Network Identification Encryption Reassuring Approach Using Cryptography Techniques

[1] K. Aruna Kumari, M.Tech, Asst.Professor, [2] N.Srinath, M.Tech, Asst.Professor,
[3] G. Pavani, M.Tech, Asst.Professor, [4] A. Naga Raju, M.Tech, Asst.Professor,
Chalapathi Institute of Engineering & Technology
[1] aruna.jeswin@gmail.com, [2] narnesrikanth619@gmail.com,
[3] gottipati.pavani04@gmail.com, [4] raju051285@gmail.com

Abstract: Open Flow is gained tremendous interest within the network community. Moving Target Defense (MTD) is received focus in technical models. The approach is describe MTD methods is modify some attribute of the computer network fundamentals. - Cryptography is an art and science of achieving security and encoding message to make them non-readable. The design of secured cryptographic based algorithms is mapping and low power cache design by employing methods is change nested XOR operations extended new codes and multi-bit clustered. The private key generation using the two different algorithm AES and RSA where AES is symmetric and RSA is asymmetric cryptographic algorithm. Network security refers to all the features, characteristics, measures, operational procedures, rules and administrative new required changing unauthorized access and to provide an acceptable level of security data transmission layers network and at the same time preserve the integrity availability and confidentiality of information. The implementation many new security defenses as Open Flow security services to examine many performance and efficiency models of our proposed framework. The experimentation environments that support contemporary technologies used in MTD methods such as software defined networking (SDN), are also identified and discussed.

Index Terms: metrics; defensive work factors, Encryption, symmetric and asymmetric cryptography, cryptanalysis, Side Channel Attack, Timing Attacks, Data Security, Key Generation.

1. INTRODUCTION

Moving Target Defenses (MTD) is a class of computer network defenses to modify specific parameters of network. MTD is objective of disrupting an attacked ability to reconnaissance and exploitation of a computer network by changing in unpredictable process parameters of a computer system [1]. The number of applications available now in these days by which the private and sensitive data is transmitted using entrusted network basically most of the time user sends the data from a trusted network to a trusted network [2]. Cache lines and blocks have address fields which are divided into dynamic and static. Tag holds higher address bits and index holds lower address bits [3]. Recently the usage of cloud computing is increases rapidly easy accessibility. It allows people to do any things at any time and any were without buying and building IT models [4]. The cryptography and cryptanalysis together are called cryptology. Encryption is the process of converting ordinary information (called plaintext) into unintelligible text (called cipher text). Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext [5]. Flow-based security detection algorithms can also be redesigned as OF security apps, but implemented much more concisely and deployed more efficiently [6]. MTD techniques and applications can be applied to most any part of a system with the objective of inducing changes in individual host network system structure, architecture, and/or parameters segmenting [7].

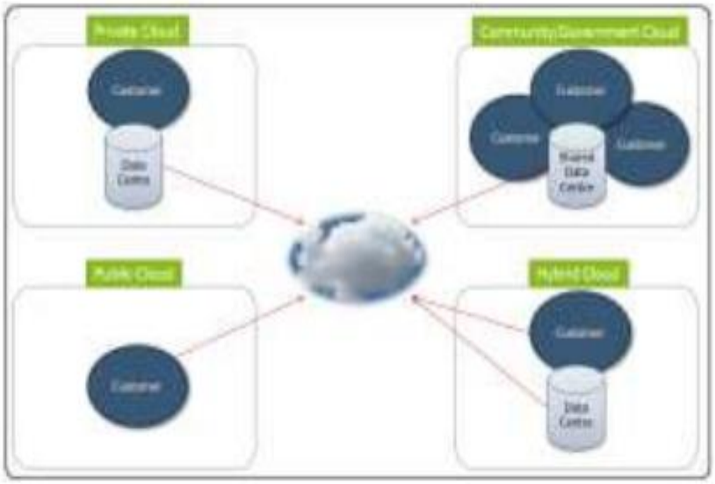

Fig.1 Models of cloud computing

2. RELATED WORK

An ideal security protocol should always be protecting the security of connections in many aspects and leaves no trapdoor for the attackers.

Nowadays one of the popular cryptography protocols is hybrid cryptosystem that uses private and public key cryptography to change secret message [8]. Cubic based set associative cache encoded mapping2 involves in handling internal and external interrupts of bunch of words to be loaded into cache memory [9]. This is to make sure the security proposed solution consists of using cryptography to ensure confidentiality and integrity of involved data [10].It does not recognize which encryption algorithms used. But, this solution does not recognize the encryption algorithm to be used [11]. Various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography is the combination of the disciplines of mathematics and computer science [12]. With the combination of symmetric cipher and public key which is RSA with some hash function a new design protocol is proposed. Encryption can be converted in some form that will make it difficult to read and make it more secure [13].

3. SYSTEM MODLE

Open Flow controllers do not uniformly capture and store TCP session information among other key state tracking data, which is often required to develop security functionality. We call this an information deficiency challenge [14]. The FRESCO architecture incorporates a database module that simplifies storage and management of session state shared across applications. a security module design to recognize certain traffic patterns that may represent a threat should be easily linkable to a variety of potential threat mitigation modules that when triggered by the detection module produce appropriate flow rule responses [15]. These technologies also have a need to express more complex security response directives that may span many flow rule even address network wide attack scenarios. We call this the threat response translation challenge [16].

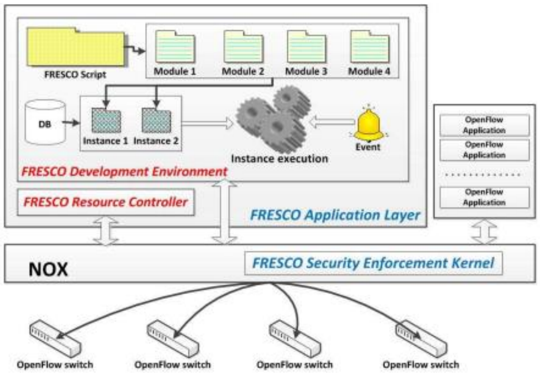

Figure 2. High-level overview of the FRESCO architecture

4. PROPOSED WORK

Some of the critical parameters to be considered while designing cache memories are size, access time, area occupied, power consumption, latency and speed. Cache memory becomes insecure when targeted. It is difficult to generate random vectors [17]. Nested XOR operations and error detection mechanism such as implementation of Hamming code to detect single bit errors can also come under reckoning. The Proposed technique uses RSA and AES for the encryption and decryption. RSA uses two keys private key and public key through which a digital signature is also produced [18]. Now for digital signature generation the output B which is our private key is converted from bit to byte and a message on which hash function is applied and then they both i.e. private key in byte and message with hash function are encrypted and finally digital signature is generated [19].

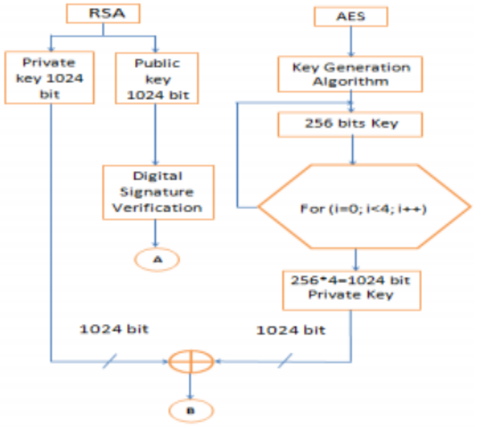

Figure 3. Diagram of private key generation process

5. MOVING TARGET DEFENSE TECHNIQUES

MTD techniques can be applied to most any part of a computer network system with the objective of inducing changes to the system structure, architecture, and/or parameters. In this paper, we segment MTD techniques into three classes: host-based, platform-based, and network-based. In test cases, the MTD technique will fall into a single class or may be a combination of varying system structure, architecture, or parameters and thus fit into multiple classes [20].

A. *Host-Based MTD Techniques*

Host-based MTD techniques are those that vary some aspect of the computing platform itself. The technique may vary aspects of the operating system

(OS), application code, or properties of the platform [5]. More specifically host-based techniques often use one or more of the following mechanisms:

B. Platform-Based MTD Techniques

Dynamic Platform: Includes mechanisms that result in variation of host platform properties such as OS type and/or version or CPU architecture.

C. Network-Based MTD Techniques

The network-based MTD technique class includes MTD techniques that dynamically vary network aspects of a distributed computer network system. Any aspect providing network connectivity and enabling system transactions across multiple computing platforms is a candidate for MTD techniques.

6. CRYPTOGRAPHY MECHANISMS

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The term is most often associated with scrambling plaintext message into cipher text then back again. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key cryptography, public-key cryptography, and hash functions, each of which is described below [21].

*1. **Symmetric Cryptosystems**:*

In symmetric cryptosystems the enciphering and deciphering keys are either identical or simply related, one of them can be easily derived from the other. Both keys must be kept secret, and if either is compromised further secure communication is impossible. Even for a moderate number of users, i.e. n(n — l)/2 for n users. This creates a key-distribution problem which is partially solved in the asymmetric systems.

2. Asymmetric Cryptosystems:

There are practical problems associated with the generation, distribution and protection of a large number of keys. A solution to this key-distribution problem was suggested by Diffie and Hellman in 1976 [6]. A type of cipher was proposed which uses two different keys: one key used for enciphering can be made public, while the other used for deciphering, is kept secret. If asymmetric algorithms satisfy certain restrictions, they can also be used for generating so-called digital signatures [9]. Examples of Asymmetric systems are Megamall, Diffie–Hellman key exchange, RSA.

3. Hash Functions:

Hash functions, also called message digests and one-way encryption, are algorithms that, in some sense, use no key. A hash function H accepts a variable-length block of data M as input and produces a fixed-size hash value h = H(M). In general terms, the principal object of a hash function is data integrity.

4. FRESCO Development Environment

The FRESCO development environment (DE) provides security researchers with useful information and tools to synthesize security controls. To realize this goal, we design the FRESCO DE with two considerations [22]. This function automatically translates FRESCO scripts to modules, and creates instances from modules, thus abstracting the implementation complexities of producing OF controller extensions. It is also responsible for validating the registration of modules. Registration is performed via a registration API. The FRESCO resource controller monitors Open Flow network switches and keeps track of their status. A flow rule that is distributed from a FRESCO application is inserted into a flow table in an Open Flow switch. FRESCO script and dynamically loads them. The FRESCO DE runs each instance (5, 6), and when it receives an action from the do action module it translates this action into flow rules, which can be understood by an Open Flow switch. Finally, these flow rules are installed into the switch through the FRESCO SEK [22].

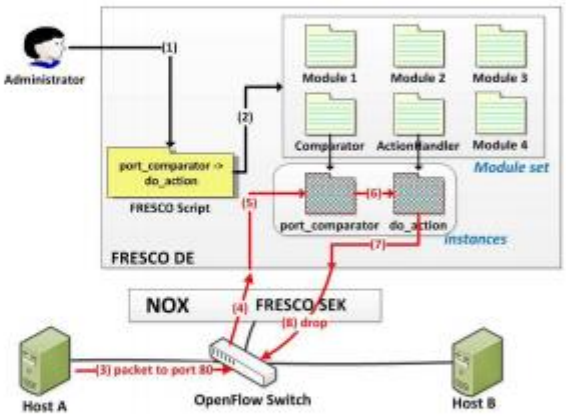

Figure 4. Operational illustration of running FRESCO script

7. RESULTS

The result for each the results we can see private key is the combination of AES and RSA private key (1024 bit) and applied in digital generation scheme in the form of bytes the Signature verification, if the signature will be same then signature will be verified and in other case signature will not be verified. With the combination of ASE, RSA and Digital Signature the function is nonlinear and more Avalanche effect is generated. The resource controller component monitors switch status frequently and removes old flow rules to reclaim space for new flow rules, which will be enforced by FRESCO applications. This job is performed by FRESCO's garbage collector, a subcomponent of the resource controller, which we test under the following scenario. We capture packets between NOX and the Open Flow switch, and measure the round trip required to submit the flow and receive a corresponding flow constraint. We observe that FRESCO applications require additional setup time in the range of 0.5 milliseconds to 10.9 milliseconds.

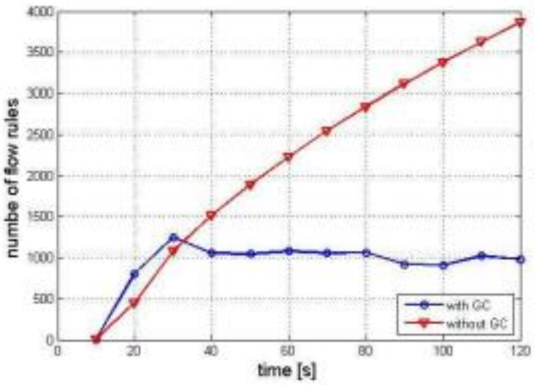

Figure 5. Operation of FRESCO garbage collector

8. CONCLUSION

Assessing properties of MTD technologies and approaches best performed with live experimentation. Well designed experiments are necessary to create necessary interactions with the MTD under study and surrounding environment, including the cyber intrusion it intends to defend. We present the FRESCO security enforcement kernel. Our evaluations demonstrate that FRESCO introduces minimal overhead and that it enables rapid creation of popular security functions with significantly fewer lines of code. Algorithm is based on hybrid cryptography as it uses asymmetric that is sender and receiver key and asymmetric key that is both sender and receiver uses same key pair for both process encryption and decryption the DES and RSA hybrid cryptographic algorithm is relatively more secure and easier. Network security is a continuous process and demands regular network analysis, testing and maintenance. Furthermore there is a prominent need for continuously upgrading the security protocols, policies, mechanisms and their dynamic adaptation to cope with the evolving security threats.

REFERENCES

[1] S. Jajodia, A. K. Ghosh, V. Swarup, C. Wang, and X. S. Wang, Moving Target Defense Creating Asymmetric Uncertainty for Cyber Threats. Berlin, Germany: Springer, 2011.

[2] E. Al-shaer, W. Marrero, A. El-atawy, and K. Elbadawi. Network Configuration in A Box: Towards End-to-End Verification of Network Reachability and Security. In The 17th IEEE International Conference on Network Protocols (ICNP), 2009.

[3] J. R. Ballard, I. Rae, and A. Akella. Extensible and Scalable Network Monitoring Using OpenSAFE. In INM/WREN, 2010.

[4] Z. Cai, A. L. Cox, and T. E. Ng. Maestro: A System for Scalable OpenFlow Control. In Rice University Technical Report, 2010.

[5] M. Canini, D. Venzano, P. Peresini, D. Kostic, and J. Rexford. A NICE Way to Test OpenFlow Applications. In Proceedings of NSDI, 2012.

[6] M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. McKeown, and S. Shenker. Ethane: Taking Control of the Enterprise. In Proceedings of ACM SIGCOMM, 2007.

[7] M. Casado, T. Garfinkel, M. Freedman, A. Akella, D. Boneh, N. McKeowon, and S. Shenker. SANE: A Protection Architecture for Enterprise Networks. In Proceedings Usenix Security Symposium, August 2006.

[8] K. S. Quan Jia and A. Stavrou, "Motag: Moving target defense against internet denial of service attacks." In International Conference on Computer Communications and Networks (ICCCN), 2013.

[9] Dunlop Matthew, Groat Stephen, Urbanski William, Marchany Randy and Tront Joseph, "MT6D: A Moving Target IPv6 Defense", MILITARY COMMUNICATIONS CONFERENCE, 2011 - MILCOM 2011, pp. 1321-1326.

[10] Zhuang, R., DeLoach, S., Ou, X., "Towards a Theory of Moving Target Defense," Kansas State University, Manhattan, KS USA.

[11] M. Torgerson, "Security Metrics for Communication Systems," 12th International Command and Control Research and Technology Symposium, Newport, Rhode Island, June 19-21, 2007.

[12] Cybenko, G., Hughes, J., "No Free Lunch in Cyber Security," MTD Workshop, Scottsdale, Arizona, November, 2014.

[13] Rivest, R.L., Shamir, A., and Adleman, L: 'A method for obtaining digital signatures and public-key cryptosystems', Communication of the ACM, 1978, 21, pp. 120-126.

[14] Steel Central Riverbed Modeler, http://www.riverbed.com/products/ steelcentral/steelcentral-riverbed-modeler.html

[15] C. Yoon, S. Lee, "Attacking Sdn Infrastructure: Are We Ready For The Next-Gen Networking?," BlackHat-USA-2016, August 2016.

[16] T. Richardson, J. Levine, RealVNC Ltd., "The Remote Framebuffer Protocol," IETF RFC 6143, March 2011

[17] E. Hutchins, M. Clopperty, R. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin Corporation

[18] N. Abrek, "Attack Taxonomies and Ontologies," Seminar Future Internet SS2014, Network Architectures and Services, March 2015

[19] Shucheng Yu Cong Wang ;KuiRen ; Wenjing Lou, Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing, INFOCOM, 2010 Proceedings IEEE.

[20] KalpanaParsi, SingarajuSudha. "Data Security in Cloud Computing using RSA Algorithm". International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012. pp. 145.

[21] Sood S K, Sarje A K, Singh K. "A secure dynamic identity based authentication protocol for multiserver architecture". Journal of Network and Computer Applications 2011, 34(2), pp. 609–18.

[22] N. Shimbre and P. P. Deshpande, " Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES algorithm," IEEE, pp. 35-39, 2015.

[23] W. Wang, Z. Li, R. Owens, B. Bhargava, Secure and efficient access to outsourced data, in: Proceedings of the 2009 ACM workshop on Cloud computing security, CCSW '09, ACM, New York, NY, USA, 2009, pp. 55–66.