International Journal of Information Processing, 8(2), 37-46, 2014
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

Detecting Intrusion and Designing of CCRX Dynamic Encryption Algorithm of a Network System

Nandita Sengupta[a], Jeffrey Holmes[b], Jaya Sil[c]

[a]University College of Bahrain, P.O. Box 55040, Manama, Kingdom of Bahrain,
Contact: ngupta@ucb.edu.bh

[b]University College of Bahrain, P.O. Box 55040, Manama, Kingdom of Bahrain,
Contact: jeffreyholmes@hotmail.com

[c]Bengal Engineering Science University Shibpur, India, Contact: js@cs.becs.ac.in

In today's world, security of network system is an important research area. As size of data is increasing exponentially, protection of the same is getting more and more importance. Day by day, difficult security mechanism is being applied for protecting the system from cryptanalyst. In spite of the fact, security is broken by undesired users in many cases. Our paper is focused to apply a hybrid encryption algorithm for transferring data. Learning mechanism is applied to detect intruders while data is in transmission. Once, intruder is detected or suspected, dynamic encryption algorithm is applied to protect future data in the following secured connections.

Keywords : Cryptanalyst, Dynamic Encryption Algorithm, Learning.

1. INTRODUCTION

Importance of maintaining security in the network data, has led the researchers to think, find out more and more difficult security mechanism. Objective of finding such security mechanism is to make the job of unauthorized user, harder. An unauthorized user has to face a challenge to break the security system as the computational difficulty is involved in designing the security mechanism. Therefore, breaking of security system for an unauthorized user will be challenging task. Attacks can be classified into two, passive attack and active attack. In Passive attack, unauthorized user tries to enter into the system and read the message in the media. In active attack, user tries to modify the message. In our work, plain text has converted into cypher text applying a hybrid encryption algorithm. Using this hybrid algorithm, confidential data is being sent from one server to another server through Virtual Private Network. Learning based Intrusion Detection System [1], [2], [3], [4], [5] has been implemented in both the two servers to monitor the network data, to detect the intruder. If any intruder is detected by any of this server, immediately, dynamic encryption algorithm [6], [7], [8], [9], [10] is applied to send further data into the network.

Section 2 depicts detecting intusion, Section 3 narrates Encryption, Section 3 explicates our Proposed Hybrid Encryption CCRX algorithm, Section 4 describes Dynamic Encryption, Section 5 explains the implementation part in Experimental Results, Section 6 concludes our work as well as focuses future work.

2. Detecting Intrusion

Intruders are defined as unauthorized users who want to access the network or system to access or damage important information of the system. It is very important to study the characteristics of the network traffic, classify normal and anomaly traffic and stop accessing the network or system by anomaly traffic to protect the system from intruders. Intrusion Detection

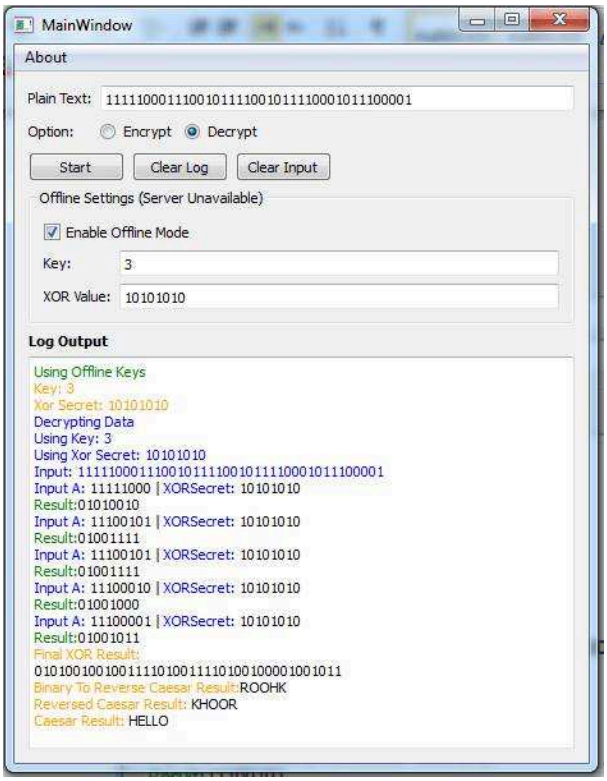

Figure 5. Screenshot of the result of Dynamic Decryption CCRX Algorithm.

CCRX Encryption Algorithm without any additional information added to the frame size of the message. Therefore, computational time for decrypting the Cipher Text Message will be more for the Cryptanalyst.

7. Conclusions and Future Work

Our proposed system provides a complex encryption algorithm and also provides the mechanism of changing encryption algorithm for the user whose data has been attempted for stealing. For each user, each and every time unauthorized user is detected, dynamic encryption algorithm will be applied depending on the random number generated from the system and the time of detection of attack. From time complecity analysis, it is clear that computation time of CCRX Hybrid Decryption algorithm is higher than any single decryption algorithm. In future work, emphasis will be given on designing of learning system of Intrusion Detection System.

REFERENCES

1. M Jun and F Shuqian. Research of Intrusion Detection System Based on Machine Learning, in *Proceedings of 2nd International Conference on Computer Engineering and Technology (ICCET), IEEE*, 2010.
2. B J Kim and I K K Kim. Kernel based Intrusion Detection System, in *Proceedings of Fourth Annual ACIS International Conference on Computer and Information Science, IEEE*, pages 13–18, 2005.
3. P S Gou, Y Wang, L C C Jiao, J Feng and Y Yao. Distributed Transfer Network Learning Based Intrusion Detection, in *Proceedings of IEEE International Symposium on Parallel and Distributed Processing with Applications*, pages 511–515, 2009.
4. Y Peng, Y Niu and Q Hu. Research on Intrusion Detection System Based on IRBF, in *Pro-*

ceedings of 2012 Eighth International Conference on Computational Intelligence and Security (CIS), IEEE, pages 544–548, 2012.

5. L Li, D Z Yang and F C Shen. A Novel Rule-based Intrusion Detection System using Data Mining, in *Proceedings of 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), IEEE*, pages 169–172, 2010.
6. Y H Zhang, Q S Zhou and Y Tao. A Kind of Dynamic Encryption Algorithm and its Application, in *Proceedings of Second Pacific-Asia Conference on Circuits, Communications and System (PACCS), IEEE*, pages 15–18, 2010.
7. H P Yu and U W Pooch. d-key Dynamic Encryption - A Security Enhancement Protocol for Mobile Ad Hoc Network, in *Proceedings of First International Conference on Ubiquitous and Future Networks, ICUFN 2009, IEEE*, pages 183–188, 2009.
8. T R Rahman. A Dynamic Encryption Algorithm for Multicast/Broadcast Streaming Applications, in *Proceedings of the Fourth Asia International Conference on Mathematical/Analytical Modelling and Computer Simulation, IEEE Computer Society, AMS 2010*, pages 591–596, 2010.
9. A H Omari, B M Al-Kasasbeh, R E Al-Qutaish and M I Muhairat. DEA-RTA: A Dynamic Encryption Algorithm for the Real-Time Applications, *in International Journal of Computers*, 3(1), 2009.
10. H P Yu and U W Pooch. A Secure Dynamic Cryptographic and Encryption Protocol for Wireless Networks, in *Proceedings of EUROCON 2009, IEEE*, pages 1860–1865, 2009.
11. N Sengupta, J Sen, J Sil and M Saha. Designing of On Line Intrusion Detetion System Using Rough Set Theory and Q Learning Algorithm, *in Elsevier, Neorocomputing*, vol. 111, pages 161–168, July, 2013.

Dr. Nandita Sengupta is currently Assistant Professor, University College of Bahrain, Bahrain. She obtained her Bachelor of Engineering, Masters Degree and Ph.D in Engineering, Computer Science and Technology from Bengal Engineering and Scieence University Shibpur. She has 23 years of working experience. 11 years she dedicated in design department of Electrical Manufacturing Company Limited. Last 12 years she is in academics and taught various subjects of IT. Her area of interest is Analysis of Algorithm, Theory of Computation, Soft Computing Techniques, Network Computing. She achieved "Amity Best Young Faulty Award" on the occasion of 9th International Business Horizon INBUSH 2007 by Amity International Business School, Noida in February, 2007. She has around 21 publications in National and International conference and journals.

Dr. Jaya Sil an alumnus of BESUS(Bengal Engineering and Science University, Shibpur) and JU(Jadavpur University), completed her Ph.D. in Engineering from JU, Kolkata, India. She holds Masters in Computer Science and Engineering from JU and Bachelors in Electronics and Tele Communication Engineering from BESUS (formerly known as Bengal Engineering College). She has been working in Academics for last 27 years. Presently she is working as Professor of Computer Science and Technology Department and Director of School of VLSI Technology in BESUS. Under her leadership and guidance many sponsored projects have been successfully conducted. She has more than 90 publications in International Conferences and Journals. She has already supervised four Ph.D theses. and more than 10 Ph.D students presently working under her guidance. Dr. Sil worked as Post-Doc Fellow in Nanyang Technological University, Sngapore on 2002-03 and visited Heidelburg University, Germany on 2007. Dr. Sil contributed a Book Chapter - Adaptive Agent Integration in Designing Object- Based Multiagent System. LNCS, Volume 3215/2004 Dr. Sil acts as Guest Editor In International Journal On Artificial Intelligence And Soft Computing And Editor of GA Issue Of Materials and Manufacturing Processes. Delivered Tutorial lectures in two International Conferences NGMS 2006, 2008 and INDO US workshop in Kolkata. Her areas of research include Image Processing, Soft Computing Techniques, Multiagent Systems and Bio-Informatics.

Mr. Jeffrey Holmes is currently studying his Bachelors of Science in Information Technology with Computer Science Concentration at the University College of Bahrain. His main interest are in Software Development, Computer Security and IT overall. He also enjoys working as a IT Consultant / Web Developer for various clients in the Kingdom of Bahrain (freelancing) and continues to do so today. In his spare time, he enjoys learning new programming language frameworks, programming languages and utilizing engines like 'Google Engine' for Cloud Computing or Unreal Development Kit (UDK) for game development.