Document Number: DSP-IS0403

Date: 2012-03-23

Version: 1.0.0

Application and Desktop Virtualization
A White Paper from the Virtualization Protection Profile Incubator

Document Type: White Paper

Document Status: Informational

Document Language: en-US

Implementation of certain elements of this standard or proposed standard may be subject to third party patent rights, including provisional patent rights (herein "patent rights"). DMTF makes no representations to users of the standard as to the existence of such rights, and is not responsible to recognize, disclose, or identify any or all such third party patent right, owners or claimants, nor for any incomplete or inaccurate identification or disclosure of such rights, owners or claimants. DMTF shall have no liability to any party, in any manner or circumstance, under any legal theory whatsoever, for failure to recognize, disclose, or identify any such third party patent rights, or for such party’s reliance on the standard or incorporation thereof in its product, protocols or testing procedures. DMTF shall have no liability to any party implementing such standard, whether such implementation is foreseeable or not, nor to any patent owner or claimant, and shall have no liability or responsibility for costs or losses incurred if a standard is withdrawn or modified after publication, and shall be indemnified and held harmless by any party implementing the standard from any and all claims of infringement by a patent owner for such implementations.

For information about patents held by third-parties which have notified the DMTF that, in their opinion, such patent may relate to or impact implementations of DMTF standards, visit http://www.dmtf.org/about/policies/disclosures.php.

CONTENTS

Foreword ... 4
1 Executive summary ... 5
2 Introduction ... 5
3 Business scenarios ... 7
3.1 Healthcare (Assisted living facility/Nursing home) ... 7
3.1.1 Overview ... 7
3.1.2 Security issues ... 8
3.1.3 External financial auditor ... 8
3.1.4 Physician ... 8
3.1.5 Medical transcriber ... 9
3.1.6 Administrative assistant ... 9
3.1.7 HR services ... 9
3.1.8 Security auditor ... 10
3.1.9 Security guard ... 10
3.1.10 Burglar ... 10
3.1.11 Summary ... 10
3.2 Financial ... 10
3.3 Energy ... 11
3.4 Government ... 11
4 Reference system ... 12
4.1 Organizational roles ... 12
4.2 Technical considerations ... 12
5 Conclusion ... 13
Bibliography ... 14

Figures

Figure 1 - Display virtualization ... 5
Figure 2 - Display virtualization with server virtualization ... 7
Figure 3 - Organizational roles ... 12

Foreword

This white paper was prepared by the Virtualization Protection Profile Incubator Working Group. It describes use cases for Application and Desktop virtualization. These use cases are different from those in typical server virtualization.

The goal of the Virtualization Protection Profile Incubator Working Group is to define Common Criteria Protection Profiles [CC-1] for virtualization. The Common Criteria allow product security to be independently certified, and for these certifications to be recognized worldwide. The incubator leverages existing bodies of work, along with the experiences of members and customers.

DMTF is a not-for-profit association of industry members dedicated to promoting enterprise and systems management and interoperability. For information about the DMTF, see http://www.dmtf.org.

Acknowledgments

The DMTF acknowledges the following individuals for their contributions to this document:

- Eric Betts, VMWare Inc.
- Tim Gaylor, Citrix Systems Inc.
- Phyllis Lee, US Department of Defense
- Chris Mayers, Citrix Systems Inc.
- Kurt Roemer, Citrix Systems Inc.
- Jim Wiese, VMWare Inc.

Application and Desktop Virtualization

1 Executive summary

In today's workplace, users employ a range of different devices to access applications and data - not just desktop computers, but also tablets, smartphones, and other devices. Some organizations permit users to access corporate applications and data from their own devices, which are not under direct corporate control.

Many organizations are concerned about security implications of data proliferation in this environment; for example, users may copy data around, to simplify their work.

One approach that satisfies the user need while tackling the security challenge is display virtualization (also known as presentation virtualization); applications execute remotely within a virtual desktop in the datacenter, and only display images that are sent to the client device. With this approach, data never leaves the datacenter.

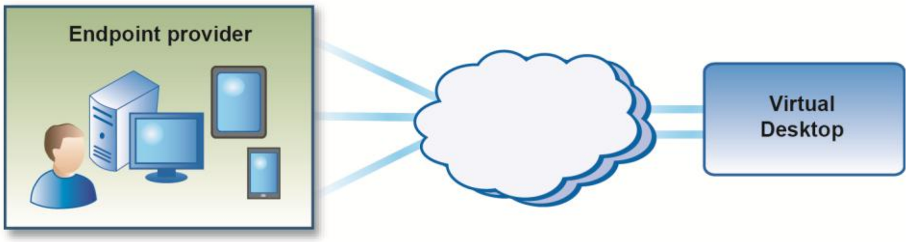

Figure 1 - Display virtualization

Adopters of this approach ask questions such as the following:

- How does display virtualization relate to other types of virtualization?
- How does display virtualization affect users and administrators?
- What other security benefits exist?
- Which kinds of application is display virtualization appropriate for, and which less so?
- What are the deployment considerations?

2 Introduction

Display virtualization provides access from a client device to applications, even though the application itself is not installed on the device. It operates by capturing the keyboard and mouse input and transmitting via a secure connection to a datacenter, where the application is installed. The display from the application is then sent back over the secure connection to the client device, where it is shown on the screen. The client device can be a desktop computer, a terminal, or a mobile device such as a smartphone or tablet.

Display virtualization has benefits beyond security. It simplifies desktop and application management; makes it easier to provide access from the latest mobile devices; and allows the workforce to reach their desktops and applications from any location, subject to policy.

Display virtualization is a flexible technology. It can be used for:

- single applications (both general office applications such as spreadsheets, or business-specific applications)
- multiple applications
- entire desktops, within which applications and data can be accessed

In one common usage, display virtualization delivers a single business-critical application, possibly for a task worker who uses that application throughout the day; for example, a helpdesk specialist.

In another usage, display virtualization delivers multiple applications. A user can interact with these applications simultaneously, possibly transferring information between them.

In yet another usage, display virtualization delivers a full (virtual) desktop. The user can launch applications from within that desktop. This usage is typical of a knowledge worker.

In practice, display virtualization technology handles more than just the display, keyboard, and mouse. It can enable:

- use of a printer connected to the client device
- transfer of files to and from the client device
- audio output, and audio input (from a microphone or headset)
- webcams, and other peripherals

Use cases later in this document illustrate these capabilities.

Mobile devices have different security characteristics than desktop devices:

- Mobile devices are more likely to be lost or stolen.
- Security software may be unavailable for particular mobile devices.
- The standard configuration of mobile devices may be insecure.
- Support policies for mobile devices may not match enterprise needs.
- It is impractical to secure a mobile device by physical means.
- It may be difficult to apply enterprise controls to mobile devices.

For example:

- According to a regular survey, more than 50000 mobile phones are left in London taxis every 6 months. This pattern is reflected by a similar survey in New York [CR-1], and other surveys at US [CR-2] and UK airports [PO-1].
- Firewall, anti-virus, and anti-malware software may be unavailable for a smartphone.
- The smartphone may not prevent inappropriate transfer from a business application to a non-business app; cut-and-paste via e-mail access is a likely example of this.
- Application software may only be distributed via a consumer app store, without enterprise security controls.
- Application software might be upgradable, but not downgradable if problems are found.
- A consumer smartphone might receive security updates only irregularly, and for no longer than 18 months from purchase [GO-1]; and, in any case, there is little that the enterprise can do to influence this policy – it is determined by the device vendor.

Mobile devices therefore generally pose a different set of risks. However, when used with display virtualization, the extra risk is smaller, because data is not stored on the mobile device.

On mobile devices, display virtualization operates in a similar way to other devices. Notable differences are:

- touch or stylus input is used instead of a physical keyboard
- the small screen size of smartphones can limit the practical use of some applications

Additionally, display virtualization can be used in conjunction with server virtualization:

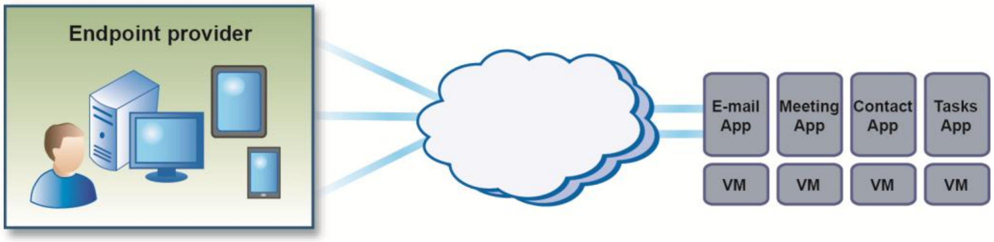

Figure 2 - Display virtualization with server virtualization

(Note that client virtualization, where different applications run in separate virtual machines, lies outside the scope of this document.)

The following sections of this document describe:

- business scenarios, with typical use cases that illustrate the potential security risks in everyday user behaviour;
- a typical deployment of application, desktop, and virtualization
- how this deployment mitigates many of the security risks in those business scenarios

3 Business scenarios

This section describes scenarios that illustrate how security issues can arise during day-to-day operations, and how these issues can then be mitigated without excessive cost or effort. Scenarios include a variety of different user roles (sometimes called personas). A user role may be malicious; so, deliberate and accidental user actions are covered.

These scenarios are examples only; many more possibilities exist.

One scenario is described in detail: a healthcare environment (assisted living facility/nursing home).

Other scenarios are summarized, illustrating similarities and differences: these environments are financial, government, and energy.

3.1 Healthcare (Assisted living facility/Nursing home)

3.1.1 Overview

Full-time residents/patients occupy an assisted living facility (nursing home). They are supported by full-time employees, part-time employees, and visiting/part-time medical professionals. These medical professionals - typically contractors to the assisted living facility - may carry out treatments while visiting, and require access to patient records. These medical professionals may visit other assisted living facilities, and other healthcare sites. Occasionally, patients may be transported elsewhere for treatment, and may be attended by the same medical professionals, or by others. Medical professionals also require access to review patient records when the patient is not present; this might be when working from home, if this is permitted.

Additionally, administrative staff will require access to treatment data for accounting purposes.

External audit staff will require limited access to financial data; this access may be remote.

External professional service staff will fill the need for jobs at the facility.

A variety of equipment is used for data access, including:

- managed desktops
- unmanaged devices (laptops, desktops, and tablet devices), within and outside the facility

3.1.2 Security issues

This scenario shows diverse user roles, some of whom roam. These need access to different data. Some of this is sensitive (requiring confidentiality). Regulations about data access controls may vary, depending on local law.

Inadequate security can have a broad impact, both on the organizations and on individuals. Lack of regulatory compliance may mean the organization cannot bill insurers, or cannot accept payments; and, fines may be imposed. For individuals, failure of patient confidentiality may expose the person to anything from personal embarrassment to blackmail from deliberately stolen medical data.

Reported examples are:

- a fine for violations of the HIPAA Privacy Rule [HHS-1]
- a lawsuit for data breach attributed to a third party [CW-1]
- regulation forbidding the texting of orders [JC-1], [IHB-1]

3.1.3 External financial auditor

An external financial auditor is contracted by a healthcare insurer to audit the treatments of patients at the assisted living facility (nursing home).

The auditor visits the facility. The auditor connects their laptop to the wired network in an office at the facility. The auditor accesses the system containing the financial data for treatments, using an account and password reserved for auditors. The auditor inspects a sample of records. Financial data is visible, but not data regarding the treatments themselves. The auditor is not shown records relating to patients that are covered by other healthcare insurers. The auditor cannot modify any of the records.

The auditor inspects the financial data for a particular patient, and observes that an expensive treatment has been recommended and authorized. The auditor makes a note to confirm that the treatment has actually been carried out.

At the end of day, the auditor informs the system administrator that their use of the system is complete. The system administrator disables the audit account.

3.1.4 Physician

A physician treats patients at the assisted living facility (nursing home).

The physician visits the facility, bringing a tablet device with them. (This tablet device is solely for that physician's use.) The physician attends the first patient, and examines the patient record using the tablet device. Speaking with the patient, the physician updates the patient's notes. The physician decides to adjust the patient's treatment plan. Using a public Internet site, which contains information linked together from multiple sources, the physician displays some general information about the new treatment, and shows it to the patient. The physician discusses it with the patient, and updates the treatment plan.

The physician walks to the next patient, but is called to an emergency in another room. The physician abandons the tablet device. A nurse obtains emergency access to the patient's allergy record, and determines that the patient has no known allergies. The physician administers the emergency treatment. After ensuring the patient is stable, the physician retrieves the tablet device and updates the patient record.

The physician continues with the next patient.

3.1.5 Medical transcriber

A medical transcriber, working for an outsourced service, transcribes handwritten and voice recordings of patient notes.

The outsourced service supports many medical organizations. Medical transcribers change employers frequently.

The medical transcriber logs on in the morning, and selects the first patient recording to transcribe. The transcriber selects the audio recording and starts listening to and transcribing it. After a minute, there is a network glitch After the connection is reestablished, the transcriber completes the audio transcription, but misses a handwritten note. After the transcription is complete, the transcriber neglects to completely delete the patient recording from the system’s clipboard. The transcriber selects the next patient record, but mistakenly begins by transcribing the handwritten note.

Later, the transcriber tries to access a patient record of another transcriber and the patient record of a transcription that was completed previously. Neither action should be permitted.

3.1.6 Administrative assistant

An administrative assistant carries out various administrative tasks at the assisted living facility (nursing home). These tasks included keeping of time records for other staff, maintaining the calendar of supervisors, booking meeting rooms, ordering meeting room services (e.g. lunch), taking and keeping of meeting minutes. Other tasks include tracking patient room usage, and which patients are present. The assistant is employed by a professional services firm. The assistant requires very limited access to any patient information, for example food allergies. This assistant also needs access to an external time recording system for the professional services firm.

The administrative assistant is organizing a set of meetings for the next few weeks. One of these involves a medical specialist for an unusual condition likely to be of interest to the public. The assistant organizes the meeting, and notes that a particular patient is mentioned. The administrator attempts to access that patient's medical record.

3.1.7 HR services

An HR specialist is responsible for recruiting a replacement part-time physician. The HR specialist is employed by a professional services firm.

The HR specialist logs on the system, and reviews five resumes (CVs). From these, the specialist selects two. The specialist then logs on to a separate Internet-based system to check that the qualifications and status of the physicians are appropriate. For one of these two, resume information is incomplete. The specialist routes the resume for an additional check. For the other, the specialist schedules an interview.

The specialist then examines the employee information for a part-time physician that is leaving, and confirms that the final payment is being made. The specialist then checks whether the part-time physician has any uncompleted treatments.

3.1.8 Security auditor

A security auditor is responsible for investigating potential security breaches, deliberate or accidental. This includes specific incidents, their cause, and whether the system was in compliance at the time.

An external financial auditor (see 3.1.3 above) is investigating a potential fraud. Evidence needs to be gathered, to determine who might have been involved, and at which location. The security auditor inspects the security log. This shows the names of the user accounts who logged on successfully, and when; and also the location of the logon. Unsuccessful logons are also recorded. There is a record of the system configuration at the time of the incident, and also changes to it since then.

3.1.9 Security guard

A security guard is responsible for securing physical access to the site, its buildings, rooms, and its resources. The security guard does not need access to any computer systems.

While unobserved, the security guard approaches a terminal, which is already logged in. The security guard selects the medical records system, and is prompted for credentials. The security guard dismisses the prompt, and walks away.

3.1.10 Burglar

A burglar enters the building during daylight. The security guard does not observe this. Trying a door, the burglar discovers an unattended laptop and smartphone. Stuffing them in a bag, the burglar leaves. The security guard does not observe this. Knowing that these devices can contain valuable medical data, the burglar examines the laptop. No data is visible. The burglar also examines the smartphone. No data is visible. The burglar sells the devices on an auction site. The purchasers do not discover any data.

3.1.11 Summary

In the descriptions above, the security risks are addressed, principally by:

- not storing data on the device (by virtue of display virtualization)
- systematically checking that users are permitted access (simplified by display virtualization)
- systematically recording access attempts by users (simplified by display virtualization)

3.2 Financial

Financial sector organizations have many regulatory requirements to satisfy (possibly in more than one jurisdiction); they also have intellectual property to protect. These requirements may entail separation of duties, and also specific data retention and storage rules. Desktop and application virtualization can simplify meeting these requirements. Specific additional needs for financial institutions may include:

- Application-specific audit logs: recording which users have used particularly sensitive applications
- User authentication: two-factor user authentication, and also subsequent authentication when a threshold is triggered
- Device authentication: device authentication by client certificate
- Mobile devices: Only limited access may be permitted from unmanaged devices (for example, specific non-sensitive applications)

3.3 Energy

Desktop and application virtualization usage within the energy sector provides remote access, isolation, and support activities for aging technologies. Many energy-related systems are not immediately accessible and must therefore be accessed remotely, either for centralized access to distributed interfaces, remote support, or for physical safety. Isolation is required to keep sensitive systems, sensors, and information away from public networks, and to provide an airgap for accessing critical infrastructure. Many systems and applications supporting the energy sector make use of obsolete technologies and security mechanisms that must be effectively bridged to modern infrastructure.

Examples of energy sector-specific usage include:

- SCADA system support, access and monitoring
- embedded systems in power generation and distribution
- SmartMeter and other grid-attached premise power infrastructure
- mobile device access and interface with energy systems, including mobile device management (MDM) requirements for field-based mobile technologies

3.4 Government

As a regulated sector, Government will benefit from the security that display virtualization offers. Government typically has additional specific needs beyond those highlighted in the healthcare example. Those needs depend on national regulation and the sensitivity of data, but often involve:

- Certified products: products need to be independently tested for security before use
- Cryptography: only Government-approved encryption can be used
- User authentication: two-factor user authentication with Common Access Card (CAC)/PIN, plus username/password
- Device authentication: device authentication by client certificate
- Monitoring: detailed logs of access need to be kept
- Secure communications: the mobile platform should provide two independent layers of secure communication protocols (e.g. two independent VPNs)
- Mobile devices: only particular types of mobile devices may be permitted. Unmanaged devices may not be permitted. Only Government-approved apps may be downloaded
- Local device encryption: any data at rest must be encrypted
- Tamper-evident configuration: attempts to tamper with the configuration of the device must be detected

This means that display virtualization must be correctly deployed for Government use.

4 Reference system

4.1 Organizational roles

A system supporting Application and Desktop Virtualization may involve more than one organization, with corresponding responsibilities (including security responsibilities). This document identifies three organizational roles:

- Endpoint provider – enables access to applications and desktops
- Application provider – provides and supports virtualized applications
- Desktop provider – provides and supports virtualized desktop

These appear as follows:

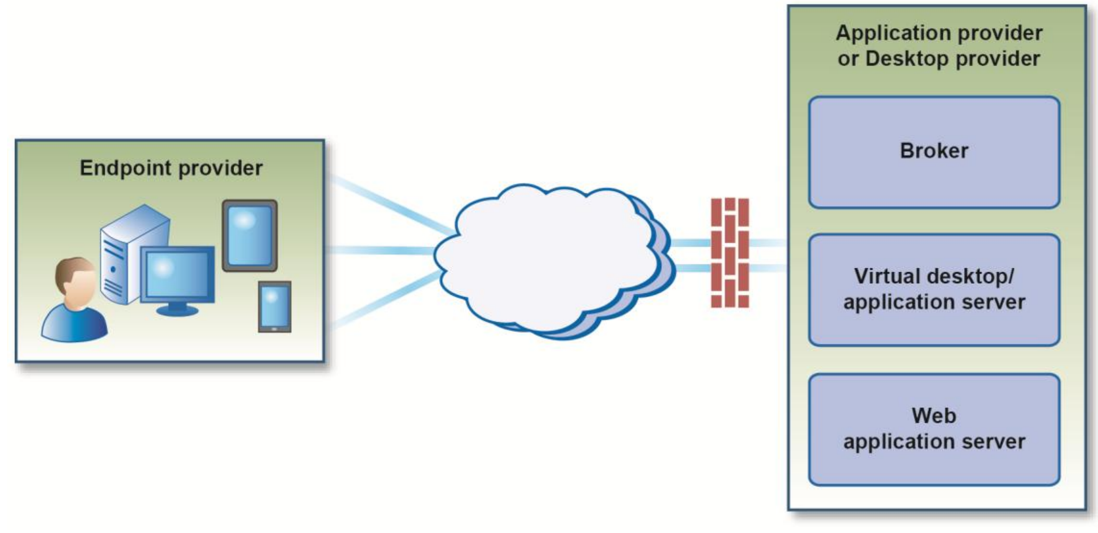
Endpoint provider
Application provider or Desktop provider
Broker
Virtual desktop/ application server
Web application server

Figure 3 - Organizational roles

The role of the endpoint provider depends on whether devices are managed or unmanaged (or possibly either), and also the device type. The endpoint provider may be responsible for purchasing, configuring, administering, and monitoring the device (including the software on it). Even if the device is user-supplied, the endpoint provider will have responsibility for providing the display virtualization software on the device. As can be seen for the scenarios described earlier, different customers will scope the job of the endpoint provider depending on the nature of their business.

The role of the desktop provider will include helpdesk for the desktop. It will also include application provisioning for applications delivered via the desktop.

The role of the application provider is similar to the desktop provider, but for applications only.

4.2 Technical considerations

The organizational roles described above require technical interfaces for communications, including protocols. These may be open standards or proprietary. Particularly important are:

- display virtualization protocols, for remote access
- configuration protocols, for both endpoint and application/desktop

- monitoring protocols, for logging of events and intrusion detection
- data encapsulation protocols, for secure communications
- authentication and authorization protocols, for access control

5 Conclusion

This white paper has used different scenarios and use cases to describe the security requirements for Application and Desktop Virtualization, across a range of customer types. It has explained how display virtualization relates to other types of virtualization, and the inherent security benefits of display virtualization. It has also explained how mobile devices affect overall system security, and how display virtualization copes with mobile devices.

Future work will refine these security requirements, allowing products and services to be independently assessed and tested with respect to these requirements.

Bibliography

[AJC-1] *Ambulances turned away as computer virus infects Gwinnett Medical Center computers*
http://www.ajc.com/news/gwinnett/ambulances-turned-away-as-1255750.html

[CC-1] *Common Criteria*
http://www.commoncriteriaportal.org/

[CR-1] *Thanksgiving Shopping Period Worst Time for Leaving your Mobile Devices in the Back of Cabs - Warn NY Cab Drivers*
http://devweb.credant.com/news-a-events/press-releases/218-leaving-your-mobile-devices-in-the-back-of-cabs.html

[CR-2] *CREDANT Survey Finds Consumers Left Thousands of Laptops and Smartphones at Airports Across the United States*
http://www.credant.com/news-a-events/press-releases/238-credant-survey-finds-consumers-left-thousands-of-laptops-and-smart-phones-at-airports-across-the-united-states.html

[CW-1] *Stanford Hospital blames contractor for data breach*
http://www.computerworld.com/s/article/9220626/Stanford_Hospital_blames_contractor_for_data_breach?taxonomyId=17

[GO-1] *Android Market For Developers*
http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en//events/io/2011/static/presofiles/android_market_for_developers.pdf

[HHS-1] *HHS imposes a $4.3 million civil money penalty for violations of the HIPAA Privacy Rule*
http://www.hhs.gov/news/press/2011pres/02/20110222a.html

[IHB-1] *Joint Commission: Text Messages Should Not Be Used in Patient Orders*
http://www.ihealthbeat.org/articles/2011/11/21/joint-commission-text-messages-should-not-be-used-in-patient-orders.aspx

[JC-1] *Is it acceptable for physicians and licensed independent practitioners (and other practitioners allowed to write orders) to text orders for patients to the hospital or other healthcare setting?*
http://www.jointcommission.org/standards_information/jcfaqdetails.aspx?StandardsFaqId=401&ProgramId=1

[PO-1] *Airport Insecurity: The Case of Lost Laptops*
http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/LostLaptopsDell%20EMEA%20Final%208.pdf