Cloud Computing

- Cloud Issues and Challenges
  Security

Agenda

- Introduction
  - Issues & challenges
- Cloud Security
  - Security & attack
- Cloud Standard and Law
  - Guideline for secure cloud
  - Law and privacy

Cloud Computing

- Cloud computing collects all resource and all data in the same place
  - Centralization increases the efficiency of management.
- Cloud computing provides many useful and interesting services
  - Hundreds of thousands of users access services.
- But, cloud computing also attracts the attention of malicious users.

Cloud Computing (cont.)

- End users or companies want the benefits of using cloud computing
  - They also worry about the disadvantages of cloud computing.
  - Vendors propose many benefits and advantages, but never mentioned any possible harm.

Viewpoints

- Companies have large amount of data that cannot be disclosed to others
  - Finance reports
  - Consumer list
  - New product and novel techniques
  - …etc
- Data leakage could lead to economic loss or legal proceeding

Viewpoints (cont.)

- End users may not want to let others know too much
  - Family members
  - Phone numbers
  - Salary
- And some important information should be kept secret
  - ID number
  - Credit card number
  - Bank account
  - …etc

Questions

- Before jump into cloud computing, consumer may ask the following questions
  - What's the security strategy?
  - How to prove the reliability and security that vendors claimed?
  - Can someone access my data without my permission?
  - Who is responsible for policy distribution, management and control?
  - What are the emergency response measures and compensation mechanisms?

The Real World is ?

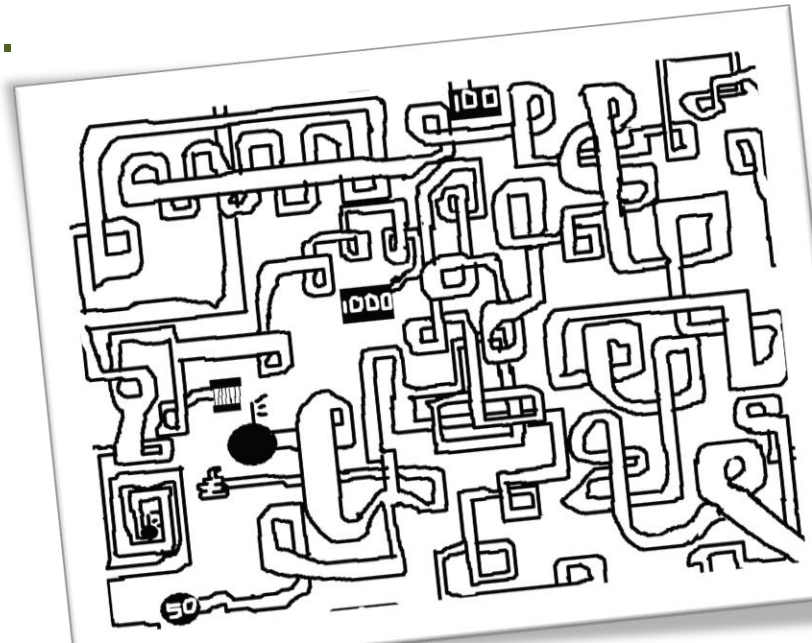
- System may crash caused by incorrect operation.
- Sensitive information data may be stolen caused by loose access management.
- Network may break caused by someone stealing cable.
- …

Compass

- When we invest in the cloud computing
  - How to build the secure cloud environment or platform?
  - How to maintain the cloud service?
  - How to migrate from one cloud vendor to another safely and painless?
- There are many key issues for cloud security
  - Data protection, service quality guarantee, disaster recovery …etc.
  - Customers need a guideline to search a secure cloud vendor.
  - Cloud vendors also need a guideline to build a secure cloud environment.

Loss of Direction

- When the cloud companies or customers lose direction on cloud security
  - They may pay lots of money and resource on the useless efforts.
  - They may pay lots of money and lose intangible assets on the unsecure cloud services.



Remaining

- Introduce the cloud security and issue
  - There are lots of attacks in Internet, and cloud computing still can not escape.
  - Some properties of cloud would avoid some attacks, but some properties could increase the scope of damage.
- Introduce the cloud standard, law and privacy issue
  - The cloud security standard classifies the security issues and provides the security suggestions.
  - Two security examples: law and privacy.

Agenda

- Introduction
  - Issues & challenges
- Cloud security
  - Security & attack
- Cloud standard and law
  - Guideline for secure cloud
  - Law and privacy

Cloud Security and Issues

Outline

- Introduction
- Attack scenario
  - Attack method and possible solutions
  - Real case in the world
- Summary

INTRODUCTION

Security

- Security is the degree of protection against danger, damage, loss and crime.
  - Security is focused on hardware mechanism, software vulnerability and information hiding.
  - Malicious attackers want to steal data or destroy system
- Security evolution can be divided into three parts
  - Secure technique
  - Secure management
  - Cyber security

Secure Technique

- Original security that provides the basic protection mechanism
  - **Authorization** specifies the access right to resource and reject the request from the unknown users.
  - **Encryption** makes information unreadable to anyone except those possessing special knowledge.
  - **Uninterrupted power supply (UPS)** and **remote backup server** avoid the data loss or server interruption caused by natural disasters.

Secure Management

- Proposed and executed one or more feasible security policy
  - **Access-control-policy** is high elasticity that authorizes a group of users to perform a set of actions on a set of resources.
  - **Some sort of industry guidelines** train and teach employee the computer security concept.
  - **Incident response plans** are the standard procedures for dealing with emergencies

Cyber Security

- Internet now is a new battlefield that everyone is in Internet everyday
  - **Intrusion prevention system (IPS)** monitor, identify and log information about network and/or system activities for malicious activity.
    - Attempt to block/stop activity, and report immediately.
  - **Social engineer** is manipulating people into performing actions or divulging confidential information, rather than by breaking in or using cracking technique.

Information Security

- Information security means to avoid to access, record, disclose, modify and destruct without authorizing.
- There are three core principles of information security
  - Confidentiality
  - Integrity
  - Availability

CIA

- Confidentiality
  - User access the sensitive data only when getting the permission.
  - Data or information could be separated into several secure level
    - Normal, security or top secret.

CIA (cont.)

- Integrity
  - Data cannot be modified undetectably.
  - Information keeps accurate and complete during transmission.
- Availability
  - User can get all data what they need anywhere and anytime.

In Real Life

- Users or companies would skip the confidentiality
  - The convenience is more important than the secret.
  - High confidentiality needs complexity passwords and frequent changes.
  - Confidentiality also keeps principle of least privilege, that increases the convenience of use.

Unbalance…

- When convenience and confidentiality is not balanced anymore
  - Everyone will leave since environment is *not friendly*.
  - Everyone will leave since users *no longer have secret*.
- Service vendors try to give the optimal solution
  - A novel authentication method
  - A perfect access control mechanism
  - An immediate emergency response program
  - …

In Cloud Computing

- Properties of cloud computing reduce the part of security issue
  - The property of availability provides the services anytime and reduce the probability of downtime.
  - The property of scalability avoids the starvation of resource and can accommodate a large number of users.
- But cloud computing still needs to maintain a high degree of attention on security

In Cloud Computing

- Cloud computing provides services to everyone
  - There is a lot of sensitive information.
  - Users do not want any delay or stop service.
  - Cloud vendors want more and more users to use cloud service.
- But some people also think this is a business.

ATTACK SCENARIO

Malicious Attacker

- Malicious attackers hide in Internet and try to
  - Steal the important or sensitive information
  - Collect user' data and sell the data
  - Control or destroy the compromised system
  - Raise awareness
- Focus on the attackers' motivation.
  - Money
  - Philosophy
  - Show off

Hacker Economics

- How much of your personal information
  - Name, phone number and address
  - ID number
  - Credit card number
  - …etc
- But the price of data has been reduced
  - Hacker must work hard
  - Automation
  - Large deployment
  - …etc

Fun or Show Off

- Hackers may want to get some pleasures or show their special talent
  - Hackers attack those websites what they don't like.
  - Patriotic hackers change the home page and show some messages.

How to Attack?

- How does a hacker attack the system or steal some information?
- Hacker is not the God
  - Still need some background and practices.
  - Still need to prepare some preprocess work.
  - Still need some tools.
- There are two parts of attack behavior
  - Penetration
  - Attack and destroy

Workflow

- Penetration
  - Collect all public information.
  - Try to find the weakness or vulnerability.
  - Try to get the access right or administrator privileges.
- Attack and destroy
  - Steal or delete data
  - Crash the system
  - Monkey business

Penetration

- Hacker finds the weak point to access the target server and leave without trace
  - Weak password or SQL injection
  - Program vulnerability
  - Erase all log file
- Penetration test (also called pentest) is a method of evaluating the security
  - Simulate an attack from a malicious source.
  - Analyze the feasibility of an attack and guide improving the system security.

Attack and Destroy

- Hackers try to steal data, block service and destroy system
  - Compared with penetration, attacks do not need to be hidden.
  - Paralysis of the operational capabilities of the host and the firewall.
  - Install malicious code to destroy the system and data.
- An attack action may be accompanied by penetration.

In Cloud

- Penetration
  - The server in Internet would suffer hundreds of attacks
  - Ping and port scan
  - Try to log in or get the correct password
- Cloud computing also collects ten to hundreds PB information per day
  - Hacker may get millions of information items with successful attack.
  - Malicious attack will not stop.

Methods

- Cloud computing environment is also a group of computers
  - Old attack methods can still pose a threat in some case.
  - But some methods cannot damage system anymore.
- Cloud properties can reduce the probability of the system under attack
  - Scalability
  - Accessibility
  - Management
  - …

Brute force

Phishing

Sniffer

DDoS

ATTACK SCENARIO

Password

- In general, password is the basic method for authentication
  - Length of password and characters determine the strength of security.
  - Only lowercase with 4 characters has 45,000 possibilities.
  - Common words can be crack in few minuets by dictionary attack.

In Cloud

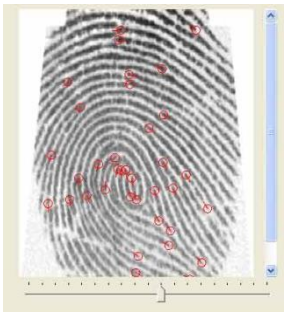
- The number of users is grown more than million to billion
  - Hacker can use the few possibilities to try all of users.
  - Based on birthday attack, hacker has a high chance to get the correct password.
  - Always some people use unsafe passwords.

Solution

- Basically, in the registration phase
  - Force users to use alphanumeric passwords.
  - Force users to use more than 8 char passwords.
  - Limit users from using the common words in dictionary.
- Set security password policy
  - Limit the number of incorrect attempts.
  - Ban the attacker's IP with few minutes.
- But in some cases, brute force could block the user's normal use
  - A kind of deny of service.

Solution (cont.)

- Service vendors can use other security technology to provide a high degree of security protection
  - Communication lock – unlock the account by user dialing to a special phone number.
  - Smart card - contain volatile memory and microprocessor components that provide strong security authentication.
  - Fingerprint – each one has his own fingerprint that cannot easily be forged.



Brute force

Phishing

Sniffer

DDoS

ATTACK SCENARIO

Phishing

- Phishing is a way of attempting to acquire sensitive information by a fake web page
  - Cloned the normal web pages.
  - Steal password or credit card account
- There are three way of phishing
  - URL shortening
  - A confusing link
  - SEO (Search Engine Optimization) poisoning

Phishing (cont.)

- URL shortening is a technique on WWW in which URL may be made substantially shorter in length and still direct to the required page.
  - Long URL cannot post in some forums, like Twitter or BBS.
  - Trying to type long URL by hand will be time-consuming and result in errors.
  - But short URL cannot determine the actual one or fake until link to.

www.shorturl.com/ABCEFG

Phishing (cont.)

- A confusing link is a URL that replaces the similar characters or uses the same meaning words
  - example.com vs examp1e.com
  - www.candy.com vs www.candies.com
- SEO (Search Engine Optimization) is the process of improving the visibility of a website in search engines.
  - Users usually find a website by search engine
  - Hacker may poison SEO to increase the rank of phishing pages

In Cloud

- Cloud vendor provides many services and many service webpages
  - Users cannot remember all of URLs
  - Users may fall into phishing web pages
- User can log in once and gain access to all services by Single sign-on (SSO)
  - Reduce phishing success, and users are not trained to enter password everywhere.
  - Each service can redirect to other service.

In User

- User should be careful on account needing to be verified or any other topics used by phishing
- User should improve security of emails
  - All legitimate e-mail messages contain an item of information that is not readily available to phishers.
- User can use plug-in or software to help identify legitimate sites

Brute force

Phishing

Sniffer

DDoS

ATTACK SCENARIO

Communication

- A packet is a formatted unit of data
  - Computer communication links simply transmit data as a series of bytes.
  - A message is separated into several segment packets and each packet is transmitted to target computer.
  - Receiver reconstructs message from these packets.
- Each packet may pass through several computers and switches.

Sniffer

- Sniffer means someone intercepts and logs traffic passing over a digit network or part of a network.
- NIC (network interface card) drops any packet whose receiver is not his MAC address
  - NIC in promiscuous mode would not drop any packet.
  - Hacker can get any packet passing through his NIC by setting promiscuous mode.

Network Device

- In some network devices, packets are redirected to other computers
  - Hub connects multiple transmission cables together and makes them act as a single network segment.
  - Switch connects network segments and redirect packets into particular computer.

Network Device (cont.)

- Hub works at the physical layer of the OSI model.
- The device is a form of multiport repeater
  - Receive a packet and broadcast out on all other ports.
  - Easy for Hacker to get the packet in the same network.
- Switch works at the data link layer of the OSI model.
- Switch records MAC address by ARP protocol
  - Redirect a packet to the particular computer by MAC route table.
  - Hacker cannot get a packet by using promiscuous mode.

Open Systems Interconnection **model** (**OSI model**)

Address Resolution Protocol (ARP)

ARP Spoofing

- Switch uses ARP protocol to record the pair of MAC address and IP address
  - Hacker uses ARP spoofing to attack a LAN (local-area network)
  - Hacker sends the ARP request and registers his MAC address before the legal user.
  - Hacker also can send lots of useless ARP requests for DoS (denial-of-service) attack

VLAN switch

- Using VLAN switch, users only can access switches and cannot connect to other users
- In high-end devices, switches can detect the ARP spoofing/attack and alert administrator the malicious behavior.
- Switches can also set the static route table
  - But in many case, the IP address would be dynamically decided

A virtual LAN (**VLAN**) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer.

In Cloud

- Cloud service venders limit the environment setting that can reduce the probability of sniffer.
- Using SSL/TSL cryptographic protocols that provide communication security over the Internet
  - Even hacker getting the packet also cannot get the sensitive message.

Transport Layer Security (TLS) and its predecessor, **Secure Sockets Layer (SSL**), are cryptographic protocols that provide communications security over a computer network.

Brute force

Phishing

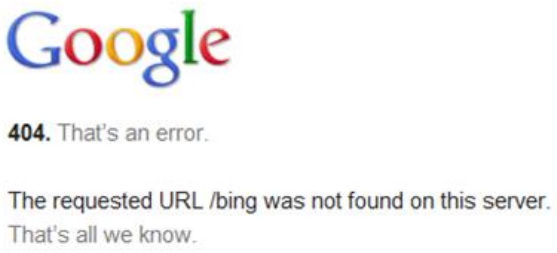
Sniffer

DDoS

ATTACK SCENARIO

DoS

- Denial-of-Service (DoS) is an attempt to make a computer resource (like storage service) unavailable
  - Hacker sends lots of requests to a server such that the server cannot respond to legal users.
- Server can only provide services to fixed users
  - Hackers use all the resource as much as possible.
  - Other users wait until server is available.



Attack

- In general, a server can handle hundreds of requests at once
  - A desktop can send hundreds of small requests to attack a server.
  - But in a large-scale server, a host can easily handle thousands to hundreds of thousands of requests.
  - Hacker must need more resource.
- DDoS (distributed denial of service) occurs when multiple systems flood the bandwidth or resources of a target system.

Botnet

- Hackers want more resource to attack
  - Hackers using Trojans and worms control lots of computers.
- A botnet is a collection of compromised computers that are used for malicious purposes
  - The average size of a botnet is estimated at 20,000 computers
  - Hackers control compromised computers to send spam and DoS target.

In Cloud

- Cloud computing provides service to many users
  - One of the cloud properties is availability.
- User access cloud service anytime and anywhere
  - This means cloud platform must can serve thousands of users.
  - Cloud platform can distribute workload across multiple computers and services.
- The general DDoS attacks cannot affect the cloud environment.

In Cloud (cont.)

- Cloud vendors offer pay-per-usage or pay-as-you-go access to computers and services.
- Hacker may burn your quota
  - DDoS may not affect the end users, but can increase the quota of usage of bandwidth.
  - Hackers can send lots of queries to increase spending of company

REAL CASE

In the Real World

- Cloud computing is providing services to users
  - End user are using cloud benefits.
  - Service providers are using cloud environment to provide service
- Hackers are already to attack the cloud.

Zeus and Amazon

- In 2009, the Zeus banking Trojan has been spotted using the Amazon service as a C&C (command and control) server.
  - Compromised computers report to EC2 for new instruction and updates.
  - Amazon's Relational Database Service is a backend alternative in case losing access to original domain.
- Crimeware will dive deep into the cloud.
  - Facebook
  - Google App Engine
  - …

Google Phishing

- In 2011, Google announced that hundreds of Gmail accounts were compromised in phishing
  - Attackers have enough information to create an e-mail that seems like someone you know.
  - Attackers try to steal your password and access your e-mail account.
  - Attackers secretly reset settings to copy and forward all e-mails.

Google Phishing (cont.)

- Hackers attack Gmail to steal the login details
  - Senior US and South Korean government officials
  - Chinese political activists
- Chinese Gmail attack raises cyberwar tensions
  - There is no direct evidence that the hackers were in the pay of the Chinese government.
  - The US government classifies cyber-attacks as acts of war.

Wikileak and Anonymous

- WikiLeaks is an international non-profit organization
  - publishes submissions of private, secret, and classified media.
  - under DDoS attack around the time of an expected release of classified State Department documents.
- WiliLeaks want to move into Amazon EC2
  - EC2 were successfully defended against large-scale DDoS attack.

Wikileak and Anonymous (cont.)

- But in 2011 December, many cloud computing providers stop service for WikiLeaks
  - EveryDNS dropped its domain name service.
  - Amazon took it off its computers.
  - PayPal and MasterCard cancelled its account.
- Anonymous (hacker group) attacks on the opponents of WikiLeaks
  - PayPal and MasterCard are forced to stop online service.
  - But hackers stop attack Amazon because realizing how little impact it was having.

Dropbox Security

- In 2011, Dropbox security glitch meant any password works
  - Everyone can access dropbox if he knows the e-mail.
  - Dropbox's authentication is failed in one hour and stop service for up to three hours.
- Dropbox claims that they encrypt user data on client
  - In fact, workflow of encryption is on server.
  - Staff could access the sensitive data.

Summary

- Cloud computing provides a new service model
  - A way to increase capacity or add capabilities
  - Need not a new infrastructure, training new personnel, or licensing new software.
- Cloud computing also becomes a big target for malicious attackers.
- Hackers try to access computer, steal data and destroy system
  - Everyone would be the victim.

Summary (cont.)

- According to the principle of CIA, cloud computing vendors need to provide a safe, secure and reliable environment.
  - Increase the accessibility and availability and reduce the inconvenience on usage.
  - Protect data and avoid to be stolen.
  - Analyze and trace the security event, improve system security at any time.

Reference

- Wikipedia http://en.wikipedia.org/wiki/Wiki
- News
  - http://www.zone-h.org/
  - http://www.zdnet.com.tw/news/software/0,2000085678,20143834,00.htm
  - http://udn.com/NEWS/WORLD/WOR3/6025617.shtml
  - http://tw.nextmedia.com/rnews/article/SecID/109/art_id/42470/IssueID/20110623
  - http://lieberman.senate.gov/index.cfm/news-events/news/2010/12/amazon-severs-ties-with-wikileaks
- All resources of the materials and pictures were partially retrieved from the Internet