Enhancing the Hypervisor as a Second Layer of Authentication

Mohammed Ali Kamoona¹, Ahmad Mousa Altamimi²
¹(Computer Science Department, Faculty Of Information Technology/Applied Science Private University, Jordan)
²(Computer Science Department, Faculty Of Information Technology/Applied Science Private University, Jordan)
Corresponding author: Mohammed Ali Kamoona

ABSTRACT:
Hosting Services Over The Internet Has Become One Of The Most Terms Pervaded The IT World. Cloud Computing Is A General Term Refers To The Platform Of Hardware And Software Being Used To Migrating Computing Resources To A Virtualized Environment. It Enables Users To Consume Resources, Such As A Virtual Machine (VM), Storage, Or Use A Utility From Anywhere. In This Regard, Hypervisor Or Virtualization Is A Program Designed Specifically To Facilitate The Hosting Of Several Different Virtual Machines On A Single Hardware. Being Said That, Hypervisors May Also Provide Additional Attack Vectors As They Are Commonly Supported By A Simple Password Authentication Scheme. Such Scheme Is Entirely Based On Confidentiality And The Strength Of The Password, Which Is Vulnerable To Various Attacks Such As Offline Password Guessing Attack And A Privileged Insider's Attack. In This Paper, A Second Level Of Authentication Process Is Introduced To Provide Further Security Countermeasures For The Hypervisor Management System. Because Of The Maturity Of These Systems In General, It Is Important To Ground Our Approach. To This End, A Model Is Provided That Utilizes The Encryption Technique In Order To Introduce Better Authentication Process For The Existed Multiple Hypervisor Systems With Little Modification.

Keywords - Cloud Computing, Hypervisor, Virtual Machine, Authentication

Date of Submission: 31-03-2018
Date of acceptance: 16-04-2018

1. INTRODUCTION
In Recent Years, The Using Of Cloud Systems Is Becoming More Essential In Our Life As The Computer Resources Can Be Migrated To A Virtualized Environment With Low Costs. This Is Supported, In Part, By The Development Of Connecting Computers Over The Internet. One Of The Main Aspects Of Cloud Computing Is Virtualization, Which Enables Enterprises In Order To Virtualize Or Expand The Capabilities Of Their Resources To Improve The System's Reliability. In Other Words, Virtualization Allows To Share A Single Physical Instance Of A Resource Or An Application Among Multiple Users Or Even Multiple Enterprises As Virtual Machines [1]. However, In Order To Determine The Access Of Shared Resource, Hypervisor Is Introduced To Isolate And Control The Different Virtual Machines From The Underlying Computer Hardware [4].

Specifically, A Hypervisor Allows The Underlying Host Machine Hardware (E.G., A Server) To Independently Operate One Or More Virtual Machines As Guests. This Permits Multiple Guest Vms To Effectively Share The System's Physical Compute Resources Such As Processor Cycles, Memory Space, Network Bandwidth And So On [7]. In Fact, There Are Two Main Types Of Hypervisors: The First Type Is Running On A Local Machine Presenting A Virtual Operating System For Operating Various Virtual/Guest Machines. The Second Type Is Installed On A Cloud Server, Called Cloud Virtualization, Which Can Be Subdivided Into Two Categories: Hypervisors That Are Deployed Directly Atop The System's Hardware Without Any Underlying Operating Systems Or Other Software, And Hypervisors That Are Running As A Software Layer Atop A Host Operating System And Is Usually Called Hosted Hypervisors [10]. In This Work We Will Consider The Hosted Hypervisors And Proposed A Model For Enhancing Its Authentication Process. Figure 1 Illustrates These Types.

Practically, Many Hypervisors Have Been Developed, One Can Consider For Example: XEN, KVM, OPEN VZ, VMW WEAR, And HYPER-V. Some Of These Hypervisors Are Closed Source And The Others Are Opened Source Like XEN And KVM [17,19,13]. Our Major Concern Here Is Securing The Shared Resources. In Particular, The Hypervisor Determines How Much Each Virtual Machine Can Use And What Can Access The Host Recuces. It Does Not Allow Direct Access To The
Host Physical Resources Before It IsAuthenticated First. Unfortunately, Most Of The Hypervisors AreGenerally Equipped By A Simple PasswordAuthentication Scheme [20].

Fig. 1: Types Of Hypervisors

However, Password AuthenticationScheme Is Entirely Based On Confidentiality AndThe Strength Of The Password, Which IsVulnerable To Various Attacks (E.g., OfflinePassword Guessing Attack And A PrivilegedInsider's Attack) And Needs Resources SharingAccess Control [3]. As A Result, Many SecurityMethods Have Been Developed In The Literature,Cryptography, Intrusions Detection, AndAuthentication Are The Most Used [8]. WhileSome Of Them Have Been Proposed For SecuringThe Virtual Machine From Unauthorized Access,The Others Have Been Focused On The OperatingSystems. We Note That The Most ImportantSecurity Aspect In Term Of Protecting TheOperating Systems And The Virtual Machines IsKeeping Unauthorized Personal From Doing AnyMalicious Activity That May Compromise TheSystem [18]. In The Case Of VirtualizedEnvironment, The Problem Of Security ArisesEven More Due To Fact That It Contains MultipleDevices That Are Subjected To Attacks And OneOf Them Can Be Used To Gain Access To TheShared Environment Of The Rest Devises [16].

In This Paper, We Propose A Model ForEnhancing The Authentication Process ForHypervisors, Where An Encrypted RandomNumber Associated To Each Machine Is CreatedAnd Stored In The Host Machine. When A LoginAttempts From A Machine, Its Encrypted NumberIs validated Along With The Other Credentials InOrder To Establish The Session. If This ValidationIs Failed The User Will Be Notified. The CompleteProcess Is Discussed In Section IV. While TheRelated Work Done On Securing The HypervisorsIs Given In Section II, An Overview Of TheAuthentication Methods Is Provided In Section III. And Finally, The Final Conclusion And The FutureWork Are Offered In Section V.

II. RELATED WORK

Hypervisor Acts As A Controller AndManager Of The Virtual Machine And ResourcesSharing Over The Internet. In Fact, Securing TheEntire Virtual Infrastructure Relies On TheSecurity Of The Virtualization ManagementSystem That Controls The Hypervisor And AllowsThe Operator To Start Guest Oss, Create NewGuest OS Images, And Perform Other Actions [. Because Of The Security Implications Of TheseActions, Access To The Virtualization ManagementSystem Should Be Restricted To Authorized Administrators Only. Indeed, ManyMethods Have Been Proposed In This Regard ToProvide Better And More Secure Experience ForThe Hypervisor. A Review To The Related WorkIs Given In This Section.


The Mandatory Access Control (MAC)Architecture Was Employed In [3]. Shype WasDesigned To Isolate The Virtual Machine From TheHost And Allow Access Only When ItSatisfies The MAC. So, The Virtual Machines CanOnly Get The Resources According To The PreDefined Access Policy Stored In The MACStructure.

To Eliminate The Hypervisor AttackService, A Method Based On NOHYPEArchitecture That Provides More Security In TermsOf Multiple Virtual Machine Systems WasDeveloped By [4]. In This Approach, PreAllocating Resources Are Assigned To EachVirtual Machine, Then Each Virtual Machine IsEnforced To Only Access Its Pre-AllocatedResources. Here, Resources Could Be Memory,Input/Output Devices, Or Others. The NOHYPEAlso Provides The Guest OS With Boot UpMechanism With A Modified Cache SystemConjunction For Later Use In Order To MinimizeThe Changes To The Guest OS [4]. A DynamicVirtual Machine Dependability MonitoringNOHYPE Was Proposed In [6]. In Which It UsesThe Existed Virtual Machines As Trap To TheExecution And Transferring Control To The
Hypervisor Monitoring Ability. It Is Simpler Dynamic And Able To Monitor At Application Level To Providing Better System With Less Venalities.

In [2], HYPERPASS Model Was Proposed To Provide Security Enhancement Through Providing Two Environments One For User And The Other For HYPERPASS. In Short, An Online Password Is Associated With The Remote Service Only Without The Need For The Typical User Password. The Set Of Related Passwords Is Stored And Managed By The HYPERPASS That Makes The Password Scheme More Reliable And More Secure [2].

In The Term Of The Authentication, A Work Has Been Done To Enforce And Protect The Password-Based Systems [15]. It Bases On Two Steps Authentication By Using The Mobile Phone Where The User Is Entre The System With His Own User Name And Password But From A Different Device. Then A Further Authentication Process Is Applied Using The Mobile Phone Of The User In Order To Proof The Legit Identity Of That Person.

Ultimately, Resources Partitioning Was Also Considered. Here, The Partitioning May Be Physically Or Logically. In Physical Partitioning, The Hypervisor Assigns Separate Physical Resources To Each Guest OS, Such As Disk Partitions, Or Disk Drives. On The Other Hand, Logical Partitioning May Divide Resources On A Single Host Or Across Multiple Hosts As In A Pool Of Resources With The Same Security Impact Level Categorization, Allowing Multiple Guest Oss To Share The Same Physical Resources, Such As Processors And RAM. Physical Partitioning Sets Hard Limits On Resources For Each Guest OS Because Unused Capacity From One Resource May Not Be Accessed By Any Other Guest OS. Having Physical Separation For Resources May Provide Stronger Security And Improved Performance Than Logical Partitioning. However, Hypervisors Can Theoretically Support A Level Of Logical Isolation Nearly Equivalent To Physical Isolation, Mediating All Communications From Each Guest OS To Have Full Control Over Each Guest OS’s Actions. In Fact, Guest Oss Are Often Not Completely Isolated From Each Other And From The Host OS Because That Would Prevent Necessary Functionality Such As Access Files, Directories, The Copy/Paste Buffer, And Alike.

III. AUTHENTICATION METHODS

Authentication Is The Process Of Proving The Identity Of A Person And Proving It As The True Valid Form? In Other Words, When Someone Claim That He Is Himself It Is A Way To Prove That It Is Indeed Himself Like Proof Of Identity. Password Is Considered The Simplest And Earliest Method Of User Authentication That Is Still In Use Nowadays, Since We Are Focusing Of A Virtual Machine Security In Our Work, It Is Essential To Focus On Access Control And Authentication Of The Virtual Machines To The Host Server Machine.

Each Machine In The System Have An Id And A Password That Would Be Matched With An Existing Table In The Server. It Is Used To Proof The Correctness Of It In Order To Grant The Access. Such Passwords Are Kept In A Table, Which Is Called Password Confirmation Table [12]. Most Common Password Systems Suffer From Many Problems Such As The Weakness Of Passwords, Losing The Password, Or Even Stealing Them. Thus, Using A Stronger Shame Is Required To Maintain Security In This Manner [11].

There Are Many Alternatives To The Basic Password-Based Authentication Shames Like The Graphical, Image, And Audio-Based Authentication Process, Which Are Currently Used In Various Applications [5]. Although Password Is Highly Used And Common In Many Systems, It Has Major Weak Point Of Getting Stolen By Others Through Attacking Servers, Network, Or Hosts, Thus A Better Solution Is Needed [2].

In Short, A Protected Password Scheme Is Needed To Be Applied To Gain Further Security For The Password In The Case Of Stooling It By An Attacker And Then Using It To Access The System [15]. In This Case, The Threat Is Not Only On The Users’ Accounts But Also On The System Itself.

IV. THE PROPOSED MODEL

In This Work, We Have Reviewed The Topics Of The Hypervisor And The Authentication Process In Order To Develop A New Security Model For Hypervisors. Since The Hypervisor Acts As A Monitor And Manager Of The Virtual Machines, It Can Act As The Security Guard For Them By Yet Providing Another Level Of Securing For The Virtualization Process. We Propose A Model In Which It Would Act As A Monitor Of A Second Level Of Authentication Process, Thus Providing A More Secure Environment.
Despite the fact that the user name and password mechanism or the password-based authentication is highly used in most of the current systems, it has a major drawback as it is easy to be forgotten or even stolen by attackers and then used to access the server to compromise it.

To solve this problem, an enhancing to the hypervisor is proposed, where an encrypted random number/key associated to each machine is created and stored in the host server to serve as a second level of authentication. So, when a machine attempts to login the host server, its associated encrypted key is validated against the valid list stored in the host server along with the other credentials. If the validation process is failed, an interrupt is accrued, and the user is notified. Figure 2 and 3 illustrate these steps.

ACKNOWLEDGEMENTS

The authors are grateful to the applied science private university, Amman-Jordan, for the full financial support granted to cover the publication fee of this research article.

REFERENCES


