Enabling MultiLevel Secured Framework for Remote Attestation

Sharmila Priya A.V, Mr Saishanmuga Raja

M-Tech, Computer Science and Engineering
Dr. MGR Educational and Research Institute University.
Chennai-6000095, India.

Assistant Professor, Computer Science and Engineering
Dr. MGR Educational and Research Institute University.
Chennai-6000095, India.

***Abstract*— In distributed computing environment, computers have necessity to work closely together. In such an environment a single compromised machine can put the entire system integrity in danger. To mitigate the risk we propose a remote attestation framework for establishing the trustworthy platform between the system to ensure the secure data transfer and maintain system integrity. Our Framework validates the recent change of state, rather than considering the entire system configuration. With this model we set the tolerable risk level which provides efficient way to resolve host system with vulnerabilities and construct effective attestation result.**

***Keywords*— Remote Attestation, Trusted Platform, Trusted Computing group, Tolerable Risk Level.**

I. INTRODUCTION

In a distributed environment where systems are connected to an internet, it is likely that malicious program will exploit the vulnerabilities of target machine. These attacks can render the software to behave anomalous. Additionally, these kinds of attacks can exploit bugs in software which is running on a machine. Identifying the presence of malicious program will help to maintain the integrity and security of a system. The goal of remote attestation is to measure whether the remote system runs buggy, malicious application code and data or it's not properly configured. The flow based information helps the remote party to verify the configuration and current state of platform (i.e. Software and hardware component) and decide whether the remote system should be trusted or not. Thus, remote attestation aims to build the trust and enable secured platform in distributed computing environments. For example, if it is found to be violating the system integrity, then the violating component can be distrusted and removed from the network by others in the system. In this context some basic and challenging issues are how to measure the dynamic properties of remote system.

Various attestation techniques and methodology have been proposed. Trusted platform module (TPM) introduced by Trusted computing group is a chip that can be installed on desktop motherboard. It is specifically designed to enable integrity measurement of remote system.TPM has ability to create and store keys, facilitate the cryptographic algorithm. Enormous attestation techniques have been proposed to address privacy properties, static behaviour and so on. Existing remote attestation methods focused on static approach which doesn't derive the runtime properties of remote system.Static approach is incompatible with today's heterogeneous distributed computing environment and results in Boolean format.

They are unique challenges in designing the Dynamic remote attestation framework.First, due to diversity in dynamic object and their properties, it is difficult to find and derive the "Known" good states of dynamic object. In contrast, "known" good state can be easily measured by the cryptographic checksum of static objects. Second, continual integrity measurement is required for large number of dynamic object.

The main difference between the static and dynamic attestation is one-time check for static attestation techniques and need to measure their integrity repeatedly.

To overcome the disadvantages of an existing system we propose a framework to measure the dynamic properties of a remote system in an effective way and set a tolerable risk level to allow attestee to rectify the integrity violation by themselves if the malicious action is by an innocent user.

By this we are making system intellectual to determine whether the system attack is made by an attacker or accidental act. Our framework verifies the recent change of system state rather than measuring the entire system configuration.

Hardware and software components are measured from the boot block to ensure the system integrity.

II. BACKGROUND AND RELATED WORK

Most of the existing works focus on describing and maintaining the integrity status of system. The Existing flow based integrity model are PRIMA [1], Biba [2], LOMAC [3], and ReDAS [4].

An integrity measurement approach based on information flow integrity is Policy-Reduced Integrity Measurement Architecture (PRIMA).PRIMA approach to enable measurement of flow integrity and prove that it achieves a goal.
BIBA integrity property is satisfied if a high-integrity process cannot access a lower integrity object nor obtains a low integrity data in any other way.
ReDAS [4] (Remote Dynamic Attestation System) that provides dynamic system properties.
ReDAS provides two types of dynamic system properties of application. 1. Structural integrity and global data integrity.
Integrity is measured based on runtime dynamic objects.
Clark-Wilson states information flow from low-integrity objects to high-integrity through a particular program called transaction procedures (TP).
The Author propose model-driven remote attestation [5] .Model driven remote attestation verifies two compliance i.e. expected behavior compliance and enforced behavior compliance.
Another Author propose semantic remote attestation [6], its VM directed approach to trusted computing.Using language based virtual machines enables the remote attestation of complex, dynamic and high-level program properties in a platform.Though remote attestation for trustworthiness of computing platform is a future work in Trusted Computing.
Another work by propose Load-time binary attestation.
On the creation of user level processes, the kernel measures the executable code loaded into the process (i.e., the original executable and shared libraries) and this code can measure
Subsequent security sensitive input its loads (e.g., arguments, configuration files, shell scripts).

III.SECURED FRAMEWORK FOR REMOTE ATTESTATION

Our Framework provides effective and efficient way of remote attestation. Remote attestation helps to identify the changes of user's computer by the attester or authorized parties.

Framework consists of three main components 1. An attester
2. An attestee 3. Trusted Authority.
In our context, Attester is a challenger; Attestee is a Target system, Trust Authority also called as verifier/Trusted Component as shown in Fig. 1. Integrity of the remote system is measured by checking the software components, policy updates. Attestee has to provide the system state details to the attester for verification.
Assume that the target/attestee machine is in trusted state initially and the current system state is updated to a new state after certain system behaviours.

1. A reporting daemon runs in the attestee machine round the clock and it captures new system state, when there is a change in system behavior with IMA.

2. This reporting daemon obtains AIK signed PCR values and forward it to the attester.

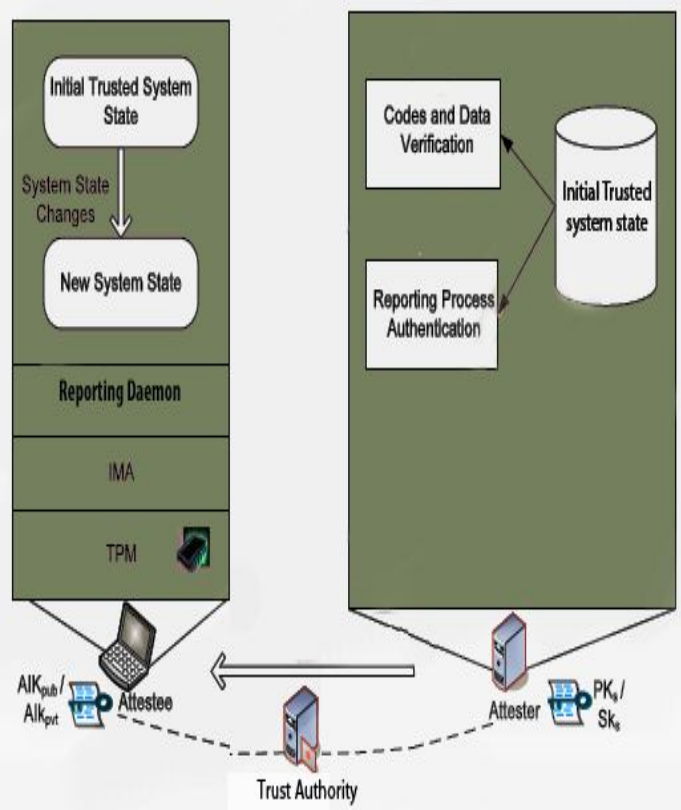

Fig. 1. Secured Framework for Remote Attestation

3. Attester role is to authenticate the information received by an attestee with AIK key generated from Trust Authority,
It verifies the attestee's integrity through codes and data verification. For successful attestation, the result is forwarded to the attestee in an encrypted format otherwise the result is sent to the Trust Authority.

4. Partial verification process is delegated to the Trust Authority by an attester to improve the performance of an attestation process .It consumes comparatively less time to complete the verification task. Trust Authority classifies the risk level into HIGH and LOW. Trust Authority
Checks the measurement list with the help of IMA and generate the result. Finally the result is forwarded to the attestee, attester in encrypted format and notification sent to the System Administrator.

A. Tolerable Risk Level

Risk is the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence. Vulnerability is a weakness that can be accidentally triggered or intentionally exploited. Vulnerability here is a malicious code running on attestee machine. Setting a tolerable risk level simplifies the system complexity. Risk Level is classified as HIGH, LOW.

Lower risk level is considered to be a tolerable one. The attester instructs the user to remove the malicious software from the system to continue working in a distributed environment. If it's not intentional user removes malicious software from the system.

Higher risk level is not tolerable. After couple of remainder from the attester to remove the software if there is no change in system state it's considered to be malicious and terminated from network.

B. Attestee Restructure.

System integrity is measured based on the current system state of an attestee. If it doesn't satisfy the integrity requirement, System Administrator may streamline the system configuration based on attestation result to strengthen the system integrity and improve its trust level.

Administrator must be capable of resolving different identified violation with respect to the risk matrix under different circumstances.

C. Information Flow measurement.

As our attestation party checks dynamically the processes and objects related to the target program. It allows the challenger to verify the interaction between the target programs and objects it depends on. To enhance the Flow checking, we added the risk level matrix.

IV.Comparative study of static and dynamic attestation.

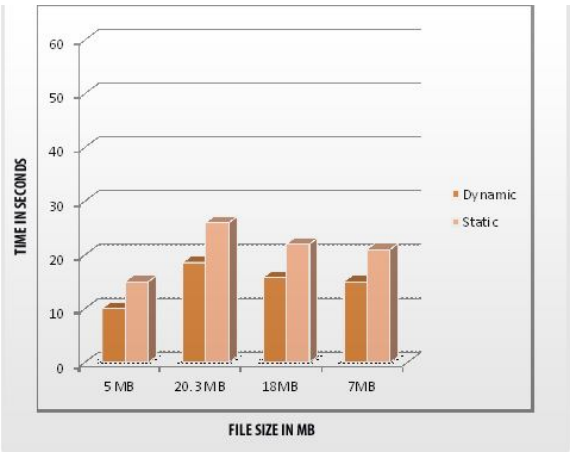

Fig. 2 ATTESTATION PERFORMANCE ANALYSIS GRAPH

The above graph will give clear statistics on performance analysis between static and dynamic attestation model.

V.Conclusion

In this paper, we presented a Novel Secured Remote Attestation Framework to overcome the existing Static Attestation techniques. Our Framework verifies the integrity of remote system by checking the recent state of the system to enhance the trustworthiness. To improve the security we have added the tolerable risk level to streamline the system verification process. Which reduces the administration overhead. In this approach some part of verification task is delegated to the Trusted Authority which improves the performance. Our future work would seek a more flexible and systematic way to address issues.

References

[1] T. Jaeger, R. Sailer, and U. Shankar, "PRIMA: Policy-reduced Integrity Measurement Architecture," Proc. 11th ACM Symp. Access Control Models and Technologies (SACMAT '06), 2006

[2] K.J. Biba, "Integrity Consideration for Secure Computer System," Technical Report 3153, Mitre Corp., 1977.

[3] T. Fraser, "Lomac: Low Water-Mark Integrity Protection for Cots Environment," Proc. IEEE Symp. Security and Privacy (SP '00), May 2000.

[4] "T r u s t e d Computing Group , " h t t p s : //www.trustedcomputinggroup.org, 2011.

[5] Liang Gu, Xuhua Ding, Robert H. Deng, Yanzhen Zou,Bing Xie, Weizhong Shao, Hong Mei, Model Driven Remote Attestation: Attesting Remote System from Behavioral Aspect. The 9th International Conference for Young Computer Scientists, Zhang jiajie, China,November 18, 2008.

[6] Vivek Haldar, Deepak Chandra and Michael Franz, Semantic Remote Attestation —A Virtual Machine directed approach to Trusted Computing. USENIX Virtual Machine Research and Technology Symposium, 2004

[7] W. Xu, M. Shehab, and G. Ahn, "Visualization Based Policy Analysis: Case Study in Selinux," Proc. ACM Symp. Access Control Models and Technologies, 2008.

8] M. Green, "Toward a Perceptual Science of

Multidimensional Data Visualization: Bertin and Beyond,"http://www.ergogero.com/dataviz/dviz2.html.

[9] S. Brin and L. Page, "The Anatomy of a Large-Scale Hypertextual Web Search Engine," Computer Networks and ISDN Systems, vol. 30, nos. 1-7, pp. 107-117, 1998.

[10] W. Xu, X. Zhang, and G.-J. Ahn, "Towards System Integrity Protection with Graph-Based Policy An alysis," Proc. 23rd Ann. IFIP WG 11.3 Working Conf. Data and Applications Security, 2009.

[11] "Piccolo ToolKit," http://www.cs.umd.edu/hcil/jazz/. 2011.

[12] TCG, TCG Specification Architecture Overview, Specification Revision 1.4, 2nd August 2007, http://www.trustedcomputinggroup.org

[13] Trusted Computing Group (TCG). About the TCG http://www.trustedcomputinggroup.org/about/

[14] Benzel, T.V., Irvine, C.E., Levin, T.E., Bhaskara, G., Nguyen, T.D., Clark, P.C. Design principles for security.Technical Report NPS-CS-05-010,Naval Postgraduate School (September 2005)

[15] ZHANG Qiang, ZHU Li-na, ZHAO Jia. Research on Method of Remote Attestation in Trusted Computing, Control & Management, Microcomputer Information, Vol.24, No.4, 2008

[16] Joshua Guttman,Amy Herzog,Jon Millen,Leonard Monk,John Ramsdell, Justin Sheehy, Brian Snien, George Coker, NSA,Peter Loscocco, NSA. Attestation: Evidence and Trust, MITRE TECHNICAL REPORT, MTR080072

[17] YU Rong-wei, WANG Li-na, KUANG Bo. Method of designing security protocol for remote attestation, Journal on Communications, Vol.29 No.10, October 2008

[18] C. Xiao. Performance Enhancements for a Dynamic Invariant Detector. Masters thesis, MIT Department of Electrical Engineering and Computer Science, February 2007.

[19] E. Shi, A. Perrig, and L. van Doorn. BIND: A Time-of-use Attestation Service for Secure Distributed Systems. Proceedings of the IEEE Symposium on Security and Privacy,Oakland, California, May 2005.