RESEARCH ARTICLE OPEN ACCESS

Enhancing the Hypervisor as a Second Layer of Authentication

Mohammed Ali Kamoona[1], Ahmad Mousa Altamimi[2]
[2]*(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

I. 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 Recuses. It Does Not Allow Direct Access To The

Host Physical Resources Before It Is Authenticated First. Unfortunately, Most Of The Hypervisors Are Generally Equipped By A Simple Password Authentication Scheme [20].

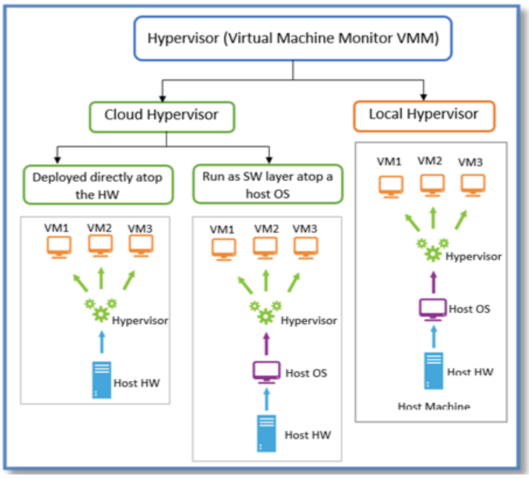


Fig. 1: Types Of Hypervisors

However, Password Authentication Scheme Is Entirely Based On Confidentiality And The Strength Of The Password, Which Is Vulnerable To Various Attacks (E.G., Offline Password Guessing Attack And A Privileged Insider's Attack) And Needs Resources Sharing Access Control [3].As A Result, Many Security Methods Have Been Developed In The Literature, Cryptography, Intrusions Detection, And Authentication Are The Most Used [8]. While Some Of Them Have Been Proposed For Securing The Virtual Machine From Unauthorized Access, The Others Have Been Focused On The Operating Systems. We Note That The Most Important Security Aspect In Term Of Protecting The Operating Systems And The Virtual Machines Is Keeping Unauthorized Personals From Doing Any Malicious Activity That May Compromise The System [18]. In The Case Of Virtualized Environment, The Problem Of Security Arises Even More Due To Fact That It Contains Multiple Devices That Are Subjected To Attacks And One Of Them Can Be Used To Gain Access To The Shared Environment Of The Rest Devises [16].

In This Paper, We Propose A Model For Enhancing The Authentication Process For Hypervisors, Where An Encrypted Random Number Associated To Each Machine Is Created And Stored In The Host Machine. When A Login Attempts From A Machine, Its Encrypted Number Is Validated Along With The Other Credentials In Order To Establish The Session. If This Validation Is Failed The User Will Be Notified. The Complete Process Is Discussed In Section IV. While The Related Work Done On Securing The Hypervisors Is Given In Section II, An Overview Of The Authentication Methods Is Provided In Section III. And Finally, The Final Conclusion And The Future Work Are Offered In Section V.

II. RELATED WORK

Hypervisor Acts As A Controller And Manager Of The Virtual Machine And Resources Sharing Over The Internet. In Fact, Securing The Entire Virtual Infrastructure Relies On The Security Of The Virtualization Management System That Controls The Hypervisor And Allows The Operator To Start Guest Oss, Create New Guest OS Images, And Perform Other Actions []. Because Of The Security Implications Of These Actions, Access To The Virtualization Management System Should Be Restricted To Authorized Administrators Only. Indeed, Many Methods Have Been Proposed In This Regard To Provide Better And More Secure Experience For The Hypervisor. A Review To The Related Work Is Given In This Section.

Authors Of [14] Proposed A Protected Hypercall Approach. Here, The Hypercalls Are Authenticated Against A Trusted Access Table. The Authentication Process Is Done By Adding Extra Arguments To The Hypercall That Would Represent The Access Policy And Also Adding A Message Authentication Code (MAC), Which Is Encrypted To Maintain The Correctness Of The Hypercall. The MAC Is Calculated By The Access Policy Taking Into Account The Access Policy And The Call Address.

The Mandatory Access Control (MAC) Architecture Was Employed In [3]. Shype Was Designed To Isolate The Virtual Machine From The Host And Allow Access Only When It Satisfies The MAC. So, The Virtual Machines Can Only Get The Resources According To The Pre-Defined Access Policy Stored In The MAC Structure.

To Eliminate The Hypervisor Attack Service, A Mothed Based On NOHYPE Architecture That Provides More Security In Terms Of Multiple Virtual Machine Systems Was Developed By [4]. In This Approach, Pre-Allocating Resources Are Assigned To Each Virtual Machine, Then Each Virtual Machine Is Enforced To Only Access Its Pre-Allocated Resources. Here, Resources Could Be Memory, Input\Output Devices, Or Others. The NOHYPE Also Provides The Guest OS With Boot Up Mechanism With A Modified Cache System Conjuration For Later Use In Order To Minimize The Changes To The Guest OS [4]. A Dynamic Virtual Machine Dependability Monitoring NOHYPE Was Proposed In [6]. In Which It Uses The Existed Virtual Machines As Trap To The Execution And Transferring Control To The

DOI: 10.9790/9622-0804028589

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.

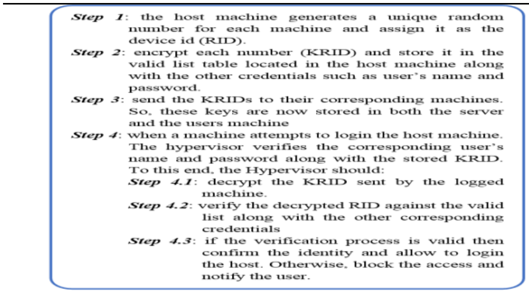
Each Machine In The System Have An Id And A Password That Would Be Matched With An Existing Table In The Server. It Is Used To Proof The Correctness Of It In Order To Grant The Access. Such Passwords Are Kept In A Table, Which Is Called Password Confirmation Table [12]. Most Common Password Systems Suffer 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.



Step 1: the host machine generates a unique random number for each machine and assign it as the device id (RID).

Step 2: encrypt each number (KRID) and store it in the valid list table located in the host machine along with the other credentials such as user's name and password.

Step 3: send the KRIDs to their corresponding machines. So, these keys are now stored in both the server and the users machine

Step 4: when a machine attempts to login the host machine. The hypervisor verifies the corresponding user's name and password along with the stored KRID. To this end, the Hypervisor should:

- ***Step 4.1***: decrypt the KRID sent by the logged machine.
- ***Step 4.2***: verify the decrypted RID against the valid list along with the other corresponding credentials
- ***Step 4.3***: if the verification process is valid then confirm the identity and allow to login the host. Otherwise, block the access and notify the user.

Fig 2. The Proposed Model's Steps

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 Machine 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.

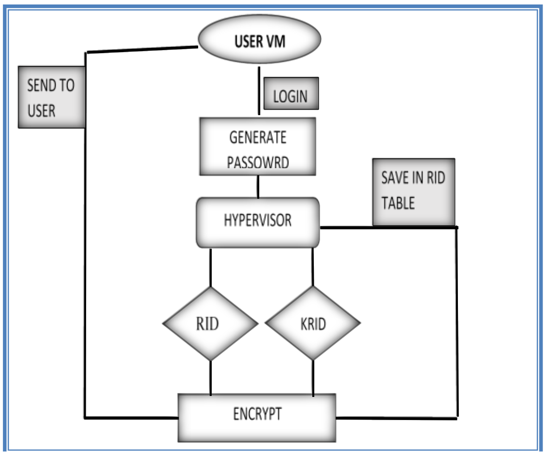


Fig 3. The Proposed Model's Flowchart

V. CONCLUSION AND FUTURE WORK

The Hypervisor Is A Complex Software That Manages And Controls The Access Of The Virtual Machines To The Host Server Hardware. While The Hypervisor Protected By A Password-Based Authentication Scheme, Which Off Course Provides Good Security Countermeasure, It Is However Considered Weak Mechanism In Terms Of Determining The Real Identity Of The Virtual Machines In Cloud Environment. In Order To Improve The Hypervisor's Authentication Process, We Proposed A Model For Enhancing It By Making The Hypervisor Do A Further User Authentication Step. Where A Unique Numbers Or Keys Are Created For The Virtual Machines And Kept In Encrypted Format In The Host Server. These Keys Are Used For Improving The Authentication Process. We Believe That The Suggested Model Will Provide A More Secure And Reliable Environment To The Cloud Systems And Virtual Machines In Verity Domains. In The Future Work, We Are Planning To Implement It Using A Large Real-Life Hypervisor Application To Gain Real Response To Make The System Even More Reliable.

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

[1] Nancy Arya, Mukeshgidwani, Shailendra Kumar Gupta, "Hypervisor Security - A Major Concern," International Journal Of Information And Computation Technology, Volume 3, Number 6, 2013.

[2] James "Murphy" Mccauley, Radhika Mittal," Hyperpass: Hypervisor Based Password Security.

[3] Sailer, Reiner, Et Al. "Building A MAC-Based Security Architecture For The Xen Open-Source Hypervisor." Computer Security Applications Conference, 21st Annual. IEEE, 2005.

[4] Szefer, Jakub, Et Al. "Eliminating The Hypervisor Attack Surface For A More Secure Cloud." Proceedings Of The 18th ACM Conference On Computer And Communications Security. ACM, 2011.

[5] Lopes, Hezal, And Madhumita Chatterjee. "A Survey Of User Authentication Schemes For Mobile Device." International Journal Of Modern Engineering Research (IJMER) 1.3: 3012-3019.

[6] Estrada, Zachary J., Et Al. "Dynamic Vm Dependability Monitoring Using Hypervisor Probes." Dependable Computing Conference (EDCC), 2015 Eleventh European. IEEE, 2015.

[7] Lowe, Scott. Mastering Vmware Vsphere 5. John Wiley & Sons, 2011.

[8] HASHIMOTO, Masaki. "A Survey Of Security Research For Operating Systems."

[9] Msjayshridamodarpagare, Dr. Nitin A Koli" A Technical Review On Comparison Of Xen And KVM Hypervisors: An Analysis Of

Virtualization Technologies", International Journal Of Advanced Research In Computer And Communication Engineering Vol. 3, Issue 12, December 2014.

[10] Obasuyi, G., And Arif Sari. "Security Challenges Of Virtualization Hypervisors In Virtualized Hardware Environment." International Journal Of Communications, Network And System Sciences 8.07 (2015): 260.

[11] Sahu, Saraswati B., And Angad Singh. "Survey On Various Techniques Of User Authentication And Graphical Password." International Journal Of Computer Trends And Technology (IJCTT) 16 (2014): 98-102.

[12] Tsai, Chwei-Shyong, Cheng-Chi Lee, And Min-Shiang Hwang. "Password Authentication Schemes: Current Status And Key Issues." Intentional Journal Of Network Security 3.2 (2006): 101-115.

[13] Hirt, Timo. "Kvm-The Kernel-Based Virtual Machine." Red Hat Inc (2010).

[14] Le, Cuong Hoang H. Protecting Xen Hypercalls: Intrusion Detection/Prevention In A Virtualization Environment. Diss. University Of British Columbia, 2009.

[15] Czeskis, Alexei, And Dirk Balfanz. "Protected Login." International Conference On Financial Cryptography And Data Security. Springer Berlin Heidelberg, 2012.

[16] Reuben, Jenni Susan. "A Survey On Virtual Machine Security." Helsinki University Of Technology 2 (2007): 36.

[17] Perez-Botero, Diego, Jakub Szefer, And Ruby B. Lee. "Characterizing Hypervisor Vulnerabilities In Cloud Computing Servers." Proceedings Of The 2013 International Workshop On Security In Cloud Computing. ACM, 2013.

[18] Muhammad Waqas, Maria Iram, Rehamat-E-Bari Wajeeha" SECURITY SURVEY OF FAMOUS OPERATING SYSTEMS", International Journal Of Computer Science And Mobile Computing, Vol. 3, Issue. 10, October 2014.

[19] Pawar, Swati. "Performance Comparison Of Vmware And Xen Hypervisor On Guest Os." (2015): 56-60.

[20] Denz, Robert, And Stephen Taylor. "A Survey On Securing The Virtual Cloud." Journal Of Cloud Computing: Advances, Systems And Applications 2.1 (2013): 17.

Mohammed Ali Kamoona"Enhancing the Hypervisor as a Second Layer of Authentication"InternationalJournal of Engineering Research and Applications (IJERA) , vol. 8, no. 4, 2018, pp. 13-17