International Journal of Information Science and Education.
ISSN 2231-1262 Volume 4, Number 1 (2017) pp. 11-19
© Research India Publications
http://www. ripublication.com

An Cyber Incident Detections Using Key Pairs in Distributed Computing Community

[1]Aurobind. G, [2]Barath. A, [2]Suganya. M, [2]Vijiyakumar. K
[1]Virtual Knowledge Network (VKN)
National Institute of Mental Health and Neuro Sciences (NIMHANS), Bengaluru, India
[2]Department. of Information Technology
Manakula Vinayagar Institute of Technology, Pondicherry, India

Abstract

Communities are under attack from a variety of threat agents. Communities have a devastating impact on the individuals and organization. So the attacks on community become increasingly reliant upon cyberspace. The cyber attacks mainly detecting using a fast and effective response. In this paper kv_pairs (key values) of keys used to transmit the information in the networks. The four main attributes which are unique to every user are joined to determine the pairs of keys. These attributes can be formed in a different combination while transmitting the information between communities. So it is not easy to detect the keys in a network. kv_pairs is used as the routing key in the DHT(distributed hash table).In the receiver side, the pairs of keys are hash using SHA hash function technique to compare the pairs of keys. RSA algorithm is used for the encryption and decryption of both the side in networks. In addition with this, a secret key is added through the network to protect the unauthorized monitoring through the network by eavesdropping attack. So the anonymity is maintained between communities in the organization thereby it encourages the participation of user to share their information without any hesitation and in a secured manner.

Keyterms: Kv_pair keys, DHT(Distributed Hash Table), MD-5 hash function technique, Secret Key

1. INTRODUCTION

Cyber attacks on a community can have a devastating impact on the individuals, organizations, and governmental entities within the community. Throughout this paper, when we refer to a community we do so from a geographic perspective rather than from a sector-based perspective[1].

Communities must prepare for cyber incidents by following a defense in depth strategy that includes prevention, detection, response, and recovery. The timely and useful detection of community cyber incidents is the first step towards a fast and effective response and recovery. Performing information sharing and detection in a distributed manner requires that we assign each *kv_pairs* to a node in the network. No matter where or when a specific *kv_pairs* is observed[2], it is consistently sent to its assigned node, which is responsible for counting the number of observations throughout the community. In order to achieve this *kv_pairs* is used as the routing key in a DHT (Distributed Hash Table).

Detecting attacks on communities can be viewed as similar to CIDSs (Collaborative Intrusion Detection Systems). In a CIDS, member nodes share information with each other to improve detection accuracy. We however, want to share information in order to detect attacks on the community as a whole. A recent survey of CIDSs found three open problems that still need to be addressed: expressiveness, scalability, and accuracy[3]. We believe the information sharing and detection framework presented here meets the objectives of expressiveness and scalability.

2. REVIEW OF RELATED WORKS

Here they use the random keys concepts to transfer the information from one node to the other node. Since because of using the random keys there is no strengthening of security among the networks. There is no strengthening of networks against the smaller scale and large-scale systems. No node to node authentication between the networks when data is transmitted. There is an increase of vulnerabilities in large-scale systems [4]. So in this paper, we use the pair of keys for transmitting the message. The pair of keys is unique and much secure for every message.

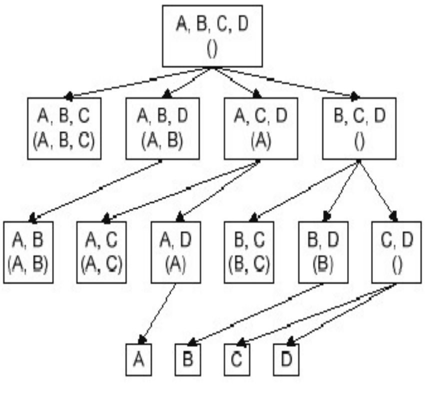


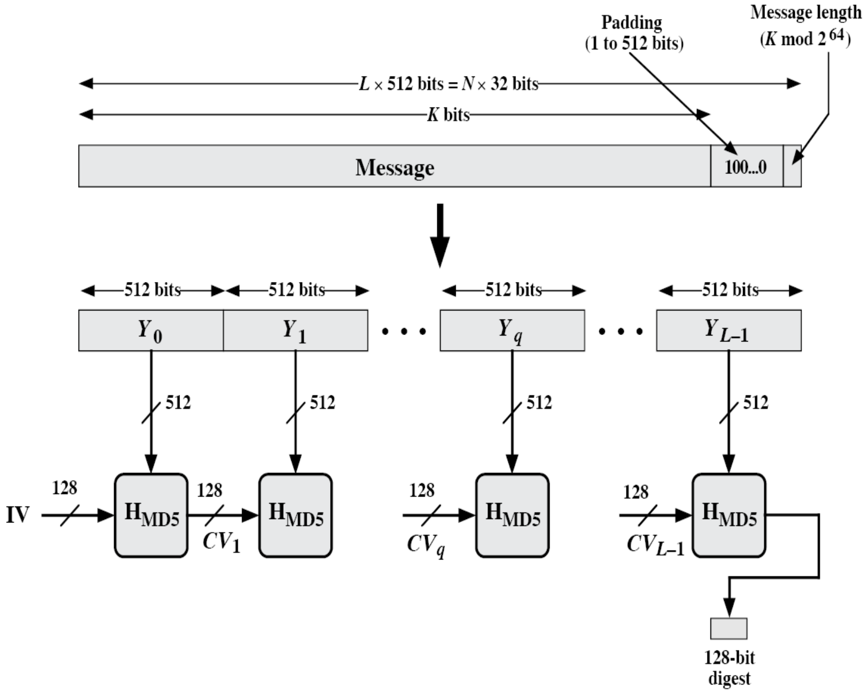
Figure 2. Efficient distributed combinatorial tree traversal

HASHING TECHNIQUE

Hashing includes an effective way of storing a set of elements by detaching the possible keys from the universe[5][6][7]. The data elements in the memory are placed in a position by ciphering directly from the key. It performs many operations like insert, search, modify and delete.

The data are transferred at a high speed due to the hashing function. So it has a high performance and an efficient storage system. In this method, we use MD-5 Hashing technique.

Messages are authenticated because of hashing function and so the messages are get digested and sent in the network system. Using hashing technique, it compares the messages at another side.

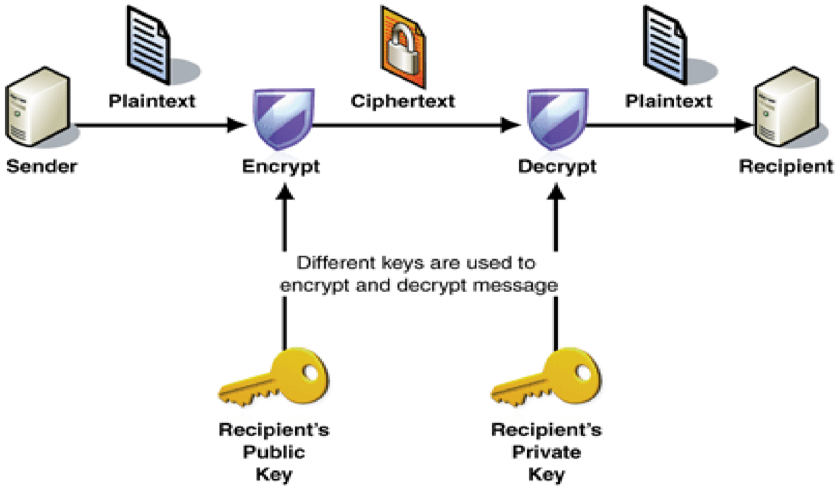


The function is applied on operand (file) which results on message digest or digital signature where the mathematical formula acts as a hash function. Just like the mathematical function “multiply by seven” will produce 49 when the operand is seven and 35 when the operand is five, the hash function will create a unique message digest based on the contents of the file[8][9].

ENCRYPTING TECHNIQUE

When the message digest is created by the hashing technique, it gets encrypted.

Encryption is a way of encoding the messages in such a way that a hacker or a keypuncher cannot understand it but the authorized parties can access it. In an encryption technique[10], the message or information (plain text) is encrypted using an encryption algorithm and the output reaches in an unreadable format (cipher text)[12].



An individual requires a unique digital identity to which he is constrained (social security number) to encrypt any message[13][14][15]. The pair of keys are issued to the unique identifier, one is private (known only to the individual) and another is public (used by individuals for exchanging encrypted messages with the owner of the private key)[16][17].

Encrypting is converting the original message (plain text) to secret message (cipher text) and it is mainly used for security purpose[18].

At both sides of the network, a private key is used between the members of the organization for encryption and decryption. RSA algorithm is majorly used in this paper and it provides the confidentiality to all the messages which are in the form of secret code.

Since it contains the source and destination IP address and port address it provides a good security to the message transmitting through the network. This pair of keys also changes for every 1 minute and so it is not easy to detect or guess the message patterns in the network. Collaborative intrusion detection framework: characteristics, adversarial opportunities, and countermeasures complex internet attacks may come from multiple sources, and target multiple networks and technologies[19]. Here too intrusion detection system cannot find all types of attacks in the large-scale systems[20].so, we go for collaborative intrusion detection systems(CID's) which CID's also help to cope with classical problems of intrusion detection systems (ids) such as zero-day attacks[21], high false alarm rates, and architectural challenges[22].

3. PROPOSED SYSTEM

In the proposed System attributes of keys are used to transmit the information from source to destination to maintain the security in the network.

The attributes are:

→ ip_src: The Source IP Address

→dst_port: The Destination Port

→src_port: The Source Port

→alert_type: The IDS Alert

Here we transmit the information using the pair of Keys called kv_pairs. Each combination of pairs is referred to every community. These four attributes are combined in the form of different pairs and sent in the network. So it is not that much easy to detect since it is of different pairs which are different for each information. Unlike symmetric key cryptography, we do not find historical use of public-key cryptography. It is a relatively new concept.

Symmetric cryptography was well suited for organizations such as governments, military, and big financial corporations were involved in the classified communication.

With the spread of more unsecure computer networks in last few decades, a genuine need was felt to use cryptography at larger scale. The symmetric key was found to be non-practical due to challenges it faced for key management. This gave rise to the public key cryptosystems.

The most important properties of public key encryption scheme are −

- Different keys are used for encryption and decryption. This is a property which set this scheme different than symmetric encryption scheme.
- Each receiver possesses a unique decryption key, generally referred to as his private key.
- Receiver needs to publish an encryption key, referred to as his public key.
- Some assurance of the authenticity of a public key is needed in this scheme to avoid spoofing by adversary as the receiver. Generally, this type of

cryptosystem involves trusted third party which certifies that a particular public key belongs to a specific person or entity only.

- Encryption algorithm is complex enough to prohibit attacker from deducing the plaintext from the ciphertext and the encryption (public) key.
- Though private and public keys are related mathematically, it is not be feasible to calculate the private key from the public key. In fact, intelligent part of any public-key cryptosystem is in designing a relationship between two keys.

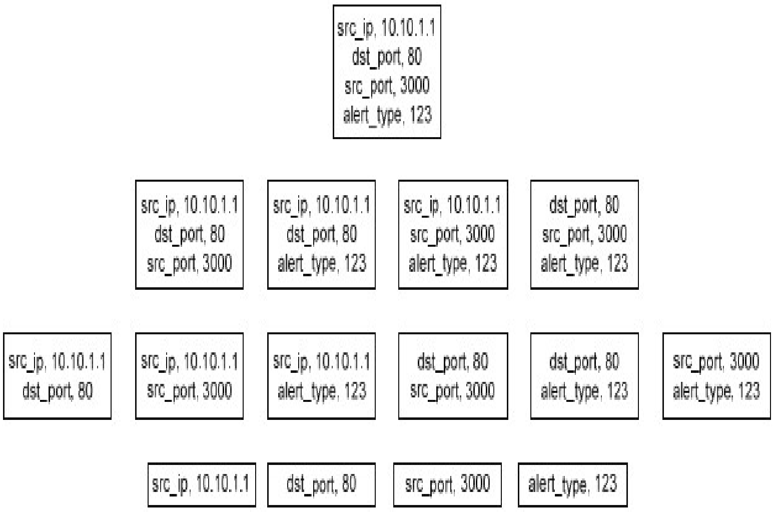


Figure 1. All *kv_pairs* resulting from a specific IDS alert

That is the source IP address, source port, destination port, ids alert type are different for each and every users who transmit the information.

It differs from one to one and it is much unique.

The attributes can be made into a different combination such that the pairs cannot be detected by the attackers or hackers.

COMBINATION PAIRS OF ATTRIBUTES

The different combinations are:

→ src_ip, dst_port, src_port

→ src_ip, dst_port, alert_type

→ src_ip, src_port, alert_type

→ dst_port, src_port, alert_type

→ src_ip, dst_port

→ src_ip, src_port

→ src_ip, alert_type

→ dst_port, src_port

→ dst_port, alert_type

→ src_port, alert_type

→ src_ip

→ dst_port

→ src_port

→ alert_type

A node observing an IDS alert calculates all possible combinations.

This allows a single node in the network to store and analyze all occurrences of specific kv_pairs for the entire community.

CONCLUSION

Hence in this paper, there is more security in transmitting the message. The members in the organizations can share the messages with each other without any hesitation in them. More anonymity is provided to the organizations. Security maintained by using key pairs which is unique to every message, key pairs changing per 1 minute, hashing technique, encrypting and decrypting, secret key sharing and IDS alert messages. Hence the message which is transmitted through the network is much secure between the distributed community by cyber incident detection.

REFERENCES

[1] Cristina Abad et al., "Log correlation for intrusion detection: A proof of concept," in *In Proceedings of the 19th Annual Computer Security Applications Conference*, 2003, pp. 255-246.

[2] Michael K. Reiter and Aviel D. Rubin, "Crowds: Anonymity for web transactions," *ACM Transactions on Information and System Security*, vol. 1, pp. 66-92, 1997.

[3] Cristina Abad et al., "Log correlation for intrusion detection: A proof of

concept," in *In Proceedings of the 19th Annual Computer Security Applications Conference*, 2003, pp. 255-246.

[4] Donald E. Knuth, *The art of computer programming, volume 2: Seminumerical algorithms,* 3rd ed. Boston: Addison-Wesley, 1998.

[5] *An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks.* O Depren, M Topallar, E Anarim, MK CilizExpert systems with Applications 29 (4), 713-722

[6] Coifman, B. (1999) "Using Dual Loop Speed Traps to Identify Detector Errors," TRB, *Transportation Research Record* 1683, pp 47-58.

[7] Coifman, B., Cassidy, M. (2002). "Vehicle Reidentification and Travel Time Measurement on Congested Freeways", *Transportation Research. Part A: Policy and Practice*, 36(10), pp. 899- 917.

[8] Jain, M., Coifman, B., (2005) "Improved Speed Estimates from Freeway Traffic Detectors," *ASCE Journal of Transportation Engineering*, Vol 131, No 7, pp 483-495.

[9] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing,* 1(1):11-32, January-March 2004.

[10] R. Bobba, "PBES: A Policy Based Encryption System with Application to Data Sharing in the Power Grid", *Proc. 4th Int'l Symp. Information Computer and Communications Security (ASIACCS 09)*, pp. 262-275, 2009.

[11] "Public key infrastructure", *Wikipedia,* Feb. 2010.

[12] H. Chan, V. D. Gligor, A. Perrig, and G. Muralidharan. On the distribution and revocation of cryptographic keys in sensor networks. *IEEE Trans. Dependable Secur. Comput*., 2005

[13] L. Eschenauer and V. Gligor. A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM Conference on Computer and Communications Security, pages 41-47, 2002.

[14] M. Luk, G. Mezzour, A. Perrig, and V. Gligor. Minisec: A secure sensor network communication architecture. *In Sixth International Conference on Information Processing in Sensor Networks (IPSN 2007)*, April 2007.

[15] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. E. Culler. Spins: Security protocols for sensor networks. *Wireless Networks,* 8(5):521-534, September 2002.

[16] Kong, D. and Yan, G. (2013) Discriminant Malware Distance Learning on Structural Information for Automated Malware Classification. *Proceedings of*

the ACM SIGMETRICS/International Conference on Measurement and Modeling of Computer Systems, 347-348.

[17] Tian, R., Batten, L., Islam, R. and Versteeg, S. (2009) An Automated Classification System Based on the Strings of Trojan and Virus Families. *Proceedings of the 4th International Conference on Malicious and Unwanted Software*, Montréal, 13-14 October 2009, 23-30.

[18] Hall, M., Frank, E., Holmes, G., Pfahringer, B., Reutemann, P. and Witten, I. (2009) The WEKA Data Mining Software: An Update. *ACM SIGKDD Explorations Newsletter*, 10-18.

[19] Santos, I., Nieves, J. and Bringas, P.G. (2011) Semi-Supervised Learning for Unknown Malware Detection. *International Symposium on Distributed Computing and Artificial Intelligence Advances in Intelligent and Soft Computing*, 91, 415-422.

[20] Moskovitch, R., Stopel, D., Feher, C., Nissim, N. and Elovici, Y. (2008) Unknown Malcode Detection via Text Categorization and the Imbalance Problem. *Proceedings of the 6th IEEE International Conference on Intelligence and Security Informatics*, Taipei, 17-20 June 2008, 156-161.

[21] Santos, I., Nieves, J. and Bringas, P.G. (2011) Collective Classification for Unknown Malware Detection. *Proceedings of the International Conference on Security and Cryptography*, Seville, 18-21 July 2011, 251-256.

[22] Siddiqui, M., Wang, M.C. and Lee, J. (2009) Detecting Internet Worms Using Data Mining Techniques. *Journal of Systemics, Cybernetics and Informatics*, 6, 48-53.