Issue of Cyber Threats in Distributed Systems

Chigurupati Vamsi Krishna[1], Challagulla Akshay Kumar[2], Gopichand G[3]

[1,2,3]*School of Computer Engineering, Vellore Institute of Technology, Tamil Nadu, India*

Abstract - *Cyberspaces faces a range of highly ranged threats that rapidly spread in different types of distributed systems such as spreading rumors in the social media about the virus. Unexpected failures causing rolling blackouts in grids called as smart grids. These threats fall into category of transmissible threats having caused tremendous loss in finances and damage to many users in different distributed systems. In this field, cyber threats have been extensively studied and received considerable attention in recent years. Modeling and restraining are the current issues. These can also help in developing the risk assessment methods on exposing the compromised internet users. In addition to that, modeling will contribute to develop the interactive algorithms to capture the threat dynamics and examine the defense strategies.*

Key Words: **cyber threats, parallel, distributed systems, transmissible threats**

1. INTRODUCTION

Network Cyber Physical systems are the fundamentally constrained by the light coupling and closed loop control and actuation of the processes that are physical. to address this actuation in such loops in wireless control systems, there is a strong basic need to think about communication architectures and network protocols for the maintenance of stability and performing in the presence of disturbances to the network, environment and for the whole system. We review the current state of network control efforts and present the two complementary approaches for optimal and compassable control over networks. We introduce a computer system approach with embedded virtual machines, where controller tasks, with their control and timing properties, are to be maintained across physical node boundaries. Controller functionality is decoupled from the physical substrate and is capable of runtime migration to the most competent set of physical controllers to maintain the stability in the presence of changes to the nodes.

Regarding the recent scenarios, the distributed systems are widely used across the world by many people from various companies to connect their various branches all over the world wherever they have been located. Distributed system co-ordinate the use of physically distributed computer. Security comes under a vital thing for distributed applications such as video-conferencing, clustering etc, which are operated in dynamic network surroundings and communicate over secure network. Some important concern the user needs to face when they use the distributed systems is the security authentication, integrity, confidentiality and transparent open way. User should interact with the resources of a system in a scalable way. Openness in distributed systems means each of the sub-system is continually open to the server and the client which are to be taken as other systems. Scalability may be either load scalability or geographic scalability and administrative scalability. Researchers are now concentrating about the distributed computing. As the use of these systems in daily life is going to reduce the usage of man's power.

We therefore organize this special issue to reduce the gap between practices and academics research. This special issue in distributed systems field to publish state of art findings in transmissible cyber threats, especially, focusing on propagation of modeling, threat restraining and their applied techniques.

1.1 Synopsis of The Problem

Historically, the control systems are in secured, protected environments and under constant monitoring. Such perimeter isolation is impractical because control systems are mostly likely to be located at unmanned and not so secured installations. Security of these places is by a literal fence and locks of some kind. Such kind of securities are easily diluted by a well informed and equipped intruder who can gain the physical access being undetected and leave such remote systems subjected to control by hostile intruders.

Extending perimeter of the security may be not so practical, if not possible. Furthermore, it is possible that a trusted insider can also commit such thing, which raises the risk of system compromise to the greater control systems as well as for the equipment under the control or both.

The need to secure of high-value infrastructures against remote and any external cyber intruders or internal agents is becoming intense. The risk of finding such middle ground opportunities increases as the infrastructures become needier on unified cyber connections. These current considerations also contain defending against the cost of unplanned attacks follow-on in the non-hostile or naive reliable entities in the system. Unsettling actions are inevitable as the system becomes compound and distributed. The key goal of such a control system is to go forward through the attack without any serious fiscal or efficiency cost or maybe even loss in the human life.

1.2 Future Scope

As well know that distributed computing is the latest trend in all the fields. They are more widely used all over the world. As there are many positives from this, there are also certain aspects that might make distributed computing a menace to the world. The main issues regarding this menace will be the security issue. Which is to be implemented very strongly such that, the systems are protected from whatever the attack, it might get even in the upcoming future. So we

can expect well protected systems that are free from cyber threats and will be effective in the functioning and making the user satisfy his/her basic needs or the system must reach the requirements of the user.

2. MIGITATING STRATEGIES

As the topic is regarding providing the security for the distributed systems, we ought to present some of the strategies that are to be implemented in order to prevent the Distributed systems from getting effected from cyber threats. There are many ways that are to be planted in a system such that, the threats can be removed or can be stopped from being affecting the further of the system. The techniques are

- Authentication
- Redundancy and diversity
- Design and Analysis of principles.
- System recovery of critical functions
- Robust networked control systems.

2.1 Methodology Used For Security Issues

AUTHENTICATION

Verifying authentication and honesty are dependably with one another. For instance, let us consider a conveyed distributed system that backs up the authentication in the interest of an affiliation, yet does not give rules to guaranteeing the uprightness of the message. At the other hand, if a framework just backings message uprightness, while there is no system for confirmation. In this manner, the message validation and uprightness must be as one. In numerous conventions, this mix functions admirably. To guarantee trustworthiness of information traded after authentication, we utilize encryption of uncommon keys to the session keys. Session key is a mutual mystery key applying to encryption of message uprightness and classification. Such key is usable while, the set up channel exists. At the point when the channel is shut, the session key is lost. In following, we examine about the verification strategies dependent on the session key.

a. Authentication based on shared keys

Authentication protocols based on shared keys is displayed in Figure 1.First person M sends his/her identity to person N (message 1) and suggests that wants to establish a contact channel between them. Then N sends the test RN to M (message 2). Such a test can be a random number. M must encrypt the challenge with XM, N secret key, which is shared by Band sends the encrypted challenge to N(message 3). When N receives a reply from XM, N(RN) to its own test RN, it can decrypt the message using the shared key to check whether including RN. In this way, she knows M exists on the other side and determines who else needed for encryption of RN with RM,N. N demonstrates that speaks with M, but M still did not prove speaks with N, so it sends the test RM (message 4) that it is replied with return of XM,N (RM)(message 5).When M decodes this by XM,N and RM see itself, it knows speaks with N.

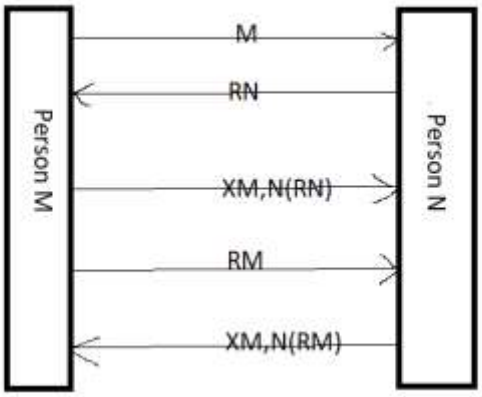

Figure 1

b. Authentication Using a Key Distribution Center

Another authentication scheme, is the by means of of a key distribution centre (KDC). KDC will collaborate with each every other node/person for secret key, but any pair of nodes/persons does not necessarily require to have shared key. With KDC, it is necessary to manage Z keys. M initially sends a message to the KDC and wants to talk with N. M returns a message that contains secret shared keys XM,N that M can uses it. Moreover, KDC also sends the shared key XM,N to N that is encrypted with secret key XB, KDC. Needham-Schroeder authentication protocol is calculated on the bases of this model.

3. EXPECTED OUTPUT

A distributed system in which many systems are connected parallel over a system of network. This helps to work load of a user such as dividing to work among systems. This will reduce the manual work of the system. A perfect distributed system is a system which is adaptive more to the nature and is capable of working more efficiently by producing good results more than singly working systems. The systems must not be affected by viruses or any kind of cyber threats that may lead to effecting of one system to the other parallel connected systems.

4. CONCLUSION

In this research paper, diverse security aspects are discussed like information, physical and technical security and some techniques. All these should be appropriately managed and implemented to defend the distributed systems. Causes of the cyber threats have also been discovered in this paper for the educational purpose. The solutions for the problem of causing the transmission of the cyber threats also have been discussed. However all these studies topics and theories will make the distributed system

work dynamically and efficiently without any lag to the user even thought there are many processes that are involved in the execution. The distributed systems will be more adaptive a reliable. This states the importance of the security to the system and their complexity.

ACKNOWLEDGEMENT

We have succeeded in doing a special issue on this topic about the protection of the distributed computing systems from the cyber threats which are prone to attack easily on the systems that are distributed physically, and they are also having the capability of attacking the wireless networks easily rather than the connected with wire devices. We have many problems while researching about this, but we were able to overcome with the help of my faculty GOPICHAND G, and we would like to gladly thank him for his efforts and making this successful.

REFERENCES

[1] Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism. Oxford: Clarendon, 1892.

[3] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, "Title of paper if known," unpublished.

[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[8] Electronic Publication: Digital Object Identifiers (DOIs):

[9] D. Kornack and P. Rakic, "Cell Proliferation without Neurogenesis in Adult Primate Neocortex," Science, vol. 294, Dec. 2001, pp. 2127-2130, doi:10.1126/science.1065467. (Article in a journal)

[10] H. Goto, Y. Hasegawa, and M. Tanaka, "Efficient Scheduling Focusing on the Duality of MPL Representatives," Proc. IEEE Symp. Computational Intelligence in Scheduling (SCIS 07), IEEE Press, Dec. 2007, pp. 57-64, doi:10.1109/SCIS.2007.357670. (Article in a conference proceedings)