Virtualization and Risk – Key Security Considerations for your Enterprise Architecture

Taking a structured and systematic view of the impact of hardware virtualization on IT risk management

Authors:

William Hau
Vice President Professional Services
Foundstone Professional Services

Rudolph Araujo
Senior Principal Consultant
Foundstone Professional Services

Abstract

As virtualization technology gains a stronger foothold in IT departments, many questions are being raised: *“How will this technology affect my existing security posture?”; “What new concerns need to be addressed to mitigate this risk?” and “What elements of risk does virtualization share with physical deployments?”* As you would expect, there is no one size fits all solution to security, let alone one that can be extrapolated for virtualization technology. This white paper takes a pragmatic view of the different components of virtualization technologies and provides a perspective on how enterprises that are looking to deploy such technologies should think about their threat profile. It describes the people, process, and technology concerns that should be addressed before a full-scale deployment is undertaken. And finally, it provides some food for thought about the road ahead as this technology becomes more widespread.

Introduction

Hardware virtualization has been around for several years. But it seems like only recently that it has become the top story in the technology world. As a technology, virtualization seems to represent one of those revolutionary paradigms that could fundamentally change the way we think and approach computing—both with regard to servers as well as desktops and workstations. There are interesting indicators of the impact such a technological shift can have. A recent industry conference drew more than 10,000 attendees[1], putting virtualization in the same league of technologies as Java and Linux. Recently, IPO activities have seen a rise in the stock[2] of one of the principal companies in the virtualization space. Server and desktop virtualization has moved from being a buzzword to becoming a reality that will define the way organizations leverage information technology. As with any new information technology revolution, it is important to question the impact virtualization will have on an organization’s security risk. With virtualization, companies have the

[1] http://www.eweek.com/article2/0,1895,2183565,00.asp
[2] http://stocks.us.reuters.com/stocks/charts.asp?symbol=VMW&WTmodLOC=L2-LeftNav-10-Charts

advantage of evaluating the risk of deploying this new technology at the onset rather than being too deeply entrenched before answering the most critical questions.

This paper focuses on some of the wide ranging security issues and risks that organizations should consider when implementing virtualization technology. We will also explore how best to mitigate the new, enhanced, or diminished risks that this technology exposes. By breaking it down into the three major aspects that most mature organizations think about when considering information technology: people, process, and technology – we have taken a systematic and structured approach in our analysis of virtualization technology and the associated security issues.

Note that there are some topics we have specifically chosen not to cover in this paper. There are several existing white papers that focus on the benefits that virtualization has to offer with regards to security and on how virtualization can be used for malware analysis, so these topics have not been included here. Recently more attention has been given to virtual machine isolation – between virtual machines themselves as well as between a virtual machine and the host on which it runs. Not surprisingly, the security of the hypervisor[3] is also gaining a lot of attention. The hypervisor essentially represents the core virtualization platform, and it thus presents an attractive target for attackers. The theory is that if an attacker is able to compromise the hypervisor, the attacker could potentially obtain highly privileged access to the array of guests that run on top of it. That discussion, including whether it is possible to build an undetectable[4] hypervisor based root kit, is worthy of its own white paper so we will not cover it in detail here. Nor will we discuss in detail exploits in any specific virtualization platform.

Security in a Virtualized World

With the advent of virtualization, it is quite likely that you would ask yourself whether all of your current security investments count for anything in this new era. Do the old tried and tested strategies continue to

[3] http://en.wikipedia.org/wiki/Hypervisor
[4] Much has been made about being undetectable. However, as some of the leading minds on virtualization have recently written this represents a losing effort both from a technological standpoint as well as from a hacker economics perspective. http://www.cs.cmu.edu/~jfrankli/hotos07/vmm_detection_hotos07.pdf

work? If they do, are they just as effective? What about all the tools you have invested in? Perhaps the best way to answer these questions is to consider the changes that virtualization will bring and how it impacts the core of your information technology.

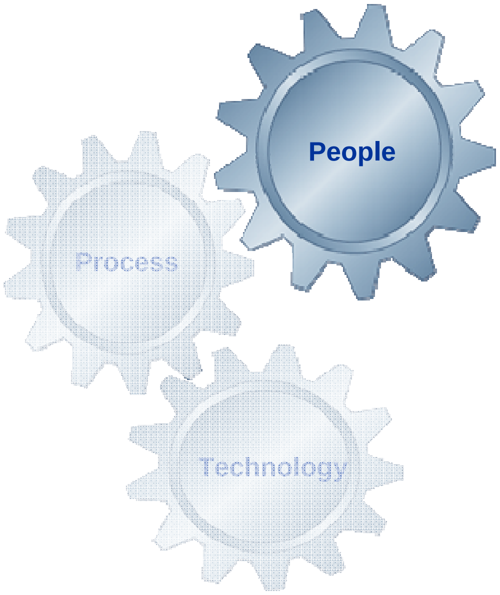
One of the common mistakes people often make is to think of information technology as just that: only technology. Unfortunately, this is a short-sighted approach that causes companies to make wrong, and sometimes costly, decisions. Years of research have shown that information technology should not only focus on technology aspects but also the people and process elements if it is to be truly effective in acting as a business enabler and in enhancing competitiveness. As one would expect, the same triad also applies to information security. Organizations can make the mistake of viewing this as a purely technological problem and deal with it using a myriad of tools rather than adopting a consistent strategy based on the core concepts of risk management.

As companies deploy more and more virtual machines, there are key considerations that should be considered for each factor; people, process, and technology. We will discuss each of these from the security impact of virtualization—positive or negative—as well as the best practices that need to be adopted to fit into this exciting new paradigm. It is important to note that many of the age-old practices that have worked in physical computing environments will continue to work in virtual ones. This paper focuses primarily on what has changed and what is new.

People

Training and Education

Frequently when we assess our customers' security implementations we find significant attention is focused on the technology at the detriment of the people aspects. It is vital that your people have access to the right training and educational material about the new technology to understand and plan for the organizational process change required to manage any new solution implementation. We recommend training your administrators, operational staff, solution architects and users on the various security aspects covered in this



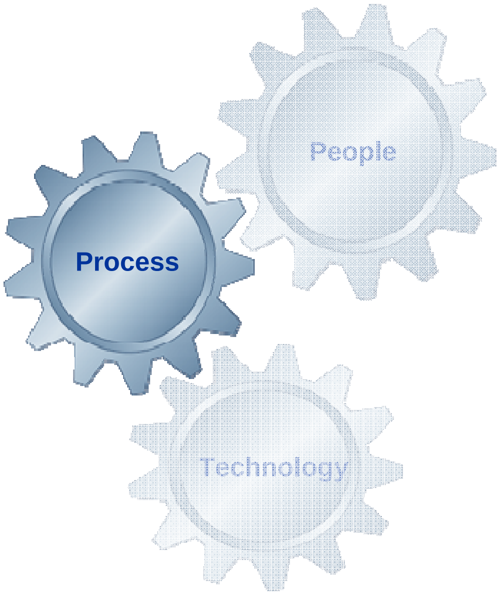
paper. For example, it is important administrators understand how to harden a given virtualization installation. Security requirements might often define a higher bar than the default installations provide. How do administrators go about locking down features that are enabled by default but are seen as risky in their specific environment? For example, any feature that opens up non-traditional connectivity between the guest and the host might be problematic. This could include features such as clipboard sharing or drag and drop support for files and data from or to the guest / host. Another example that may require specialized training is using virtualization to run the guest in a kiosk mode where the host or host controls are not visible or accessible. Administrators need to know the proper way to set up such a configuration and the pitfalls they should be watching for. It is also important for administrators to understand what the security capabilities of the underlying technologies are and the assurance provided. For instance, certain features can be disabled by the administrator at a global level, but they can still be enabled by individual users for their own virtual machines. An awareness of such features is crucial so that other control mechanisms can be put in place or at least an audit trail can be enabled.

Process

There are several areas of concern when deploying virtual machines: change control, asset tracking and management, patch management, and well-defined contingency planning.

Change Control

Traditionally, change control focuses on the operating system and includes server software, such as the database or web server. With virtualization, there is often a piece of software or perhaps firmware at a level below what is considered the operating system. This could be a mainstream host operating system such as Microsoft Windows or Linux, or a custom operating system that is optimized for virtualization like VMware® ESX Server. Change control and review boards should carefully consider any changes to this base infrastructure level before they are approved. Making changes at this level is similar to upgrading the hardware or firmware on a physical machine; such operations in the physical world are performed after



careful consideration and treated as significant. In a virtualized environment the same care must be applied to updates, upgrades, and installation of any software or changes to configurations of the underlying system. These changes can often affect all three fundamental security concepts: confidentiality, integrity, and availability.

One of the potential traps to watch for is that unlike upgrading hardware or firmware which is an involved affair, making changes to the virtualized host can be viewed as “simply editing a file” and may not even require a reboot. A lax attitude can result in such changes being treated lightly. Organizations are advised to treat such changes with the same level of oversight given to changes in the physical environment. This means that changes should follow basic change control processes such as:

- Any change should be tested in staging environments to ensure the change does not adversely affect either the host or guest operating systems. This could mean running a battery of security tests before and after the change ranging from a simple port scan to see if the TCP/IP fingerprint has changed to a full-blown, vulnerability scan as new services on the host come online for virtual management.
- Once testing is complete, changes should only be made during approved change control windows, no matter how trivial or small the change appears to be on the host.

All of the change control best practices continue to apply for the guest workloads. Some of these practices are touched upon in other parts of this white paper.

Asset Tracking and Management

Virtualization can also have an impact on how information technology assets are tracked and managed. Consider, for example, the process that might typically be followed when a new server is brought online in the physical world. This would start with some level of approval within the information technology group. Next, procurement and legal might also get involved. This implies that there is a significant amount of oversight throughout the process. In the virtual world, however, the process of provisioning a new server changes significantly. In many ways, this could be both the most important selling point of this technology as well as its biggest risk. Getting a new server up and running can be as simple as a single click which clones an existing virtual machine or imports an existing physical machine. When coupled with features such as live virtual machine migration and dynamic load balancing, which can result in new machines being “spun up” on the fly, this can lead to a nightmarish situation from an asset tracking perspective. Lack of asset tracking and management puts companies at risk of falling out of compliance with their licensing requirements. With virtual machines being brought up and torn down, it is also quite possible that licenses may be lost. To manage this risk it is imperative that operations applied in a virtual environment adhere to the same oversight, process, procedures and standards that have been created for physical systems. This means the same levels of oversight, process and procedures must be followed, the same standards applied to base virtual images, and the same controls for images to be pushed into production.

Another important aspect of virtualization is that assets can be downloaded from the Internet. A number of virtualization vendors offer preconfigured virtual appliances. These appliances are built and optimized, often through community contributions, and are typically meant to serve very specific purposes such as a firewall or an Internet browser appliance. The security risk associated with these appliances is lack of control on the contents of the appliance itself. Malware or other dangerous elements could be downloaded with the appliance. Once installed within a corporate environment, malicious software can then go about its nefarious activities for example, passive information gathering over the network. Just as organizations have very strict rules with regards to placing unapproved hardware (and software) onto the network or even powering it on, it is equally important to enforce a similar set of rules on virtual machines and especially downloaded third-party appliances. A further complication to keep in mind is that most of the virtualization technologies available today support complex networking schemes that could make such “rogue” virtual machines essentially undetectable by the network while still providing them with unrestricted access to the host as well as the network itself.

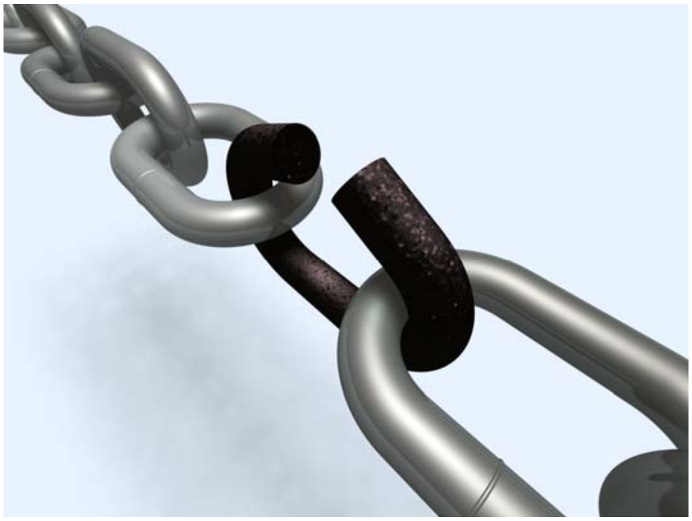
Patch Management

This goes hand-in-hand with the discussion above on change control. A common problem we see with many organizations, even before the introduction of virtualization in the environment, is that patching efforts tend to focus only on the perceived big targets. This includes the operating system and possibly server software—web servers, application servers, and database servers. Unfortunately, the smaller, seemingly inconsequential components, especially those from third parties or open source libraries, tend to be forgotten. This can leave your infrastructure vulnerable to a number of critical security issues that have been discovered and quite possibly publicly known and even patched.

Organizations should create and maintain detailed inventories of the software and components (including libraries) installed on their servers and workstations. Once the inventory is created it is important to track the usual vulnerability news sources such as security mailing lists, vendor websites, and the popular security press to watch for any discovered vulnerabilities and their associated mitigation options.

Adding virtualization to the mix, it is essential to include all of the components installed, whether on servers or client workstations, in the inventory described above. Patching virtualized systems should include the host and the guest from the operating system and applications perspectives, as well as patching the virtualization software. In addition, there could well be other components including management software for the virtual machines and software installed on end-user workstations that enables them to run the virtual machines. This is common when using a custom virtualization-aware operating system. Such systems may run a number of standard components that could have vulnerabilities of their own. It is, therefore, critical to consider these as well when patching the host.

Another consideration that might affect your choice of products is where the hypervisor is located. Traditionally, the choices have been between a virtualization-aware operating system and a hypervisor that executes above an unmodified conventional operating system. Companies have recently moved the hypervisor into firmware with a small footprint. This smaller, more compact footprint means a number of extraneous components have been removed from the default installation. However, it also implies that if a vulnerability is discovered it is likely to be harder to patch due to the usual complexity associated with flashing firmware-based components.



Contingency Planning

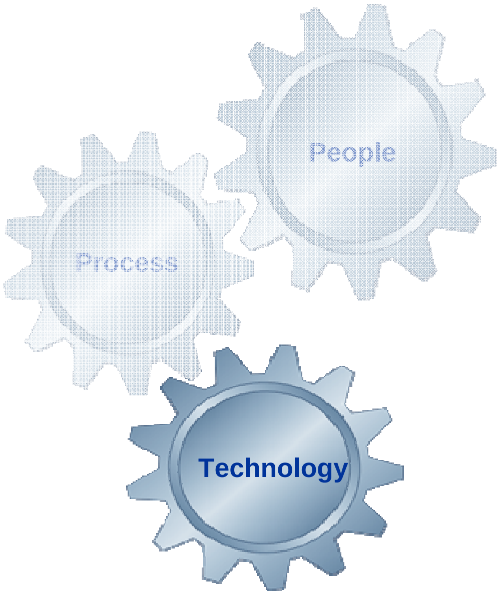
One of the major advantages of virtualization is that it can provide tremendous options for resilience in the face of failure. Many of the asset management aspects discussed above can also provide advantages over purely physical environments. For example, the ability to bring a backup server online at the click of a button in response to increased load can increase operational efficiency. Organizations should definitely take advantage of these powerful capabilities. However, these capabilities also raise some concerns. In a simple, three-tier web application with a web server in the DMZ, and an application server and a database on the ‘internal’ network, each of these could be loaded onto independent virtual machines and perform their tasks. However, consider an environment where these virtual machines all run on the same host. While this is efficient from a utilization standpoint, there is now a single point of failure. If the underlying physical server experiences hardware problems in the setup described, all three tiers would also be compromised and potentially go offline. This is further complicated if the database is shared with another application hosted elsewhere. This application would now also be affected and would have to be taken offline.

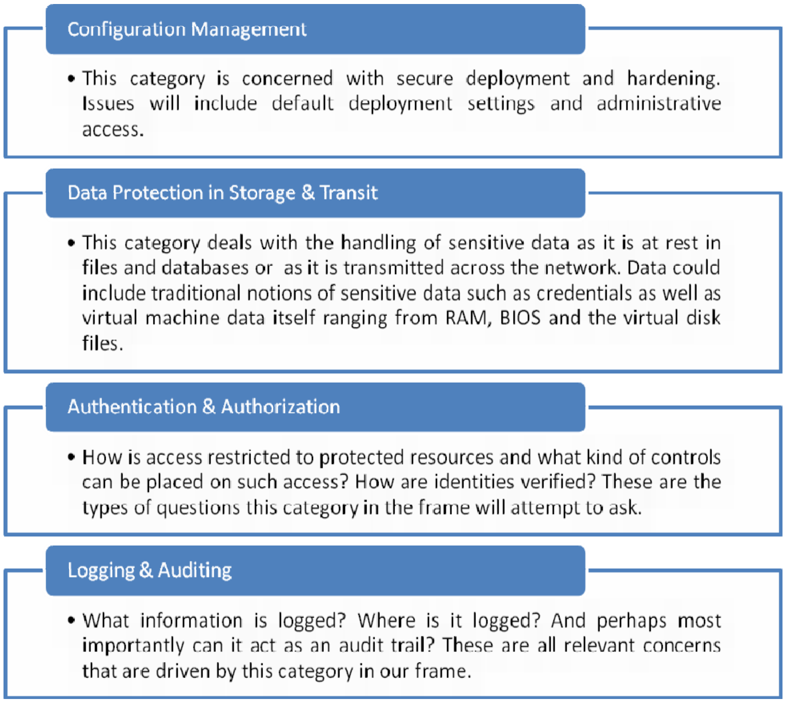
When implementing and deploying virtualization technology, IT managers must include contingency planning as part of their risk management plan. It is important to have a tried and tested plan in place before the problem occurs so engineers know exactly how to respond to minimize downtime.

Such planning can take advantage of key virtualization features such as live migration of running virtual machines or use of virtual images as part of an integrated continuity plan. These features allow administrators to set rules that can detect spikes in usage. They can use this information as a trigger to migrate a running virtual machine to another host that is not running at peak utilization. The virtual machine now runs from this new host with no loss of state or downtime. This is an extremely powerful feature for which no equivalent exists in a pure physical setup. In the future, an automated response mechanism may be scripted and/or integrated into diagnostic software to provide this functionality as part of a truly ‘self healing’ system.

Technology

In any discussion of the technological security issues associated with virtualization technology, it is essential to define an evaluation framework. Such a framework allows us to take a systematic, structured and thorough view of the system. In this case, we adapted the Foundstone® Security Framework used to securely develop and deploy applications. We did this by determining which categories are relevant for an organization that is considering the impact of virtualization on their security. We also eliminated less relevant categories and arrived at the following assessment framework categories:





Configuration Management

- This category is concerned with secure deployment and hardening. Issues will include default deployment settings and administrative access.

Data Protection in Storage & Transit

- This category deals with the handling of sensitive data as it is at rest in files and databases or as it is transmitted across the network. Data could include traditional notions of sensitive data such as credentials as well as virtual machine data itself ranging from RAM, BIOS and the virtual disk files.

Authentication & Authorization

- How is access restricted to protected resources and what kind of controls can be placed on such access? How are identities verified? These are the types of questions this category in the frame will attempt to ask.

Logging & Auditing

- What information is logged? Where is it logged? And perhaps most importantly can it act as an audit trail? These are all relevant concerns that are driven by this category in our frame.

Configuration Management

The first configuration decision related to virtualization technology that organizations will often make that could impact their security posture is the specific technology they choose to deploy. By this we do not mean which vendor is selected, but rather the specific virtualization stack they decide upon. Companies are faced with two choices:

1. Use a virtualization-aware operating system or run on a “highly optimized for virtualization layer” with no standard operating system in the mix at the host layer.
2. Run on a “vanilla” unmodified operating system like Microsoft Windows XP or Red Hat Enterprise Linux where the virtualization layers are built as applications and drivers on top of this standard operating system.

Based on which choice organizations make, the levels of performance would differ as would the feature sets and the level of administrative complexity. It is important to make this choice carefully, taking into account the staff skill sets. For example, if your team’s security skills are primarily around Windows administration, then it might not be prudent to select a Linux-based hypervisor technology without first augmenting the skill set.

Using a virtualization-aware operating system could also bring in an entirely new set of services. New patching policies and processes would need to be created. This selection also influences the features that are available to users of the virtual machine, such as sharing of the clipboard. Hence, one version might be more appropriate to a locked-down environment than others, especially in their default configuration. Fortunately, most of the technologies available do support further lock down and could be adapted in most cases.

Another important configuration management issue is that most of the virtualization vendors support features that might unintentionally present security risks in your environment. These could include features such as clipboard sharing, drag-and-drop support, file sharing between the host and guest, and APIs for programmatic access. Each of these features would break the isolation between the host and a guest, or potentially between guests, in a controlled manner. It is, therefore, important to fully understand the implications of these features before turning them on and off. While there are usability benefits from these features, the security tradeoffs must also be considered, especially if they are enabled by default. It is also important to consider how to lock down these features so that end users cannot enable them if corporate policy dictates disabling them.

One final configuration management issue is the level of trust placed on the host with regards to being able to access the guest. As you would expect, a user with physical and logon access to the host would have significant access to the guest and could turn the guest off by powering off the host. Organizations need to address the following:

- What access rights should low privilege users with access on host systems have compared to those assessing virtual machines?
- Should an administrator on the host have any access to the guest?
- What users would be allowed access to the host?

To resolve these, an organization may need additional solutions over and above the virtualization layer to lock down the guest and possibly the host. These could include:

- Enforcing network access control rules on the host and guest
- Restricting what networks the host and guest can join and which resources they can access

It also means guest operating systems should enforce many of the same information security policies we almost take for granted these days for instance password complexity rules and account lockout policies. Additionally, many of the host technologies available also come with some level of support for host-based intrusion detection, at least in the form of a firewall. Organizations might choose to augment these existing security services.

Data Protection in Storage and Transit

This security framework category can be split into two parts.

1. Just as in the physical world, with virtual systems there are concerns about data flowing from within the guest and across the network and about data stored within the guest. For example, consider a guest running a database server storing credit card information. How are credit card numbers stored in the database and how are they transmitted over the network? These concerns are no different from the same database workload running on a physical machine. The technological solutions in use today are relevant in this environment. These include hashing, encryption, and protocols such as the Secure Socket Layer (SSL). Virtualization solutions may require you to enable more network services or software components than expected. These services and components will also need protection within your infrastructure. For example, some virtual machine management products are potentially web enabled or provide remote connectivity options for accessing the guest or host. These are not unique issues but need to be understood properly so that solutions are configured appropriately to maintain data protection.
2. The second part of this category is unique to virtualization. Virtual disks are typically stored as files on the host and it is important to consider the security of the virtual disk files especially if these are deployed on mobile computers or in untrusted physical environments. Most virtual disk formats store data in plain text giving an attacker who has access to these files effectively has the same level of access as anyone with a hard drive from one of your corporate servers or laptops. In addition to the information disclosure threat there is another risk—that of injecting malware, such as a keystroke logger, into the virtual disks as well as into the contents of RAM and the BIOS information for the guest. Organizations might want to consider strong access controls (discussed later) and encryption of these sensitive files on the host. This can be done using add-ons available from the virtualization vendors themselves or using host physical disk encryption technologies that encrypt the partitions on which the virtual machine artifacts are stored. Which of these is appropriate depends on who you are

trying to defend the organization from—the external attacker who steals the virtual machine files or a legitimate user on the same physical host.

Virtualization can also add new channels of network traffic that could come under attack. For example, when machines are cloned or migrated, we would see traffic flowing over the wire. If machines are converted from actual physical servers, even more traffic would flow over the wire. All of this traffic would need to be protected if it flows over public networks. In addition, all of the typical network injection attacks could allow an attacker to influence the guest being created. Therefore, it is important to understand which protocols used by the virtualization vendors are secure, which are not and what networks these protocols use. In some cases, the data protection may not be turned on by default and it is important to understand the implications of this.

Some additional data protection issues are not markedly different from other applications and products. For example, most of the products in this space come with support for SSL but ship with default self-signed certificates. These must be replaced by SSL certificates issued by trusted third parties to prevent “man in the middle” attacks against the users and the system. This must be done before the system is pushed into production. Finally, it is also important to consider all of the key management issues that are essential to the security of any cryptographic system including how keys are generated, whether they have sufficient entropy, whether they are changed at regular intervals, where these keys are stored, whether access to the keys is controlled appropriately, and whether they exchanged securely.

Authentication and Authorization

Nothing changes significantly from the physical world when it comes to authentication; best practices continue to be relevant. However, virtualization products do add new components to the mix, and there are some additional considerations even though the basic security threats do not change. For example, an issue already briefly discussed above is account provisioning on the host. This should be handled carefully, since providing a user with access to the host can potentially give very powerful privileges to the guest. It is a good idea to link authentication to the host to existing identity management solutions. This can include integrating with Active Directory or another corporate directory solution. Organizations would be best served by using the capabilities of existing technologies to bring virtualization into the current infrastructure.

A secondary issue is the use of service accounts by components in the virtualization stack. It is highly recommended that these service accounts have strong passwords that are changed frequently to avoid compromise. In general, organizations should attempt to integrate these systems into existing user provisioning and de-provisioning processes and technologies so that concerns such as leftover or orphan accounts are addressed.

At a very basic level, a virtualized environment adds new sets of resources for which access must be controlled. As discussed in other sections of this paper, weak access controls on these resources can severely undermine the security of organizations' virtualization efforts as more and more resources get virtualized and offer access to other resources through inherent trust relationships set up by administrators. It is vital to make correct authorization decisions and access control lists should be defined at the start of any implementation to avoid security breakdowns.

It might also be necessary to consider an entire new set of operations and the corresponding functionality that users are allowed to perform in a virtualized environment. This includes sensitive operations such as the ability to power-on or power-off a virtual machine, create a copy of it, issue commands from the host to execute within the guest, and create and delete virtual machines and virtual disks. Organizations need to determine who will be responsible for these tasks and perhaps create new roles, such as virtual machine administrators, virtual machine authors, virtual machine users, and other similar designations.

Logging and Auditing

It is important to log and maintain a strong audit trail of all activities occurring in a virtual environment. This can be used to determine who powered off the web server virtual machine or who created a copy of the database server virtual machine. Most of the virtualization solutions currently available do provide some support for such audit trails. However, these should be augmented to integrate with existing event notification systems in use within your environment. It is important to treat the virtual machines just like physical hardware that would provide SNMP traps or WMI notifications when they detect an error or other unexpected conditions. These notifications, in turn, could be delivered as emails or pager beeps through the common event notification systems available. Both guest and host events should be included in the notification process. As previously mentioned, one possible risk is that a physical hardware fault could take down multiple virtual machines. It is therefore vital to know about such problems as early as possible which is best done by monitoring the host machine in addition to the guest.

Logs should be monitored to maintain an operational, efficient, and secure network. Any logging capability is only useful if the logs are actually monitored. It is essential that administrative staff monitor the system for alerts and respond to them appropriately. This ties into the training and awareness requirements for operational staff. Administrators responding to alerts must understand at a very deep level their options, the impact of each option, and why it's critical to choose the right option for the business. In many ways, virtualization only increases the number of options available to administrators as compared to a pure physical infrastructure. However, while more options do provide greater flexibility, they also add to complexity and create a higher probability of making the wrong decision.

From an audit trail perspective, it is critical that log files have proper access controls in place to prevent unauthorized tampering. Logs may need to be retained and archived based on your compliance requirements and environment. Logs from virtualization systems should be treated like those from operating systems on physical machines, perhaps with even more caution, since they can contain data about multiple virtual machines.

The Challenges Ahead

This paper only scratches the surface as we know it today. As virtualization technology becomes more and more deeply entrenched in IT environments across the globe, new challenges are likely to manifest themselves and new problems will come to light. This is natural with any new technology, particularly one that is fundamentally as revolutionary as virtualization. Let's take a look at other considerations when deploying virtual systems now or in the future.

Tools

Just as the invention of the PC spawned an entire industry for applications that could run on them, virtualization technology will likely trigger greater innovation as products leverage the many benefits of being virtualization-aware. The risk is that it may quickly become the Wild West, and in the rush to get to market, bad, buggy, or insecure software gets delivered. Before you deploy such tools and applications in your environment, it is vital that you do a thorough review of these products to determine the effect they have on your security posture. This could include performing threat modeling, security code reviews, or other forms of security testing. It is also important that your existing tools quickly adapt to some of the differences inherent in virtual machines. For instance, virtual networks could potentially be an unknown quantity for tools that scan networks for vulnerabilities. It is likely that we will soon need intrusion detection or general network monitoring software that is optimized for purely virtual networks.

Roles and Responsibilities

For this new technology it may be necessary to create new roles and responsibilities to deal with new paradigms that are likely to emerge. It will be important to invest some time to understand the different privilege levels for administrators, operational staff, users, and other groups that leverage virtualization technology. Enforcing these privileges using tools, process, human workflows or some combination of all of these will be necessary. As you would expect, this list of privileges will only grow as new functionality is added to the underlying virtualization technologies. As these features and privileges increase, the ability to provide accountability within the organization should also increase.

Performance

Traditionally, the desire for performance will or can be in conflict with security requirements. It will be interesting to see how virtualization performance adds to this mix. Would vendors be willing to skip critical security checks to eliminate virtualization overhead? Or can the security tools, especially those that focus on network traffic, deal with packets that do not flow over conventional channels but are transmitted using a shared memory section and similar techniques? As virtualization technology improves and optimizations become more robust, security technology will have to keep up to continue protecting customers. Of course, the other aspect of this is that resource utilization by security tools is likely to become an even bigger concern with regards to performance. As virtual machines strive to share underlying physical resources, it will be vital that security tools become virtualization-aware and constrain their resource utilization when running on a virtual machine.

Interoperability

One potential hazard is that all the major virtualization vendors are only now beginning to standardize on disk formats, virtual network implementations, and other interoperability measures. This means that companies could quickly end up with incompatible solutions as virtual machine technologies and the virtual machines themselves proliferate. While every effort should be made to control this, organizations should also be prepared for this eventuality. With that in mind, selection of tools and resources, hiring of skilled personnel, and setup of environments should take this into account. Further, as “virtualization only” tools begin to hit the market, it is important to consider how these will operate with your legacy physical infrastructure. Ideally, most organizations would select tools that can span both worlds and provide a unified experience. This is most important in the area of security management infrastructure, which is likely to demand integration immediately.

Summary

In many ways virtualization represents a pivotal change in a technology world that is already evolving rapidly. As companies and users begin to leverage all of the advantages and benefits this technology has to offer, it is quite likely that security might not get the attention it deserves. This paper attempts to draw attention to the components of business security risk that are impacted by adoption of this technology. We now have the unique opportunity to consider security from day one rather than as an afterthought. This means that when you acquire security and virtualization products, you need to consider how they impact one another. Companies should consider the gaps in their security posture that virtualization will expose and review their security architectures to implement strategies covering people, process, and technology that bridge these gaps. It is important to implement new security policies before deploying virtualization on a large scale. Fortunately, none of the problems and areas of concern described above are unsolvable. It is just a matter of preparing yourself in advance for the challenges that this revolution will bring as well as the potential hiccups that will manifest themselves as virtualization becomes entrenched in your environment.

About the Authors

William (Bill) Hau, Vice President, Foundstone Professional Services

As vice president, Bill is responsible for running and growing the Foundstone Professional Services consulting business. William also has extensive experience in Information Security across all industry sectors from Managing Security for Global organizations through to performing technical assessments in the US and Europe. Bill holds the standard information security professional certifications as well as a MSC in Information Security. He has presented to many audiences on the matter of Information Security and proactively contributed to the Open Web Application Security Project (OWASP) project. This included contribution to whitepapers, helping to organize the successful 1st Conference in NY in 2004 and the follow-up conference in London in 2005.

Rudolph Araujo, Senior Principal Consultant, Foundstone Professional Services

Rudolph is responsible for creating and delivering the threat modeling and security code review service lines. He is also responsible for content creation and training delivery for Foundstone's Building Secure Software and Writing Secure Code – ASP.NET and C++ classes. Rudolph's code review experience is varied and includes among others custom operating system kernels, hardware virtualization layers, device drivers and user-mode standalone, client / server and web applications.

About Foundstone Professional Services

Foundstone® Professional Services, a division of McAfee. Inc., offers expert services and education to help organizations continuously and measurably protect their most important assets from the most critical threats. Through a strategic approach to security, Foundstone identifies and implements the right balance of technology, people, and process to manage digital risk and leverage security investments more effectively. The company's professional services team consists of recognized security experts and authors with broad security experience with multinational corporations, the public sector, and the US military.