Trusted Computing in Containers

Bhavith Patnam
Masters in Telecommunication
Department of Computer Science
Blekinge Institute of Technology
Karlskrona, Sweden 37179
Email: bhpt18@student.bth.se

Nishkal Gupta Myadam
Masters in Telecommunication
Department of Computer Science
Blekinge Institute of Technology
Karlskrona, Sweden 37179
Email: nimy18@student.bth.se

***Abstract*—The information age is driving the exponential growth of devices which are connected over the internet. As more and more devices are being added, trust is one of the key issue which needs to be addressed. One of the fundamental ways of establishing trust is by measuring and assessing various hardware and software components of a system. These systems run various services which are being deployed using containers to reduce the overhead. Establishing trust with the container environment is the major concern in its widespread adoption. This paper describes various steps and key components that are involved in building trust with the containers.**

Keywords: Trusted computing, Containers, Trusted Platform Module, Attestation

I. Introduction

Ever since the dawn of information age, security has been a major concern. One of the key aspect of security in computing system is establishing trust with the host system and also with remote system. Trust is achieved by assessing measurements of various hardware and software components. These measurements are used for determining the behavior of the system. Trusted computing standards are drafted by Trusted Computing Group (TCG) which is a consortium of leading technological organisations. TCG was formed in the year 2003 by Hewlett Packard, IBM, AMD, Microsoft and Intel whose goal is to design and develop Trusted Platform Module (TPM). A TPM is a hardware implementation that is used to provide authentication and attestation to a computing device [1].

Virtualization became one of the key aspects of computing by allowing abstraction of physical resources of a system or network into multiple logical resources. It helps in providing better efficiency and economic scaling of the system.[2]. One technology that has evolved on top of Virtualization is Containerization which is an Operating System level Virtualization. It's main advantage is reducing the overhead caused by virtual systems and the main point of concern is establishing trust in them [3].

II. Methodology

The papers for this article were selected from the Scopus, IEEE and Google Scholar databases using the keywords Trusted computing and Containers. Boolean logic was used in our search mechanism to select papers more relevantly. Later screening process was performed to select the papers based on our requirements.

III. Trusted Computing

Trusted computing refers to technologies and proposals that enforces the behavior of a system through hardware and software implementations [4].

A. Trusted Platform Module

Trusted Platform Module (TPM) was created by a group of companies in the computer industry known as Trusted Computing Group (TCG) for building trust among the systems. TPM is a hardware processor that is embedded to the CPU who's main role is to measure and assess the integrity of the system. The TPM module can access and monitor the

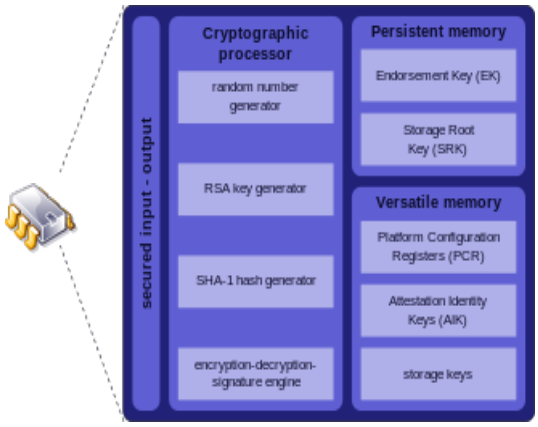

Fig. 1. Trusted Platform Module Architecture [13]

main bus of the system thus tracking the configuration state of the system.It consists of a cryptographic processor which is responsible for key and hash generation. The cryptographic processor consists of a random number generator, RSA key generator, SHA1 hash generator and a encryption-decryption module for signatures. The memory space of TPM is divided

into Persistent memory, which is non-volatile in nature, consisting of Endorsement Key (EK) and Storage Root Key (SRK) and Versatile memory, which is volatile in nature, consisting of Platform Configuration Registers (PCR), Attestation Identity Key (AIK) and storage keys [1].
Platform Configuration Register (PCR),one of the main component in TPM, is a set of secure memory region that holds the measured data of both the configuration and running state of the software. TPM is equipped with private and public key pair where the private key is used for signing the PCR and public key is used for verifying it [5].

B. Attestation

The role of TPM is only to collect and store the measurements of a system in a secure encrypted manner. In order to verify the measurements "Attestation" is required. Attestation is the process of authenticating a user's hardware and software to a trusted party which can be both a component in the user's system or a remote host. Remote attestation is the process of transporting the evidences/measurements collected by the TPM from the target system to the remote host.

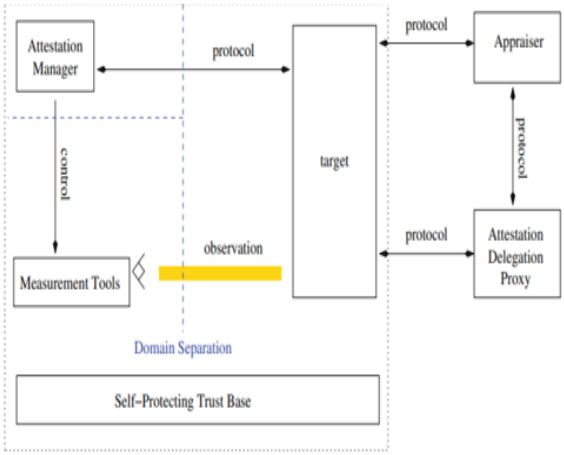

Fig. 2. Remote Attestation Architecture [6]

From the remote attestation architecture we define the following terms.
Target - It the system whose measurements have been calculated and stored by the TPM.
Appraiser - A node in the network that makes decisions about another nodes.
Attestation Manager - It's the party which performs attestation.
Attestation Protocol - Cryptographic protocols used to transfer the measurements securely to the remote host [6].

IV. Trust in Containers

A. Containers

Containers are standard software units that binds up the code and it's dependencies for the application to run quickly and reliably from one computing environment to another [3]. Containers on host OS have a higher performance, better portability and faster speed than Virtual machines [7].

B. Building Trust in Containers

Containers are vulnerable as they operate on same OS kernel. The problems related to trust in containers are :

- Current trust chain mechanism doesn't involve taking into account the trust of the containers.
- Remote attestation protocols are not enough to establish trust with containers.

Before verifying the integrity of the containers, we need to establish trust within the host system, in order to do so once the system is booted the control is transferred to core root of trust for measurement (CRTM) which uses TPM to store the measurements of both hardware components and BIOS until the control is transferred to the operating system. Once the trust within the system is established we extend the chain of trust to other applications using Integrity Measurement Architecture (IMA) [8]. IMA is used to measure all the executables which relies on TPM to protect the measurement list.
Trust in containers is established by generation of certificates which consists of list of programs that can run on operating system known as signature list . Public Key Infrastructure (PKI) [9] is used to generate and verify the host and user certificates. Host certificates consists of the programs that are authorized to be executed on the host system where as user certificates consists of a list of authorized programs that can run on their own containers. A private-public key pair is used for generating and verifying the certificates.
The next step involves verification of the signature list which is accomplished by the following process [7]:

- Authorization of the host executables by the administrator.
- Loading the user certificate and signature list into the kernel for modifying it.
- Identification of the containers with the mount name space id.
- Organizing data in the kernel based on kernel key retention service [10].
- Next, the executables in the Linux Security Module hooks are measured and verified.

C. Container Attestation

Container attestation is performed in order to report the measurements of the container and the host. This is done by assigning a vTPM to each container, where the vTPM (Virtualized TPM) instances are run in the kernel on top of the TPM module. Creation of valid attestation identity key (AIK) [11] by vTPM for authenticating itself to a remote party. The TPM binds the the AIK'vTPM, which is the AIK of the container image, and the identity of the container using TPM-Quote request [12]. The AIK'vTPM is validated with AIK owned by TPM.
Container State Challenge Protocol [7] is used to report the measurement list of containers and host to the challenger which is done by deploying an attestation service on the host thus by extending the trust chain from host operating system

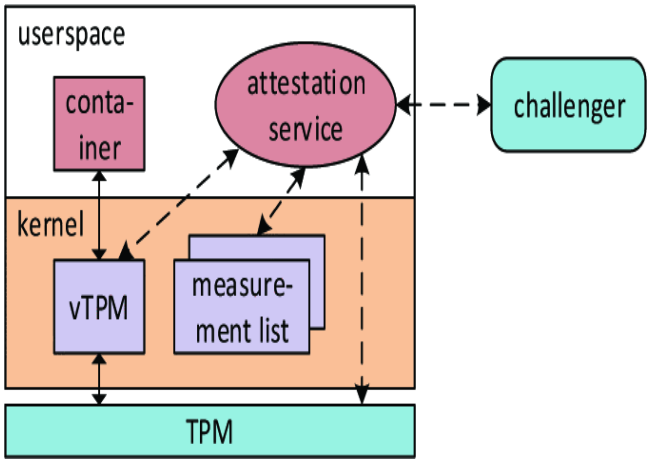

Fig. 3. Container State attestaion Architecture [7]

to the containers.

The role of the attestation service is to accumulate the results from both TPM and vTPM modules and report the collected measurement list to the challenger, a challenger is a 3rd party entity which assesses the measurement list reported by the attestation service.

The steps involved in Container State Challenge Protocol are:

- Creation of 160-bit non-predictable nonce.
- Preparation of attestation data.
- Identity of the container and the generated random nonce is sent in form of a request to the attestation service.
- Different quotes generated are included in the response which is sent by the attestation service to the challenger.
- Validation of attestation data by the challenger [7].

The protocol can prevent replay attacks, masquerading, tampering and reboot attacks to a major extent which tends to be its main advantage.

The performance evaluation by employing this method to establish trust can be assessed by measuring Delay and overhead introduced into containers [7].

V. Discussions

Based on the findings this paper provides a method to establish trust between the host system and the containers where the host measures the integrity of the containers. The trust issue could further be addressed by the owner signing the container image for its authenticity. Further work could be carried out where the owners of the container check the integrity of the Host as it builds a two-way trust. Vulnerability assessment tools can be further researched and examined to improvise the security features in containers.

VI. Conclusion

The recent trends in virtualization suggests that Containerization technology is gaining a lot of attention and is believed to reach 3 billion dollar market size by the year 2020. Security is the one key barrier in it's wide spread adoption. This paper addresses one of the solutions to resolve the trust issues between the containers and the host system, which is done by implementing a hardware based solution with the help of a cryptoprocessor known as Trusted Platform Module (TPM). This paper discusses various components involved in establishing trust such as TPM, Remote Attestation, Public Key Infrastructure and Container State Challenge Protocol which extends the remote attestation to containers.

Acknowledgment

We would like to thank Dr. Kurt Tutschku and Dr. Dragos Ilie for taking out their time and providing their valuable insights and expertise for this research. We would also like to extend our gratitude to Yuliyan Maksimov for helping us formulate this paper.

References

[1] "Trusted Platform Module (TPM) Specifications". Trusted Computing Group. [Online] Available At: https://trustedcomputinggroup.org/resource/tpm-main-specification. Retrieved 2019-12-17.

[2] Graziano, Charles. "A performance analysis of Xen and KVM hypervisors for hosting the Xen Worlds Project". Retrieved 2019-12-17.

[3] What is a Container?, [Online] Available At: https://www.docker.com/resources/what-container. Retrieved 2019-12-17.

[4] Chris Mitchell (2005).Trusted Computing.IET.ISBN 978-0-86341-525-8.

[5] Lauer, H., Sakzad, A., Rudolph, C., and Nepal, S. (2019, August). A Logic for Secure Stratified Systems and its Application to Containerized Systems. In 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 562-569). IEEE.

[6] George Cocker et.al., "Principles of remote attestation", Int. J. Inf. Secur. 10:63–81, DOI 10.1007/s10207-011-0124-7, 2011.

[7] Guo, Y., Yu, A., Gong, X., Zhao, L., Cai, L. Meng, D. 2019, "Building trust in container environment", Proceedings - 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering, TrustCom/BigDataSE 2019, pp. 1.

[8] R. Sailer, X. Zhang, T. Jaeger, L. Van Doorn, "Design and Implementation of a TCG-based Integrity Measurement Architecture", USENIX Security symposium, vol. 13, pp. 223-238, 2004.

[9] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, "Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile", 2008.

[10] "Kernel Key Retention Service", Linux kernel Documentation, [online] Available At: https://www.kernel.org/doc/html/v4.13/security/keys/core.html. Retrieved 2019-12-17.

[11] B. Parno, J. M. McCune, A. Perrig, "Bootstrapping trust in commodity computers" in 2010 IEEE Symposium on Security and Privacy, IEEE, pp. 414-429, 2010.

[12] R. Perez, R. Sailer, L. van Doorn, "vTPM: virtualizing the trusted platform module", Proc. 15th Conf. on USENIX Security Symposium, pp. 305-320, 2006.

[13] Trusted Platform Module, [online] Available At: http://en.wikipedia.org/wiki/Trusted_Platform_Module. Retrieved 2019-12-17.