

▶ Virtual Desktop Threats

Tech Tip
by Philip Cox

© Copyright 2010 SystemExperts Corporation. All rights reserved.

► Virtual Desktop Threats

Introduction

This Tech Tip is focused on identifying the most common security issues that solution providers run into when deploying virtual desktops for customers and some practical ways to solve them.

What are the threats?

To begin with, I see three security areas that really stand out as needing to be addressed when virtualizing the desktop. They deal primarily with the loss of the physical boundary and the fact that everything passes over the network. Those three critical areas are:

- **Authentication:** In a traditional desktop environment, a username with a reusable, sufficiently strong password is considered adequate for authentication a user onto that system. There was an unstated assumption of physical proximity and control of the system being logged into. In a virtualized environment this additional mitigating control is no longer present, so the authentication must be bolstered in other ways.
- **Transport protection:** The loss of the physical system, and the ability to store and process information that would never be seen outside the system boundary places increased responsibility for protecting that information as it transits the network.
- **Data protection (specifically confidentiality, integrity, and non-repudiation):** In a physical system, I can ensure that no one else has access to the information on my system. Think of it in terms of a chain-of-custody. If I unplug the network and lock the system in a safe when I am not physically next to it, I can feel very comfortable that any information on that system is mine, and conversely anyone would have an easier time proving that the information on the system had to be put there by me and not a malicious user. This is not the case in many Virtual Desktop scenarios (i.e., hypervisor administrators will have access to the “system” even when it is powered off and disconnected from the network).

These are important in many aspects, and are critical not only to real security, but in meeting compliance and regulatory requirements as well.

What are the best solutions?

The answer as always really depends on the deployment. Are you using VMWare? XenDesktop? Microsoft RDP into a virtual machine? Individual blades or multiple VMs on a system? All of these will have specific implementation differences, but there are some general “things to do” that should work regardless of the specific implementation you decide to go with.

Authentication

First, you need to determine if the connections are over a trusted internal network or if ANY part of the desktop traffic passes over an untrusted network. For our purposes, all public networks are untrusted, and some private networks may be untrusted. Once you determine the trust level, then apply the following algorithm: If trusted, integrate (securely) with their current internal authentication mechanism. You should also make sure that this internal authentication mechanism has appropriate strength as well (if not, recommend they change it). If you determine traffic passes over an untrusted network, then help them implement a 2-factor authentication service.

Transport

This is pretty easy to mitigate. Just ensure that the solution is using transport level encryption. Typically Secure Sockets Layer (SSL) or Transport Layer Security (TLS) are the best solutions. Be wary of “home grown” encryption solutions. Use publicly vetted crypto, it is the best and safest (from liability standpoint) option for you to use. If you happen to be deploying a solution based on shared keys, make sure that the key management and rotation policy is appropriate (i.e., changing keys every 2 years is probably not adequate). One last piece of advice, use transport layer protection regardless of whether you trust the network or not.

▶ Virtual Desktop Threats

There are some issues with Intrusion Detection and troubleshooting when you do this, but you can do IDS and troubleshoot on the host, and the benefit of the secured connection is worth the inconvenience.

Data Protection

Provide a mechanism that will allow the user to be assured of information protection. I am thinking in terms of giving them a level of assurance that the data they leave on their desktop is only accessed by them. An example of this would be using something like PGPdisk, where the user's information is encrypted and after a user logs in, he would have to enter a password to open the encrypted "disk".

Anything based on the user having to supply something (smartcard, password, key on a USB, etc.) to access the data would give them a level of assurance that does not typically exist in the virtual desktop deployments I see. This not only provides them confidence of the protection of their data, but also gives them accountability for it as well.

In closing

With the loss of the physical system, there are steps we must take to mitigate the added risk. We have talked about the three things I see providers being able to help with:

- ▶ Strong authentication
- ▶ Transport level security
- ▶ Data protection

Help your clients with these, and you will have put them in a good position to be secure and compliant, as well as done your job well.

Author Information

Philip Cox
CISSP, CISM, PCI QSA, NSA IAM/IEM
Principle Consultant
SystemExperts Corporation
Email: phil.cox@systemexperts.com
Phone: (530) 887-9251