Security Policy Concerns in a Virtualized Network Environment

Dennis C. Guster*
Professor
Department of Information System
St. Cloud State University
St. Cloud, MN 56301-4498, USA
E-Mail: dcguster@stcloudstate.edu

Olivia F. Lee‡
Affiliate Assist. Professor
Department of Marketing
University of Washington
Seattle, WA 56301-4498, USA
E-Mail: oflee@u.washington.edu

Dustin C. Rogers*
Security Officer
Business Computer Research Lab
St. Cloud State University
St. Cloud, MN 56301-4498, USA
E-Mail: rodu0601@stcloudstate.edu

Abstract

Virtualization has become an important concept among organizations' information technology managers in their efforts to promote data centers that feature green computing, reduce personnel costs, and save physical space. While these benefits are most enticing, the security concerns associated with virtualization are often not addressed in security policy at an operational level. Based on real world problems gleaned from the log files of an autonomous research laboratory's system, the authors present practical solutions to address vulnerabilities of a network with over 200 hosts 40 of which are virtualized. The paper provides an overview of three common threats related to virtualization including two related to side-channel attacks, and develops solutions to mitigate those security vulnerabilities. The proposed study provides important implications to security policy management in light of the characteristics of virtualization.

Dennis C. Guster*, Olivia F. Lee‡ and Dustin C. Rogers*
* St. Cloud State University, St. Cloud, MN
‡ University of Washington, Seattle, WA
* Primary Contact E-Mail: dcguster@stcloudstate.edu

1 Introduction

Virtualization has become an important concept among organizations' information technology managers in their efforts to promote data centers that feature green computing, reduce personnel costs, and save physical space [1]. While these benefits are most enticing, the security concerns associated with virtualization are often not addressed on a policy or operational level [2]. Virtualization creates a new layer of abstraction that often complicates an organization's security strategy. This is because information technology personnel tend to focus on hardware issues such as protecting the computer hosts but not the virtual zones that are created within the host. A recent Gartner Group survey reveals that by 2012 about 60% of virtualized data centers are expected to be less secured than they are now [3]. Many experts argue that over the next decade almost all major data centers will take advantage of virtualization [4]. Notwithstanding that some features of virtualization can enhance security, many unknown threats are troublesome and dealing with the unknowns can be risky [5]. A popular way to cope with complexities of virtualization involves extensive automation of processes [6]. While automation offers some degree of promise, it requires a well thought-out and effective security policy in place to drive the automation. The purpose of this paper is to delineate security concerns associated with virtualization and propose a series of policy solutions to mitigate some of those security issues. Based on real world occurrences within an autonomous system using virtualized in a research laboratory, the authors present practical solutions to address several major virtualized problem related to virtual design and side-channel attacks.

2 Methodology

This paper presents a series of attacks on virtual resources within an autonomous system of a research laboratory. A series of attacks including, side-channel attacks, were reported by the research laboratory' security personnel. The attacks represent real-time incidents that occurred during a period of several months. It is noteworthy to report that the attacks were not caused by experiments or stimulations generated for research purposes. Rather, they represent random attacks by unknown sources to obtain information by exploiting security loop holes caused by virtualizing hosts. The log files generated by the system are methodically analyzed and a research team was setup to investigate the nature of these attacks. The data was gleaned by observation and through a careful analysis. The log files provide a record of the various operating level system events related to the virtualization process. Fortunately, the majority of the attacks occurred while the system was still in research/development mode. As a result of these observations the design was modified several times and the security team is in the process of devising tools to protect against timing/monitoring side-channel attacks.

2.1 Autonomous System Characteristics

The autonomous system of the research laboratory has a clearly defined routing policy that defines access to over 200 hosts, approximately 40 of which are housed in virtual

zones. This research laboratory provides resources to support instruction within the university, resource to support graduate student/faculty research and high performance computing resources used in sponsored research. The system is physically located in a mid-western university and it was in designed to reduce the: (1) number of physical hosts, (2) amount of physical space required to store the hosts, (3) amount of electricity required to run and cool the hosts, and (4) complexity of the design as a means to save personnel costs for regular maintenance. Prior to virtualization, 10 physical hosts were required to support the production related services. This was reduced to one physical host with 10 virtual zones. Each zone represents one service such as domain name service (DNS) or dynamic host configuration protocol (DHCP). Because these services are mission critical three replicas were configured to provide fault tolerance and load balancing. The main production physical computer and Replica number 1 are housed together in the same equipment room. Replica number 2 is housed in a different building on campus about two blocks away and the third replica is housed in another city about 500 miles away. These computing resources are monitored and managed by about five technical staff.

2.2 Problems Identification

The unexpected attacks on the research laboratory's autonomous systems provided the researchers an opportunity to identify real-world design deficiencies and side-channel attacks. In this section, the paper outlines three common attack scenarios the author's observed related to their virtualized configurations.

2.2.1 Problem 1: Replication, Fault Tolerance and Fail-over Procedures

In a modern virtualized environment where software applications are deployed, direct communication channels across the host system's motherboard are used to optimize data flow as illustrated in Figure 1. The traffic going through the internet cloud is the wide area network (WAN) traffic. In this type of virtualized setting, there will always be replication traffic limited by the available bandwidth within the WAN. The traffic denoted by the dotted lines is moving across the motherboard at a high rate of speed. The replication/fault tolerance/fail-over can be accomplished by duplicating the virtual environment on a remote or second host or the replica. If the original host expires, then the entire virtualized environment will fail over to the second host. When configured properly, communication between the virtual machines will continue over the second host's motherboard.

In the event when only one system fails on the original host, only that system will fail-over to the remote or the second host. This situation means that some traffic is still traversing the first system's motherboard, while some of the traffic must rely on a slower media either a LAN or WAN connection. The progression of the fail-over process is illustrated in Figure 2. In this figure only the domain name service (DNS) is configured to fail-over. The dynamic host configureation protocol (DHCP) tends to be site-specific so it may not be logical to fail it over. Hence, some traffic is traversing through a slow WAN

via the internet cloud. The traffic indicated by the dotted lines is motherboard only which offers improved performance especially if compared to a WAN. Since connections across a WAN coupled with the security overhead can significantly slow transmission time, network services can immediately be brought to a standstill, effectively crippling the whole autonomous system.

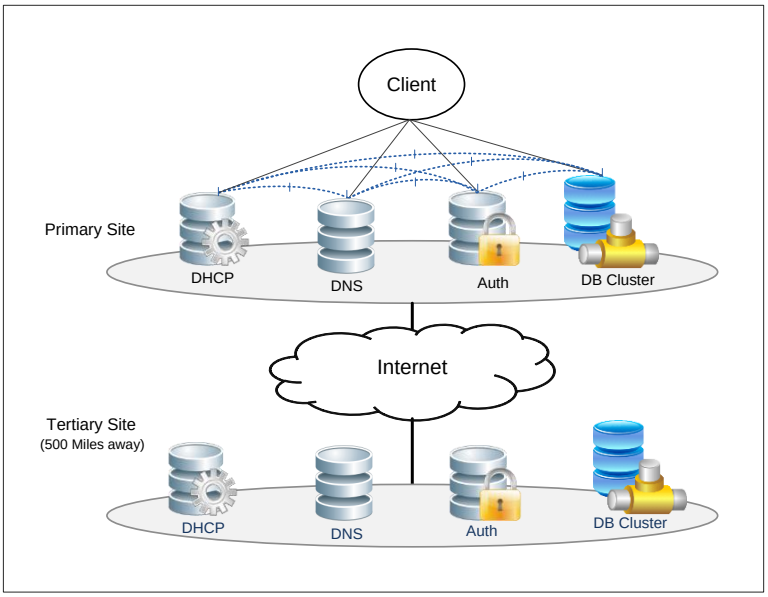

Figure 1: A Virtual Host in a Non-Fail-Over State.

2.2.2 Proposed Solution

There are three possible ways to solve problem 1as described in the preceding paragraphs.

Understanding service dependencies. The first solution involves writing a policy that takes into account dependencies when services are transferred. For example, When the DNS service is transferred, a database server that takes advantage of distributed resources should be transferred as well to allow DNS to find those resources. In other words, services that intercommunicate with one another need to be on the same replica to maintain adequate communication speed. Figure 3 illustrates the process of a fail-over state in which all services except DHCP are configured to fail-over to the tertiary hypervisor. The traffic traversing through the internet cloud indicates slow, WAN traffic while the traffic indicated by the dotted lines is being transferred across the motherboard and would run rather quickly.

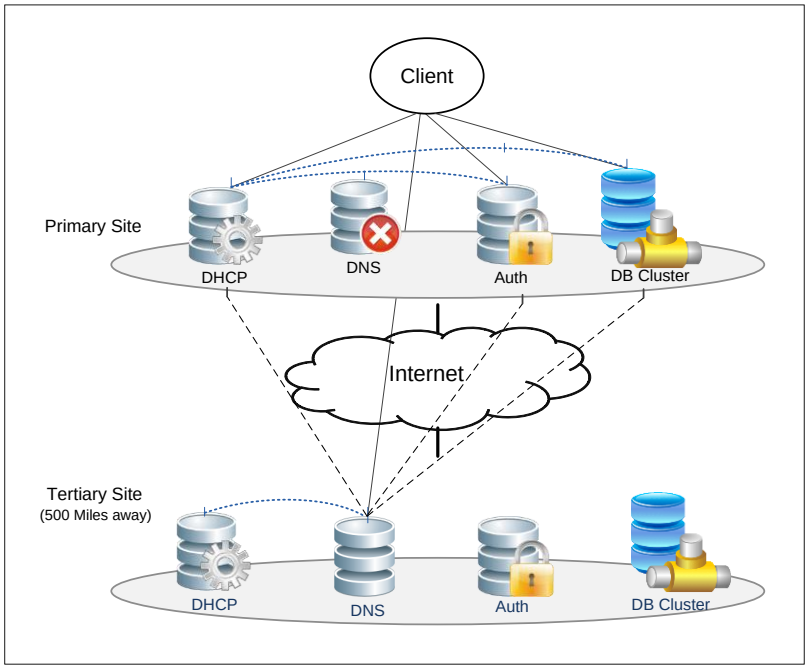

Figure 2: A Single Service Failover

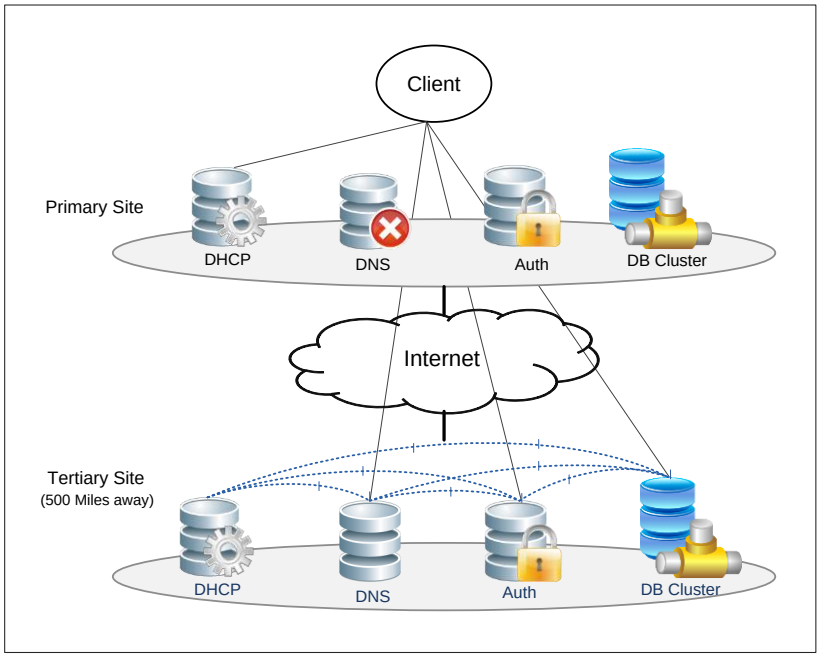

Figure 3: All Services Transferred During a Fail-Over

Define optimal utilization. The second solution involves writing a policy that defines optimal utilization of "host-only" network traffic so that LAN/WAN speeds are more equivalent. Essentially, this policy would state that bandwidth across the motherboard

would be regulated by policy to be limited to the same speed as the WAN links. Traffic flows would always run at the same speed and maintain the security boundary that motherboard-only traffic flows would provide. This solution will equalize access opportunity to the media but would result in reduced data transmission speeds.

Allow only necessary services. The third solution involves writing a policy that defines that only necessary services should be running during any fail-over. This is a short term solution that may slow down the recovery of those services that are deemed not crucial. Since the WAN link becomes more crucial during a fail-over state, it is advisable to eliminate unnecessary WAN-type services.

In the current study, the research laboratory hosts a package repository service that is available to the public, but it exists primarily for the use of the researchers. A package repository in this case refers to a server that caches downloaded Linux updates for local clients. Only one copy of the update is downloaded from the internet to the repository, and the local clients download the update from the server. During a fail-over state the security policy would require that the backup repository server only be made available to its system's clients via a WAN link. Therefore, by not configuring a backup repository server, the system would be using its WAN link to communicate with the backup replica anyway during a fail-over state. So given this state it makes sense to just have the clients download the updates individually from the internet instead.

2.2.3 Problem 2: Backup Problem

A common method in use today is to simply back up the entire host system as a single entity. By backing up the host system, each of the "guest's" virtual machines is backed up as part of one contiguous file. This process is problematic because if a small portion of the file becomes corrupted then the entire file in effect becomes corrupted, thereby incurring the loss of the virtual machine's backup copy.

2.2.4 Proposed Solution

To solve this backup problem, it is essential to write a policy that defines the extent to which virtualized machines are backed-up. Because the virtual zone can be viewed from two different perspectives: an independent entity with its own data and a subpart of the physical host, backing up the file system in its natural hierarchy, and as a single file within a virtualized host would be a good practice. Storage capacity can quickly limit the amount of space available for large backups, thus it is imperative to have both a large amount of space for storage, and limit the size of virtual machines to only consume the amount of space that is absolutely necessary.

2.2.5 Problem 3: Danger Associated with Shared Resources

Data centers taking advantage of virtualization often outsource institutional hardware requirements to other organizations. When one of those virtual hosts resides on the same physical host as some other company's virtual host, it creates vulnerability for side-channel attack when resources such as central processing unit (CPU) and/or memory (RAM) are shared between the victim and attacker. Since anyone with a virtual host on a physical machine has access to the hardware, hacker can monitor traffic moving across the main-bus and intercept another users' sensitive data. In addition, a virtual machine on the same physical host could create a denial of service attack just by running a higher workload. Figure 4 illustrates how a virtual host might be (mis)configured to be highly vulnerable. In this example, virtual machines are only configured to use one processor core that regrettably the web server clearly shares with potential attacker. Memory or RAM is also shared with the attacker and thus could be exposed to be "mined" for sensitive data.

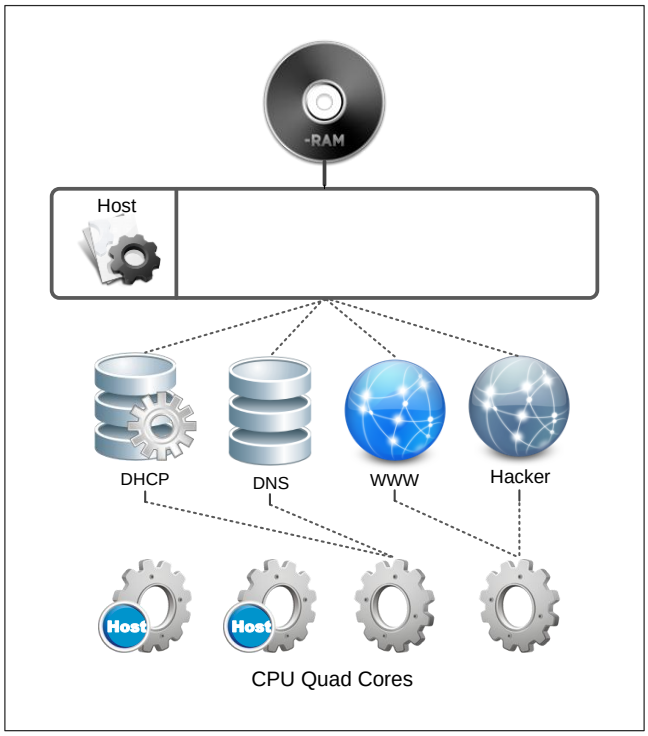

Figure 4: Highly Vulnerable Hardware Configuration

2.2.6 Proposed Solutions

There are two possible solutions to address problem 3 as described in the preceding paragraphs.

Restrict outsourced activities. First solution involves writing a policy that clearly defines the acceptable characteristic of a vendor that will provide safe outsourced virtual resources. Certainly it is critical that virtualization centers follow strict screening procedures of the clients they are willing to accept. Organizations need to write policy

that demands that outsourcing of virtualized systems only be allowed on hardware that is dedicated only to their use and therefore, other clients of the virtualization center will not share the same allocated hardware. Therefore, select datacenters should feature: (1) professional-grade hypervisor for their virtualization host applications; (2) operating systems that employ symmetric multi-processing; (3) assigned multiple cores; (4) RAM dynamically allocated in a discrete fashion; and (5) memory isolated from other virtual machines.

Figure 4 depicts a vendor configuration that would be considered vulnerable because virtual zones share memory and CPU resources. Figure 5 show a second configuration that is less vulnerable. In this improved design all VMs and the Host (H) are configured to use symmetric multiprocessing (SMP), thus they all use two processor cores, and no two machines share the same two cores. Also, memory (RAM) is dedicated to each machine, so no one VM, or the host, shares memory with the potential attacker.

Limit failed attempts. The second solution involves writing a policy that defines the maximum number of failed attempts to access cryptographically protected services such as (HTTPS), or secure shell. Once the failed maximum has been reached, a particular IP address associated with that activity would be locked out. However if the attacker is controlling a botnet or spoofing IP addresses as an extension, this hacker is allowed many attempts on the cryptographic service. Such policy needs to cover the CPU level and limit the attempts based on the process or parent process ID.

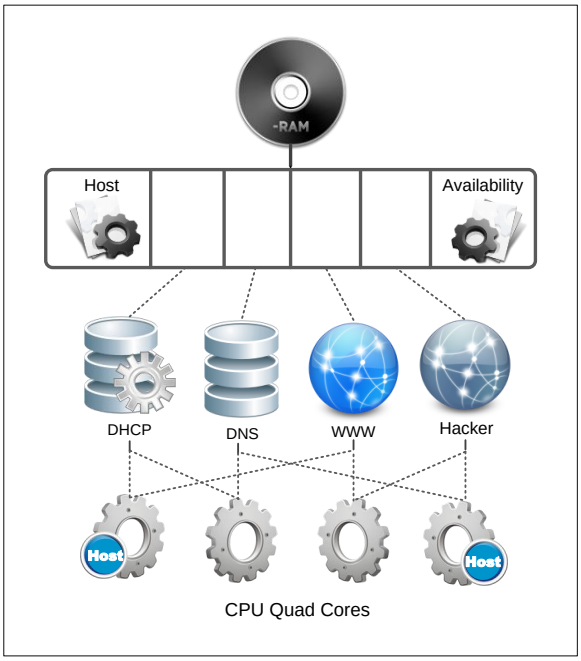

Figure 5: Safer Virtualized Host Configuration

3 Discussion

More and more modern organizations are open to the idea of adopting a virtualized data center for its many well documented advantages such as simplicity, cost effectiveness, and the benefits of creating a green computing environment. The concept of virtualization rests on the premise that hosts and applications are isolated, and the data center is not required to house each application or service in a separate physical machine.

While virtualization offers attractive isolation, it also creates vulnerabilities when hardware is shared. These vulnerabilities are backup/fault tolerance considerations, virtualization (design) configuration, equal access configurations and side-channel attacks typically related to timing/monitoring considerations. These vulnerabilities might appear subtle in nature but their identification and diagnosis requires a fairly high level of sophistication in regard to hardware configuration and functionality. Based on a series of unexpected design deficiencies and side-channel attacks on an autonomous system supporting a research laboratory, the authors presented practical solutions to address the three identified problems. These solutions are particularly noteworthy for newly virtualized data centers. Because the corrective measures related to timing/monitoring attacks need to occur in real time to be effective automating the process is crucial.

This need to automate is particularly applicable to problem 3 in that the implementation of the policy defines the maximum number of failed attempts allowed to access services that are cryptographically protected. To be effective this process needs to be automated because thousands of brute force attempts to break an encrypted password can take place in one second. A strategy to prevent this is well developed in regard to attacks coming from a network. That strategy simply blocks the attacking IP address in some form on the network firewall. This strategy can be simplified as follows: a monitoring process once detecting such a problem sends a request to the firewall to block the offending IP address and that change can take place in a matter of milliseconds. In the case of virtualization those attacks may originate from the physical host's mainbus and therefore this same logic must be applied in which a monitoring process (i.e., analogous to the network firewall) identifies brute force attacks and kills the appropriate offending processes and/or their parent process.

In summary, virtualization does offer numerous benefits, but there are numerous vulnerabilities that need to be addressed particularly in situations in which an organization with limited IT resources is using outsourced virtual machines.

References

[1] D.C. Guster, C. Hemminger, and S. Krzenski, "Using virtualization to reduce data center infrastructure and promote green computing," *International Journal of Business Research*, 9(6), 133-139, 2009.

[2] H. Clancy, "Tech watch: Security pros want strong policy for virtualization," Retrieve online on August 9, 2010 from http://searchitchannel.techtarget.com/news/article/0,289142,sid96_gci1357537,00.html.
[3] Help Net Security, "Six common virtualization security risks and how to combat them," Retrieve online on August 9, 2010 from http://www.netsecurity.org/secworld.php?id=9023.
[4] F. Siebenlist, "Challenges and opportunities for virtualized security in the clouds," Proceedings of the 14th ACM Symposium on Access Control Models and Technologies, Stresa, Italy, 2009, pages 1-2.
[5] S. Vaughan-Nichols, "Virtualization Sparks Security Concerns," *Computer*, 41(8): 13-15, 2008.
[6] S. Cabuk, C. Dalton, K. Eriksson, D. Kuhlmann, H. Ramasamy, G. Ramunno, A. Sadeqhi, M. Schunter, and C. Stuble. "Toward automated security policy enforcement in multi-tenant virtual data centers," *Journal of Computer Security*, 18(1): 89-121, 2010.