Research Proposal

By: Ian Edington
Student ID: 3236986
Date: July 28th, 2017

Barriers of implementing a Trusted Computing Platform in a Public Cloud Environment

In recent years there has been a shift in enterprise computing platforms away from private data centers to cloud providers. A cloud provider is a company that provides a data center that hosts virtual machines from many companies. Because of the economies of scale these providers are better able to utilize system resources. This shift has brought with it flexibility, reduced cost, and in general better security, but it has also introduced a security concern that was non existent in private data centers. In a private data center a company controls everything including the physical security, the hardware, the operating system, all the way up to the applications running on that system. However, In a cloud environment the company doesn't control the physical security, the hardware or the Virtual Machine Manager(VMM).

Although working with a trusted cloud provider is sufficient in most cases, having assurances of control is necessary for certain applications, especially in the finance, healthcare, and public sectors. Two types of security assurances are required in order to confirm the integrity of a system. Accreditation of the physical, hardware, and software solutions through third party audits, and software assurances that an application is running on the platform it is expected to run on. Accreditation of systems has largely been solved, but the challenge of an untrusted system to prove it's trustworthiness is still unsolved.

This paper will explore the technical challenges for VMM in cloud providers and virtual machine operating systems, in providing a trusted platform.

References

[1] Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences, 305,* 357-383.

[2] International Organization for Standardization. (2015). *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services(ISO/IEC FDIS 27017)*.

[3] Tomlinson, A. (2017). Introduction to the TPM. In *Smart Cards, Tokens, Security and Applications* (pp. 173-191). Springer International Publishing.

[4] M. Achemlal and S. Gharout and C. Gaber. "Trusted platform module as an enabler for security in cloud computing." *Conference on Network and Information Systems Security (SAR-SSI)*, 2011, pp. 1-6.

[5] Achemlal, M., Gharout, S., & Gaber, C. (2011, May). *Trusted platform module as an enabler for security in cloud computing. In Network and Information Systems Security (SAR-SSI)*, 2011 Conference on (pp. 1-6). IEEE.

[6] Bursuc, S., Johansen, C., & Xu, S. (2017). *Automated verification of dynamic root of trust protocols (long version).* arXiv preprint arXiv:1701.08676.

[7] Chiregi, M., & Navimipour, N. J. (2017). *A comprehensive study of the trust evaluation mechanisms in the cloud computing.* Journal of Service Science Research, 9(1), 1-30.

[8] Tang, M., Dai, X., Liu, J., & Chen, J. (2017). *Towards a trust evaluation middleware for cloud service selection.* Future Generation Computer Systems, 74, 302-312.

[9] Selvaraj, A., & Sundararajan, S. (2017). *Evidence-Based Trust Evaluation System for Cloud Services Using Fuzzy Logic.* International Journal of Fuzzy Systems, 19(2), 329-337.

[10] Braga, B., & Santos, N. (2016, June). *P-Cop: A Cloud Administration Proxy to Enforce Bipartite Maintenance of PaaS Services.* In Cloud Computing (CLOUD), 2016 IEEE 9th International Conference on (pp. 888-893). IEEE.

[11] Lufei, Z., & Zuoning, C. (2017, April). *vStarCloud: An operating system architecture for Cloud computing.* In Cloud Computing and Big Data Analysis (ICCCBDA), 2017 IEEE 2nd International Conference on (pp. 271-275). IEEE.