Intrusion Analysis in Inter Process Communication

Ramzan Talib[†], M Kashif Hanif[††], M Yahya Saeed[†††], and M Umer Sarwar[††††],
Department of Computer Science, Government College University, Faisalabad, Pakistan

Summary
Various communication responses are part of any deployed software, and these are the indispensable means of inter process connections of operating system over client applications. This research paper focuses various software features of such communications, which can be potential source of intrusion and may be able to result in insecurity. There is no way of opening communication architecture of any software without reverse engineering. Additional code of communication monitoring can be attached with the software over client for capturing miscellaneous traffic patterns. Network traffic patterns are presented in this paper with certain conditions and reactions of software messages over network relating inter-communication. Scenarios in this study bear various situations in controlled environment and certain variations in it. The results show that the multi mode protection is the best criterion to assure the security for communication patterns generated by various communicating applications.

Keywords:
Intrusion Detection System, Communication Architecture, Traffic Patterns, Pluggable Authentication Modules, Firewall.

1. Introduction

The secure intelligent bridge is a very important aspect of communication. There have been always some collaborating companies on both sides on network in a real time situation. On one hand, global network has brought great business potential scope of extended terms of use and on the other hand, it has brought many operational risks [1]. Network has harmless and harmful users i.e. hackers or malicious user could access company's internal systems for various reasons. Intrusion Detection System (IDS) is needed to be deployed over softaware and Communication Architecture (CA) to monitor Traffic Patterns (TP). Software defects are mostly known as security vulnerabilities, fault managing, default system configuration etc and all of these require special form of security. Different organizations around world deploy IDS on public network to protect private network from communication risks [2].

However, any network having Firewall (FW) could not control all intrusions indeed. Companies need to ensure security through effective forms of IDS, which are capable of allowing specific services of ID to allow or restrict security policies as per business needs. IDS could also protect organization from malicious network connections and unknown sources [3]. To deploy intrusion detection system suitably in the network design depends on the study of all elements and services of the network. IDS could be compared as including an alarm in underlying system e.g. vehicle anti-theft protection etc [4]. If someone tried to steal data and destroy locks of system or lock detecting service is broken, it results into the raising alarm for system administrators. IDS works for malicious network attacks against organization's IDS protection. [5]. Core objective of the study is to relate the concepts of TP with IDS. The traffic generated can be sniffed inside or outside of software; application through network and its various conditions are explored here.

2. Related Work

Dinh et al discussed the various approaches and of the mobility and security. They carried out their work as the survey. They mainly focused on cloud computing and its secure architecture their work mainly focus the wireless communications and specific to mobile computing [1].

Majhi et al studied about the suitable placement of security equipments in the cloud bases data centers over the remote communication and network. The made recommendations as the design issues [2].
Joseph et al studied that effective intrusion detection technology might be also used to process the large data. His proposed method uses a RF algorithm. Further several algorithms can be used for missing data and it can provide an additional advantage to the algorithm. The algorithm proposes future enhancements to include a certain level of data sets for scalability algorithms [3].

Rajendran et al carried out research over for technologies e.g. PHP, Perl or Python and implementation of cloud deployment etc. He worked for the web authoring and its relation with the platforms and traffic patterns [4].
Krishnan et al worked on IDS common classification system built on principle of long-term monitoring and classification of behavior-based detection. The process proposed is critical to be implemented because of the random network of communications [5].
Vladimir et al presented a model based on ID rules, which requires a thorough maintenance of database of all modes of attacks. It needs to be regularly updated at every node of the network element. It was studied that these methods will bring computational costs, and might be not so effective in detecting new attacks [6].
Israeli et al took attention on how IDS can be carried for technical issues in a promising way for network clients.

Manuscript received July 5, 2017
Manuscript revised July 20, 2017

Intrusion Detection technology for better computation is proposed in their study and it is investigated on basis of some specific real time problems [7].
Azazi et al presented essentials of the design for a very innovative mobile robot. The design for this robot has secure navigation, which is based on the embedded form with security on Linux platform [8].
Hassanzadeh et al contrary to above suggested that the integration of solutions is preferred to optimize monitoring mechanisms in mesh wireless intrusion detection systems. They recommended classification of solutions in this field of research [9].
Callegari et al focused on classification of non-cooperation as best proposed wireless mobile network surveillance solution, including awareness of traffic and resourcefulness. They studied about similarities of solutions based on different models. They seen how best are it to monitor traffic patterns in miscellaneous situations and they made various recommendations accordingly [10].
Sen used the evolutionary approach and conducted the survey for IDS. His approach was based on the natural algorithms, which mostly relates to the class of bio inspired computing [11].
Santana targeted the weakness of the Linux and UNIX platform. The study was based on the insecurity issues cased by API's of the built in networking facility of this these OS. He suggested ways for eliminating the security weakness operating systems [12].
Salaha et al, focused the mitigating of the starvation caused by the design of Linux in ht e CPUbound multiple processes. His work falls in the category of the operating systems security and the software design and architecture [13].
Callegari et al, investigated the behavior analysis regarding the TCP Linux and its variants [14]. Weerachai et al, worked over the USB Security Camera Software for Linux. The combined concept was the port sharing in these researches. The TP can be categorized on the priority bases and these can be assigned tags to be monitored by ID detection devices [15].

All the above studies focus the not only the network issues but all related issues like the issues of operating system, network operating system, the communication patterns, the API's of the network etc. All the researchers have focused on the various aspects of network and communication and their vulnerabilities, which can be potential area of the intrusion. The main issue is to focus on those parts of network and computer system, which requires attention for possible threats and attacks. The findings over the Linux platform have focused.

3. Methodology of Research

Design of study is based on IDS filtering for incoming traffic from network patterns. Study cares communication controls of traffic attacks and following points kept in view [13] [14]. The IDS based on real-time monitoring agent is required on host. Each Intrusion detecting system has an attack signature database. Attack signature is patterns, which are previously detected different types of attacks. IDS check all packets looking at packet format, the intruders do not detect observations etc and IDS results are valid. Data by IDS generated by real-time monitoring of network traffic by detecting malicious network activity based on configuration of IDS. IDS could detect malicious attacks even if IDTs rejects such an attempt. This information could be very useful for forensic analysis, as presented in paper. In entire procedure, no additional hardware is required for host-based intrusion detecting. Therefore, it does not need to deploy additional hardware and results in reducing deployment costs. For data collection study consisted over following techniques as study pattern i.e. controlled scenario, Intensive Network (I/N)based over Wide Area Network (WAN), mixed mode including multimedia data.

Following are the criteria or basic conditions evaluated:

Criteria A: ID excluding Firewall (FW).
Criteria B: ID including Use of FW.
Criteria C: ID including Astaro Security Linux (ASL).
Criteria D: ID including Pluggable Authentication Module (PAM).
Criteria E: ID including above three.

Table 1 contains the situations tested for above. Results of each of following is shown in tables and figures. The study carried out in real-time environment on network with verifiable results. In all cases privacy and secrecy of users kept at top level. No illegal network activity or misuse of network equipment made.

Table 1. Cases Tested

Sr No	***Various network situations tested as per mentioned criteria***
1	Over Same N/W-Client including Internal Illegal SW's with N/W-Client Machine
2	N/W-Client -to- N/W-Client Communication
3	N/W-Client -to- File Sever
4	N/W-Client -to- Multi-N/W-Client
5	Clients for Average Response
6	N/W-Client - Internal Illegal SW's
7	N/W-Client-to-N/W-Client Communication
8	N/W-Client -to- File Sever (Over Network and I/N (WAN))
9	Single Client -to- Multi-N/W-Client (Over Network and I/N (WAN))
10	N/W-Client -to- Multi-N/W-Client (Over Network and I/N (WAN))

4. Results

This portion is based on checking the effectiveness of the ID techniques. table below shows the percentage of threats controlled. These threats were taken as the test case and these are controlled by the software routines and various softwares. The nutshell of the finiding is shown in these table as the recommandation for the similar situations. The results and tables are based on the observation made on the parameters like: Ackn number, Checksum for header & data, Destination-Port number, Ethernet-Destination-Address, Ethernet-Source-Address, Finger-Buffer Overflow, Header length, IP on Ports, LAND Attack, Length of H/W-Address, Length of Protocol-Address, Ping Deaths, Ping-Flooding, Protocol of carried packet, RIP Trace, Sequence number, SRC-port number etc. The data is presented in tables as percentages of the values obtained from different scenarios. The figures are generated from these tables and the core result is discussed below [14][15].

4.1 Over Same N/W-Client including Internal Illegal SW's with N/W-Client Machine

For five mentioned categories data is gathered and shown in Table 2.

Table 2. Internal Illegal SW's

Category	*Percentage*
A	25
B	55
C	65
D	63
E	91

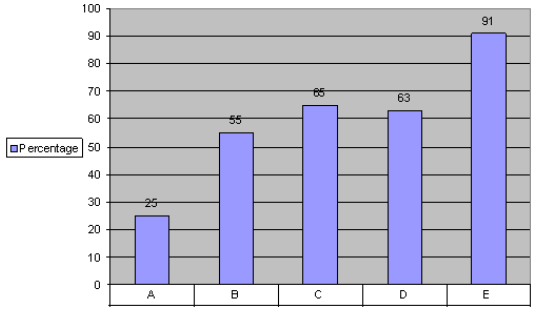

Fig. 1. Over Same N/W-Client including Internal Illegal SW's

In the Figure 1, the intrusion introduced in a controlled environment over same network client including based on internal illegal software with network client machine. Data checked with excluding FW, With FW, including both and including last three. As result it has shown that last the three of these is optimum and successful.

4.2 N/W-Client -to- N/W-Client Communication

For five mentioned categories data is gathered and shown in Table 3.

Table 3. N/W-Client -to- N/W-Client

Category	*Percentage*
A	12
B	60
C	70
D	77
E	87

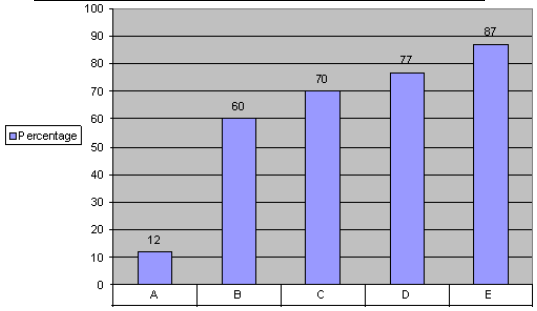

Fig 2. N/W-Client -to- N/W-Client Communication

Figure 2 shows N/W-Client -to- N/W-Client communication. Data checked with excluding FW, With FW, including both and including last three. As result it has shown that last the three of these is optimum and successful**.**

4.3 N/W-Client -to- File Sever

For five mentioned categories data is gathered and shown in Table 4.

Table 4. N/W-Client -to- File Sever

Category	*Percentage*
A	30
B	70
C	71
D	72
E	95

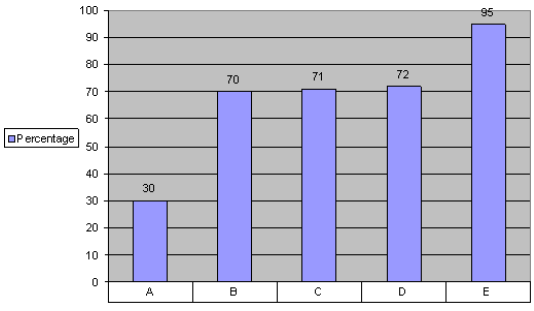

Fig 3. From N/W-Client -to- File Sever

In the Figure 3, N/W-Client -to- File Sever communication is

presented. Data checked with excluding FW, With FW, including both and including last three. As result it has shown that last the three of these is optimum and successful**.**

4.4 N/W-Client -to- Multi-N/W-Client

For five mentioned categories data is gathered and shown in Table 5.

Table 5. N/W-Client-to-Multi-N/W-Client

Category	***Percentage***
A	40
B	57
C	70
D	71
E	83

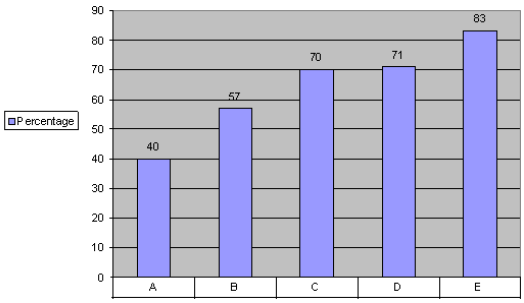

Fig 4. From N/W-Client -to- Multi-N/W-Client

In the Figure 4, N/W-Client -to- Multi-N/W-Client communication is presented. Data checked with excluding FW, With FW, including both and including last three. As result it has shown that last the three of these is optimum and successful**.**

4.5 Clients for Average Response

For five mentioned categories data is gathered and shown in Table 6.

Table 6. Group Clients Avg Response

Category	***Percentage***
A	37
B	58
C	69
D	71
E	83

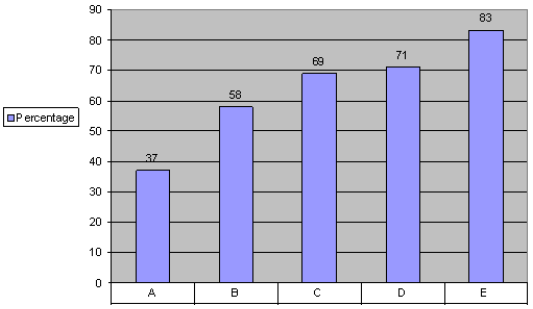

Fig 5. Group of Clients for Average Response

In the Figure 5, Clients for Average Response is presented. Data checked with excluding FW, With FW, including both and including last three. As result it has shown that last the three of these is optimum and successful**.**

4.6 N/W-Client including Internal Illegal SW's

For five mentioned categories data is gathered and shown in following Table 7.

Table 7. Over Same N/W-Client including Internal Illegal SW's

Category	***Percentage***
A	30
B	60
C	64
D	67
E	87

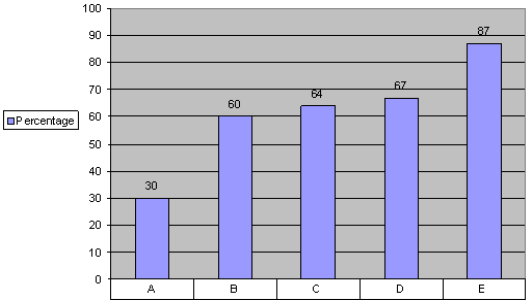

Fig 6. Same N/W-Client including Internal Illegal SW's

In the Figure 6, N/W-Client with Internal Illegal SW's communication is presented. Data checked with excluding FW, With FW, including both and including last three. As result it has shown that last the three of these is optimum and successful**.**

4.7 N/W-Client -to- N/W-Client Communication

For five mentioned categories data is gathered and shown in Table 8.

Table 8. N/W-Client -to- N/W-Client

Category	*Percentage*
A	12
B	54
C	65
D	69
E	84

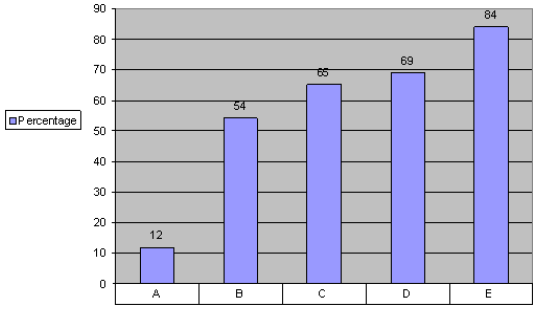

Fig 7. N/W-Client -to- N/W-Client Communication

In the Figure 7, /W-Client-to-N/W-Client Communication is presented. Data checked with excluding FW, With FW, including both and including last three. As result it has shown that last the three of these is optimum and successful**.**

4.8 N/W-Client -to- File Sever (Over N/W and WAN)

For five mentioned categories data is gathered and shown in Table 9.

Table 9. From N/W-Client -to- File Sever (Over Network and I/N (WAN))

Category	*Percentage*
A	22
B	72
C	67
D	70
E	84

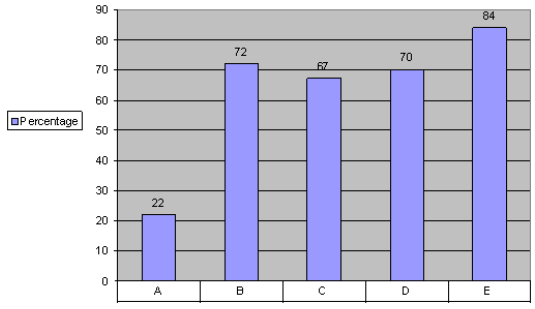

Fig 8. From N/W-Client -to- File Sever (Over Network and I/N (WAN))

In the Figure 8, N/W-Client -to- File Sever over network and internetwork over WAN is presented. Data checked with excluding FW, With FW, including both and including last three. As result it has shown that last the three of these is optimum and successful**.**

4.9 Single-Client -to- Multi-N/W-Client (Over Network and I/N (WAN))

For five mentioned categories data is gathered and shown in Table 10.

Table 10. From Single-Client -to- Multi-N/W-Client

Category	*Percentage*
A	50
B	54
C	68
D	69
E	85

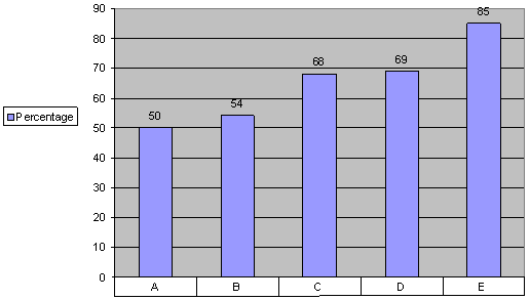

Fig 9. From Single-Client -to- Multi-N/W-Client

In the Figure 9, Single Client -to- Multi-N/W-Client over network and internetwork over WAN is presented. Data checked with excluding FW, With FW, including both and including last three. As result it has shown that last the three of these is optimum**.**

4.10 N/W-Client -to- Multi-N/W-Client (Over Network and I/N (WAN))

For five mentioned categories data is gathered and shown in following Table 11.

Table 11. Group of Clients for Average Response

Category	Percentage
A	27
B	56
C	67
D	70
E	86

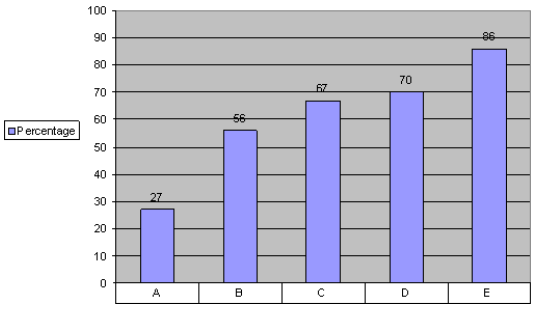

Fig 10. Group of Clients for Average Response

In the Figure 10, N/W-Client -to- Multi-N/W-Client over network and internetwork over WAN is presented. Data checked with excluding FW, With FW, including both and including last three. As result it has shown that last the three of these is optimum and successful.

5. Conclusion

IDS with more collective options enables automatic detecting of malicious activity and notify administrator, to prevent from malicious access connections. Although IDS has not reached at stage that it could give ideal detection at any level of invasion. The successful implementation of IDS depends largely on how it is deployed. Many plans require design and implementation stages. It is observed that desirable solution based on a mixed network host-based IDS is benefiting in above situations. Therefore organizations can implement a hybrid solution. IDS have been always been reactive rather than proactive. IDS technology is suitable for attack signatures. Attack should be characterized by a previous attack mode. IDS in mixed mode ensured monitoring and reporting intruders attempting illegal jobs. IDS function must be an integral part of company's security policy.

References

[1] Dinh, Hoang, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," Wireless communications and mobile computing, vol.13, no. 18, pp. 1587-1611, 2013.

[2] Majhi, S. Kumar, and S. Dhal, "Placement of Security Devices in Cloud Data Centre Network: Analysis and Implementation," Procedia Computer, vol. 78, pp.33-39, 2016.

[3] Joseph and R. Bala, "Enhanced Tree Based Real Time Intrusion Detection System in Big Data," International Journal of Computers & Technology, vol. 15, no. 3, pp. 6563-6569, December 15, 2015.

[4] Rajendran, P. Kumar, B. Muthukumar, and G. Nagarajan, "Hybrid intrusion detection system for private cloud: A systematic approach," Procedia Computer Science, pp. 325-329, 2015.

[5] Krishnan and Deepa, "A distributed self-adaptive Intrusion Detection System for Mobile Ad-hoc Networks using tamper evident mobile agents," Procedia Computer Science pp.1203-1208, 2015.

[6] Vladimir, Rubanov and D. Silakov, "Ensuring portability of Linux applications through standardization and knowledge base driven analysis," Science of Computer Programming pp. 234-248, 2014.

[7] Israeli, Ayelet, and D. Feitelson, "The Linux kernel as a case study in software evolution," Journal of Systems and Software, vol. 83, no. 3, pp. 485-501, 2014.

[8] Azazi, Khafizuddin, R. Andrean, W. Atmadja, M. Handi, and J. Lukas, "Design of Mobile Robot with Navigation Based on Embedded Linux," Procedia Computer Science, pp.473-482, 2015.

[9] H. Amin, A. Altaweel, and R. Stoleru, "Traffic and resource aware intrusion detection in wireless mesh networks," Ad Hoc Networks, pp.18-41, 2014.

[10] G. Calarco and M. Casoni, "On effectiveness of Linux containers for nebothrk virtualization," Simulation Modelling Practice and Theory, vol. 31, pp. 169–185, 2013.

[11] Sen, "A Survey of Intrusion Detection Systems Using Evolutionary Computation," Bio-Inspired Computation in Telecommunications, pp. 73-94, 2013.

[12] M. Santana, "Eliminating Security Weakness of Linux and UNIX Operating Systems," Computer and Information Security Handbook, pp. 183–196, 2013.

[13] K. Salaha and A. Maneab, "Mitigating starvation of Linux CPU-bound processes in presence of nebothrk I/O," Journal of Systems and Software, vol 85, no. 8, pp. 1899–1914, 2012.

[14] C. Callegari, S. Giordano and M. Pagano, "Behavior analysis of TCP Linux variants," Computer Networks, vol 56, no. 1, pp. 462–476, 2012.

[15] J. Weerachai and P.Siam, "USB Security Camera Software for Linux," Procedia Engineering, vol. 8, pp. 171–176, 2011.

Ramzan Talib is Associate Professor at the Department of Computer Science at the Government College University, Faisalabad. He received his PhD from the University of Bayreuth, Germany. His research interests include Databases and Information Systems, Data Mining, Data Warehousing, Business Process Management, Workflow Management Systems.

Muhammad Kashif Hanif is Assistant Professor at the Department of Computer Science at the Government College University, Faisalabad. He received his PhD from Hamburg University of Technology. His research interests cover big data analytic, parallel scientific computing, social media networks, and data mining.

Muhammad Yahya Saeed received the MSc degree from UAAR, Rawalpindi, in Computer Science in 2003 and M.S degrees in Computer Science from UAF, Faisalabad in 2007. He has also done MSc from UAF, Faisalabad in Statistics in 2000. Currently he is doing PhD from GCUF, Faisalabad in Computer Science since 2015. He is faculty member in GCUF in software

Engineering Department.

Muhammad Umer Sarwar is PhD scholar at the Department of Computer Science at the Government College University, Faisalabad. His research interests are database systems, text and data mining.