ICCT 2013
"The 3rd International Conference on Convergence Technology 2013"

Vol.2 No.1

- **Date:** July 3~6, 2013
- **Place:** Chiang Mai, Thailand
- **Co–organized by:**
  - Korea Convergence Society
  - NTIS Division and GSDC Center at Korea Institute of Science and Technology Information (KISTI)
  - Korea Institute of Information, Electronics and Communication Technology
  - IT Convergence Society for SMB
  - The Society of e–Learning
  - The Korea Society of Digital Policy & Management
  - The Korean Association for Comparative Government
  - Xian Jiaotong–Liverpool University, China

- **Sponsored by:**
  - KISTI NTIS Division & GSDC Center, Selim Technical Service Group (Co.), SK Telecom Co., Ltd,
  - KYUNGDOONG Co., Ltd, LG CNS, MA Information Technology Co., Ltd, DUPLEX Co., Ltd., Informade Co., Ltd,
  - SANE Co., Ltd., ALLFORLRND Co., Ltd, DongHaTech Co., Ltd, KTNET, LOTTE Data Communication
  - Company, SUNGWON Information Technology Co., Ltd, Korea IT Consulting Co., Ltd, UNIEVER Co., Ltd,
  - UCUBE Co., Ltd, Daewoo Information System Co., Ltd, LG Hitachi, LG N–sys INC., Hanbit Media, Inc.,
  - Samsung SDS, SK C&C, Hyundai Information Technology Co, Ltd., Innogdn, Inc, GS Intervision, Blueriver,
  - APPLTEK, WithUSTech Co., Ltd, SEJOONG Information Co., Ltd, I&T Inc, HIMS, DAEILIM Co. Ltd,
  - BOKANG SYSTEM Co., Ltd,

KCS KOREA CONVERGENCE SOCIETY
http://www.kcons.or.kr
44. w-15-01_Design of Mobile-based 3D e-Learning Framework  
   Jung Soo Han(Baekseok University), Kee Nam Choi(Semyung University), Gui Jung Kim(Konyang University)

45. w-15-02_An Predictive Analytics of Business Model for Self-Adaptive Software  
   Su-Jin Baek(BaekSeok University), Sung-Ho Sim(Semyung University)

46. w-15-03_Change Management using multi-Agent Message Technique  
   Kyoung-Hun Kim(Gandong College), Tae-Won Kyung(R&D PatentCenter), Sang-Ho Na(Kyung Hee University),  
   Ga-won Lee(Kyung Hee University), Gyeng-Taek Yu(Gangdong College)

47. w-15-04_A Study on Meta-Collector for Web Services Selection meta-matching Information Extraction  
   Sung-Ho Sim(Semyung University), Su-Jin Baek(BaekSeok University)

48. w-15-05_Threats Evaluation for SLAs in Cloud Computing  
   Sang-Ho Na(KyungHee Univ), Kyoung-Hun Kim(Gang Dong College), Eui-Nam Huh(KyungHee Univ)

49. w-15-06_Cloud-based Smart Home System (CbSH) Architecture Design for Virtual Home Gateway and Cloud Interworking  
   Ga-Won Lee(Kyung Hee University), Sang-Ho Na(Kyung Hee University), Kyoung-Hun Kim(Gangdong College),  
   Eui-Nam Huh(Kyung Hee University)

50. w-15-07_A Study on Security Scheme in 13.56MHz RFID Environments  
   Jungho Kang(Soongsil University), Hyungjoo Kim(Soongsil University), Moonseog Jun(Soongsil University)

51. w-15-08_Refundable Cloud Service Architecture for Smart Brokering  
   Young-Rok Shin(Kyung Hee University), Myeong-seob Kim(Kyung Hee University),  
   Kyoung-Hun Kim(Gangdong College), Eui-Nam Huh(Kyung Hee University)

52. w-15-09_Access Control Framework Design for Personal Cloud  
   Jun-young Park(Kyung Hee University), Young-rok Shin(Kyung Hee University),  
   Kyoung-hun Kim(Gang Dong College), Eui-nam Huh(Kyung Hee University)

53. w-15-10_Mobile VDI Performance Optimization with Hybrid Parallel Computing and System Level Hooking  
   Myeong-seob Kim(Kyung Hee University), Jun-young Park(Kyung Hee University),  
   Kyoung-hun Kim(Gang Dong University), Eui-nam Huh(Kyung Hee University)
Abstract: Explosive growth of the cloud computing drives the cloud paradigm shift to cloud collaboration and mobile cloud. This tendency that security is getting more complex in cloud computing becomes more pronounced as time passes. In this sense, numerous studies have attempted to address security Service Level Agreements. The purpose of this paper is to discuss a methodology of how quantized and evaluated security threats employing hierarchy model in user perspective for the security SLAs and measures weight values of each security threat to consider which security controls are required to meet the needs of a user’s security SLAs.

Keywords: Cloud, Threats Evaluation, SLA

1. Introduction

Emerging cloud collaboration services based on mobile devices seem to be very efficient and effective solution to manage and access the data. But, we have to bear in mind that the security vulnerability and risk, especially regarding the privacy and data lose, have been increasing. Increasing a service complexity make a need of Service Level Agreement (SLA) arise and traditional security aspects such as integrity and confidentiality also should be covered by SLA to give convincing answers to users how their data are securely managed and ensured.

In this paper, we will provide security threats evaluation model to be used for negotiating the security SLAs and measure the threats. This paper organized as follows: In section 2, we will introduce related works, and then we will propose hierarchy model and describe threats correlation model in section 3. The threats are analyzed based on relative priorities in section 4. Section 5 concludes our approach and describe future works.

2. Related Works

A Security vulnerability of cloud computing has been given a considerable attention in recent years [1]. The studies in [2, 3] illuminated the question of how cloud providers could cover security aspects that a user wants such as integrity and confidentiality in SLA perspective and outlined well about security controls. As has been noted by [3], cloud security SLAs are negotiated between user and cloud providers. A part of this view is particular important in regard of current emerging world cloud collaboration service market [4].

Among the various articles of the Cloud Security Alliance (CSA), “The Notorious Nine” [5] provides top threats ranking, implications and security controls based on a survey of industry experts. That ranking did not considered a correlation between threats but implication of security breach. To satisfy specific security SLAs of users’, the security aspects should be addressed in users’ point of view.

3. Threats Evaluation Methodology

To negotiate the specific security SLA, above all things is evaluate relative importance of security aspects like threats ranking of the CSA. We will discuss here how to measure the security threats in user perspective. Before going on with the question of how to negotiate security SLA, it should be define specific elements such as threats, security aspects and etc.

3.1 Define of Security Threats & Aspects

We considered threats correlation in user perspective and sorted five from the nine top threats of CSA. The five threats are Data Breaches (DB), Data Loss (DL), Account Hijacking (AH), Insecure APIs (API), and Malicious Insiders (MI). After that, we categorized security aspects (figure 2) regarding SLA within a framework for security mechanisms [3]. The figure 1 shows correlated threats’ implication. For an example of threats correlation is that an insecure APIs might break into a user’s account, and then her data will disappear permanently from cloud.

3.2 Establish Priorities of Security Threats

The priorities of each threat means relative importance among of threats. We suggest constructed hierarchy model (figure 2) employing an Analytic Hierarchical Process...
(AHP) which is mathematical and psychological based decision-making technique by Saaty in 1971.

The criteria are evaluation bases to decide security aspects within alternative and the each criterion has weight values which presents the relative importance between threats.

4. Threats Evaluation

According to the AHP methodology, there are many types of relations between elements such as criteria, alternative. The one has independence condition and another one has subordinate to the one or more other elements. The CSA ranking is a result by the former that has independence condition between threats. Whereas our approach is employed subordinate AHP that is considered threats correlation.

The pair comparison matrix of \( T \) regarding to the criteria is \( T = (t_{ij}) \), \( t_{ij} = 1 \) and \( t_{ji} = 1/t_{ij} \) is a reciprocal matrix. The dominant eigen vetor of \( T \) is \( W_c = (W_{DB}, W_{DL}, W_{AH}, W_{API}, W_{MI}) \) where are weight values (Priorities base) and presented in table 1 as CSA. We calculated a dominant eigen vetor \( W_c' \) considered impact between threats. The \( W_c' \) is a pair comparison matrix of impact in respect of threat \( t \).

<table>
<thead>
<tr>
<th>Table 1. Dominant Eigen Vetor</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSA</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td>0.5120</td>
</tr>
<tr>
<td>0.2619</td>
</tr>
</tbody>
</table>

\[ W_c' = W_c \times (W_{DB}' W_{DL}' W_{AH}' W_{API}' W_{MI}') \] where are shown in table 1 as Proposed. The consistence index (CI) value of \( W_c' \) are (0.0194API, 0.0279AH, 0.0271MI, N/A DL, 0.0271DB) which are lower than 0.1, where the CI of \( T_{API} \) is not available according to the figure 1.

When a dominant eigen vetor \( W_c' \) in respect of impact \( p=1 \) between threats is \( [W_c']_1 \),

\[ \lim_{n \to \infty} [W_c']_1 = (0.3220API, 0.6780MI, 0DL, 0DB) \]

It means that the most of security breaches begin from the essential elements such as insecure API and malicious insider. The API is the essential element of technology to deliver service to users and the MI which is human resource is the fundamental element to deal with technology. Human resource, consequently, is more important than technology. This result recalls us that managing human resource is the starting point of security.

5. Conclusion

This paper has employed constructed hierarchy model to evaluate security threats and attempted to establish priorities based on AHP approach. This study lays the foundation for future work on SLAs negotiation scheme.

Acknowledgements

This research was supported by Next-Generation Information Computing Development Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (2012-0006418)

6. References