Security and Privacy Challenges in Cloud Computing

By: Indir Avdagic
Objectives

- What is Cloud Computing?
- Security Problems and Liability
- Privacy Concerns
- Solutions
- Recap - Challenges for the Customer
What is Cloud Computing?

Not single, agreed-upon definition exists yet, but the best in opinion is NIST’s definition: Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.”
The Key Delivery Cloud Models:

- Platform as a Service (PaaS)
- Software as a Service (SaaS)
- Infrastructure as a Service (IaaS)
Cloud Computing Benefits & Risks

**Benefits:**
- Avoid start-up costs
- Applications and services can be accessed from any computer, anywhere in the world
- Only pay for what is used
- Increased agility by immediately acquiring services
- Can be scaled easily.

**Risk:**
- Users don’t hold physical access to data
- Applications and services can be accessed from any computer, including those of attackers
- Information security for data are customer responsibilities in many cases
- Lack of well-designed SLA
Security & Privacy Challenges

- Multi-domain environment in which each domain can have different security and privacy requirements
- Authentication, access control, accounting, and IDM mechanism
- Trust Management
- Secure Service Management
- QoS, prices, and SLA
Phishing

Hotmail password breach blamed on phishing attack

Bobbie Johnson, San Francisco
guardian.co.uk, Tuesday 6 October 2009 07.58 BST
Article history

Microsoft has confirmed that the publication of thousands of Hotmail passwords was the result of a phishing attack against users of the popular email service.

Precise details of the strike, which was first uncovered on Monday, remain unclear. But in a statement, the American software company said...
Privacy

• As more information is put online, there is more risk and more danger associated with your online identity
• You might think that online identity theft or online identity fraud wouldn’t happen but it can happen to the best, even Matt Honan.
Who is Mat Honan?

- Mat Honan is the last person you'd consider fall prey to hackers
- Matt Honan
  - Senior writer at wired.com (technology magazine)
  - covered the technology industry for over a decade
  - very tech-savy; owns all the new devices
- About a month ago his whole digital life was erased
How did Matt Honan fall?

- Hackers grabbed publicly available information; name, billing address and email
- Used that to get into his amazon account
- Got enough information to get into his apple ID account
- Wiped his MacBook, iPad, and iPhone
- Got access to Gmail account
- Got access to twitter account
Matt Honan's story continued

- Lost thousands of pictures, thousands of emails, thousands of documents
- Lost his real Twitter, and his Gmail account
- In his personal article, Matt says "Yet still I was actually quite fortunate."
  - Because they could’ve used the information to empty his financial accounts
  - They could’ve used his information to steal sensitive information from the Wired news organization
What where Matt’s mistakes?

- Use of a simple password that can guessed using knowledge about him
- Using the same password across different logins
- Having accounts linked for the purpose of password recovery
Password Security Guidelines

Length

• Make sure they're longer than 10 characters. A short password can be guessed more easily or cracked with brute force.

Strength

• Include letters, punctuation, symbols, and numbers. Use the entire keyboard, not just the letters and characters you use or see most often. The greater the variety of characters in your password, the better.
Password Security Guidelines

Variation

- Change passwords often; at least once a year but the more often the better

Variety

- Don’t use the same password for everything; hackers steal passwords from less secure sites and use it on more secure sites. Don't use things like names and things that can be easily guessed.
Better Solution

Two Factor Authentication
Google – 2 SV Example

- **2 Factor Authentication** is currently in place for many cloud service: Gmail, Dropbox, etc.
- Let’s let Google explain in the video below their 2 Step Verification – 2 SV:
Recap - Challenges for the Customer

- Who is responsible for lost data?
- Where is the data really stored?
- Is it backed up somewhere?
- Is the service provider storing your data or tracking your use of their resources in some way?
- What about retention?
  - Will deleted material really be deleted?
- It is important for the user to look into these issues before becoming a customer of the cloud.
SEAS Information Security Resources

- SEAS Information Security Basics Brochure:

- For any other information security needs:
  - Visit SEAS Information Security Office Web Site:
  - http://security.seas.harvard.edu
  - Call SEAS Information Security Office at 617-496-3502
  - Send email to security@seas.harvard.edu
Questions? Comments? Concerns?

Contact: Indir Avdagic
Director of Information Security
security@seas.harvard.edu or
security.seas.harvard.edu