

An effective intrusion detection algorithm for packet transmission in security trust architecture

¹S. N. PANDA and ²GAURAV KUMAR

¹Professor, Regional Institute of Management and Technology [RIMT],
Mandi Gobindgarh, Punjab (INDIA)
E-mail: panda.india@gmail.com

²Sr. Lecturer, Computer Applications
Chitkara Institute of Engineering and Technology, Rajpura, Punjab (INDIA)
E-mail: kumargaurav.in@gmail.com

(Acceptance Date 20th January, 2010)

Abstract

Intrusion detection and corrective measures in the networks is one of the challenges in the fast growing world of Cyber Crime. The network establishments are facing various types of threats on routine basis. To efficiently transmit information across a network, there is need of an improved and reliable architecture. The intrusion detection systems should be developed with utmost care to avoid any natural or intentional attempts. Moreover, the packet encryption algorithm should be developed in such a way so that cracker is not able to change even a single bit in the confidential data. This paper proposes an efficient algorithm for Packet Encryption as well as the standard to detect any kind of intercept attempt.

Key words : Intercept Detection, Intrusion Detection, Trust Architecture, E-Transactions, Interception Analysis and Forensics, Packet Encryption, Packet Decryption.

Introduction

Business as well as defense applications are expected to have highly secured and consistent architecture so that packets can be transmitted in the network without any risk. Trust is the groundwork of the relationship which is established by a business organization with their customers, vendors, and employees.

The speed at which computer network communications is taking place is increasing. It is therefore important to make the routines that send and receive network communication packets as efficient as possible such that information can be transmitted as fast as possible.¹

In order to achieve security and privacy

in Wireless Sensor Networks, it is necessary to implement and deploy a certain number of mechanisms.²

According to the ITU-T X.509, Section 3.3.54, trust is defined as: “Generally an entity can be said to ‘trust’ a second entity when the first entity makes the assumption that the second entity will behave exactly as the first entity expects.”³

Network Intercept provides solutions

for Individuals and businesses looking to detect and avoid malicious intent on the internet, improve productivity, and protect their online privacy.⁴

Proposed architecture and algorithms :

The proposed architecture consists of various phases which will include algorithms for encryption and decryption of data packet alongwith the technique to analyze the overall interception patterns.

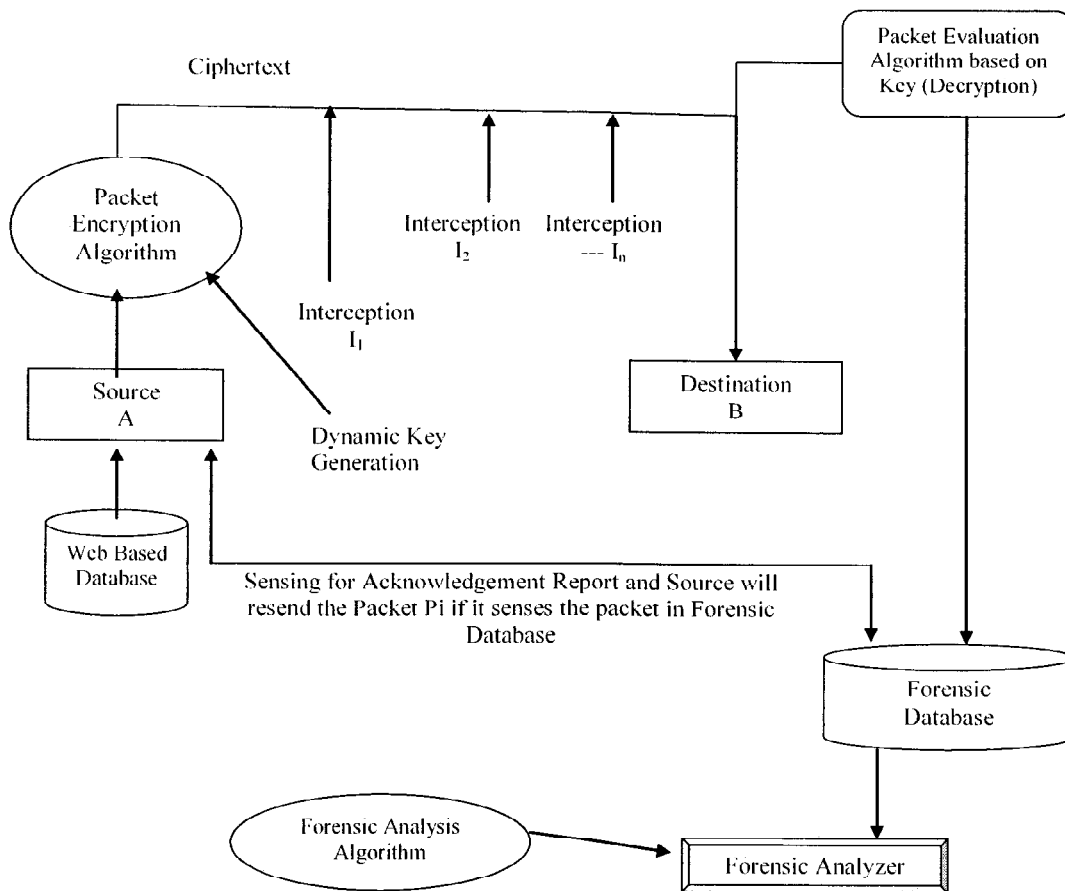


Figure 1. The Proposed Trust Architecture for Intercept Management

Algorithmic approach :

Step 1: Initialize & Activate Packet P_i at Source S_i for transmission to Destination D_i

Step 2: Packet Encryption Module PE_k based on Dynamic Key k Generation, once the Packet moves from Source S_i

$$C_i := PE_k(P_i)$$

Step 3: Transmission of Encrypted Packet C_i using specified Path/Route R_i , $C_i \rightarrow D_i[R_i]$

Step 4: Packet Authentication on Decryption

IF ($C_i = PD_k(C_i)$ // Packet Decryption Module PD_k to decrypt the packet at destination BEGIN

(a) DEST $[i] := PD_k(C_i)$

(b) Successful Delivery of Packet

(c) ACK sent to Source S_i // Acknowledgement ACK is delivered to Source in case of Success

END

ELSE

BEGIN

(a) A record will be inserted in the Forensic Database. The Interception Table will consist of the Structure (Id, Interception Type, Timestamp of Interception). // Acknowledgement ACK is sent to Forensic Database in case of Failure Attempt

(b) Source S_i senses the Forensic Database. Select All Records from Forensic Database IF (true) Then

print "Failure Delivery, Retransmit the

packet"

(c) GOTO Step 1

(d) Update Forensic Analyzer Database for taking remedial actions. END

Step 5: Forensic Analyzer

(a) Retrieve Records for analysis of interceptions.

(b) Analyze the type T_i of Intercept

(c) Perform remedial stroke for avoiding the stored interception type

Packet encryption algorithm :

Step 1: Activate and Initialize the Packet P_i

Step 2: Generate a Random Key K_R by analyzing number of 1s in Packet.

(a) Develop a routine to count bits in the Data Packet

(b) Set $N := \text{Count}(P_i)$ // Count Number of 1's in the Data Packet.

(c) Set $K_R := N$ // Store N in Random Number K_R

Step 3: Apply XOR (Exclusive-OR) Operation

(a) Set $E_K := P_i \oplus K_R$

(b) The Encrypted Packet E_K is generated using XOR Operation.

(c) Set $PE_K := E_K$ // Utilize E_K as Encrypted Packet

Step 4: Packet equipped for Transmission

Decryption and intercept detection algorithm:

Step 1: Receive the Encrypted Packet PE_K

Step 2: Check the Front PF_i and Rear End PR_i of Packet

if ($PF_i = PR_i$)
Accept PF_i
Set $K_R := PF_i$
else
goto Step 5

Step 3: Generate the Binary Equivalent of K_R
 $PB_i = \text{Binary}(K_R)$

Step 4: Perform XOR Operation

if ($PB_i = PE_K$)
Decryption Successful
Accept the Packet
else
goto step 5

Step 5: Insert the Record of Corrupt Packet in Forensic Database

Conclusion

There is need for securing the network from multiple interceptions using efficient algorithms. The packet encryption algorithm

explained in the paper is an efficient algorithm based on Exclusive-OR operation which is a unique method. Using this method, encryption and decryption can be performed effectively.

References

1. Cochavy, Baruch, Method of efficiently sending packets onto a network by eliminating an interrupt, US Patent Issued on August 18 (1998).
2. Dimitris M. Kyriazanos, Neeli R. Prasad, Charalampos Z. Patrikakis, A Security, Privacy and Trust Architecture for Wireless Sensor Networks, 50th International Symposium ELMAR-2008, 10-12 September, Zadar, Croatia (2008).
3. Donna Andert, Robin Wakefield, and Joel Weise, Professional Services Security Practice, Sun BluePrints™ OnLine - December, Trust Modeling for Security Architecture Development (2002).
4. Security, Encryption, Acceleration, <http://www.networkintercept.com> Last Accessed July 27, (2009).