Protocol for preventing Insider Attacks in an Untrusted Environment

S.Manohar
Faculty of computer science and engineering
SRM University
Vadapalani

Priyanka Pillai, Rubeena Shabab, Shubhangi Gupta
B.tech Computer Science and Engineering
SRM University
Vadapalani

ABSTRACT-
The recent advances in utility computing have allowed businesses to move their applications to the cloud, providing features such as auto-scaling and pay-as-you-go facility. Here we are presenting a model for protecting the confidentiality and integrity of client data and computation from insider attacks has been presented. We demonstrate a scenario of how the origin integrity and authenticity of content processed can be verified without revealing the watermark details to the administrator using digital watermarking in an isolated environment .Finally we have tested a prototype system using two different approaches in order to verify that confidentiality and integrity of the client's data is maintained. Verification using ProVerif tool proves that by using a realistic hacker model cryptographic operations and protocol communication cannot be altered. Finally our implementation demonstrates that it adds negligible overhead.

1. INTRODUCTION

Small scale industries encounter the trouble of expansion and reduction in their employee workforce as the business and economy changes. Access to specific strength should be changed as well to fit the current role of that employee. Lack of operation, to ensure that employee's access is restricted to data that is required to do his or her job, is the only issue that most companies continue to grapple with. This problem is confronted when an employee is promoted from operations to board and their permissions to systems are not updated to reflect their new part[1]. Failure to remove access to delicate forte for those employees that no longer have a legal business demand increases an asset's exposure to unauthorized disclosure or alteration. This can be a common possibility of insider attacks which is often unnoticed.An insider is an employee of the company that has major access to secret information, comprehend internal processes, and facts of high-value goals and possible weaknesses in security. An insider attack has the intend to cause notable, even crisis, damage to the targeted IT-infrastructure. While this problem is recognized in the security communities, many companies still incline to rely survey logs after the insider attack has occurred instead of concentrating on developing tools and techniques for analyzing and solving the actual problem.This paper will focus on identifying some high level areas of insider threats and how to engage some base practices to protect against them. The degree of difficulty required to establish controls that protect against intruder threats will depend on the locations of systems, size of the company, number of employees, number of systems, and vendor types. The basic aim of this paper can be applied to any company looking to accept a minimum set of controls to protect value from insider threat.Authentication is the process of establishing identity and ensuring the person is who they claim to be. This is usually accomplished through meeting in person and connects to them with a new employee and a role. The authorization component is the stipulation of access to specific internal resources based on who they are.

Restrictive employee access to areas needed to carry out their job is a better means of providing security as contrasting to granting all employees the same access to all locations and systems. Granting access based on roles limits experience and strengthens liability.

2. PROBLEM BACKGROUND

2.1 VIRTUALIZATION

Network, front end, VM disk image archive, hardware, VMM are the fundamental components of cloud computing[2]. Out of all these, virtualization is main component of an IaaS based cloud. Virtualization cheaply uses system resources and simultaneously support multiple heterogeneous operating system. Here the networking resources are also virtualized. In order to support and execute multiple clients VMs a hypervisor is used. The Xen uses a special administrative VM named dom0, that runs and controls the client guest VMs. And the platform owner controls the dom0 VM.

2.2 LATE LAUNCH

After running un-trusted softwares on any system there are technologies that allow the execution of a secure kernel or VM on the same system.This implies that trust chain does not start from boot but is initiated at a later stage dynamically.

2.3 SEALED STORAGE

One of the key features provided by the TPM for securing sensitive code and data is sealed storage. A TPM contains a special 2048-bit key called Storage Root Key (SRK). The private part of the SRK never leaves the TPM in plaintext. The storage key is used to seal other data and sensitive information. The seal operation takes a set of PCRs as input, and then encrypts the given data using the SRK. The seal operation outputs cipher text C along with the list of PCRs provided and its corresponding values.

2.4 FLICKER

Flicker is an infrastructure based on late launch technology for secure execution of a small piece of security sensitive code, called Piece of Application Logic (PAL), on systems where BIOS, OS and DMA devices are not trusted. On Intel platforms, invoking a Flicker session suspends the current execution environment (OS and VMM) and then executes the SENTER instruction for setting up the secure environment for PAL execution. At the end of Flicker session, the previous execution environment is resumed.

2.5 PROTOCOL VERIFICATION

We will later define security protocols for secure VM launch and secure computation. As the adversary is actively looking for weaknesses, correctness of security protocols is very important. However, significant flaws have been found in widely used protocols, often years after the protocol has been defined.

2.6 LEVEL I VS LEVEL II SECURITY

Definition 1 Level I security: Platform Integrity Attestation, where before transferring computation and data, a remote party verifies through remote attestation, that the target platform belongs to the actual cloud hosting provider as well as executes trustworthy hardware, firmware and software[3][4]. The client can then trust the challenged platform after verifying its current state through remote attestation for future operation.

Definition 2 Level II security: Integrity and confidentiality, where a remote party not only verifies the integrity of the target platforms hosting provider, hardware, firmware and software but also requires additional security measures to ascertain that the confidentiality and integrity of sensitive operations executed on the target platform will not be compromised. Level II security assurance can be provided with Intel TXT technology based mechanism called Flicker and will be detailed in the coming sections.

2.7 SECURE VM LAUNCH

The client VM is stored in an encrypted form on the CS, so that it can only be launched on trusted NCs. The purpose of the secure VM launch protocol is to get the VM decryption key Dk V M securely from the client, decrypt the VM and then launch it on a trusted node. The protocol proceeds in two phases[4]. In

the first phase, we certify the public keys of the client (pkc) and Flicker (pkf). This is performed by using the TPMs of the client and the NC to establish a secure channel between the client and the Flicker.

3. PROPOSED WORK

Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence. The manager allocate project to all employees. So the managers choose one image and our important project details hide to that image using Watermark encoding algorithm. This Watermark encoding Algorithm work with manager gives input for project details those details are hide to image and managers sends image, project stating date and ending date send to employees. Then managers allocate to shift for all employees. Employee gets the manager sending image. Then employee chooses that Manager sending image and decodes the manager sending project details using Watermark Decoding Algorithm. employee generate project report based on manage sending project details. Employee first generates project report and that project details hide to image using watermark encoding algorithm[5]. Then employee sends to That image and project finishing date to managers. manager gets employee sending project report. The manager takes the employee hiding image use watermark decoding algorithm. This module manager verifies the employee sending every project.

4. RESULT ANALYSIS

In fig., encryption window is given. In this image, the information or the task that has to be provided to the employee has to be sent by encrypting it in an image. Chose the image and then enter the text in the project detail box. When you press encrypt button,text file is encrypted and hide into image and saved into your preferred location.

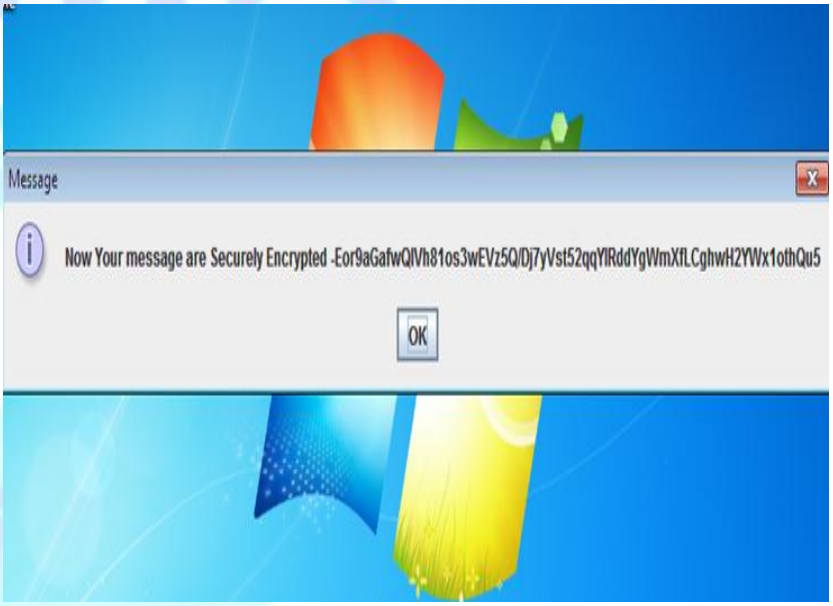
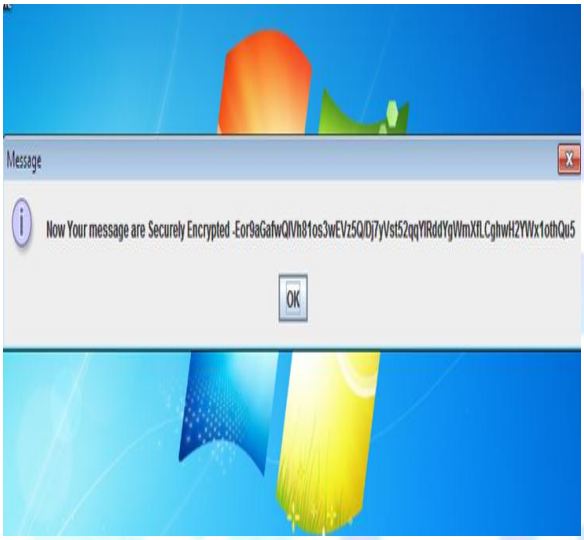


Fig: (A) Original text

Fig: (B) Encrypted text



(A)Encrypted File

(C) Stegnographic Image

(B) Image File

5. CONCLUSION

Cryptography and steganography are two major techniques of data security. These two techniques are used for providing higher security. First the information is encrypted by using Watermark algorithm which is better than DES and AES algorithm then the encrypted information is hidden by approach. The entire work is done in Java and MySql. So our techniques provide two layers of security for secret data. It is very hard for unlawful user to find out your top-secret information Thus the proposed technique is operative for secret data. It is very hard for unlawful user to find out your furtive data. Hence we concluded that the proposed technique is effective for secret data communication.

6. REFERENCES

[1] Imran Khan, Zahid Anwar, Behzad Bordbar, Eike Ritter, and Habib-ur Rehman, "A Protocol for Preventing Insider Attacks in Untrusted Infrastructure-as-a-Service Clouds" IEEE Transactions On Computers, Vol. 65, No. 5, June 2016 IEEE Transactions On Computers, Vol. 65, No. 28 April 2016.

[2] William Stallings, "Cryptography and Network Security: Principles and practices", Pearson education, Third Edition, ISBN 81-7808-902-5.

[3] M.Grace Vennice, Prof.Tv.Rao, M.Swapna, Prof.J.Sasi kiran, " Hiding the Text Information using Steganography" , international Journal of Engineering

Research and Applications (IJERA) Vol. 2, Issue 1, Jan Feb 2012.

[4] Dipti Kapoor Sarmah, Neha Bajpai , "Proposed System for data hiding using Cryptography and Steganography " in international gournal of computer applications,2010.

[5] Ankita Agaral , "Security Enhancement Scheme for Image Steganography using S-DES Technique" in International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 4, April 2012.

[6] Phad Vitthal S., Bhosale Rajkumar S., Panhalkar Archana R. " A Novel Security Scheme for Secret Data using Cryptography and Steganography" in I. J. Computer Network and Information Security, March 2012.

[7] Harshitha K M and Dr. P. A. Vijaya , "secure data hiding algorithm using encrypted secret message" in International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012.