International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 01 | Jan 2023 www.irjet.net p-ISSN: 2395-0072

Secure Desktop Computing In the Cloud

Priyanka Shankar Bhingardeve[1], Prajkta Mahendra Ghadge[2], Asst.Dr.S.P.Jadhav[3], Asst.prof.S.V.Thorat[4]

[1st]Priyanka Shankar Bhingardeve, MCA YTC, Satara
[2nd]Prajkta Mahendra Ghadge, MCA YTC Satara
[3rd]Dr.S.P.Jadhav,[4th]Prof.S.V.Thorat, Dept. of MCA Yashoda Technical Campus,Satara-415003

Abstract—

Computation that employees perform on their desktop and the management of the desktop computing infrastructure to the cloud, the need for securing such cloud-hosted user computing tasks and environments become paramount. In this paper, we present Venia, a secure cloud-based desktop computing platform designed to protect against both external and internal threats. Accessible to end-users through a thin Remote Desktop Protocol (RDP) client Venia isolates end-user's applications and data into containers and subjects the interactions with and among the containers to security policies. Following a principle of least privilege, Venia security policies control user's access to containers, network and file system interaction of the containers, cross-container data sharing and also enables collection of detailed logs for auditing purpose. Venia has been deployed to a 3rd party test environment where it demonstrated that end-users can perform the tasks they need on a daily basis, without introducing greater risk to the overall organization, and its currently undergoing security and performance evaluation by an independent evaluation team.

1. INTRODUCTION

The next step within the trend of moving backend services and supporting computing infrastructure to the cloud, is to maneuver end-user computing and its supporting infrastructure to the cloud additionally. Cloud computing provides economy of scale, eliminates the headache of computer code and hardware management and maintenance, and permits on-demand scaling and pay as you utilize rating. Properly architected, moving end-user computation to the cloud will offer a security profit. A conscientious cloud seller can offer stronger perimeter protection, specialised employees, and established tools, techniques and procedures for handling security incidents than a typical enterprise will generally deploy. However, sharing machine resources within the cloud presents a brand new set of security challenges for ensurinorganization and even worse, users from completely different organizations cannot breach security to attain malicious objectives.

2. Related Work

Secure Desktop computing in the cloud Current solutions for desktop computing within the cloud square measure based off of a Virtual Desktop Infrastructure (VDI) approach. VDI could be a variety of virtualization wherever entire desktop solutions are hosted within the cloud, so accessed employing a skinny consumer, usually with RDP. One such technology is Horizon seven by VMWare. in hand with these solutions is their wholesale exporting of the desktop atmosphere to the cloud. While helping to modify the digital geographic point and providing a centralized management over resource and network access, these solutions still maintain the appliance primarily based security problems inherent in a very ancient desktop.

3. Design Goals And Approach

The main style goals for Venia were:

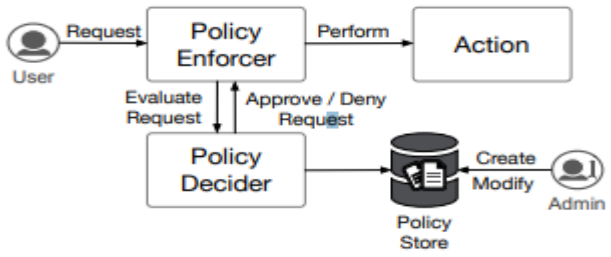
• Role-specific UCEs: UCEs for individual users ought to consist of role-specific application bundles, wherever a job defines that desktop applications and resources area unit required to perform a particular job connected operate. A single user might have multiple roles, presumably requiring use of applications from multiple operative systems (e.g., Linux and Windows) in a very single role, and resources will be shared among completely different roles.

• Enterprise-specific security management and auditing:

Interaction between end-user skinny consumer and UCE ought to be encrypted. Resource access, data sharing and use of UCEs ought to be subject to enterprise-specific security controls and auditing policies.

• End-user expertise: End-user experience shouldn't change drastically from exploitation desktop atmosphere, in particular, end-users shouldn't need to re-authenticate themselves for role specific resource access, ought to realize familiar applications in their UCE, and be able to cut and paste wherever allowed by the enterprise policy.

• Administration: Venia ought to give a straightforward approach for administrators to outline enterprise-specific security and auditing policies, and a straightforward to outline role-specific application bundles and instantiating user-specific UCEs. To attain these goals, Venia was designed as distinct components a collection of microservices establishing the required enterprise IT services for a useful corporate infrastructure, a User cipher atmosphere (UCE) that defines the end-user space, together with their desktop, keep files and applications.



A. Enterprise IT Services as Microservices Enterprise IT services play a necessary and vital half in a corporate infrastructure. These services area unit liable for, among others, managing user access and authorization, and managing shared resources, like email servers, printers, and centralized filesystems. Venia contains a collection of microservices for performing aspects of those IT management functions, independent of the end-users space. Separating individual aspects of IT management responsibilities into distinct microservices that interoperate via a well-defined Representational State Transfer (REST) Application Programming Interface (API), and subjecting these interactions to strict security controls and auditing [6] reduces the chance of abusing the UCEs through the enterprise IT services, resulting in associate degree overall reduction of the attack surface of the UCEs.

Venia contains four microservices:

• **User Service:** provides the initial entry purpose into the Venia system, via a web-portal, and contains all of the business logic for authenticating a user against a directory service, like Active Directory, and obtaining all of their out there roles.

• **Virtue Service:** The Virtue Service coordinates communications between the opposite microservices, and is responsible for constructing the UCE. Once created, the only reference the UCE maintains back to the microservices is for coverage work events. This eliminates the potential for lateral attacks on the enterprise assets.

• **sensing element Service:** The sensing element service aggregates all of the logs across the Venia system. This centralized service provides the required observance and analysis of system activities.

• **Admin Service:** The admin service provides for the definition, management, and dissemination of policies

B. User Compute Environment (UCE)

UCE supports the acquainted daily interaction of the end-user to perform their daily tasks. The Venia UCE may be a single cloud based mostly machine instance that uses policy controlled containers to protect every Virtue, providing application isolation, and the ability to tightly management and monitor all actions and interactions. The UCE incorporates security mechanisms at multiple levels to ensure Associate in Nursing operational end-user expertise, whereas maintaining the goals and objectives of the policy.

4. Implementation

The current version of Venia is enforced as Associate in Nursing Amazon Web Services (AWS) application. This implementation consisted of two-subnets running in a very single Virtual Private Network (VPC). The sub-nets were divided between enterprise microservices in one, and UCEs in another. The only microservices that area unit accessible outside of the VPC area unit the Admin service, for policy construction, and also the Login service, for UCE creation.

A. UCE Implementation

Each Virtue lives through one LXC The display of every Virtue is shared to the host's X Server show to give a unified desktop look. The displays of every Virtue are shown within the sort of another window that identifies the containing Virtue. The Windows instance is connected throughRDP inside every Virtue on Associate in Nursing application basis. this permits Windows applications to own native support with the appearance of being on one seamless desktop among the Virtue. UNIX system applications area unit supported through the LXC containers the Virtues live to tell the tale. A writing board manager at the host level has been other to manage copy-paste options between the Virtue windows.

B. Demonstrative Examples

To verify our policy approach, we created and tested a few unique Virtues to exercise the capabilities of the system. Each of these Virtues were defined to address a specific security, or operational scenario.

5. Evaluation

To evaluate VENIA, we have a tendency to performed a series of performance overhead tests to estimate user perceptible overhead. For these many typical user operations, and compared against a regular desktop environment. every take a look at was conducted thrice, and the average was computed For these measurements, the quality desktop system was a VM on physically native hardware with four processor cores and 8GB of memory. VENIA was running on AWS t2.xlarge with four processors and 16GB of memory. To verify our policy approach, we have a tendency to created and tested many unique Virtues to exercise the capabilities of the system. Each of these Virtues were outlined to handle a particular security, or operational state of affairs. The automobile industry is investing in autonomous vehicles for driverless cars, which will have to analyze and make decisions on data that pertains to their surroundings for movements and directions. These vehicles need to transmit Data to the manufacturers so that they can track their usage and also get the required maintenance

alerts. The data will be transmitted through networks resulting in congestion. To achieve low latency when accessing the network, it is necessary for the manufacturers to device new effective computing ways

6. CONCLUSION

As more front-end applications and computation continue to migrate to the cloud, the need for a secure and usable platform is paramount. With Venia, we have demonstrated an architecture for a secure cloud-based end-user computing solution. With this architecture, we were successful in separating enterprise IT functions from end-user tasks, which helped to reduce the amount of information available to an attacker while still providing an operable environment for the user. We further emonstrated that enterprise specific security controls and auditing requirements can be enforced on the UCEs, and provided an easy to use administrative toll to construct well□defined policies for Virtues. Initial results show that running the applications in virtues within cloud-based UCEs subject to the applicable security controls and auditing policies do not drastically change the user's perception of the applications' response time, or constrain access to and use of information and resources they need to perform their job functions.

7. References

[1] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring knowledge run in third-party cypher clouds," in Proceedings of the sixteenth ACM conference on portable computer and communications security - CCS '09, Chicago, Illinois, USA, 2009, p. 199.

[2] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the public Cloud," IEEE net Comput., vol. 16, no. 1, pp. 69–73, Jan. 2012.

[3] K. Hashizume, N. Yoshioka, and E. B. Fernandez, "Misuse patterns for cloud computing," in Proceedings of the ordinal Asian Conference on Pattern Languages of Programs - AsianPLoP '11, Tokyo, Japan, 2011, pp. 1–6.

[4] "VMware Horizon seven is that the leading platform for virtual desktops and applications.," VMWare. [Online]. Available: https://www.vmware.com/products/horizon.html. [Accessed: 29-Apr□2019].

[5] N. Dragoni et al., "Microservices: yesterday, today, and tomorrow," ArXiv160604036 matter, Jun. 2016.

[6] T. Yarygina, "Exploring Microservice Security," p. 144.

[7] G. Nath Nayak and S. Ghosh Samaddar, "Different flavours of Man-In□The-Middle attack, consequences and potential solutions," in 2010 third International Conference on engineering and knowledge Technology, Chengdu, China, 2010, pp. 491–495.

[8] S. Jeuris and J. E. Bardram, "Dedicated workspaces: quicker commencement times and reduced psychological feature load in ordered multitasking," Comput. Hum. Behav., vol. 62, pp. 404–414, Sep. 2016.

[9] S. S. Clark, A. Paulos, B. Benyo, P. Pal, and R. Schantz, "Empirical Evaluation of the A3 Environment: Evaluating Defenses Against Zero□Day Attacks," in 2015 tenth International Conference on convenience, Reliability and Security, Toulouse, France, 2015, pp. 80–89.

[10] C. Smutz and A. Stavrou, "Malicious PDF detection exploitation data and structural decisions," in Proceedings of the twenty eighth Annual portable computer Security Applications Conference on - ACSAC '12, Orlando, Florida, 2012, p. 239.

[11] R. Sandhu, V. Bhamidipati, and Q. Munawer, "The ARBAC97 model for role-based administration of roles," ACM Trans. Inf. Syst. Secur., vol. 2, no. 1, p. 31.

[12] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding Attributes to Role□Based Access management," IEEE Comput., vol. 43, no. 6, p. 4, 2010.

[13] D. Thomsen and E. Bertino, "Network Policy human action exploitation Transactions: The heavy particle Approach," in Proceedings of the 23nd ACM on conference on Access management Models and Technologies - SACMAT '18, state capital, Indiana, USA, 2018, pp. 129–136.

[14] R. Rosen, "Linux Containers and in addition the long haul Cloud," p. 85.

[15] S. D. Wolthusen, "Security policy human action at the arrangement level in the Windows organisation code package family," in Seventeenth Annual Computer Security Applications Conference, port of entry, LA, USA, 2001, pp. 55–63.

[16] C. Boettiger, "An introduction to working person for duplicatable analysis, with examples from the R setting," ACM SIGOPS Oper. Syst. Rev., vol. 49, no. 1, pp. 71–79, Jan. 2015.

[17] A. Driscoll, Microsoft Windows PowerShell three.0 initial look: a fast, succinct guide to the new and exciting decisions in PowerShell three.0. 2012.

[18] B. Chandra, "A technical scan of theOpenSSL 'Heartbleed' vulnerability," p. 18.