International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 6 Issue 4 July 2016
International Manuscript ID : 2249054XV6I4072016-10

SECURED AND EFFECTIVE DATA COMMUNICATION APPROACH USING METAHEURISTICS

Priyanka
Assistant Professor, EE Department
YMCA University of Science and Technology
Faridabad, Haryana, India

ABSTRACT

The network establishments are facing numerous threats on routine basis and number of algorithms has been developed to transmit the data packets through secured and reliable architecture. To efficiently transmit information across a network, there is always the need of an improved and reliable architecture. An intrusion or intercept refers to an active sequence of events that deliberately try to cause harm, such as rendering system unusable, accessing unauthorized information, or manipulating such information. Security professionals may want to have Intercept Detection Systems record information about both successful and unsuccessful attempts so that security professionals will have a more comprehensive understanding of the events on their networks. The intercept detection systems should be developed with utmost care to avoid any natural or intentional attempts. Forensic database maintenance and analysis comes to the scene to study this aspect. There is need of an efficient technique to save all the interception attempts for further research so that these can be detected and traced out quickly. This paper proposes an efficient technique for the analysis of forensic database so that the type and nature of interception can be detected and the existing system can be improved. The proposed approach integrates the metaheuristic approach for higher security and integrity for overall performance of assorted networks.

Keywords – Intercept Detection, Intrusion Detection, Trust Architecture, E-Transactions, Interception Analysis and Forensics, Forensic Database

INTRODUCTION

With the advent of Globalization, the Business as well as Defense Applications needs 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 [1]. 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.

In order to achieve security and privacy in Wireless Sensor Networks, it is necessary to implement and deploy a certain number of mechanisms.

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." Trust is the establishment of confidence that something will or will not occur in a predictable or promised manner. The enabling of confidence is supported by identification, authentication, accountability, authorization, and availability [2].

To develop the trust between multiple parties, a set of principles or rules is to be offered so that the security of the entire model can be improved. A study by McAfee has estimated that cyber crime losses may have passed $1 trillion in 2008, and, if a solution is not identified and implemented soon, that number is projected to grow with the slumping economy. 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.

INTERCEPT DETECTION SYSTEMS AND RELATED THREATS

An intrusion-detection system (IDS) refers to the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity [3]. The intrusion detection part of the name is a bit of a misnomer, as an IDS does not actually detect intrusions—it detects activity in traffic that may or may not be an intrusion. Intrusion detection is typically one part of an overall protection system that is installed around a system or device, it is not a stand-alone protection measure.

It is also important to note that IDSs and IPSs are just two of many methods that should be employed in a strong security program. Using a layered approach, or defense in depth, based on careful risk analysis is critical in any information protection program because a network is only as secure as its weakest link. This means that a network should have multiple layers of security, each with its own function, to complement the overall security strategy of the organization.

Intercept Detection and Prevention Systems are vital for many organizations, from small offices to large multinational corporations with many benefits:

- Greater proficiency in detecting intrusions than by doing it manually
- In-depth knowledge bases to draw from
- Ability to deal with large volumes of data
- Near real-time alerting capabilities that help reduce potential damages
- Automated responses, such as logging off a user, disabling a user account, or launching automated scripts
- Strong deterrent value
- Built-in forensic capabilities
- Built-in reporting capabilities

The most common types of threats fall into categories such as:

- Actual or attempted unauthorized probing of any system or data
- Actual or attempted unauthorized access
- Introduction of viruses or malicious code
- Unauthorized modification, deletion, or disclosure of data
- Denial of service attacks

These are all very good reasons to implement these technologies, but there are three main reasons that justify the need more than the others:

Legal and regulatory issues In 1998, the U.S. Presidential Decision Directive 63 (PDD 63) established steps to increase the use of intrusion detection and prevention to protect the national infrastructure. British Standard 7799 was first published in February 1995 and identified a comprehensive set of controls defining "best practices" for information security. Regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Gramm-Leach-Bliley Act of 1999 (GLBA) require audit controls to record and examine suspicious data-access activities. The preceding regulations may or may not be necessary, depending on the nature and location of your organization. In addition, implementation of an IDS/IPS program is not a requirement for complying with any of these, but will help to meet the requirements.

Quantification of attacks IDS and IPS allow a systems administrator the opportunity to quantify attacks against the organization's network for management. IDSs and IPSs both are able to build a profile of the types of attacks that are being tried against a network. This allows a stronger business case to be made for appropriate security measures, which can often be hard to justify. IPSs and IDSs can also provide evidence against attackers if litigation is desired.

Establishment of an overall defense-in-depth strategy IDSs and IPSs have become a critical part of a strong defense-in-depth security program, and their use shows due diligence on the part of the organization because the organization is being proactive in the expectation of and reaction to intrusions. Both technologies will help provide protection for network and application layer vulnerabilities, as well as help to correlate and validate information from other devices, such as antivirus programs, firewalls, and routers.

The advantages of intercept detection include the following:

- Can detect external hackers as well as internal network-based attacks
- Scales easily to provide protection for the entire network
- Offers centralized management for correlation of distributed attacks
- Provides defense in depth
- Gives system administrators the ability to quantify attacks
- Provides an additional layer of protection

INTRUSION-PREVENTION SYSTEM (IPS)

Unlike IDS, the logic in an IPS is applied before the action is executed in memory. Other IPS methods compare file checksums to a list of known

good checksums before allowing a file to execute, and to work by intercepting system calls [4].

An IPS will typically consist of four main components:

- Traffic Normalizer
- Service Scanner
- Detection Engine
- Traffic Shaper

The traffic normalizer will interpret the network traffic and do packet analysis and packet reassembly, as well as performing basic blocking functions. The traffic is then fed into the detection engine and the service scanner. The service scanner builds a reference table that classifies the information and helps the traffic shaper manage the flow of the information. The detection engine does pattern matching against the reference table, and the appropriate response is determined.

PROPOSED SECURITY TRUST ARCHITECTURE

Metaheuristics are renowned to present very efficient elucidation to many of today's combinatorial optimization problems in engineering, industrial, economical and scientific domains such as transportation, bioinformatics, logistics, business etc. Scheduling, timetabling, vehicle routing, resource allocation are intelligently and successfully tackled with Metaheuristic approaches such as Simulated Annealing, Tabu Search, Ant Colony Optimization, Harmony Search, Scatter Search, Iterated Local Search. Metaheuristics present itself as highly promising choice for nearly-optimal solutions in reasonable time where exact approaches are not applicable due to extremely large running times or other limitations. Meta-heuristic is a master strategy that guides and modifies other heuristics to produce solutions beyond those that are normally generated in a quest for local optimality. This paper highlights the various contemporary real life applications of Metaheuristics in the domain of industrial engineering and NP-hard problems.

Metaheuristics can solve Combinatorial Optimization Problems, like cutting and packing, routing, network design, assignment, scheduling, or time-tabling problems, continuous parameter optimization problems, or the optimization of non-linear structures like neural networks or tree structures as they often appear in computational intelligence.

Evolutionary Algorithms (EAs), in particular, comprise a variety of related algorithms that are based on the processes of evolution in nature. In contrast to several other Metaheuristics, they work on a set of concurrent solutions and can easily be parallelized.

Especially the combination of evolutionary algorithms with problem-specific heuristics, local-search based techniques, approximation methods and exact techniques often make possible highly efficient optimization algorithms for many areas of application.

Metaheuristics are generally applied to problems for which there is no satisfactory problem-specific algorithm or heuristic; or when it is not practical to implement such a method. Most commonly used Metaheuristics are targeted to combinatorial optimization problems, but of course can handle

any problem that can be recast in that form, such as solving boolean equations.

In spite of overly-optimistic claims by some of their advocates, Metaheuristics are not a panacea, and their indiscriminate use often is much less efficient than even the crudest problem-specific heuristic, by several orders of magnitude.

Main Features of a Good Metaheuristics

- Population intrinsic parallelism
- Indirect Coding
- Cooperation adapted crossover
- Local search in solution space
- Diversity need to be controlled
- Easy to implement the restarts
- Randomness

Commonly used metaheuristic methods

- TS : Tabu search [Glover, 89 et 90]
- SA : Simulated annealing [Kirckpatrick, 83]
- TA : Threshold accepting [Deuck, Scheuer, 90]
- VNS : Variable neighborhood [Hansen, Mladenovi´c, 98]
- ILOCAL SEARCH : Iterated local search [Loren¸co et al, 2000]
- GENETIC ALGORITHM : Genetic Algorithm, Holland 1975 – Goldberg 1989
- MA : Memetic Algorithm, Moscatto 1989
- Hybrid Genetic Algorithm
- Ant Colony Optimization, Dorigo 1991
- Scatter search, Laguna, Glover, Marty 2000

Innumerable variants and hybrids of these techniques have been proposed, and many more applications of Metaheuristics to specific problems have been reported. This is an active field of research, with a considerable literature, a large community of researchers and users, and a wide range of applications.

PROPOSED ARCHITECTURE

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.

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 6 Issue 4 July 2016
International Manuscript ID : 2249054XV6I4072016-10

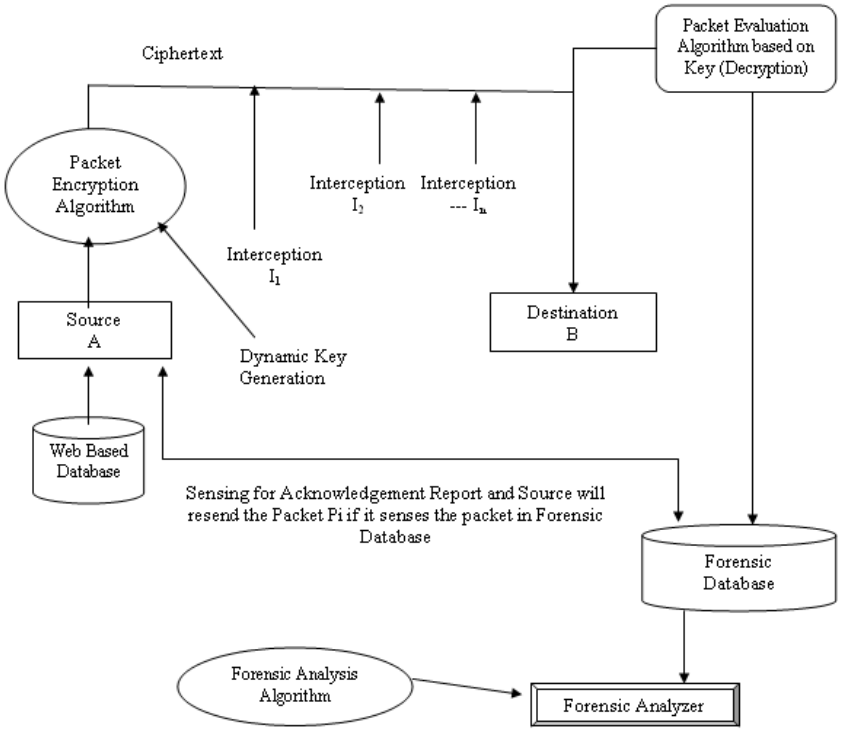

Figure 1 : The Proposed Trust Architecture for Intercept Management

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

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 6 Issue 4 July 2016
International Manuscript ID : 2249054XV6I4072016-10

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*

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.

STRUCTURE OF FORENSIC DATABASE

In the proposed architecture, Advance NoSQL Metaheuristic Compliant will be used as forensic database with following fields.

Interception Attempts

ID	***Source IP***	***Destination IP***	***Timestamp***	***Bytes Altered***

ID – Unique Auto-Increment Identification

Source IP – IP Address of Source System from where the packet was transmitted

Destination IP – IP Address of Destination System where the packet was supposed to reach

Timestamp – Time at which the record is inserted in the table

Bytes Altered – Number of bytes altered by the interception attempt

This table will be associated with another table with following fields

Interception Type

ID	***Bytes Altered***	***Occurrences***	***Interception Type***

ID – Foreign Key to Table Interception Attempt

Bytes Altered – Data imported from Table Interception Attempt

Occurrences – The number of similar attempts

Interception Type – Association of a Type to the Interception occurred

ALGORITHMIC APPROACH FOR FORENSIC ANALYZER

Step 1:

Creation of Secured NoSQL Database Connection

Step 2:

Analyze the Field Bytes Altered in the relation Interception Attempt

Step 3:

Associate a Unique Interception Type to the ID and insert a record in the Table Interception Type

Step 4:

if another same record of same Bytes Altered is encountered

Increment Occurrences

Keep other fields same

Step 5:

Full Outer Join Operation on both tables

Generate Detailed Report of the Interception Type and Number of Occurrences

CONCLUSION

Secured data communication is when two entities are communicating and do not want a third party to listen in. For that they need to communicate in a way not susceptible to eavesdropping or interception. Secure communication includes means by which people can share information with varying degrees of certainty that third parties cannot intercept what was said. Other than spoken face-to-face communication with no possible eavesdropper, it is probably safe to say that no communication is guaranteed secure in this sense, although practical obstacles such as legislation, resources, technical issues (interception and encryption), and the sheer volume of communication serve to limit surveillance. With many communications taking place over long distance and mediated by technology, and increasing awareness of the importance of interception issues, technology and its compromise are at the heart of this debate. For this reason, this manuscript focuses on communications mediated or intercepted by technology and its security using metaheuristic approach.

REFERENCES

[1] Pathan, A. S. K. (Ed.). (2016). Security of self-organizing networks: MANET, WSN, WMN, VANET. CRC press.

[2] Huberman, B. A. (2016). Ensuring Trust and Security in the Industrial IoT: The Internet of Things (Ubiquity symposium). Ubiquity, 2016(January), 2.

[3] Chaudhary, A., Tiwari, V. N., & Kumar, A. (2016). A new intrusion detection system based on soft computing techniques using neuro-fuzzy classifier for packet dropping attack in manets. International Journal of Network Security, 18(3), 514-522.

[4] Farhaoui, Y. (2016). How to secure web servers by the intrusion prevention system (IPS)?. International Journal of Advanced Computer Research, 6(23), 65.

[5] Donoso, Y., & Fabregat, R. (2016). Multi-objective optimization in computer networks using metaheuristics. CRC Press.