Sparse Matrices Technologies for APT Counter Measures

Vectors Components Contstruction

ABDULLAH SAID ALI AL AAMRI (*Author*)
Master Student: Information Systems Department.
University of Nizwa, UoN
Berkat AL-Moz, Oman

Mourad Henchiri (Co-*Author*)
Lecturer: Information Systems Department.
University of Nizwa, UoN
Berkat AL-Moz, Oman

***Abstract*— In today's world, almost all sectors either they are big, medium or small tend to use economical computing resources in their business applications by including could computing technology. It is widely accepted that cloud computing improves the performance in the organization by utilizing minimum shared resources and management support. Cloud computing is known as a set of Information Technology services that are provided to people over the Internet with the advantages of low cost, Accountability, Scalability, Reliability, Flexibility, and Efficiency.**

Security is one of the hottest topics in our daily discussions and it is the main concern for all organizations who want to use cloud services. The design of a framework for cloud computing security is proposed in this research to decrease the attacks and safeguards the information from damage by hackers.]

Keywords—APT;Cloud Computing; Accountability; Scalability; Reliability; Flexibility; Efficiency

I. INTRODUCTION (*HEADING*)

Cloud Computing technology provide consumers with services, applications, solutions and for storing large amount of data from anywhere at any time. Also, cloud computing data centers may lie in any area of the world beyond the reach and control of users. But even there is an increase in the using of cloud services in the world, there are on the other side a big growth in the security risk which has become the hot topic for today's specialists . So, users who mostly used to have the public cloud services which are not clear to them where the data is stored and who is managing it? Adding to that the issues which are recently raised regarding the security threats; the result is to have customers worried and not confidently trusting the cloud service providers.

Internet services are facing security issues and attacks which are the same ones facing Cloud Computing structure like denial off service attack, man in the middle attack, network sniffing, port scanning, SQL injection attack, cross site scripting. Also, there are security issues that occur in Cloud Computing e.g. XML signature element wrapping, browser security, flooding attacks, data protection, locks in etc . Each issue presented so far is recognized as soft practice, which are basically made by a failure in a pre-set configuration such as lack of security materials and appliances, lack in expertise for manipulating existing hard infrastructure; and missing in software requirements or even hardware. Therefore, an elaborate structure and configuration for the cloud deployment might lead reducing the likelihood of facing the above mentioned security issues.

II. VECTORS COMPONENTS

A. *People*

First, people vector has compromised its view and concern to the relation between people and APT awareness. And it's made of five components which are:

- Insider threat Awareness
- Security Awareness & Training
- Cyber skill set
- Management Support
- Information Security Management

B. *Process*

Secondly, process is a vector which is about the rules and privileges related to the security standards and how the firms are admitting the AAA standard. And it's made of eight components which are:

- Security Standards Usage
- Implementing Rules & Privileges
- Supply Chain Security Process
- Trust Behavior
- Auditing Process
- Authorization Process
- Authentication Process
- Legal Compliance Risk Process

C. *Technology*

Thirdly, technology is a vector taking care of hard and soft appliances available within firms' infrastructure in the Sultanate of Oman environment. And it's made of eleven components which are:

- Access & Identity Management Mechanism

- Data Loss & Leakage Prevention
- System Recovery & Continuity Tools
- Data Integrity Tools
- Data Availability Tools
- Data Confidentiality/Privacy Tools
- Security Operation Tools (SOC)
- Software Signing
- Networking Monitoring
- Audit and Vulnerability Assessment
- Security Appliances

D. *Legalization*

Fourthly, legalization is a vector designed to recognize how different firms are compliant to the different laws and regulations in addition to the international security standards (ISO27001). And it's made of eight components which are:

- Preset laws
- Legal Aspects (SLA)
- Legal Compliance
- Law Issuance (Government Body)
- Cyber Crime Law
- Law Spectrum (Usage Validity)
- Data Privacy Laws
- International Compliance – ISO27001

III. Analysis of the Satisfaction Survey

A. *Design*

The survey design was done with Google Forms online survey software and also paper handed copies. The questionnaire was designed during the one month before it went online[.

The survey included questions with conditional branching, that is to say, questions not concerning all users and not to appear as if the user chose the conditional response to a question attached specifically. This option would have made the questionnaire still much longer since each conditional issue forced to create a new subtopic . We therefore chose to leave exposed all questions to limit the questionnaire to four different categories, corresponding to four logical parts. This has not always been well understood by users, as some have responded to all questions, even those that were not there for the light of their previous answers .

Some questions induced a mandatory answer and some not, including open questions.

The selected software and also the paper handed copies allowed users to change answers. This option has been used in some cases for moving an answer "neutral" to a pre-established questionnaire response that people had not seen, or not understood, or because the "neutral" response allowed them to add details[.

B. *Collecting responses*

The Site Satisfaction Survey "Designing secure framework for cloud computing and counter measure the advance persistent Threat (APT) using sparse line matrix approach" took place between June 2016 Till end of September 2016, a ninety days. The collection of answers was done through :

- a link in the Google Forms portal,
- by email (mailing list Google Forms)
- paper copies drafted by hand to different categories of users.

The first two collectors have gathered a minority of results: 20 against 223 for the paper copies. 243 people completed the survey questionnaire .

Approximately 10 additional responses were deleted because the questionnaire was not completely filled. These Partial responses could indeed not be taken into account because it was difficult to differentiate between users who properly met the first pages of the investigation and whose answers could be exploited, those who were only open the questionnaire by answering randomly to the first questions. In both categories there could also find returnees subsequently answer the entire survey.

Finally, among those 10 four are questionnaires were discarded because the answers could not be considered as serious .

C. *RESULTS ANALYSIS*

Foreword

It is important to note that this APT related survey was designed, as its name suggests, to know the knowledge of the users toward the threats caused and generated by the APTs and not to know, in full, of the public within the sultanate of Oman .

Website visitor statistics indicate that in the starting of December they started responding, the site received 20 unique replies. Over the same period, only 90 users responded to the full questionnaire. This survey represents a public accustomed, motivated, involved or attached to the topic; APT and computing security related issues. They know the APT and for the most of the views, suggestions to be issued. The quality of the responses we watched .

People (questions 2-

The first part consisted of 9 related questions aimed above all to know the awareness level about APT among people and the support provided by the higher management authorities within the targeted administrations.

To the question "Third party services are a trust for your sensitive data?, "49.8% of responses indicate the " Disagree ", "28.8%" of responses indicate the “Agree” and "21.4%" of responses indicate the “Neutral ".

To the question "How much you agree that your organization will be the target of an APT?"6.2%" of responses indicate the "Disagree ", "60.1%" of responses indicate the "Agree" and "33.7%" of responses indicate the "Neutral".

To the question "Executive management within your organization is becoming more involved with cyber security activities as a result of fair of potential of APT attacks?"6.2%" of responses indicate the "Disagree ", "64.2%" of responses indicate the "Agree" and "29.6%" of responses indicate the "Neutral".

The processes (questions 11-

Three closed questions on existing processes on the field (organizations and firms and institutional organizations) aimed to evaluate these processes, but also to inform the users of the APT attacks.

The first question was about the Rules and privileges related to the security standards and how the firms are admitting the AAA standard "You have an information security incident response team working 24/7?" 243 users answered, about ?"37%" of responses indicate the "Disagree ", "35.8%" of responses indicate the "Agree" and "27.2%" of responses indicate the "Neutral".

To the question "You have multi-tenancy authentication for identity process?"7.8%" of responses indicate the "Disagree ", "57.2%" of responses indicate the "Agree" and "35%" of responses indicate the "Neutral".

Technology (questions 21-

The aim of this section is to know the limits of the awareness about the existence and the positive usage of the security appliances and software. The question "You are using isolated computers for certain sensitive data?"31.3%" of responses indicate the "Disagree ", "52.2%" of responses indicate the "Agree" and "16.5%" of responses indicate the "Neutral".

To the question "Our digital environment is equipped with respective hard and soft mechanism for incident management?"5.8%" of responses indicate the "Disagree ", "70.8%" of responses indicate the "Agree" and "23.4%" of responses indicate the "Neutral".

Legal (questions 35-

The aim of this section is to recognize how different firms are compliant to the different laws and regulations in addition to the international security standards (ISO27001). The question "You do agree that all sectors is the country (e.g health, finance, energy, education, etc.) are compliant to the law?"6.6%" of responses indicate the "Disagree ", "70%" of responses indicate the "Agree" and "23.4%" of responses indicate the "Neutral".

To the question "Your organization is an ISO27001 certified?"23.5%" of responses indicate the "Disagree ", "27.2%" of responses indicate the "Agree" and "49.3%" of responses indicate the "Neutral".

IV. Survey Quality Measures:

To build the sparse matrix, parameters are selected; and subdivided into four sections. Those parameters have been revised by different security specialists from different firms and institutions including Nizwa University, ITA-ISD, ISACA, and SQU.

Based on those parameters question has been extracted after a long discussions and meetings with those different specialists which took more than 7 months; from September 2015 till April 2016.

V. InsitiutionS received the survey:

- Middle East College
- SQU
- ITA
- ODP
- Muscat Higher Technology College
- Germany University in Oman
- Nizwa University
- Nizwa Technology College
- Nizwa Science Appliances College
- Ibri Technology College
- PDO
- Ministry of Commerce
- Royal Diwan
- Nizwa Islamic Bank
- Sohar Bank
- Oman LNG

VI. Survey results and analysis

Legalization	Results		
	Agree	Neutral	Not Agree
Preset laws	.	.	.
Legal Aspects (SLA)	.	.	.
Legal Compliance	.		.
Law Issuance (Government Body)	.	.	.
Cyber Crime Law	.	.	.
Law Spectrum (Usage Validity)	.	.	.
Data Privacy Laws	.	.	.
International Compliance – ISO27001	.	.	.

Technology	Results		
	Agree	Neutral	Not Agree
Access & Identity Management Mechanism	.		.
Data Loss & Leakage Prevention	.	.	.
System Recovery & Continuity Tools	.	.	.
Data Integrity Tools	.	.	.
Data Availability Tools	.	.	.
Data Confidentiality/Privacy Tools	.	.	.
Security Operation Tools (SOC)	.	.	.
Software Signing	.		.
Networking Monitoring		.	.
Audit and Vulnerability Assessment	.	.	.
Security Appliances	.	.	.

People	Results		
	Agree	Neutral	Not Agree
Insider threat Awareness	.	.	
Security Awareness & Training	.	.	.
Cyber skill set		.	.
Management Support	.	.	.
Information Security Management	.	.	

Process	Results		
	Agree	Neutral	Not Agree
Security Standards Usage		.	.
Implementing Rules & Privileges	.	.	.
Supply Chain Security Process	.		.
Trust Behavior	.	.	
Auditing Process	.	.	.
Authorization Process	.		.
Authentication Process	.	.	. %
Legal Compliance Risk Process	.	.	

VII. CONCLUSION

After testing the efficiency of detecting an APT behavior on a giving network by different methodologies, the final numeric factor, which is a value, concluded from a mathematical formula, which represents a linear equation, calculated to represent the positive or negative statuses. The final numerical value produced by the mathematical equation using the matrix that represents the four vectors mentioned in this research, is the status that has to be in the positive side to mention the safety and serenity of the treated network.

REFERENCES

Effective Sparse Matrix Representation for the GPU Architectures, International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.2, April 2012.

Sparsity: Optimization Framework for Sparse Matrix Kernels, *International Journal of High Performance Computing Applications* February 2004 vol. 18 no. 1 135-

W. Abu-Sufah and A. A. Karim, "Auto-tuning of sparse matrix-vector multiplication on graphics processors" in Supercomputing, pp. 151-164, 2013, Springer.

Y.-S. Kang, Y.-H. Chun, Y.-T. Shin and J.-B. Kim “A Study on the Application of Security Risk-based Airport Model to the IT Service Environment” International Conference on Future Information & Communication Engineering (ICFICE), (2014), pp. 339- .

J. M. Yang “A Review of NH Bank Cyber Attack” The Journal of Law, vol. 19, no. 2, (2011).

W. M. Shim “Nate portal for hacking incidents and Privacy Issues” The Journal of Issues & Issues (National Assembly Research Service), no. 282, (2011).

D. Y. LEE “A Study on Personal Data Hacking Case to build Corporate Security and Counter Strategy: Focused on HYUNDAI CAPITAL hacking case” Journal of Security Engineering vol. no. 4, (2013).

G. H. Gwon “Customer Information Leakage is the work of another company?” Weekly Donga no. August 13, pp. 30- .

Y. S. Chun “North Korea: South Korea's corporate computer network was hacked” Munwhailbo ( ) October 16.

H. C. Choi “An Access Control Based Privacy Protection Model in ID Management System” Journal of Internet Computing and Services, vol. 7, no. 1, ( ) pp. 1- .

D. R. Kim “Secure One-Time Password Authentication in Mobile Environments” The Journal of digital policy & management vol. 11, no. 12,