Cloud Security

Barry Denby

Griffith College Dublin

March 7, 2024

Cloud Security

- All computing systems must be secured from attack. Threats fall into a few broad categories
- Malware: Code designed to break into a system and either destroy or control systems or information in one of two means
  - Email attachment: someone runs the attachment and malware spreads
  - Buffer overflow/SQL injection etc: take advantage of software bugs to gain access (does not need user intervention)
- Rogue insider: Person working in the facility containing the computation devices who has malicious intent and physical access to the system

Cloud Security

- In this particular lecture we will discuss how the traditional risks of computing apply to the cloud
- We will also discuss new risks and threats that are associated with the cloud
- Particularly in relation to its public nature and virtualisation
- As before most of this material is based on Cloud Computing: Theory and Practice

Security: Target rich environment

- The cloud is a target rich environment (i.e. many targets for someone to attack)
- This is because there are many applications running on a cloud
- And will also have a large number of users associated with them
- Users may also have information/logins on one or more applications

Security: Target rich environment

- This is a draw for malicious activity and criminal organisations
- For example if there are 1,000 on a cloud and 99% are secure then that means at least 10 can be exploited
- 10,000 means 100
- 100,000 means 1,000 etc

Security: Threats that are the same

- Some threats carry over from other network centric environments so any threats from these categories also apply in cloud
- As cloud is built on these categories
  - Network-centric computing
  - Network-centric content
  - Service Oriented Architectures
  - Grids and Distributed systems
  - Web based services

Security: Reasons for moving to the cloud

- The main motivation for moving to the cloud was the reduction in technical concerns
- This is true but for the security the exact opposite is true as the concerns are greater
- As infrastructure is now shared with many others
- And there is no guarantee that the cloud provider will implement security for you

Security: Threat classes

- Traditional security threats
  - Standard threats that would appear in a traditional non-cloud computing environment
  - All infrastructure must be protected from attack from outsiders
  - If infrastructure can be broken into the cloud is vulnerable to attack
  - Authentication: everyone who has access to the cloud application should be given the smallest privilege set necessary for their task
  - Attack vectors in non-cloud applications also apply: DDoS attacks, phising, SQL injection, cross-site scripting, buffer overflow etc

Security: Threat classes

- System availability threats: standard threats that would be encountered in a datacentre
- Power outages, Fire, Flooding, Malicious destruction etc
- When such an event occurs a user can be faced with data lock-in, wherein the data is not accessible and be consequence the cloud application fails to function
- Detrimental to large enterprise applications

Security: Threat classes

- Third party control threats where there are concerns about data storage from outsiders
- Arises from lack of transparency and the limited control a user has over where the data is stored in the cloud
- For example a cloud provider may outsource some of their data storage to other providers
  - May not be specified by the cloud provider
  - Difficult to determine who they are and a level of trust

Security: Threat classes

- Espionage is also an issue in that there may be malicious employees in the cloud provider who could access or destroy your application data or sell it onto other companies
- Difficult for a user to prove a provider has accessed/modified data without consent
- Abuse of the Cloud: using the cloud for malicious purposes
  - Building many VMs and coordinating them to cause a DDoS attack
  - Using VMs to distribute spam
  - Using VMs to distribute or control malware

Security: Threat classes

- Shared technologies, threats due to multi-tenancy
- VMMs if not secured properly can be accessed and controlled by a VM
- This will directly affect the security of all other VMs managed by the VMM
- Can also lead to the installation of VMBRs

Security: Threat classes

- Insecure APIs: where a cloud provider has produced an API that may be exploited by attackers
- The API should protect applications and users from attack at all times
- Bugs in the API could expose routes to privilege escalation and application control
- Malicious insiders cloud also build backdoors into the API to give them full access to an application through a hidden API/function call

Security: Threat classes

- Data loss and leakage: if the cloud provider does not replicate data properly or prevents unauthorised access
- Difficult to have a full copy of data outside of cloud if datasets are large
- Ensuring consistency is another issue should be other copies of data available
- If the cloud provider maintains one copy of data and should replication fail as well as hardware then all data is lost
  - By consequence the application completely fails as there is no data to work with

Security: Threat classes

- Value of data >>> Value of an application
- Data loss can be irreparable
- Data leakage may occur as a result of malicious cloud insiders observing and copying data
- Or if an application or the API it is built on is coded in an insecure way

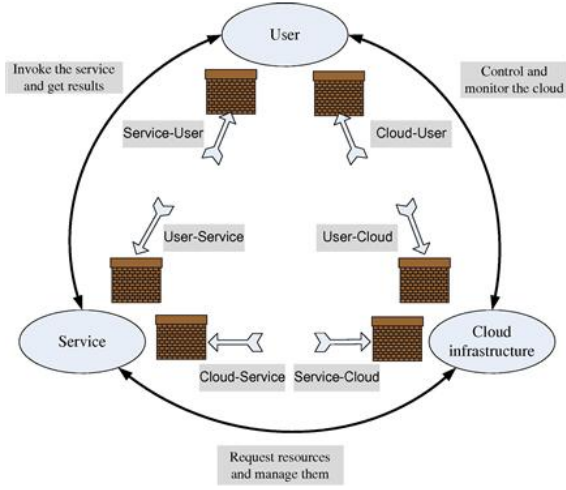
Security: Threat classes

- Account/Service hijacking: significant threat all web facing services must account for
  - There are many methods of stealing credentials and they must be guarded against in a cloud application
  - Bad passwords are one of the most common forms of account hijacking
- Unknown risk profile: Where the developer has been exposed to ignorance to the risks cloud computing poses to their applications

Security: Attack vectors

- There are three actors that are present in the cloud computing environment
- User: The end user who is interacting with the application
- Service: The application the developer has produced to run on the cloud and serve users
- Cloud infrastructure: the supporting machines upon which the application runs
- The interaction between all these components will be illustrated on the following slide

Security: Attack vectors



Security: Attack vectors

- As can be seen from the diagram there are six potential vectors of attack in a cloud system
- All attack vectors must be secured against in a cloud application
- You have zero idea where or when the next attack will come

Security: Other concerns

- There are other concerns that must be taken care of which affect the attack vectors seen previously
- No system is completely secure
- Given enough time and resources any system can be broken into
- You need to ensure that the cost to the attacker to break into your system is far in excess of the potential reward if they break in
- And that there are methods of tracking intruders if they do break in

Security: Other concerns

- Data is more vulnerable in long term storage than in transit
  - Transit is short bursts of data over communication links that can be affected by man in the middle attacks
  - Storage can be attacked for longer periods of time and will require stronger security
- Both must be secured against
- Usually a method of encryption is used
- Life cycle of data
  - In a cloud there is no guarantee as to when deleted data will be rendered unusable and deleted.
  - This poses a risk should the data not be destroyed for a period of time it may be accessible to others
  - Data may not be erased from backups thus there is still potential for access

Security: Other concerns

- Processing
  - Your application may be threatened by malicious VMs or VMBRs
  - It is also possible that employees of the cloud provider can interfere with the processing of your application.
- Standardisation: there is no standarisation among cloud vendors
  - Standarisation usually leads to increased competition thus accelerating development and security of APIs and platforms.
  - Vendor lock in can expose you to bugs that are not fixed or addressed by the provider

Security: Other concerns

- Auditing: Most systems need to know exactly
  - Who accessed the system
  - How and where they did it
  - What actions they took
  - When they happened
- This is necessary for determining attack origins
- Requires extensive reliable logging facilities
- Currently very difficult to do reliably in the cloud

Security: Other concerns

- Multi-tenancy: A core reason for cost reduction in the cloud
- Also a security concern particularly in SaaS applications
- If one user of the service is broken into potentially all users are exposed
  - A nightmare if sensitive data is involved.
- Malicious tenant can try to interfere with your processing

Security: Other concerns

- Legal frameworks: these don't tend to evolve as rapidly as technology
- May be difficult for users to defend their rights with cloud technologies
- Large cloud vendors have sites in multiple countries
  - In cases like this it's hard to determine which laws should apply
  - Particularly if a single action involves two or more countries
- Outsourcing
  - It may be possible that a cloud provider uses another provider to enable some functionality
  - Who's liable if the functionality fails?
  - Who's responsible for implementing security?

Security: Privacy

- Privacy ensures that an individual, group, or organisation has the right to prevent personal information from being disclosed to others
- Major concern in any cloud system or web facing system
- Privacy is also limited by law for reasonable things like taxation and freedom of speech
- Socail networks and voluntary information sharing has lead to information stockpiles that when stolen can lead to identity theft

Security: Privacy

- The main privacy concerns with the cloud are the following
- Lack of user control: Once data is submitted to the provider the user loses control of the data
  - No idea of location
  - Could lose access to the data
  - Data could be stored indefinitely on backup
- Unauthorised secondary use
  - The provider may sell your data to other providers to make alternate streams of revenue
  - Users have no control over how and when this is performed
  - Often no idea as to what data is given or to whom

Security: Privacy

- Dynamic provisioning: Privacy concerns due to outsourcing of data by the provider
- What data does the outsourced provider see?
- Are they secure and trustworthy?

Security: Virtual Machines

- Security issues and solutions arising from VM use in the cloud
- VMs and VMMs are potential targets of attacks in the cloud
- These are things that must be secured against

Security: VMM based threats

- Starvation of resources and denial of service
  - badly configured resource limits
  - rogue VM with capability of bypassing resource limits
- VM side channel attacks: Malicious attack on VMs by a rogue VM on the same VMM
  - Lack of proper isolation of inter-VM traffic
  - Limitation of packet inspection devices to handle high speed traffic
  - VM instances built from insecure VM images
- Buffer overflow attacks or other bugs in the VMM

Security: VM based threats

- Deployment of rogue or insecure VMs
  - Unauthorised users may start insecure instances or perform admin actions on VMs
  - Improper configuration of access controls on VM administrative tasks
- Presence of insecure and tampers VM images in repository
  - Lack of access control to the VM image repository
  - Lack of mechanisms to verify the integrity of the images