

Challenges with Cloud Security


Author: Ken Y. Chan

Timeleap Inc.

<https://ca.linkedin.com/in/chanyatwan>

Last Edited: December 4, 2016

Outline

1. Background of Cloud Computing
 2. Key Security Concerns in Traditional Data Centers
 3. Key Security Concerns in Cloud Computing
 4. Why Computing Security is so hard?
 5. Observations
 6. Recommendations
- 
- A dark blue silhouette of a city skyline is visible at the bottom of the slide, featuring various building shapes and peaks against the dark background.

Background of Cloud Computing - 1

- The concept of cloud computing and virtualization is not a new concept. It started with IBM mainframe many decades ago and then progressed to x86 hypervisors and java virtual machine in the 90s.
- In the early days of my career (90s), my Nortel colleagues and I were experimenting with java (1.0 and 1.1) virtualization and application virtualization in multi-HA cluster configuration with zero downtime.
- That was the early day of cloud computing. The pilot project was a success but the market was not ready for the technology back in the 90s.
- Our team did not solve a market problem because nobody wanted to share any infrastructure with anyone and all dot-com companies had too much money to spend.
- In the early or mid 2000s, big data service providers like Google and Amazon understood the only way to scale and to keep their operating cost to a minimum was to leverage virtualization technology in their own data centers.
- At the time, the academic and startup communities were floating the concept of utility computing and cloud computing. They believed an utopia world in which people could put their applications on " the cloud" and they paid only for the actual resources their applications consumed (pay as you go).
- Think of it as free computing market economy (capitalism - does it ring a bell?).

Background of Cloud Computing - 2

- Next, the Amazon engineers made a bold proposal to their executives: They built a massive infrastructure for their e-Commerce needs. Why not extend this massive virtualized infrastructure to gazillions of SMBs who would pay for hosting their applications and data.
- Long story short, Cloud computing economy was born !!
- Although cloud computing offers many great benefits, it poses many great security challenges.
- Many traditional 2-tier, or n-tier systems run in co-located data centers with dedicated racks/cages, or dedicated data centers where the computing resources are tightly controlled.
- All the networking appliances and servers are dedicated to that organization, and no one else.
- The IT team relies on air-tight physical and network security to reduce the attack surface to a minimum, but they tend to put application security in the back burner.
- This security model may work well in traditional data centers but it is insufficient in a cloud environment in which applications may move around in containers and the underlying infrastructure are shared among tenants, that may include (virtual) network appliances/nodes.
- One bad tenant or one compromised tenant may compromise other tenants or even the cloud provider (Not Good!)

Background of Cloud Computing - 3

- Some of my colleagues suggest just encrypting everything (transport, applications, database, logs, etc). However, that is an over-simplification.
- You can have the strongest data encryption but if your key(s) is/are compromised, your applications and data will be compromised as well.
- Let's not forget modern cryptography depends on cryptographic keys. The secret keys are either protected by physical elements (e.g. SE, HSMs, etc) or by other keys (key encrypting keys) at rest or during transport.
- The whole notion of key lifecycle management (including distribution) can be very hairy, especially in a cloud environment.
- In a cloud environment, the attack surface is very large.
- Hypervisors can be compromised. How about the OS or the container?
- An attacker can exploit just one of these vulnerabilities to get to secret keys, and then to the valuable business data
- All IT systems still rely on secret and public key cryptography (e.g. 3DES, AES, RSA, ECC, etc). They are neither post-quantum computing proof nor do they allow additional encryption to be carried out on ciphertext, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext.
- This increases the exposure of the plaintext in a multi-tenant cloud environment (Not Good!)

Key Security Concerns in Traditional Data Centers - 1

- Main offerings of Traditional Data Centers:
 1. Dedicated Servers by Data Center
 2. Co-located Servers by YOU
 3. Own Servers by Own Data Center
- Key Actors: Data Center Operator, Other Tenants, and YOU
- Data center is responsible for physical security of #1 and #2
- Data center is responsible for infrastructure and/or network security of #1
- In case of #3, you are responsible for all security controls.
- Pros: Good to control your security destiny in various degrees
- Cons: This gets expensive and also your business won't be agile (Time to Market)

Key Security Concerns in Traditional Data Centers - 2

- Physical Security

- Building security, Personnel security, Asset security, Wiring security

- Network Security

- Vulnerability in Network Protocol Configuration and Support tools
- Denial of Service attacks
- Address or Name Resolution attacks
- Network Access Restriction (Incl. Authentication and Authorization)
- Vulnerability in Network Appliances and Nodes
- Any possibilities of eavesdropping data streams that carry sensitive data

- Infrastructure Security

- Physical Tampering of Servers and Appliances
- Vulnerability in OS and Support tools (e.g. malwares, virus, worms, etc)
- Any possibilities of exposing sensitive data and cryptographic keys in unencrypted form in storage
- OS user account management (incl. User authentication and Authorization)

Key Security Concerns in Traditional Data Centers - 3

- **Middleware and Application Security**

- Vulnerability in middleware and application virtualization
- Vulnerability in middleware and application support tools
- Any possibilities of exposing sensitive data and cryptographic keys in unencrypted form in storage
- Middleware and Application account management (incl. Authentication and authorization)
- Tampering of Middleware or Application software (incl. patches)

- **Data Security**

- Vulnerability in database management software and support tools
- Any possibilities of exposing sensitive data and cryptographic keys in unencrypted form in storage
- Gaps in data lifecycle management (e.g. replication, backup, archive, purging) that leaves sensitive data available potentially to unauthorized parties
- Database account management (incl. Authentication and authorization)
- Tampering of Database Software Patches

Key Security Concerns in Cloud Computing - 1

- Current Cloud offerings in horizontal (tenant) and vertical (service) aspects
 1. Tenant-based: a) Public, b) Private, c) Hybrid
 2. Service-based: a) IaaS, b) PaaS, c) SaaS
- Key Actors: Cloud Provider, Other Tenants, and YOU
 1. Data center is responsible for physical security of #1 and #2
 2. Data center is responsible for infrastructure and/or network security of #1
 3. In case of #3, you are responsible for all security controls.
- Pros:
 1. With cloud, your operating cost is low because you are sharing common computing elements with others
 2. Your cloud provider may be better than YOU in implementing security controls because good security controls are tricky and expensive to implement.
- Cons:
 1. You have to put a lot of faith in your cloud provider
 2. What are the risks and the impacts if either your cloud provider or other tenants get compromised.

Key Security Concerns in Cloud Computing - 2

- Physical Security

- Your cloud provider is responsible for this 100%

- Network Security

- Typically a Public IaaS, PaaS, SaaS provider is primarily responsible for:
 - Vulnerability in Network Protocol Configuration, Denial of Service attacks, Address or Name Resolution attacks, Vulnerability in Network Appliances and Nodes, and some degree in Network Access Restriction, and Support tools
- However, in the case of hybrid and private cloud, both YOU and your cloud provider need to jointly implement network security controls

- Infrastructure Security

- Typically a Public IaaS, PaaS, SaaS provider is primarily responsible for:
 - Physical Tampering of Servers and Appliances, OS vulnerability (e.g. malwares, viruses, worms, etc), OS user account management (incl. User authentication and Authorization)
 - Some degree in infrastructure support tools
- However, in the case of hybrid and private cloud, both YOU and your cloud provider need to implement your own infrastructure security controls

Key Security Concerns in Cloud Computing - 3

● Middleware and Application Security

- Typically a Public PaaS, SaaS provider is primarily responsible for:
 - Vulnerability in middleware and application virtualization, and support tools
 - Any possibilities of exposing sensitive data and cryptographic keys in unencrypted form in storage
 - Middleware and Application account management (incl. Authentication and authorization)
 - Tampering of Middleware or Application software (incl. patches)
- However, in the case of hybrid and private cloud, both YOU and your cloud provider need to implement your own middleware platform or application security controls

● Data Security

- Typically a Public PaaS, SaaS provider is primarily responsible for:
 - Vulnerability in database management software and support tools
 - Any possibilities of exposing sensitive data and cryptographic keys in unencrypted form in storage
 - Gaps in data lifecycle management (e.g. replication, backup, archive, purging) that leaves sensitive data available potentially to unauthorized parties
 - Database account management (incl. Authentication and authorization)
 - Tampering of Database Software Patches
- However, in the case of hybrid and private cloud, both YOU and your cloud provider need to implement your own data security controls

Why Computing Security is so hard? - 1

- So, how to solve all these security concerns?
- First, people often take security for granted.
- First thing comes to our mind is password authentication and data encryption.
- Computing security is more than data encryption and password authentication
- A sound security framework must satisfy four properties of computing security to a very high degree; and these famous properties are:
- Confidentiality, Integrity, Non-Repudiation, and Availability
- Stronger cryptographic algorithms alone do not and will not solve all the computing security concerns

Why Computing Security is so hard? - 2

- Security, through the lens of enterprise architecture (EA), is an aspect across all EA domains (e.g. network, infrastructure, application, data).
- In a complex IT environment, there are many layers and hops between an end user to a business service.
- That may mean from a few dozen hops in network, to another a few dozen hops in infrastructure, then a few dozen hops in application, and a few dozen hops to data storage.
- We are talking about millions of possible path combinations for a single user operation or transaction.
- 100% security = every possible path combination must be validated and verified against the four security properties.
- With thousands of operation types, we have billions of combinations to validate every so often. (at least NP or EXP hard)
- No time, resources, or \$\$\$\$\$ to be 100% secure

Observations

- Yes, it could be scary to put your critical IT assets at the hands of another party (cloud provider)
- Ask yourself a question, could you implement better security controls than your cloud provider?
- For most businesses, the answer is NO
- AWS, Azure, IBM/Softlayer, Google, and others have put in billions USD in their cloud business.
- For a SMB, you don't have time and money and perhaps expertise to do the same
- Instead, put your time, money, and resources on your business service or application (software) → revenue generator!
- *Make sure all your support tools are also air-tight!!*
- *Attackers like to get in through the backdoors (support tools or support systems or workstations)!!*
- Cloud computing is the right solution for most organizations

Recommendations - 1

- Before you decide the type of cloud service to implement your business service, think about the following:
 1. Understand on your level of risk tolerance of that business service
 - i. If your cloud provider or other tenants get compromised with a given probability, then what would be the impacts?
 - ii. Could you accept the loss (e.g. reputational, financial, etc)?
 2. Compare your risk tolerance against
 - i. Business cost
 - ii. Business agility
 - iii. Asset Reuse
 3. Most importantly, how well can you implement your own security controls versus how well your cloud provider can implement theirs
 4. Then, pick the right cloud service (Public, Private, Hybrid, IaaS, PaaS, SaaS)

Recommendations - 2

Once you decide the type of cloud service, implement your security framework (which is no different from USA Secret Service):

1. Reduce your security complexity by partitioning your system based on security criteria
2. Understand the type of assets you need to protect
3. Understand who and what you need to protect your assets from
4. Prioritize resources based on business impacts and risks
5. Define your security perimeters and zones
6. Not every zone requires highest security measures

OK, That's all for now.

My next presentation will discuss security architecture and design for cloud computing ...