

Delay Analysis of File Transfer in LINUX Systems

Gayatri Chadalapaka, Monica Mamidi,
Zaahid Mohammed

School of Electrical Engineering
Blekinge Institute of Technology
Karlskrona, Sweden
{gach16, moma15, zamo16}@student.bth.se

Wlodek J. Kulesza
School of Engineering
Blekinge Institute of Technology
Karlskrona, Sweden
wka@bth.se

Abstract—While making any file transfer, a certain level of security is applied to the data being transferred. The user of this application is concerned with only the time taken to make the transfer and also the encryption algorithm applied. This paper is aimed at analyzing delays of various methods of file transfer available in Linux platform with SCP. The analysis is done to help a user of SCP understand the delay for each method of file transfer. The comparative data provided, will be helpful to a user make a decision regarding the method to be selected for optimum/ minimal delay.

Keywords— *Cryptography, Information Theory, Security, Throughput*

I. INTRODUCTION

The main aim of this paper is to perform delay analysis in LINUX systems while using SCP to transfer files from one system to the other, while they are connected to the same network. The authors' motivation for choosing this area for research origins from the emphasis placed on Cyber Security in the current day scenario. Since LINUX kernel is popular for programming, it was chosen with Ubuntu flavor for delay analysis. Performing delay analysis in LINUX is expected to be helpful for future research in the field. The techniques being tested with SCP are Blowfish, Triple DES, Rijndael. The results are expected to show that Triple DES provides less speed compared to other two.

II. SURVEY OF RELATED WORKS

Research has been done in the field of Cyber Security, while using encryption. Reference [3] provides information necessary for selection of algorithms that can be chosen for analysis of speed of data transfer as a function of level security. Reference [1] gives insight on how to narrow down the aspect of Cyber Security to encryption in data transfer for Linux systems. Reference [4] provides information on the performance evaluation of Blowfish and Rijndael algorithms.

The idea to research on this topic was brought upon by surveying various related works, main concepts being from Reference [3] and [4]. This, in turn encouraged us to provide a reference table to the end user, which enables him/her to know the consequences of the encryption choice they make while transferring files using SCP.

III. PROBLEM STATEMENT AND MAIN CONTRIBUTION

The problem that is being dealt with is, the lack of experimental data which provides information about the delay caused for file transfer using SCP, for different methods available. The research question is, how delay analysis of file transfer can be implemented in Linux systems. It is assumed

that, Triple DES may have higher delay, due to its cryptographic structure. To find out the answer to this question, the approach used by us in this paper is to use Telnet and SCP to enable file transfer between systems and thus evaluating the delay in file transfer for various cryptographic algorithms available, as the experimental procedure for delay analysis and deriving a conclusion from the results obtained.

IV. PROBLEM SOLUTION

A. Evaluation Scenario

To perform delay analysis, a file (.txt was used) is transferred from system A to system B by using the default SCP command. For the same .txt file, different encryption algorithms are chosen and delay is noted down for all the methods. SCP provides the option of choosing various encryption algorithms for file transfer.

TABLE I. EVALUATION ENVIRONMENT

Component	Description	Function
Dual-Boot Linux	Hardware	Initiates communication between 2 systems.
Telnet	Feature for Ubuntu Linux	Enables connection, while systems are on the same WLAN.
Oracle VMware	Virtual Machine software in Windows OS.	Responds to ping request and transfers data.

B. Implementation

The sequence of execution is as follows: Using Telnet, communication is established between two Linux systems connected to the same network. Changing the algorithm used, files are transferred from sender to receiver using SCP. The delays of data transfer are noted from the terminal. Multiple iterations are performed, with the same file but different techniques, while noting the values of delay in each case.

C. Results of Simulation

After performing multiple iterations of the same experiment, majority of the observations led to the conclusion shown in the table below.

TABLE II. REFERENCE TABLE

<i>Encryption Technique</i>	<i>Time Required</i>
Triple DES	High
Rijndael	Medium
Blowfish	Low

V. CONCLUSION

Based on multiple readings taken from our simulation, we thus conclude that, delay is High in Triple DES, Medium in Rijndael and Low in Blowfish.

Future work includes the study of encryption techniques on Operating Systems other than Linux and improving brute force resistance for Rijndael algorithm. A new graphic user interface containing the option to provide different types of security algorithms for the user is another future research field.

REFERENCES

- [1] Z. Yan, C. Tracy, M. Veeraraghavan, T. Jin, and Z. Liu, "A Network Management System for Handling Scientific Data Flows," J. Netw Syst. Manag., vol. 24, no. 1, pp. 1–33, Jan. 2016.
- [2] "Cryptography and Network Security, Fourth Edition." [Online]. Available: <http://williamstallings.com/Crypto/Crypto4e.html>. [Accessed: 11-Sep-2016].
- [3] G. Singh, A. Kr. Singla, and K. S. Sandha, "Superiority of Blowfish Algorithm in Wireless Networks," Int. J. Comput. Appl., vol. 44, no. 11, pp. 23–26, Apr. 2012.
- [4] M. Anand Kumar and S. Karthikeyan, "Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms," Int. J. Comput. Netw. Inf. Secur., vol. 4, no. 2, pp. 22–28, Mar. 2012.

Biographies



Zaahid Mohammed was born in Hyderabad City, Telangana, India, in 1994. He completed his secondary education from the Central Board of Secondary Education in May of 2010. He received his undergraduate Bachelor of Technology degree in Electronics and Communications Engineering from the Jawaharlal Nehru Technological University, Kakinada, in 2015. He is currently pursuing his Master of Science degree in Electrical Engineering with emphasis on Telecommunication Systems at Blekinge Institute of Technology, Sweden.

In 2015, before completing his Bachelor degree, he did a project regarding Software Defined Networks and simulated a network which showed its advantages. In summer of 2016, he worked as a TRAINEE at the GIS Training Centre at Siemens in Berlin, Germany.



Wlodek J. Kulesza received the M.Sc. and the Ph.D. degrees from Lodz University of Technology, Poland, and a docent degree from Linköping University, Sweden. In 2001 he became Professor in Measurement Science at the University of Kalmar, Sweden. Since 2005 he has held a Professor position at the Blekinge Institute of Technology, Sweden.

His current research interests are multi-sensor systems and wireless sensor networks.

Prof. Kulesza has been IEEE member since 1995.



Mamidi Mounica was born in the city of Secunderabad, Andhra Pradesh, India on August 8th in the year, 1993. She attended Jawaharlal Nehru Technical University in the year 2011 in the city of Kakinada, Andhra Pradesh, India with a course in Electronics and Communications as a B.tech undergraduate student and later graduated in the year 2015 and is currently pursuing her Masters in Telecommunications at Blekinge Institute of Technology(BTH), Karlskrona, Sweden.

Ms. Mamidi participated in the Inter-school Declamation competition held at St. Joseph High School in 2008. She came second in the painting competition held at family club summer camp in 2002 and was awarded second place in the throwball competition held during the sports day event in school in 2008. She has also completed her Foreign language certification course from 2009 to 2011 with an aggregate score of 95.



Gayatri Chadalapaka was born in Visakhapatnam city, in 1994. She is currently pursuing her Masters in electronics and communication engineering with emphasis on telecommunication systems from Blekinge Tekniska Högskola, Karlskrona.

In 2016, she published her thesis on Five-Modular Redundancy Systems and worked on P2P communication system software development project. From 2015, she has been a Teaching Associate with the Physics Department at Institute of Engineering and Medical Sciences, Hyderabad. Her research interests include Quantum Cryptography and Network Security.

Ms. Chadalapaka was a recipient of the Commitment to Excellence certificate from Institute of Engineering and Medical Sciences in July 2016.