**CS590: Privacy Constraints on Cloud Services**

*- Tulika Srivastava*

Problem Statement:

Participation in large data centers and Cloud systems is increasing in recent years. Services such as Amazon’s EC2, Microsoft’s Azure or Google’s AppEngine allow millions of individuals to create online profiles and instance and share personal information and use their services with vast networks of individuals accessing the same services - and, often, unknown numbers of strangers. Users make certain assumptions about privacy and security on the cloud which put together with the purpose of using the various services leads to many privacy threats. Also, some parties are interested in mining data from these Clouds (for research, marketing, etc) which can lead to exposure of personal information. If you entrust a cloud provider with your data, how is encryption handled, if at all? What about user authentication? What about data breach liability?

What needs to be done?

We need to study some ways to counter these privacy attacks. This is in scenario where policy changes in Cloud computing is not possible. We can assume these to be certain guidelines for cloud users to protect their privacy.

Next, we need to look at some policy related changes which can be recommended on cloud computing or features which we recommend these Clouds should support in order to provide better options for users to keep their private information private.

What has been done?

[Cachin, Keidar and Shraer 2009] mentioned a few well known cryptographic tools such as Byzantine for providing integrity and privacy for data stored in clouds and they also discussed research in cryptography and distributed computing addressing these problems.

Brian Krebs wrote an article that how Amazon's Elastic Compute Cloud (EC2) servers were responsible for sending out spam mails, which are marketed to companies -- mainly small to mid-sized businesses -- that want to purchase access to any number of computer applications hosted on the Internet, from data crunching and storage to on-demand computer processing power. These "cloud computing" services are "pay-as-you-go," so customers only pay for the resources and services they consume.

[Chen, Paxson, and Katz 2010] argue that two security issues are to some degree new and fundamental to cloud computing: the complexities of multi-party trust considerations, and the ensuing need for mutual auditability. They propose that developing security architectures early in the process can pay off greatly as systems evolve and accrue more disparate functionality.

What can be done?

We can explore and compare security, privacy issues particularly in Cloud Systems/forums. We first look at some of the recent incidents which strongly emphasize the need for having a closer look at privacy issues on Internet (like query logs, Google ads, Identity theft in general). Next, we can look at potential attacks on various aspects of users' privacy, e.g. neighborhood attack, phishing, etc.

This is followed by a survey of status of some of the popular current Clouds. As the usage of online properties increase and more and more users are starting to participate on such Cloud systems, privacy has taken a major importance. This review paper will provide a look at current status of the online properties along with a study of possible threats/attacks and some ways to counter these.

What I have done?

To understand the privacy issues in various cloud systems, I am reviewing the papers and articles that mention privacy issues and that give an overview of the functionality of the different Clouds, the amount of personal information the cloud system requests the user, the policies that they incur upon the users.

References:

* Mell, P., and Grance, T. *The NIST Definition of Cloud Computing. Version 15*. NIST, October 7, 2009.

<http://csrc.nist.gov/groups/SNS/cloud-computing>

* Cachin, C., Keidar, I., and Shraer , A. Trusting the cloud. *ACM SIGACT News,* 20:4 (2009), pp. 81-86.
* B. Krebs. Amazon: Hey spammers, get off my cloud! <http://blog.washingtonpost.com/securityfix/2008/07/amazon_hey_spammers_get_off_my.html> , July 2008.
* Y. Chen, V. Paxson, and R. H. Katz. What’s new about cloud computing security? Technical Report UCB/EECS-2010-5, EECS Department, University of California, Berkeley, Jan 2010.
* B. Brenner. Defining cloud security: Six perspectives. <http://www.networkworld.com/news/2009/092909-defining-cloud-security-six.html> , 2009.
* Tom N. Jagatic , Nathaniel A. Johnson , Markus Jakobsson , Filippo Menczer, Social phishing, Communications of the ACM, v.50 n.10, p.94-100, October 2007.