Cloud Computing Security Requirements and Threats

Bin Yu

Submission date: 2013/5/31

Abstract

This paper aims to address the new security requirements and threats in cloud computing. Though cloud computing has been studied by many researchers, arguably many of the cloud threats they described in fact just reflect traditional web application and data-hosting problems. New security threats that exist in cloud computing have been seldom investigated. This study develops threats models for identify, classify these new threats. This development addresses the problem how to study and identify the new issues in cloud computing. After study these new threats, possible solutions will be proposed. This study represents an original contribution to addressing the new threats in cloud computing and proposing the possible solutions. It also provides the introduction to the new issues in cloud computing which can be used for further study.

Keywords:

Cloud security requirement, Cloud security threats, Multi-tenancy

I. Introduction

The security threats have been studied by many researchers. Firesmith (2004) provides taxonomy of security sub-factors that can be used as a basis for organizing and identifying different security threats. Many published papers focus on the security issues like web security (Biddle et al., 2009), data outsourcing and assurance (Bowers et al., 2009) and virtual machines securities (Wei et al., 2009). Subashini and Kavitha (2011) address the new threats in cloud computing, but not investigate these threats in a certain depth. Currently underlying issues remain well-established challenges such as phishing, downtime, data lost, password weakness, and compromised hosts running botnets. Arguably many of the cloud threats they described in fact just reflect traditional web application and data-hosting problems. New security threats that exist in cloud computing have been seldom investigated. At the same time, security has emerged as arguably the most significant barrier to faster and more widespread adoption of cloud computing.

II. Objectives

This study addresses the new security requirements and threats in Cloud Computing and proposes possible solutions for them. It aims to examine contemporary and historical perspectives from industry and academia, and concentrate on CC security issues that are fundamentally new or intractable like multi-party trust considerations and the ensuing needs for mutual audit ability. After study on these new threats, possible solutions are proposed. This study represents an original contribution to addressing the new threats in cloud computing and proposing the possible solutions. In practice, the study addresses the needs to pay more attention on flexibility and multi-tenancy in cloud computing (Subashini and Kavitha, 2011). In this regards, it contribute to the security researches in the new features of cloud computing. This study also provides the introduction to the new issues in cloud computing which can be used for further study. After study security requirements and threats, threats models will be built to identify, classify the threats. Based on this threats model, possible solutions will be given.

III. Methodology

To achieve this goal, this paper uses a general architecture of a cloud platform, which is called cloud stack (Aviram et al., 2010) to have a deep study of the security and threats in cloud computing. For the security investigation of cloud stack, we try

to answer three questions. a) What are the features of this stack level. b) What kind of security requirements and issues may exist in this level. c) What are the causes of these security issues. After this study we will identify the threats that exist only in cloud environments, which are called new security threats. For these security requirements and threats, threats models will be built to evaluate and manage these threats. According to different application, different solutions will be proposed (password is enough for some occasions, some occasions may also need encryption of data storage).

Using general cloud stack to classify threats is objective, because this architecture of cloud platform has been investigated and used by many publications. And many cloud environments are built under the instructions of this general cloud stack. This study will pay more attentions on features like flexibility and multi-tenancy in cloud computing. For different applications we propose different security strategy, this can best optimize the whole system's efficiency.

One Limitations of this methodology is that some new security threats are so complicated and have interactions with more than one cloud stack. This kind of issues cannot be easily classified into one fixed cloud stack easily. Another limitation is that the solutions we proposed may not solve the threats completely. As we only use general cloud stack to identify our issues. So the solutions we proposed may only reflect one aspect of the issue. It may need different models to work together to identify, classify and manage threats.

IV. Novelty

We argue that the cloud computing threats model we built include several novel elements, though the cloud stack which we use to identify the security threats are not new.

First, this paper regards data and software are not the only assets worth protecting. Activity patterns also need to be protected. Sharing resources means that the activity of one cloud user might appear visible to other cloud users using the same resources, potentially leading to the construction of covert and side channels. Activity patterns may also themselves constitute confidential business information. Some papers like (Bowers et al., 2009) though talks about the data protection issues, but it does not take activity patterns into consideration.

Second, this paper proposes a trust chain in cloud computing threats model. For example, the application end-user could potentially use an application built by software as a service provider, with the application running on a platform offered by a Platform as a service provider, which in turn runs on the infrastructure of an Infrastructure as a service provider. While to our knowledge this extreme example cannot occur in practice today due to a lack of sufficient APIs, it illustrates that with any model of cloud computing, stakeholders' can find themselves with relationships considerably more complicated than simply a provider-user relationship.

When we built the security threats model, we also take participants behavior into consideration. Cloud computing for the outside world is like a whole distributed system. Users behaviors may have a great influence on the whole cloud system. Some participants could be subverters, who maintain the appearance of a regular cloud user or cloud provider, but in fact perpetrate cybercrime or other cyber-attacks. Examples include cloud users who run brute forcers, botnets, or spam campaigns from the cloud or cloud providers who scan cloud users' data and sell confidential information to the highest bidder.

Furthermore, the threats model this paper built also considers the competitive businesses that operate within the same cloud computing ecosystem. Because using the same cloud or ending up in a provider-user relationship can lead to strong conflicts of interest, and creates additional motives to access the confidential information of a competitor.

Last but not least this paper regards most of the new security are from the inner of cloud computing system compared with outer of cloud computing system. The security requirements from outside of cloud have been discussed by many papers. However the threats within the cloud have been rarely discussed. These kinds of threats are

more destructive because as the traditional security model cloud itself often regarded in a trust area.

V.Conclusion and Significance

This study aims to address the new security requirements and threats in cloud computing. After studying the threats in cloud computing security models are built to identify, classify and manage the threats. With the help of security models possible solutions are proposed.

This study fills the gap of new security threats researches in cloud computing, as few solutions have been proposed in current publications. This study also addresses the significant of inner cloud computing environment security. As many solutions for security requirements are only care about the threats among transmission and user data safety.

This study represents an original contribution to addressing the new threats in cloud computing and proposing the possible solutions. In practice, the study addresses the needs to pay more attention on flexibility and multi-tenancy in cloud computing. In this regards, it contribute to the security researches in the new features of cloud computing. This study also provides the introduction to the new issues in cloud computing which can be used for further study.

References

AVIRAM, A., HU, S., FORD, B. & GUMMADI, R. Determinating timing channels in compute clouds. Proceedings of the 2010 ACM workshop on Cloud computing security workshop, 2010. ACM, 103-108.

BIDDLE, R., VAN OORSCHOT, P., PATRICK, A. S., SOBEY, J. & WHALEN, T. Browser interfaces and extended validation SSL certificates: an empirical study. Proceedings of the 2009 ACM workshop on Cloud computing security, 2009. ACM, 19-30.

BOWERS, K. D., JUELS, A. & OPREA, A. HAIL: a high-availability and integrity layer for cloud storage. Proceedings of the 16th ACM conference on Computer and communications security, 2009. ACM, 187-198.

FIRESMITH, D. Specifying reusable security requirements. *Journal of Object Technology,* 2004，3**,** 61-75.

SUBASHINI, S. & KAVITHA, V. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications,* 2011，34**,** 1-11.

WEI, J., ZHANG, X., AMMONS, G., BALA, V. & NING, P. Managing security of virtual machine images in a cloud environment. Proceedings of the 2009 ACM workshop on Cloud computing security, 2009. ACM, 91-96.