Guidelines to Develop a New Generalized Discriminate Secure network Model to Promote Secure and Optimal Network Communication in Institutions

K.GaneshKumar[#1] and Dr.D. Arivazhagan[*2]

[#]Research Scholar, NDE Centre, AMET University, 135 Kanathur, ECR, Chennai, India
*Professor, IT Department AMET University, 135 Kanathur, ECR, Chennai, India
[1]ganesheclipse@gmail.com [2] arivazhagand@hotmail.com

ABSTRACT - The computer network utilityis an important component in educational institutions as classes are conducted in smart classrooms, accessing study materials, conduct of online examinations, maintaining e-governance systems, etc., are getting in to day to day activities of Institutions. Nevertheless, assessment mark entries in online portals by Institutions, conducting online certification courses and conducting government examinations[1] are also taken places as Institutions' activities occasionally. Amidst all, the security of communication which must be ensured while communication takes place is not under such attention now a day. Users,inside the institutions often annoy because of insecurity, losing data, andambiguity caused by Hijacks, network errors and spamware attacks[2]. Network Hackers and Malware Programmers still stand in their position of making fail the systems and stealing the information even though very powerful tools such as firewalls, Anti spamwares, Anti viruses, etc., invented.In this scenario, guidelines comes out from the complete review with currently available anti spamware tools[3] are expected and that must produce the secure forts over the networks. In this paper a guideline for creating a new generalized discriminated secure e-governance model is proposed to keep the security ON until the network switched OFF. This guideline was devised after thorough scrutiny of rated antiviruses in all aspects and it has strong steps to prohibit the entire network from the attackers. Initially set of questionnaire were given to reputed institutions and obtained filled in questionnaire forms for bringing in to further process. With these, the guideline which provides how do keep the networks more secure could be devised as well.

KEYWORDS: Cyber security risk analysis, Guidelines, security policy, E-Governance

I. INTRODUCTION

Internet grows in rapid way; almost all departments throughout the globe come under the umbrella of Internet. Nothing is possible without Internet right from purchasing of grocery items to providing the security to the nations. Knowing Internet is an essential even for children those who are studying KGs. Reason was that they became a prominent mobile users as same as elders[4]. Many of the gaming industries have been focusing the kids in order to make excel profits. Besides, at every home, impacts of internet could be seen everywhere through the digitalization of appliances and its connectivity to somewhere which can be called as server[5]. This concept of connection among all devices which possess transducers is familiarly known as Internet of Things (IoT) now a day. IoT is a technology which could have a connection between Internet and internet. Now talk about internet, internet is a small type of Internet thatmust contain numerable nodes and they belong to the premises or the network paves entire city[6].

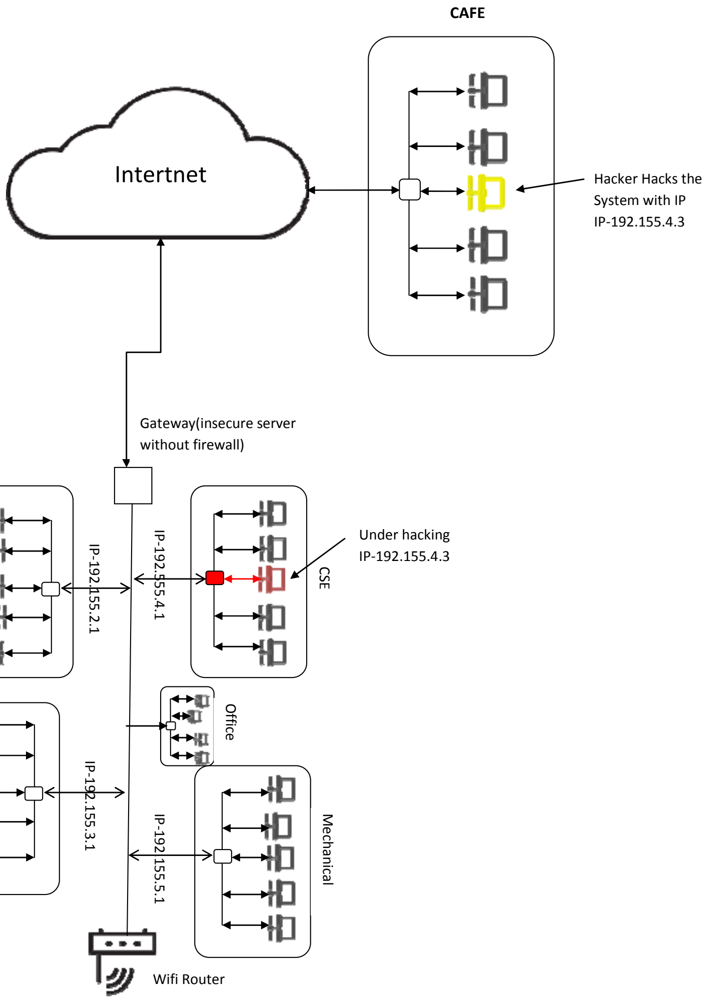
CAFE
Intertnet
Hacker Hacks the System with IP IP-192.155.4.3
Gateway(insecure server without firewall)
Under hacking IP-192.155.4.3
ECE
IP-192.155.2.1
IP-192.155.4.1
CSE
Office
CIVIL
IP-192.155.3.1
IP-192.155.5.1
Mechanical
Wifi Router

Figure1. Intruder steals data from the device in insecure network

The networks in institutions are affected a lot because of intruders and network errors. Which causes to data lose, connection loss, insecure environment[7], wastage of time since system hanging, delay at work, etc. with this institutions will not be able to have a consistent and durable network facility that they must have. Network security issues are identified in several circumstances as a route cause for lacking to provide consistent network[8]. Researches are carrying out in many places aim to keep the network in durable zone. But that researches have come with the question whether they have been achieved the aim or not, and the reason if not achieved. Since the technology grows both in right and unethical ways,no one can declare that they are in secure zone where intruders not able to get into. One's secure zone at present may become insecure soon[9]. So the deployment of anti-harming units is vain unless otherwise they get updated and upgradedoften as well. How the system faces failures to keep its data safe is clearly indicated in figure.1. The hacker sits in cafe and from there he could hack the system of any institution when it is not under secure pavement. In figure.1 a system with IP 192.125.4.3 is hacked for stealing data from the intruder who sits in cafe. Though the current scenario at several places as described above[10], In rated corporate various studies are taken for keeping the network safe and protecting the data with high privacy. The following topics cover the complete review concerning at most level of security to sort out the issues which are caused by insecure context[11].

II. AGGREGATING THE CURRENT SECURITY ISSUES

Despite the security issues raising in industries in such aspects the issues are threatening the institutions were taken in to account as our objectives have been established for that. Initially the questionnaire[12] was given to the institutions for assessing the issues which are currently in rates. Table I and figure2 show the questionnaire table and the flow chart of that respectively[13]. They show literally that the variance between the users and the maximum of answer taken in to account for further study extensions.

Table I. Questionnaire in Security Issues

Questions	**It**		**Ece**		**Mech**		**Eee**	
	Yes	**No**	**Yes**	**No**	**Yes**	**No**	**Yes**	**No**
Question 1	80	20	90	10	95	5	90	10
Question 2	70	10	80	10	90	5	80	10
Question 3	60	40	79	21	85	15	96	4
Question 4	55	5	75	4	84	1	94	2
Question 5	96	4	92	8	93	7	72	28
Question 6	84	16	95	5	95	5	82	18
Question 7	86	14	84	16	82	18	76	24
Question 8	80	6	74	10	75	7	70	6
Question 9	75	25	85	15	95	5	78	22
Question 10	97	3	98	2	99	1	90	10
Question 11	85	15	85	15	85	15	83	17
Question 12	76	24	75	25	84	16	91	9

The questions have been used for thorough assessment in the above questionnaire are

1)Have ever you felt hanging while using the system?

□ Yes □ No

2)If yes what it was happened to your pc / entire network?

□ Yes □ No

3) Have ever you suspecting any one steel your username and password, when you use the system inside the campus?

□ Yes □ No

4)If yes did you lose your username and password either in a particular system or anywhere in a network?

□PC □Network

5) Have ever you faced disturbance with unnecessary advertisements when browsing the internet?

□ Yes □ No

6) Did your browser home page change automatically?

□ Yes □ No

7) Are you allocated with unique IP?

□ Yes □ No

8) If yes do you suspect somebody using your system IP while your system is not in active?

□ Yes □ No

9)What are the necessary websites have been blocked in your institute?

□ Yes □ No

10) Are you not able to download necessary materials?

□ Yes □ No

11) Have ever you lost data because of viruses in the network?

□ Yes □ No

12) Are you using any internet security tools?

□ Yes □ No

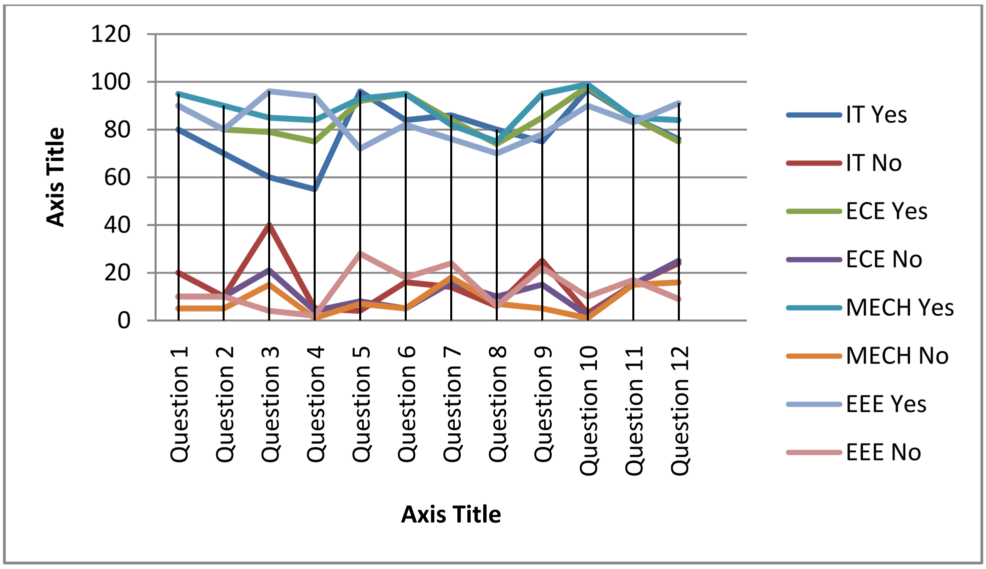

Figure2. Flow Chart drawn based Questionnaire

III. AWARENESS ON NETWORKS SECURITY AND THE INVADERS

Security is a process that protecting the things and not to get harmed. Things can be represented by any, they can be appliances, gadgets, PCs, PlayStations, [14]etc., basically the consumers don't have knowledge about the security due to lack of awareness in terms of How can we provide the security to any system and the importance?, and educate the consumer about security is a responsibility of one who provide users the device or an network to be used. Sometimes network security is concerned that the system gets failure even if it is under the network engineers or system engineers[15]. Hence the awareness about the security is necessary to those who are using the systems inside the organizations which can yield them at least withthe knowledge about preserving data as harmless. Here we describe the strategy for making awareness among the users inside the organizations and that comprises the following three 'P' levels in order to make the users bright in secure network maintenance.

1)Purpose : The purpose behind the security

2)Protection : The protection which can pave the network not to become harm

3)Persistence: The persistence which is to be followed to show consistency in network security

The above discussed three 'p's are to be conveyed to users briefly in between the establishment of network and the first user starts his work with the new network. Bringing awareness on Protection provide them an ignition to let them to enlarge their knowledge in counter action to safe their network[16]. The following are the simple way to get educated the users on security course that are already in the market.

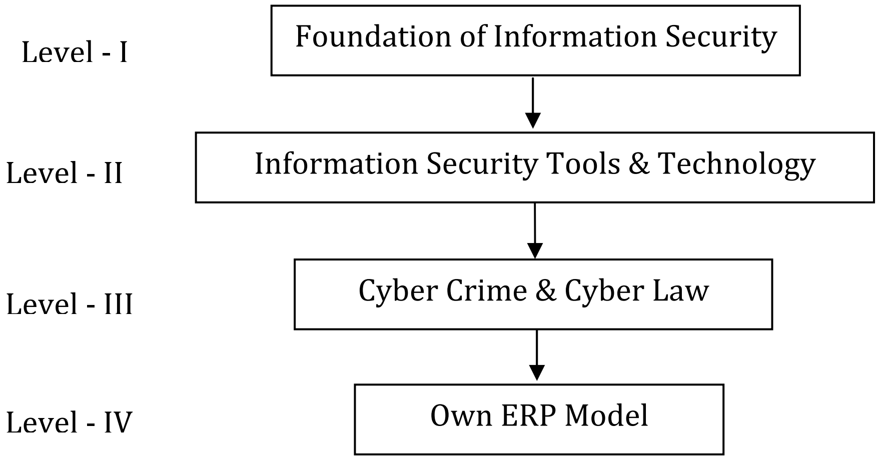

Figure 3. Security Awareness Model

In figure.3 the security model that provides awareness to the users' community are plotted clearly. Those four levels are influencing so much of elements which are useful to the network. Level-I consists of recent computer operating system, storage, TCP/IP and its application, and it guides us the recent configuration of the peripherals and gadgets. In level-II information Technology,security tools and techniques are described.The security tools proclaim the software, hardware and techniques altogether to protect the network from threats. Level-III consists all cybercrimes avoidance like identifying theft, white collar crimes identification, online scams findings, etc., The last level level-IVis having the detail explanation of ERP, online applications, threats and harmful viruses. After gone through this course the network users of the institutions are aware of the information security and their invaders.

IV. A NEW GENERALIZED DISCRIMINATE SECURE NETWORK MODEL GUIDELINES

Guideline 1: E-Governance

- For havingthe centralized E-governance policy in the institution, It must have the effective cooperation between management and employees

During the review of the existing E-Governance, It was identified that security programmes are not well satisfied their requirements as it is devised by both management and users of the Institutions, so as to make the results of misunderstanding[17].

Guidelines 2: Security policy & framework

This is the guidelines about cyber law since it is important whenever anyone wants to get in to the communication and it is even starts from simple SMS[18] services to video conferences.

- Enhance the current security policy inside the institutions
- To establish new security policy if the old one is not fulfilling the requirements
- The security policy has to ensure the objective of the security such as 1)confidentiality 2)integrity and 3)availability of the information

Table 2: Attributes in the Information Security

S.No	Criteria	Attributes
1	Objective	Confidentiality Integrity Availability
2	Threats	Attacker(insider, Outsider) Environmental Threats
3	Vulnerabilities	Model Vulnerabilities Technical Vulnerabilities
4	Safety Measures	Use Security Measure Create New Security Measures

Guidelines 3: Cyber Security Technology

This Guideline is based on the cyber security technology as bulletin below

- Creating a cyber-security technology that materializing the requirementsof information security[19].
- Produce training progrmmesto users if the tools are new

Now a day lot of hardware and software are purposely made for defending the cyber threats in network, this kind of things can be taught to the users.

Guidelines 4:Background of Security Building

This guideline that processes on the human aspect

- To maintain a high level security and following the security policy
- To Circulate the security policy among the users and Participants

To promote a cyber-security it is required a leadership quality and involvement towards the policy group materializing[21].

Guidelines 5: Research and Development

To achieve the objective of the security the organization should take care of Network Security Research and Development[22]. To develop the security policy and toachieve the goal, the objectives of the guidelines must be as

- To enlarge the security policy
- To strength the security policy

- To cultivate the growth of information security.

The outcome of the research and development could be an intellectual property of institutions and it is also protect the institution’s network.

Guidelines 6: Inter Coordination

The security environment interconnection is a sixth policy and is not come from a single head; it has to be accepted by all users of the institutions[23]. The inter coordination is explained in the figure 4. The objective of this guideless are

- Encourage volunteer participants of employee
- Promote simple guidelines for understanding

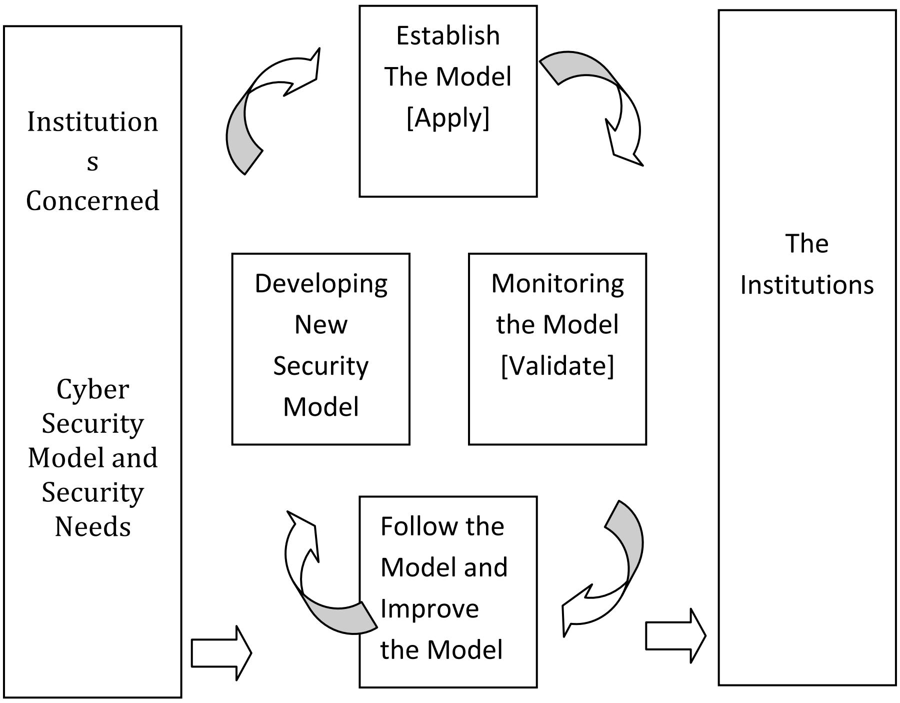

Figure.4: CAVM approach for inter coordination

V. Conclusion

Tedious is a job of providing security even to the system engineers. For their convenience by this paper a guideline for creating a new generalized discriminated secure model is devised to keep the security ON until the network switched OFF. As the discussions were in all possible security threatens, this guideline was devised and after thorough scrutiny of rated antiviruses in all aspects, it contains strong steps to prohibit the entire network from the attackers. Initially set of questionnaire were given to reputed institutions and obtained filled in questionnaire forms for bringing in to further process. Secondly, the awareness was created across the network users on the secure network and the invaders. Finally, the guideline which provides how keep the networks more secure could be possibly devise as well and it has been concluded that the guideline defends the network from invaders in several aspects.

Reference

[1] Anderson, R. 2001. Why information security is hard–an economic perspective. In: Proc. of 17th Annual Computer Security Applications Conf. (ACSAC), New Orleans, LA, 2001.

[2] Anthony, J.H., Choi, W. and Grabski, S. 2006. Market reaction to e-commerce impairments evidenced by website outages. Int. J. Accounting Information Syst.7: 60-78.

[3] Brav, A., Geczy, C. and Gompers, P.A. 2000. Is the abnormal return following equity issuances anomalous? J. Financial Econ. 56: 209-249. Brealey, R.A. and Myers, S.C. 2000. Principles of Corporate Finance, MacGraw-Hill, Boston, MA, 2000.

[4] Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L.2003. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. J. Comp. Security. 11: 431-448.

[5] Cavusoglu, H., Mishra, B. and Raghunathan, S. 2004. The effect of internet security breach announcements on market value: Capital market reactions for breachedfirms and Internet security developers. Int. J. Elec. Commerce. 9: 69-104.

[6] Cooper, M.J., Gulen, H. and Rau, P.R. 2005. Changing names with style: Mutual fund name changes and their effects on fund flows. J. Finance. 60: 2825-2857.

[7] Ettredge, M.L. and Richardson, V.J. 2003. Information transfer among Internet firms: The case of hacker attacks. J. Information Syst. 17: 71-82

[8] Garg, A., Curtis, J. and Halper, H. 2003. Quantifying the financial impact of IT security breaches. Information Management Comp. Security. 11: 74-83.

[9] Gatzlaff, K. and McCullough, K.A. 2008. The effect of data breaches on shareholder wealth, working paper, Florida State University, 2008.

[10] Gordon, L.A. and Loeb, M.P. 2002. The economics of information security Investment. ACM Trans. Information Syst. Security. 5: 438-457.

[11] Iheagwara, C., Blyth, A. and Singhal, M. 2004. Cost effective management frameworks for intrusion detection systems. J. Comp. Security. 12: 777-798.

[12] Joshi, M.J. and Patil, B.V. 2012. Computer virus: Their problems and major attacks in real life. J. Adv. Comp. Sci. Technol. 1(4): 316-324.

[13] Lin, C.H., Liu, J.C. and Chen, C.R. 2009. Access log generator for analyzing malicious website browsing behaviors. IEEE 2009. pp.126-129.

[14] Mehra, T. and Pateriya, R.K. 2013. Cyber Security Considerations for Advanced Metering Infrastructure in Smart Grid. Int. J. Sci. Engg. Res. 4(8): 939-944.

[15] Ning, L.Z. 2009. Developing a computer forensic program in police higher education in computer scienceand education. ICCSE '09. 4th Int. Conf. pp.1431-1436.

[16] Abusukhon, A. and Talib, M. 2012. A novel network security algorithm based on private key encryption. In Proc. Int. Conf. on Cyber Security, Cyber Warfare and

[17] Yehoshua, Zohar, et al. "Progression of geographic atrophy in age-related macular degeneration imaged with spectral domain optical coherence tomography." Ophthalmology 118.4 (2011): 679-686.

[18] Chan, A. 2011. A security framework for privacy-preserving data aggregation in wireless sensor networks. ACM Trans. Sensor Networks. 7(5): 1-5.

[19] Chen, G., Mao, Y. and Chui, C.K. 2004. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals. 21(3): 749-761.

[20] Ganeshkumar, K., Arivazhagan, D. and Sundaram, S. 2013. Strategies of cybercrime: Viruses and security sphere. J. Acad. Indus. Res. 2(7): 397-401.

[21] Ganeshkumar, K., Arivazhagan, D. and Sundaram, S. 2014 Journal of Academia and Industrial Research (JAIR) Volume 2, Issue 7 December 2013 401 Advance Cryptography Algorithm for Symmetric Image Encryption and Decryption Scheme for Improving Data Security

[22] K. Ganeshkumar and D. Arivazhagan October 2014 Indian Journal of Science and Technology, volume 7, Issue 1, Generating A Digital Signature Based On New Cryptographic Scheme For User Authentication And Security,

AUTHOR PROFILE

Mr.Ganesh Kumar K, is currently designated as a regular Doctoral Researcher from the Department of Information Technology, AMET University, Chennai. He was functioned as an Assistant Professor for the Dept. of Information Technology, AMET University, Chennai previously. His current area of expertise is in the domain of ‘network security’. The present article is the outcome of his research work in association with his academic guide Dr. D.Arivazhagan

Dr.D.Arivazhagan, Professor, Over twenty six years of IT experience with various platforms and programming. At present working in AMET University as Professor, Director, E-Governance, Additional Controller of Examination also worked as HOD, Department of Information Technology. Before joining this organization, worked for Main street Networks, CA to develop Utilities Management System using Java, EJB, JSP, J-Script, Style sheet, XML, SYBASE, and HTML. Worked in Unix, MVS, Windows NT, Novell NetWare and MS-DOS Operating Systems. Also coded in CGI, Perl, Cold fusion and JDBC. Strengths include creativity, project design implementation, project analysis and quick learning of new languages/packages. Currently working in the field of Network Security and Image processing. Guiding many research scholars and published many papers in National and International Journals.