Trends in Information Security

Topic Description: Security in the Cloud

Prof. Chris Johnson,
School of Computing, University of Glasgow.
Johnson@dcs.gla.ac.uk
http://www.dcs.gla.ac.uk

Introductions

Cloud computing services can be categorized in three types: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Clouds can also be public – open to subscribers; or private – where access is restricted to a small number of users. Irrespective of the type of Cloud there are a number of open research questions. Some of these are described below but in general they focus on issues of trust. If you buy computing infrastructure as a service from a third party then you may not know the hardware and software infrastructures that are used to secure your data. Conversely, Cloud service providers may only have limited access to the application software that is being run by the customers who pay for their services.

Different Perspectives

The introduction has summarised a few of the concerns that have been raised about the security of Cloud systems. Access control is critically important to ensure that different users cannot access the resources of other customers supported by the same Cloud service provider.

The proponents of Cloud services argue that these platforms offer significant security benefits. In general, many companies lack the resources to hire security specialists. In consequence, patches and updates are often delayed. However, Cloud service providers tend to have access to significant security expertise, justified by economies of scale because many end users rely on their infrastructures.

Open Research Questions

It is difficult to derive objective data on the vulnerability of Cloud infrastructures, although there have been a number of high-profile attacks/incidents.

- Security Mechanisms.
  Given the importance of security to both service providers and customers, a significant amount of research has been conducted into the access control mechanisms and associated techniques that ensure the separation of processes across Cloud infrastructures. The virtualizer is a particular focus as it controls the migration of processes across shared computational resources.

- Incident Reporting for the Cloud.
  There is a significant amount of research across Europe in particular from ENISA to develop common incident reporting systems for critical Clouds. This raises significant questions about how to report an incident when a customer might buy services from a Cloud service provider who is based in another country and whose servers are in a third state.

- Risk Perception and the Cloud.
  There is a lack of data on the relative security of Cloud infrastructures. In consequence, investment decisions are often based on subjective assessments of the risks associated with the adoption of new technologies. A number of researchers are working on techniques that help companies to make informed decisions about whether or not to hold critical data in Cloud architectures.

This is a partial list; feel free to look at other more specific areas but talk to me about any particular concerns or ideas that you might have.

References

European Network and Information Security Agency (ENISA), Cloud Computing Security Risk Assessment, Heraklion, Greece, 2009. Available from http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment, accessed December 2013.

European Network and Information Security Agency (ENISA), Critical Cloud Computing-A CIIP perspective on cloud computing services, Heraklion, Greece, February 2013. Available from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing, accessed December 2013.

National Institute of Standards and Technology (NIST), NIST Cloud Computing Standards Roadmap, Washington DC, USA, July 2013. Available from http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf, accessed December 2013.

National Institute of Standards and Technology (NIST), Guidelines on Security and Privacy in Public Cloud Computing (NIST Special Publication 800-144), Washington DC, USA, 2012. Available from http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909494, accessed December 2013.

S. Pearson, A. Benameur, Privacy, Security and Trust Issues Arising from Cloud Computing, IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), 2010 Nov. 30 2010-Dec. 3 2010, 693 – 702, Digital Object Identifier :10.1109/CloudCom.2010.66.

S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, Volume 34, Issue 1, January 2011, Pages 1-11, ISSN 1084-8045, http://dx.doi.org/10.1016/j.jnca.2010.07.006.

Ashley Chonka, Yang Xiang, Wanlei Zhou, Alessio Bonti, Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks, Journal of Network and Computer Applications, Volume 34, Issue 4, July 2011, Pages 1097-1107, ISSN 1084-8045, http://dx.doi.org/10.1016/j.jnca.2010.06.004.