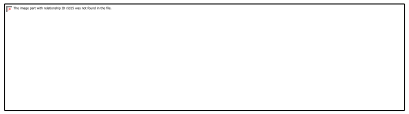
EBU7501: Cloud Computing
Week 1, Day 5: Cloud Security and Trust

Dr. Gokop Goteng

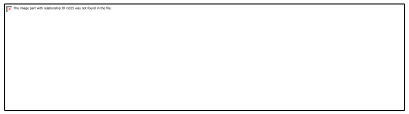
Lecture Aim and Outcome

- Aim
  - The aim of the lecture is to emphasise the importance of security and trust as an important component of cloud computing
- Outcome
  - At the end of this lecture students should be able to:
    - Know the types of computer security attacks and mitigation strategies
    - Know how to enforce data integrity and confidentiality in Servlet and JSP applications
    - Implement cloud security and trust policies



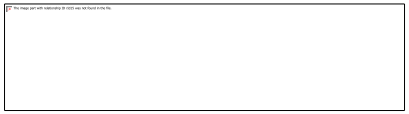
Lecture Outline

- Cloud Security
- Types of Computer Security Attacks
- Mitigating Against Computer Security Attacks
- Measures to Ensure Security and Data Privacy in the Cloud
- Data Integrity and Confidentiality
- Security Configuration in Servlet
- Apache Tomcat's Realm File
- Enable Authentication in Servlet
- Data Integrity and Confidentiality Implementation
- Amazon AWS Security Best Practices
- Cloud Security and Trust
- Implications of Cloud Security Breaches to Businesses



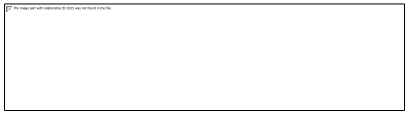
Cloud Security

- Computer Security
  - This is the measures, policies and controls put in place by an organisation to protect unauthorised access to computers, computing devices (ATMs, phones, hand held devices, e.tc.), networks, internet, emails, web sites and data
  - The methods of protecting computing systems involve authentication and authorisation
  - Encryption of data that travel across networks is an important aspect of data security and protection
  - Computer security breach is becoming the most serious threat to the use of information systems for sensitive transactions



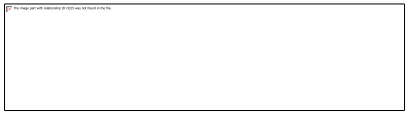
Cloud Security

- Cloud Security or Cloud Computing Security
  - This is a large scale security measures, policies and controls involving multiple distributed cloud computing layers (SaaS, PaaS, HaaS) to protect the service provider's infrastructures as well as the service subscribers' (customers') information systems
  - These measures and controls are designed and deployed for global use to protect physical systems at datacentres as well as the virtual machines deployed
  - The implementations may take into account regional, national and international security and legal policies used in different countries
  - It is a specialised field in computer security
  - The use of certificate-based authentication and authorisation is common in cloud security
  - It is one of the main reasons why organisations prefer to use private cloud than public cloud



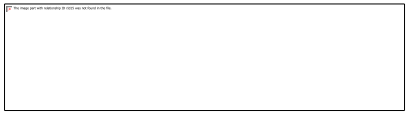
Types of Computer Security Attacks

- Eavesdropping
  - Attackers can listen to network conversation and capture data packets
- Direct access
  - An attacker can have direct physical access to unprotected systems
- Cross-Site attack
  - This attack is based on poor implementation of cloud and web services which attackers take advantage to get access to the website through the URL or other means



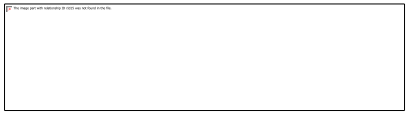
Types of Computer Security Attacks

- Denial attack
  - This type of attack is a “mischievous” way of making systems unavailable to the users as they try to log in or get access to systems
- Upgrader attack
  - This could be an internal attacker who does not have some privileges but upgrade himself/herself to perform certain sensitive functions that he/she is not supposed to
- Intrusion
  - Attackers can intrude into the system if they get access to users login details
    - They do that through brute-force method (trial and error guess) or using some password crackers (software that can crack the password into plain text)



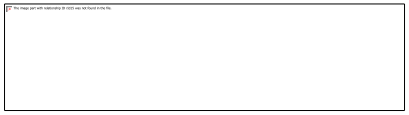
Common Cloud Security Attacks

- Distributed Denial-of-Service (DDoS) attacks
  - Prevent legitimate cloud users from accessing cloud services
    - SQL injection
    - Cross site scripting
- Account or Service Hijacking
  - Stealing credentials of cloud users



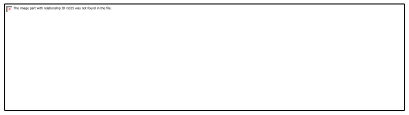
Mitigating Against Computer Security Attacks

- Preventive controls
  - Prevent or reduce the likelihood of attack happening
  - Use strong authentication passwords and upgrade browsers, anti-virus and security applications regularly
  - Deterrent controls fall under the preventive controls
    - Warning sign for the attacker that he/she will be caught
      - Ubuntu Linux systems gives warning that “this action will be reported”
- Corrective controls
  - This measure is put in place in case attackers succeed, you can reduce the damage
    - Recovery of data, stopping the spread of the attack in cloud systems, alerting users



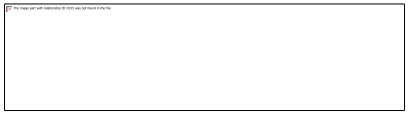
Mitigating Against Computer Security Attacks

- Detective controls
  - This measure is to quickly detect an occurrence of an attack before it is too late to control or correct it
- Access control list
  - Use access control list to deny attackers access to systems
- Secure design and implementation of systems
  - Design very secure cloud systems



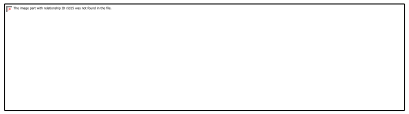
Mitigating at the SLA Level

- State explicitly the Cloud Service Provider's (CSP's) obligations to securely handle sensitive data and its obligations
- Spell out CSP liabilities for mishandling sensitive information
- Spell out CSP liabilities for data loss
- Spell out the rules governing the ownership of data
- Specify the geographical regions where information and backups can be stored



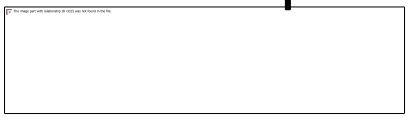
Measures to Ensure Security and Data Privacy in the Cloud

- Audit trails
  - Activities of users and intruders should be monitored constantly
  - Use tools such as AIDE (Advanced Intrusion Detection Environment) and Tripwire to detect and trail unauthorised changes to files and data
  - Logs can be used to trace any malicious changes
- Physical security
  - The hardware, software and databases should not be physically accessible to unauthorised persons
  - They should be locked in secure environment against theft, fire disaster and intrusion



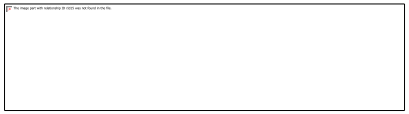
Measures to Ensure Security and Data Privacy in the Cloud

- Application security
  - Cloud service providers should implement security into the applications they are providing as a service to customers
- Identity management
  - Cloud providers should use tools such as digital certificate database access control list and single-sign-on (SSO) to control the identity of their users
- Privacy, confidentiality and legal security
  - Cloud providers should ensure that they do not share data about their customers with third parties without the consent of owners of the data within the legal requirements of data protection



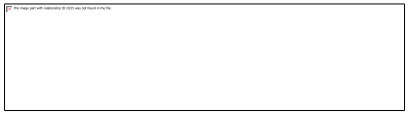
Data Integrity and Confidentiality

- Data integrity
  - The process of ensuring that the data sent across networks and cloud systems are not tampered with or changed along the way
  - Data sent should be the same data that are received
- Data Confidentiality
  - This is the process of ensuring that only people and organisations that are supposed to see or use data can see it
  - Data should be received by the right persons and not to find its way in the wrong hands



Security Configuration in Servlet

- Servlet security is used in web and cloud applications that use servlet and JSP
- The main security implementations in servlet is to address the following four concerns
  - Authentication
  - Authorisation
  - Confidentiality
  - Data integrity
- Realm
  - A realm is the complete path and file that stores the authentication information in a servlet
  - Apache tomcat stores its realm under the conf/ directory and it is usually named “tomcat-users.xml”

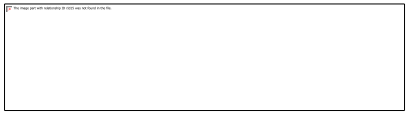


Apache Tomcat's Realm File

```
<tomcat-users>
   <role rolename="Admin" />
   <role rolename="Guest" />
   <role rolename="Manager" />
   <role rolename="Student" />
   <user username="Lu" password="mylu" roles="Guest, Student" />
   <user username="Mathew" password="matt" roles="Admin, Manager" />

     ……..

</tomcat-users>
```

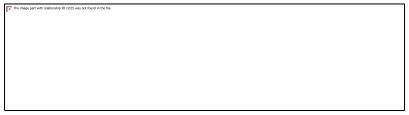


Enable Authentication in Servlet

- To ensure that a user is asked to enter a username and password in a servlet application, configure the login-config in the deployment descriptor

```
<login-config>
    <auth-method>BASIC</auth-method>
</login-config>
```

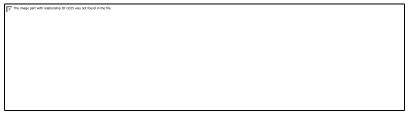
- There are 4 types of login-method values
  - BASIC
    - Authentication details (username/password) are not encrypted
    - They are sent as plain text
    - They are encoded in base 64
    - It is the least secure method of authentication



Enable Authentication in Servlet

- DIGEST
  - This is more secure than BASIC, but is not encrypted
- CLIENT-CERT
  - It is very secure and uses public key certificates infrastructure (PKI)
  - It is encrypted
- FORM
  - This is a customised authentication based on the vendor
  - It does not use encryption by default, but can be customised to use encryptions

- BASIC, DIGEST and CLIENT-CERT methods use the standard browser's authentication popup menu by default once they are activated
- The FORM method needs to be written and activated to popup for authentication

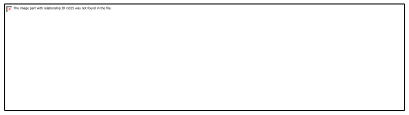


Data Integrity and Confidentiality Implementation

- This is implemented in the DD
- This protects data in transit between networks

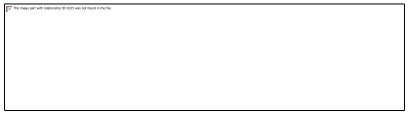
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL>/transport-guarantee>
</user-data-constraint>

- There are 3 values for <transport-guarantee>
  - NON
    - This is the default value
    - If you leave the value blank or you did not put it at all, this value will be use
    - You can specify it explicitly
    - This means that there is no protection for the data
  - INTEGRAL
    - This means that data cannot be changed on transit beween networks
  - CONFIDENTIAL
    - This means that the data must not be seen by anyone on its transit between networks
- Both INTEGRAL and CONFIDENTIAL use Secure Socket Layer (SSL) so they both implement data integrity and data confidentiality

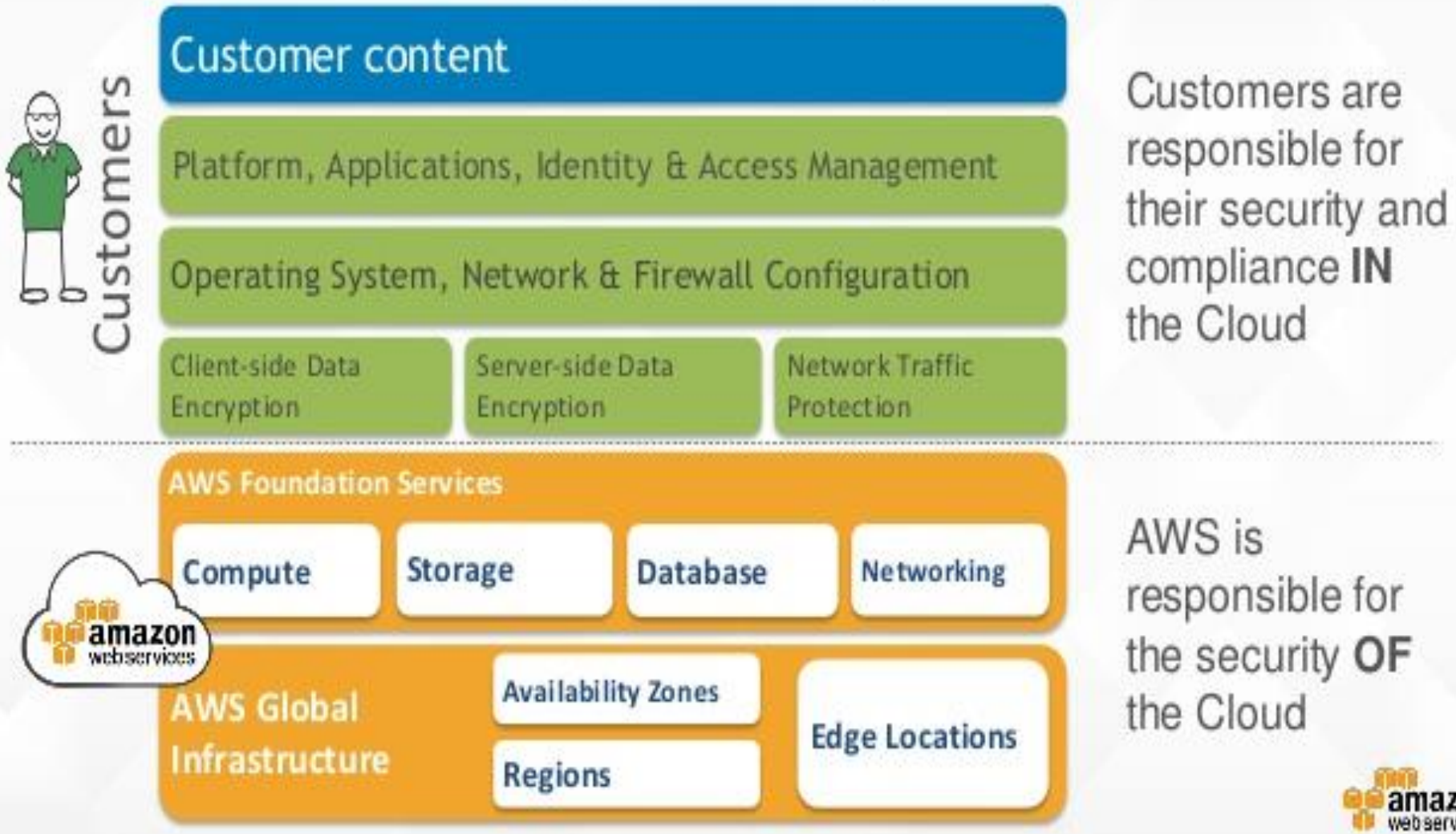


Amazon AWS Security Best Practices

- AWS Day One Best Practice
- AWS security and compliance programs
- AWS Shared Responsibility Model
- AWS Identity and Access Management (IAM)
- AWS Trrusted Advisor
- AWS CloudTrail
- AWS Config
- Constant patching, updates (browsers, antiruses, etc) and monitoring



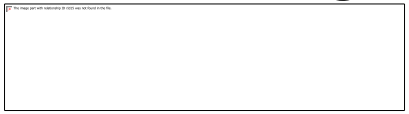
AWS Shared Responsibility Model



Source: Amazon AWS

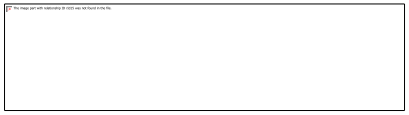
AWS IAM

- AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources.
- You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.
- When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account.
- This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the best practice of using the root user only to create your first IAM user.
- Then securely lock away the root user credentials and use them to perform only a few account and service management tasks.



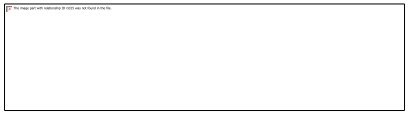
AWS IAM Multi-Factor Authentication (MFA)

- AWS IAM Multi-Factor Authentication (MFA) adds extra security because it requires users to provide unique authentication from an AWS supported MFA mechanism in addition to their regular sign-in credentials when they access AWS websites or services, eg:
  - SMS text message-based MFA: A type of MFA in which the IAM user settings include the phone number of the user's SMS-compatible mobile device.
  - When the user signs in, AWS sends a six-digit numeric code by SMS text message to the user's mobile device.
  - The user is required to type that code on a second webpage during sign-in.



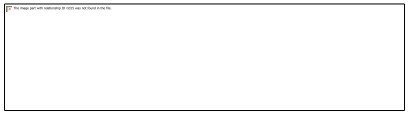
Cloud Security and Trust

- The service level agreement (SLA) between cloud providers and subscribers is the binding legal document that may be used to have trust and confidence in the relationship
- Security details should be agreed upon in the SLA
  - It should include the provider and subscriber's responsibilities
- The hypervisor used for creating the virtual machines may be created by a third party and so there should be that trust between all parties
- The middleware used should include security features to ensure that it checks systems for trust worthiness
- The provider must not share customers' data without their consent and agreement
- Backup strategies should be in place in case there is a problem with data integrity and confidentiality



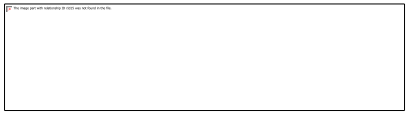
Implications of Cloud Security Breaches to Businesses

- Complete shutdown of business and loss of customers
- Loss of revenue
- Loss of trust and confidence
- Legal implications
  - Customers can seek legal action
- Competitors will seize advantage of that over a business
- Data could fall into wrong hands for further destructions
  - Terrorists, credit card fraud stars



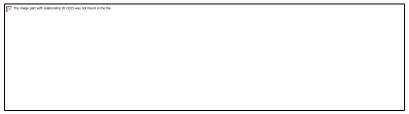
Two Conditions for Trust to Exist

- Risk
  - Probability of loss
  - Trust will not exist if there is no risk
- Interdependence
  - The interest of one party cannot be achieved without the other party



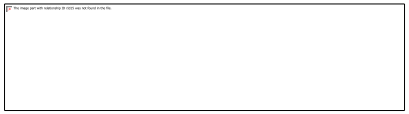
Three Phases of Trust

- A Build Phase
  - When the trust is formed
- A Stability Phase
  - When trust exists
- A Dissolution Phase
  - When trust declines



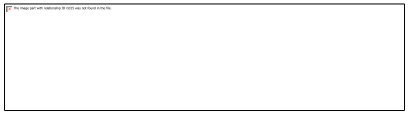
Other Areas of Security

- Operating System Security
  - Updates and patches
  - Protect sensitive paths
- Virtual Machine security
  - VMM provides this
  - VMM-based threads
    - Starvation of resources
    - VM-site channels attacks
    - Buffer overflow attacks
  - VM-based threats
    - Deployment of rough or insecure VM
    - Presence of insecure or tempered VM images
- Application layer security



Class Task

- Which method of the following security implementation is better? Explain your choice with reasons
  - Hard-coding
  - Configuration in deployment descriptor (DD)
- Discuss in 2 groups the security issues in cloud computing regarding
  - Public cloud
  - Private cloud
  - Community cloud
  - Hybrid cloud



Class Task

- What AWS Shared Responsibility Model?
- What is AWS IAM and MFA?
- Identify the main security threats for SaaS cloud delivery model on a public cloud
- Discuss conditions for trust to exist
- Discuss security threats in virtualisation
- Discuss security threats in OS