked in order of severity) [2]:

Data Breaches: A data breach occurs when confidential data is accessed by an unauthorized user. This could be as a result of a malicious attack, application vulnerabilities or poor security practices. The risk of data breach is not peculiar to cloud computing, however, the vast amount of data stored in the cloud coupled with the highly accessible nature of cloud service providers make them desired targets.

Insufficient Identity, Credential and Access Management: Lack of scalable identity and access management system can lead to compromised credentials or cryptographic keys. Weak passwords, absence of mutl-factor authentication and lack of password and cryptographic key rotation can lead to weak identity management and expose the system to various attacks.

Insecured APIs: Cloud providers expose a set of application programming interfaces (API) for customers to manage and interact with cloud services. APIs are the most exposed part of the system and the security and availability of a cloud service are highly dependent on them. Attackers can take advantage of application security flaws, weak access controls or key management and use them maliciously or accidentally to launch attacks on the system.

System Vulnerabilities: These are bugs in operating systems, middle-ware or application software that can be leveraged in a malicious attack on a cloud system. This vulnerability has been around since the advent of the computer, however, it has been amplified in cloud systems due to the multi-tenancy in cloud services. User systems run in close proximity and access shared memory. This presents multiple attack surfaces (*service-to-user*, *user-to-service*, etc.) for attackers. It is reported that 75% of attacks on computer systems use publicly known vulnerabilities in commercial software that could be prevented by regular patching [5].

Account Hijacking: Attackers use phishing or other social engineering techniques to acquire user credentials and passwords to access the users cloud services. This attack can lead to data breach, sabotage and redirection of clients to illegitimate sites. The compromised account can be used as a base to launch subsequent attacks leveraging the original owners reputation.

Malicious Insiders: A current or former employee who intentionally or accidentally misuses his or her access to an organizations information system in a manner that compromises the systems confidentiality, integrity and availability.

Advanced Persistent Threats: Attackers gain malicious access to an organization's computing infrastructure for the purpose of stealing confidential data and intellectual property. The attackers activities stealthily blend in the normal traffic patterns of the system, defeating the security measures intended to defend against them. Points of entry of an APT attack rely heavily on social engineering. Penetration through unsecured or compromised third-party networks are also common.

Data Loss: Data stored in the cloud can be lost due to accidental deletion by the service provider, by a natural disaster or poor key management policy. For example, losing the encryption keys to an encrypted data which is uploaded to the cloud means the data is lost even though the encrypted data is still available in the cloud.

Insufficient Due Diligence: Organizations moving to the cloud must perform extensive due diligence to understand the commercial, technical, legal and compliance risks of cloud technologies and service providers before doing so. Insufficient due diligence could lead to serious business impacts.

Abuse and Nefarious Use of Cloud Services: Malicious actors sometimes use free cloud service trials, or fraudulent account sign-ups on poorly secured cloud platforms, as computing resources to launch attacks (such as DDoS) on other users or the cloud service provider.

Denial of Service: Malicious actors prevent legitimate users from accessing a cloud service by forcing the target service to consume excessive amount of system resources such as processor power, memory, disk space or network bandwidth, such that system performance degrades significantly, sometimes going down completely. The attackers leverage vulnerabilities in web servers, databases and other cloud resources.

Shared Technology Issues: Cloud service providers build services on top of shared commodity infrastructure, platforms and technologies. Vulnerabilities in these low level resources (e.g., CPU caches, GPUs, NICs, hypervisors, middleware, etc) can expose the entire services ecosystem spanning multiple customers to exploitation.

IV. Defense Strategies

Security threats against cloud systems are more complex and far reaching than threats against traditional service hosting infrastructure. Therefore, defending cloud infrastructure not only include traditional defense strategies, but also new ways to deal with the additional threats that come with cloud technologies.

A. Know Your Security Responsibilities

As described earlier, securing cloud systems is the responsibility of both the cloud service provider and the customer. The responsibilities differ depending on the service model. In the order of SaaS, PaaS and IaaS, service providers gradually releases responsibility of security controls to the customer. These controls ranges from the physical security, to network security, to application security, all the way to processes and procedures at the people level. An organization's compliance model specifies the business, regulatory and legal obligations of the organization. These are fulfilled by the security control model which specifies detail security control at each layer of the cloud architectural model. For example, a SOX compliant PaaS customer must provide the necessary two-factor authentication at the appropriate cloud layer to fulfill that requirement. The CSA security guidance [6], provides and in-depth description of the relationship between the cloud compliance model, the security control model and the cloud architecture model.

B. Countermeasures

Signing up for a cloud service means the cloud service provider is trusted to provide good security for the part of the cloud architecture they're responsible for but, ultimately customers are responsible for protecting their data in the cloud.

Multi-factor authentication and encryption are good ways to protect against data breach. Customers who keep sensitive data such as personal health information or intellectual property in the cloud must not only have strong encryption and authentication schemes, they must have effective security processes ranging from how to protect the data, to how to recover or mitigate a breach. For example, Nina P. et al. [7], proposed a one-time password, multi-factor authentication service with enhanced elliptic curve cryptography with MD5 for data integrity. A challenge response process is used to authenticate a user. A one time password is then sent to the user's phone or email account, once user is successfully authenticated, data transfer is via the enhanced elliptic curve cryptography.

A strong identity management scheme is required to defend against insufficient identity threat. Strong passwords and mandatory password rotation, multi-factor authentication and cyptographic key rotation are some of the security controls for defending this type of threat.

Data flow across any untrusted interface must be carefully analyzed from security point of view. Security-specific code reviews, multi-factor authentication, encryption, strong access control, rigorous penetration testing and activity monitoring are some of the security controls necessary to deal with insecure API threat.

A robust patch management system and regular penetration testing are some of the effective ways to reduce the threat posed by vulnerabilities in the cloud system.

Phishing is an effective means attackers employ to hijack accounts. Strong social engineering awareness in addition to multi-factor authentication and account activity monitoring are effective security controls to deal with this threat.

The malicious insider threat is difficult to detect and therefore to counter. Customers should control encryption process and keys used to protect their data in the cloud. Effective logging and monitoring of administrator's activities should be enforced by both provider and customer. A promising monitoring scheme was proposed in [8]. An attacker is first identified my monitoring data access pattern for anomalies. When an unauthorized access is confirmed by using challenge questions, a disinformation attach is launched by returning large amounts of decoy information to the attacker, keeping the user's real data untouched.

Another difficult threat to detect is the APT attack. Attackers usually compromise systems using social engineering or via a trusted unsecured or compromised third-party networks. They usually circumvent the very security controls intended to detect them and can stealthily hide for an extended period. Strong social engineering awareness and robust monitoring systems as well as recovery strategy should be implemented to deal with APT.

Data can be lost due to a natural disaster or lost of encryption keys to the data. The best security control to data loss robust encryption key management policy and data redundancy across multiple geographically separated storage locations.

Organizations considering moving to the cloud should perform extensive due diligence to understand the security implications of the technologies and computing resources of the service provider. For example, is the cloud offering matured enough, does the provider provide fraudulent account detection system, or tools for monitoring account activity. Insufficient due diligence could lead to serious security impacts.

Service providers must have fraudulent account detection system to detect abuse and nefarious use of cloud services. Malicious users can launch attacks on other users or service provider from fraudulent accounts.

Denial of service attacks usually cripples the system under attack. The best mitigation is preparedness, robust detection and mitigation strategies.

Finally, to protect against vulnerabilities in cloud technologies requires combination of security controls such as multi-factor authentication, intrusion detection systems (IDS), user monitoring and robust patch management system. Emerging intrusion detection cloud services such as the machine learning based collaborative IDS service [9], and the federated IDS service across multiple cloud service providers [10], are promising ideas in the area of intrusion detection and monitoring in the ubiquitous cloud.

V. Conclusion

Securing cloud systems posses a major challenge to businesses and organizations. The high accessibility, multi-tenancy and elastic features of the modern cloud computing makes it more difficult to secure compared to traditional static IT systems. The ”Treacherous 12” threats identifies the most critical security concerns in cloud computing to date, that businesses an organizations considering migrating to the cloud should consider. Protection against these vulnerabilities include first understanding security responsibilities, strong security processes and mitigation plans, robust detection and monitoring schemes, and extensive social engineering awareness.

References

[1] N. Gruschka and M. Jensen, “Attack surfaces: A taxonomy for attacks on cloud services,” in *2010 IEEE 3rd International Conference on Cloud Computing*, July 2010, pp. 276–279.

[2] “The treacherous 12 cloud computing top threats in 2016,” Cloud Security Alliance, Tech. Rep., 2016.

[3] K. Hwang, S. Kulkareni, and Y. Hu, “Cloud security with virtualized defense and reputation-based trust mangement,” in *Dependable, Autonomic and Secure Computing, 2009. DASC ’09. Eighth IEEE International Conference on*, Dec 2009, pp. 717–722.

[4] B. Genge, A. Beres, and P. Haller, “A survey on cloud-based software platforms to implement secure smart grids,” in *Power Engineering Conference (UPEC), 2014 49th International Universities*, Sept 2014, pp. 1–6.

[5] “2014 cyberthreat defense report, north america and europe,” Cyberedge Group, Tech. Rep., 2014.

[6] “Security guidance for critical areas of focus in cloud computing,” Cloud Security Alliance, Tech. Rep., 2011.

[7] N. P. Doe and S. V., “Secure service to prevent data breaches in cloud,” in *Computer Communication and Informatics (ICCCI), 2014 International Conference on*, Jan 2014, pp. 1–6.

[8] S. J. Stolfo, M. B. Salem, and A. D. Keromytis, “Fog computing: Mitigating insider data theft attacks in the cloud,” in *Security and Privacy Workshops (SPW), 2012 IEEE Symposium on*, May 2012, pp. 125–128.

[9] H. Liang, Y. Ge, W. Wang, and L. Chen, “Collaborative intrusion detection as a service in cloud computing environment,” in *2015 IEEE International Conference on Progress in Informatics and Computing (PIC)*, Dec 2015, pp. 476–480.

[10] . MacDermott, Q. Shi, and K. Kifayat, “Detecting intrusions in federated cloud environments using security as a service,” in *2015 International Conference on Developments of E-Systems Engineering (DeSE)*, Dec 2015, pp. 91–96.