CLOUD COMPUTING SECURITY

Mesut Kose

Design of Secure Operating Systems

What is Cloud Computing?

- A model to enable convenient, on demand network access to a shared pool of configurable computing resources.
- Cloud Deployment Models:
  - **Private Cloud**: The cloud infrastructure is operated for a private organization. It may be managed by the organization or a third party.
  - **Community Cloud**: The cloud infrastructure is shared by several organizations and supports a specific community that has communal concerns such as security, policy and compliance considerations.
  - **Public Cloud**: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
  - **Hybrid Cloud**: The cloud infrastructure is a composition of two or more clouds that remain unique entities, but are bound together by standardized or proprietary technology, that enables data and application portability between clouds.

Cloud Computing Security

- Integrity means that assets can be modified only by authorized parties or in authorized ways and refers to data, software and hardware.
- Authorization is the mechanism by which a system determines what level of access a particular authenticated user should have to secured resources controlled by the system.
- Software Integrity refers to protecting software from unauthorized deletion, modification, theft or fabrication.
- In the cloud, responsibility for the protection of the software's integrity is transferred to the software's owner or administrator.

Cloud Computing Security

- Security in general, is related to the important aspects of confidentiality, integrity and availability; thus they become building blocks in designing secure systems.
- Multitenancy refers to the cloud characteristic of resource sharing.
- Data confidentiality in the cloud is correlated to user authentication.
- Software confidentiality refers to trusting that specific applications or processes will maintain and handle the user's personal data in a secure manner. In a cloud environment the user is required to delegate "trust" to applications provided by the organization owning the infrastructure.
- Privacy is the desire of a person to control the disclosure of personal information.

Cloud Computing Security

- Trust in a cloud environment depends heavily on the selected deployment model.
- Perimeter Security is a set of physical and programmatic security policies that provide levels of protection on a conceptual borderline against remote malicious activity.
- Separation is the key ingredient of any secure system, and is based on the ability to create boundaries between those entities that must be protected and those which cannot be trusted.
- Trusted Third Party within a cloud environment by enabling trust and using cryptography to ensure the confidentiality, integrity and authenticity of data and communications, while attempting to address specific security vulnerabilities.

Trusted Third Party

- In cryptography, a Trusted Third Party (TTP) is an entity which facilitates secure interactions between two parties who both trust this third party.
- TTPs are operationally connected through chains of trust (certificate paths) in order to provide a web of trust forming the notion of a Public Key Infrastructure (PKI).
- PKI implemention models: Strong Authentication, Authorization, Data Confidentiality, Data Integrity and Non-Repudiation.
- PKI in a distributed information system benefits from the coupling with a directory.
- In a Single-Sign-On (SSO) environment, a user does not need to repeatedly enter passwords to access resources across a network.

Trusted Third Party

- Cryptographic separation of data requires SaS and AaS models.
- Confidentiality and integrity, but also privacy of data can be protected through encryption. Using a combination of asymmetric and symmetric cryptographic can offer the efficiency of symmetric cryptography while maintaining the security of asymmetric cryptography.
- Certificate Based authorization
- In a cloud environment, the relationship between resources and users is more dynamic, resource providers and users are not in the same security domain, and users are usually identified by their characteristics or attributes rather than predefined identities.
- Attribute based access control, making access decisions based on the attributes of requestors, resources, and the environment, provides the flexibility and scalability that are essential to large-scale distributed systems such as the cloud.

Trusted Third Party

- PKI enables implementing IPSec or SSL for secure communications. IPSec is an IP layer protocol that enables the sending and receiving of cryptographically protected packets of any kind (TCP, UDP, ICMP, etc.) without any modification.
- SSL protocol generates end-to-end encryption by interfacing between applications and the TCPIP protocols to provide client–server authentication and an encrypted communications channel between client–server.
- IPSec is compatible with any application but requires an IPSec client to be installed on each remote device (PC, PDA, etc.) to add the encryption.
- Single-Sign-On is critical for server and client authentication.
- To maximize interoperability between communicating parties, it is a necessity to adopt widely used standards. Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization of data between security domains.

Conclusion

- This presentation attempts to propose a security solution to a number of challenges in a cloud environment by trusting a Third Party.
- Trust essentially operates in a top-down fashion, as every layer needs to trust the layer immediately below it, and requires a security guarantee at an operational, technical, procedural and legal level to enable secure communications with it.
- A trusted certificate serves as a reliable electronic “passport”
- With the developing technology, Cloud environment will improve and offer better solutions to security issues.

Works Cited

- K. Stanoevska-Slabeva, T. Wozniak
- **Grid and Cloud Computing-A Business Perspective on Technology and Applications**
- Springer-Verlag, Berlin, Heidelberg (2010)
- National Institute of Standards and Technology, The NIST Definition of Cloud Computing, Information Technology Laboratory, 2009.
- E. Naone, Technology overview, conjuring clouds, MIT Technology Review, July–August, 2009.
- Merrill Lynch, The cloud wars: $100+ billion at stake, Merrill Lynch, 2008.
- D. Harris, Why 'grid' doesn't sell, 2008.
- G. Reese
- Cloud Application Architectures: Building Applications and Infrastructure in the Cloud, Theory in Practice, O'Reilly Media (2009)
- B. Rajkumar, C. Yeo, S. Venugopal, S. Malpani
- **Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility**
- Future Generation Computer Systems (2009)
- D. Artz, Y. Gil
- **A survey of trust in computer science and the semantic web**
- Journal of Web Semantics: Science, Services and Agents on the World Wide Web (2007)
- DoD Computer Security Center, Trusted computer system evaluation criteria, DoD 5200.28-STD, 1985.
- A. Nagarajan, V. Varadharajan
- **Dynamic trust enhanced security model for trusted platform based**
- Future Generation Computer Systems (2010) http://dx.doi.org/10.1016/j.future.2010.10.008

Works Cited

- International Telecommunication Union, X-509 | ISO/IEC 9594-8, The directory: Public-key and attribute certificate frameworks, ITU, X-Series, 2001.
- D. Lekkas
- **Establishing and managing trust within the public key infrastructure**
- Computer Communications, 26 (16) (2003)
- A. Giddens
- **The Consequences of Modernity**
- Polity Press, UK (1991)
- K. Tserpes, F. Aisopos, D. Kyriazis, T. Varvarigou
- **Service selection decision support in the Internet of services**
- Economics of Grids, Clouds, Systems, and Services, Lecture Notes in Computer Science, vol. 6296 (2010), pp. 16–33 http://dx.doi.org/10.1007/978-3-642-15681-6_2
- R. Sherman
- **Distributed systems security**
- Computers & Security, 11 (1) (1992)
- D. Lekkas, S. Gritzalis, S. Katsikas
- **Quality assured trusted third parties for deploying secure Internet-based healthcare applications**
- International Journal of Medical Informatics (2002)
- National Institute of Standards and Technology. Guide for mapping types of information and information systems to security categories, NIST 800-60, 2008.
- Gartner. Assessing the security risks of cloud computing, Gartner, 2008.
- Cloud Security Alliance. Top threats to cloud computing, Cloud Security Alliance, 2010.
- R. Sherman
- **Distributed systems security**
- Computers & Security, 11 (1) (1992)

Works Cited

- D. Polemi
- **Trusted third party services for health care in Europe**
- Future Generation Computer Systems, 14 (1998), pp. 51–59
- S. Castell, Code of practice and management guidelines for trusted third party services, INFOSEC Project Report S2101/02, 1993.
- Commission of the European Community. Green paper on the security of information systems, ver. 4.2.1, 1994.
- VeriSign. Directories and public—key infrastructure (PKI), Directories and Public—Key Infrastructure, PKI.
- A. Alshamsi, T. Saito
- **A technical comparison of IPSec and SSL**
- Cryptology (2004)
- Cloud Identity Summit, Secure the cloud now, Cloud identity summit, Retrieved on 10/11/2010 from: http://www.cloudidentitysummit.com/.
- Internet 2, Shibboleth [Online] 2007, Retrieved on 10/11/2010 from: http://shibboleth.internet2.edu/.
- Internet 2, FAQ on SAML and Shibboleth relationship, Shibboleth, Internet 2, 2010. Retrieved on 10/11/2010 from: http://shibboleth.internet2.edu/Shibboleth-SAML-FAQ.html.
- UK Federation Information Centre, UK federation information centre, 2007.
- C.P. Pfleeger, S.L. Pfleeger
- **Security in Computing**
- Prentice Hall (2002)
- B. Lang, I. Foster, F. Siebenlist, R. Ananthakrishnan, T. Freeman, Attribute based access control for grid computing, 2008.
- James B.D. Joshi, Walid G. Aref, Arif Ghafoor, Eugene H. Spafford
- **Security models for web-based applications**