International Journal of Information Processing, 7(4), 35-42, 2013
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

Investigation on Error Handling Method Using Cryptanalysis Techniques of Simplified Data Encryption Standard for Block Data

Rajashekarappa[a], K M Sunjiv Soyjaudah[b], Sumithra Devi K A[c]

[a]Department of Information Science and Engineering, SDMCET, Dharwad, India
(Research Scholar, Dept. of CSE, Jain University, Bangalore.)

[b]Professor, Department of EEE, University of Mauritius, Reduit, Mauritius.

[c]Professor, Department of MCA, RVCE, Bangalore, Karnataka, India.

This paper presents an approach for the investigation on error handling method using cryptanalysis techniques of simplified data encryption standard for block data. It is estimated that over 96% of all new information produced in the world is being stored on magnetic media, most of it on physical disks. It is designed to be a guide to techniques for analyzing a cryptosystem. In this paper we used the Kerberos authentication system and the basis for the analysis is a working of the system. The Kerberos authentication system uses a trusted key server to keep track of the private keys of clients and servers and to generate session keys for client-server interaction. The Kerberos ticket contains the session key, information about the client and some other useful data. Cryptanalysis data could be store for long time with help of Self Monitoring Analysis and Reporting Technology Copyback technique from the experimental results.

Keywords: Authentication, Cryptanalysis, Data Encryption Standard, Kerberos.

1. INTRODUCTION

The purpose of this paper is to explain the Self Monitoring Analysis and Reporting Technology Copyback technique. SAS (Serial Attached SCSI) products and provide the detailed design [1],[2]. The drive vendors builds a logic in to the drives to make drives smart so that the user gets warning signal as a predictive failure whenever the drive is about to go bad for some reason. The drives built with this kind of logic are called SMART drives which is an acronym for Self Monitoring Analysis and Reporting Technology. Example: The drive monitors the number of ECC (Error Checking and Correction) errors and based on the cryptanalysis block data it can give predictive failure if the ECC error threshold exceeds internal to the drive. This paper is designed to be a guide to the sorts of techniques used for analyzing a cryptosystem.

The Kerberos authentication system is used as an example, and the basis for the analysis is a working of the system [3],[4],[5]. More recent versions of the system have fixed many of the problems described in this paper. The rest of the paper is organized as follows: Section 2 gives the Overview of tickets and the possibility of a chosen plaintext attack. Section 3 presents Data Encryption Standard and Section 4 gives the overview of the fault and tolerant method using cryptanalysis techniques of data encryption standard using block data. Section 5 gives the experimental results. Finally, Conclusion and Future work are presented in Section 6.

2. OVERVIEW OF TICKETS AND THE POSSIBILITY OF A CHOSEN PLAINTEXT ATTACK

The procedure used by a client to get a service in Kerberos is well explained, and so we shall limit our description of this procedure to

Serial No. of test case	UTC-01
Name of the Test	Disk Data Format Checking Successful Test
Item/Feature being Tested	Check given data format of the Operations for copyback
Sample Input	Given Disk Data Format
Expected output	Copyback should automatically start and after copy back completes the Dedicated Hotspare (DHSP) should be correctly dedicated to the same set of arrays.
Actual output	Whether the Dedicated Hotspare is used by same set of arrays or not
Remarks	Test Successful

Figure 2. Test Case for Data Format Checking.

Serial No. of test case	UTC-02
Name of the Test	Manual Copyback – failure test
Sample Input	Manual Copyback module to test the functionality of the function which writes data from Source Physical Disk (PD) to Destination Physical Disk (PD). Check Physical Disk (PD) Allowed Operations.
Expected output	StartCopyback should be TRUE for all ONLINE PDs StopCopyback should be TRUE for all DS_COPYBACK PDs. Start copyback manually from ONLINE to Unconf. Good/HSP.
Actual output	After copyback completes, the source would become Unconf. Good or Unconf. Bad(if it has predictive failure). The destination would become ONLINE. Note that copyback can never be started to a destination HSP which already has a predictive failure. Stop copyback on PDS_COPYBACK PDs.
Remarks	The Hotspare (HSP) size should be more than an array size or equal to an array size. As this condition is failed. Because the destination HSP size is less than an array size.

Figure 3. Test Case for Manual Copyback

certificate, could I please have yours. B can reply with his certificate. Each of them can encrypt the certificates using SSs public key. At this point, A knows Bs public key, and knows that it is genuine, and vise-versa. So now they can carry on a private conversation, secure in the knowledge that only the other can decrypt messages sent to them.

One might object that we were using the SS as a trusted key server. If anyone discovered the way to decrypt SSs messages, anyone could fake them. This is true however in our scenario it is less likely that a malicious client could discover the secret key: whereas in Kerberos the TGS has to be on the network, and is constantly sending out tickets, our SS can be quite isolated electronically. Further, if the TGS goes down, no new session keys can be issued, and two perfectly healthy machines may not be able to communicate. In the public key method, the SS going down has no effect on whether two machines with certificates can communicate. In this case we were using cryptanalysis data could be store for long time with help of Self Monitoring Analysis and Reporting Technology (SMART) Copyback technique from the experimental results.

REFERENCES

1. Rob P, Sean D, Robert G and Sean Q. Interpreting the data: Parallel Analysis with Sawzall, in *Journal Scientic Programming,*

Serial No. of test case	UTC-03
Name of the Test	SMART Error – success test
Item/Feature being Tested	Ctrlprop.SMARTerEnabled should be TRUE for copyback to start on SMART errors.
Sample Input	Create any RAID level(even RAID0) with a predictive failure drive. Create a HSP
Expected output	Once SMART Poll detects an error, copyback should automatically be started from the predictive failure drive to HSP. After copyback completes, HSP becomes ONLINE and predictive failure PD Unconf. Bad. It is also same as expected output what above mentioned.
Actual output	It is also same as expected output what above mentioned
Remarks	Test Successful

Figure 4. SMART Error Success Test

Special Issue on Grids and Worldwide Computing Programming Models and Infrastructure, 13(4):277–298, 2010.

2. Rajashekarappa and Dr. K M S Soyjaudah, Self Monitoring Analysis and Reporting Technology (SMART) Copyback, in *proceedings of International Conference on Information Processing 2011 (ICIP 2011), 8th-9th Aug, Bangalore*, pages 463–469, 2011.
3. Rajashekarappa and K M Sunjiv Soyjaudah. Overview of Linear Cryptanalysis on S-DES and Block Ciphers using Hill Cipher Method, *IJCA*, 63(21), 2013.
4. Elerath J G and Shah S. Server Class Disk Drives: How Reliable are they?, in *Proceedings of the Annual Symposium on Reliability and Maintainability*, pages 151–156, 2004.
5. Behrouz A Forouzan. Cryptography and Network Security, in *First Edition, McGraw- Hill*, 2006.
6. Eli Biham, Rafi Chen, Antoine Joux, Patrick Carribault, Christophe Lemuet and William Jalby. Collisions of SHA-0 and Reduced SHA-1, Advances in Cryptology, in *Proceedings of CRYPTO, LNCS 3494, Springer Verlag*, pages 36–57, 2005.
7. Atul Kahate. Cryptography and Network Security, TMH, 2003.
8. Stallings W. Cryptography and Network Security, Third Edition, 2003.
9. Elmasri Navathe., Fundamentals of Database Systems, *Third Edition, Pearson Education*, 2003.
10. Silberschatz, Korth and Sudarshan. Database System Concepts, *Third Edition, McGraw-Hill*, 2003.
11. Steiner J. An Authentication Service for Open Network Systems, 1988.
12. Lan Sommerville. Software Engineering, *Sixth Edition, Pearson Education Asia,* 2006.
13. Pankaj Jalote. An Integrated Approach to Software Engineering, *Third Edition, Springer publishers,* 2005.
14. Rajashekarappa and Dr. K M S Soyjaudah. Heuristic Search Procedures for Cryptanalysis and Development of Enhanced Cryptographic Techniques, in *International Journal of Modern Engineering Research*, 2(3):949-954, May 2012.
15. Kohl J. The Evolution of the Kerberos Authentication, 1992.
16. Garg P. Evolutionary Computation Algorithms for Cryptanalysis: A Study, in *International Journal of Computer Science and Information Security*, 7(1), 2010.

Mr. Rajashekarappa is working as a AP, in the Department of Information Science and Engineering at SDMCET, Dharwad. Mr. Rajashekarappa worked as a Lecturer for around three years in the Department of Computer Science and Engineering, JSS Academy of Technical Education, Avenue Droopnath Ramphul, Bonne Terre, Vacoas, Mauritius. He has one and half years of experienced as a Project Assistant at Indian Institute of Science (IISc), Bangalore, India. He worked as Project Internee in Indian Space Research Organization (ISRO), Bangalore, India. He has one and half years of experienced as a Project Trainee at LSI Technologies Pvt. Ltd, Bangalore, India. Mr. Rajashekarappa obtained his Bachelor of Engineering in Computer Science and Engineering from Anjuman Engineering College, Bhatkal, India. He has qualified in Graduate Aptitude Test in Engineering (GATE), Computer Science and Engineering, 2006. He received his Master Degree in Computer Science and Engineering from R. V. College of Engineering, Bangalore, India. He is pursuing his Ph. D in Computer Science and Engineering at Jain University, Bangalore, India, under the guidance of Dr. K M Sunjiv Soyjaudah, Professor, University of Mauritius, Reduit, Mauritius. Mr. Rajashekarappa area of interest and research include Cryptography, Data mining, Mobile Communication, Computer Networks and Cloud Computing. He has published several Research papers in international journal / conferences. He has guided many students of Bachelor degree in Computer Science and Engineering in their major projects. Mr. Rajashekarappa is a member of ISTE, IETE, IACSIT, IAEST, IAENG and AIRCC.

Professor K M Sunjiv Soyjaudah received his B.Sc (Hons) degree in Physics from Queen Mary College, University of London in 1982, his M.Sc. Degree in Digital Electronics from Kings College, University of London in 1991 and his Ph. D. degree in Digital Communications from University of Mauritius in 1998. He is presently Professor of Communications Engineering in the Department of Electrical and Electronic Engineering of the University of Mauritius. His current interest includes Source and Channel Coding Modulation, Image Processing, Cryptography, Voice and Video through IP, as well as Mobile Communication. Dr. K M S Soyjaudah is a member of the IEEE, Director in the Multicarrier (Mauritius), Technical expert in the Energy Efficiency Management Office, Mauritius. Registered Ph.D Guide in University of Mauritius, Reduit, Mauritius and Jain University, Bangalore, Karnatka, India.

Dr. Sumithra Devi K A Professor and Director, in Master of Computer Applications at R V College of Engineering, Bangalore, India. She received BE from Malnad College of Engineering, Hassan. She received ME and Ph.D from UVCE, Bangalore and Avinashilingam University for Women, Coimbatore, INDIA respectively. Reviewer for many International Journals / Conferences like WEPAN, WICT, EDAS, IACSIT, ISCAS, JEMS, Published 14 journals and 65 International/ National Conferences. Professional Member in many IEEE, IETE, CSI, ISTE. Member in BoS and BoE, for Visvesvaraiah Technological University, Belgaum, Karnataka. Registered Ph.D Guide in Visvesvaraiah Technological University, Belgaum; Jain University, Bangalore; Prist University, Sathyabhama University, Tamilnadu. Authored a chapter CAD algorithm for VLSI design in the book "VLSI Design ", published by In-Tech Publications, ISBN 979-953-307-512-8, 2011 and authored book on Operating System, published by Shroff Publisher India.