Security Considerations for Digital Signage Technology Selection and Implementation

An Insight by **Real Digital Media**

Introduction

Digital signage networks have witnessed rapid growth across multiple industries the past few years. Complex projects that require a number of disciplines, these networks task marketers with understanding a number of expert domains. Most notable among these is security. What questions need to be asked? How do the architectural designs of vendor platforms mitigate, eliminate or actually increase security risks?

This insight outlines the core components of a digital signage network and the vast majority of security questions marketers should be aware of as they determine the security risks and requirements for a digital signage project.

Digital Signage Platforms

In simple terms, the standard architecture of a digital signage platform involves centralized management software sending digital media files and playout instructions to remote media players. While some vendors employ a managed, Software as a Service (SaaS) architecture, others require their software installation on-premise. Likewise, some vendors use appliance-based systems, while others employ PC-based digital media devices. These architectural differences have an impact on the security questions required for a digital signage implementation:

- Does your organization have the physical security necessary to prevent intrusion for an on-premise installation? What about the host site?
- What is the media player-server communication protocol? Does it support encrypted transport?
- What is the operating system on the centralized server? On the media players?
- Is the management software web-based or client-side? How does the software manage user access?

These are just a few of the security questions that need to be addressed when undertaking a digital signage project. Knowing your digital signage platform specifications will help answer these questions. Whichever architecture you choose, the core security considerations of any digital signage implementation include:

- Physical
- Device
- Network
- Software
- Operational

Security Considerations

Physical Security

Physical security is frequently the most overlooked element in a security plan. Institutions spend millions on firewalls and intrusion detection systems, but often fail to implement physical safeguards to prevent unwanted access or information technology assets from simply being uprooted and carried out the door.

Physical security describes any measures that prevent or deter intruders from accessing a facility, resource or information stored on physical or digital media. It can be as simple as a locked door or as elaborate as biometric authentication. Whether you are deciding on a SaaS or on-premise implementation for your digital signage network, physical security parameters need to be defined, assessed and implemented. In either case, there are two physical security profiles that need to be addressed for your digital signage network:

- Physical security of facilities that house servers and digital media
- Physical security of locations where media players are installed

Physical Security of Facilities

Whether electing to install on-premise or use a managed solution provider, one has to determine the physical security of the facilities. For a managed solution provider, physical security is paramount. While many organizations may think they have airtight physical security, managed solution providers understand they require this level of physical security because their business simply depends on it.

Typically, many managed service providers implement the following to control facility access:

- Biometric readers (e.g., fingerprints)
- Card/PIN access (e.g., one-time pin)
- Combination lock cabinets
- 24x7x365 monitored video surveillance
- Motion/vibration detectors
- Verification and supervision of 3rd party access (e.g. maintenance and service personnel)

Does your organization employ these security measures? If not, what security measures are in place?

The next step in determining your on-premise or off-site facility security is whether or not a multi-level security access protocol has been implemented. For example:

- Level 1: Key-card and pin-pad combination to get access to the building
- Level 2: Biometric scan (e.g., fingerprints) to authorize entry
- Level 3: Secured cabinets requiring a PIN that only authorized personnel know

Most managed service providers will have their security profile well-defined and documented. If you elect to use a digital signage provider that leverages one of these facilities, ask who their provider is and request documentation on the facilities security measures and protocol. Then ask yourself if your organization can provide this same level of security if installed on-premise.

Physical Security of Locations

Once you have determined the physical security of the facility that will house the centralized servers and software, you need to determine the physical security of the locations that will house the media players.

To assess the physical vulnerabilities of your media player and display installations, determine the existence of the following security measures:

- Availability of security at point of entry at location
- Availability of wiring closet to secure media player behind lock and key
- Availability of enclosure or other physical lock-down device for media player connected at display in public area
- Availability of enclosure or mounting system to protect and secure display
- Awareness of who has physical access to these locations
- Placement of display to deter smash-and-grab tactics

Unlike the physical security at the centralized facility, which can be isolated, location-specific security may span thousands of sites. Some sites may have new construction with the latest security measures and amenities, while older sites may simply employ lock and key. Conducting a thorough site survey will go a long way in determining the security requirements for your locations across the network.

Device-Level Security

Assuming the physical security of the facilities managing the servers and locations housing the media players are sound, the next security item to consider is device-level security. This component is as critical as any other, as there is a potential to have hundreds if not thousands of devices involved in a network. Selecting a device that does not have airtight security puts your network at risk for theft, malicious attacks that may degrade your network, or even worse, allow a hacker to upload inappropriate content.

To determine the security of a media player device, consider the following aspects:

- Local Accessibility
- BIOS or Boot-ROM Accessibility
- Operating System

Local Accessibility

When selecting a media player, determine how easily the media player device can be accessed through handling. Can the case be easily taken apart? If so, how easy is it to remove the hard drive or compact flash media? A well designed case will have limited access, and even the use of an adhesive on the screws will deter the opportunistic thief.

Once media players have been selected and installed, you want to make sure they are safe from tampering or unauthorized access.

Physical installation should be safe from radio interference, and any CD/DVD drive access, power buttons and remote control (infrared) ports should be locked, secured and generally inaccessible. Any ports that are available should require authentication for use, and no automatic run settings should be activated when peripheral devices (e.g., keyboard or mouse) are connected. Therefore, it should not be possible to simply push content into the player by inserting a CD/DVD or USB card.

If the vendor you are researching grants local access to their media player device (typically for on-premise troubleshooting), ensure a keyboard-access-password system is in place that allows local access at a very granular level (i.e., restricting access to one physical player on one single day).

BIOS or Boot-ROM

The primary function of the BIOS or Boot-ROM on a media player is to identify, configure and initiate hardware components and prepare the machine so the operating system can load, execute, and assume control of the device. This process is chiefly known as the bootup sequence.

The BIOS controls such features as the boot order, which determines the sequence hard drives and other storage devices are considered for locating and launching the operating system. To ensure security during this process, only the secured storage devices should be configured in the sequence. For example, media player devices should not allow external USB ports to be considered as a boot media, as active USB ports will provide a path for access to the device itself and possibly the installation of unwanted or malicious software. Most BIOS or Boot-ROMs allow for the password protection of these settings.

Another consideration is the method in which a media player boots its operating system. A PC desktop will load parts of the operating system and system software as needed directly from storage media. While the system runs, changes are written back to the storage medium as necessary. When the system restarts, the changes are still present on the storage media and are reloaded at startup. This is how spyware and viruses survive system reboots, as they become part of the permanent configuration of the operating system.

An alternative, and more secure approach, is to load an image of the operating system into its memory and run. Changes made to the system are performed in memory and are lost on restart. This ensures that even if a virus or spyware were able to access a media player, a simple reboot would delete any additional software installed.

Questions about the BIOS that you want to ask your vendors include:

- Is the system password protected?
- Does it allow external drives to be locked out?
- Can updates be made remotely?
- Is the operating system loaded from an image or storage media?
- Is the deployed version up to date?

Operating System

An operating system is the software component of a computer system that is responsible for the management and coordination of activities and the sharing of the resources of the computer. The operating system (OS) acts as a host for application programs that run on the machine.

A well designed OS implementation will restrict or remove the launching of services that are not required. The implementation will be streamlined, evoking only those services required for the operation of digital signage media player device. The removal of these additional services offers security benefits such as:

- Lower memory utilization
- Smaller attack footprint (lower chance a vulnerability will be present in the software components)
- Ease of maintenance
- Fewer moving parts leading to fewer conflicts and bugs

Many times an embedded version of an operating system allows a vendor to build their environment upwards from a very small core. When working with traditional desktop systems, a vendor must spend a great deal of time and care to work downward to remove/uninstall/secure components. It is far more difficult and error prone to work downwards and thus vendors may choose not to be as thorough in their development efforts to streamline their systems.

When assessing media player devices, it is recommended no path exists to load 3rd party applications, spyware or viruses on the media player devices. Dedicated, optimized media player appliances are stripped down to satisfy one function, playing digital media. Solutions that simply take a computing device like a PC and install media player software may not have engineered the safeguards to prevent third party access and installation of unwelcome software.

Questions about the operating system that you want to ask your vendors include:

- What version of the operating system is running on the devices?
- What services and features have been locked down, removed, or simply not installed? Are only the essential elements running? Are all non-essential software components removed from the device?
- How are OS upgrades and patches managed?

Network Security

Network security is paramount to having a healthy and well-performing digital signage network, and includes firewalls and VPN considerations as well as the media player server communications protocol implemented by the vendor.

First and foremost, secure media player architecture should connect out, not in. What this means is that your media players cannot be reached by inbound signals – neither yours nor those from potential hackers. Having this protocol style means you have only one potential hack site to watch: the centralized enterprise server installed on-premise or hosted by a managed service provider. Watching one server site is much easier than watching hundreds or thousands of media players.

Below is a list of network functions that at minimum should be available in the digital signage platform you are reviewing:

- Media players should only speak to their host servers, or other authorized servers (e.g., Content Distribution Network or CDN, RSS sources)
- Media players should have a software firewall enabled as an extra layer of “just in case” security

- Media players should be installed behind a NAT device (simple off-the-shelf routers such as those from Linksys/D-Link/Netgear) provide a firewall between the media player device and the Internet. This makes it far more difficult for a remote attacker to gain access to the media player device
- Media players should use standard protocols like FTP and HTTP for data transfer. However, if encrypted HTTPS communication is available, it is recommended that all communications between media players and the central server are encrypted
- Media players should only support encrypted wireless networks which require authentication to access
- Media player control protocol should be simple, transparent and based on standards to allow customers with stateful protocol inspectors to perform QoS (Quality of Service) variation

Extra security measures you may want your digital signage vendor to support include:

- VPNs – Virtual Private Networks allow the reuse of public networks such as the Internet as if they were private. VPNs create tunnels through another network in which all traffic is encrypted and directed such that 3rd parties may not eavesdrop on the communication. VPNs typically exist in large corporate WANs that use public or semi-private communication channels. VPNs are superior to using a protocol such as HTTPS in that all traffic is encrypted in a VPN configuration. However, VPNs require significant investment in hardware, software, staff and management tools
- HTTPS - A standard and highly secure mode for bi-directional encryption of information
- Authentication and Identification – Protocols that allow for secure identification should be used when available. If not, the vendor's protocol should allow for some level of identification to ensure that the player is receiving trusted information from the servers it communicates with. This removes nearly all forms of "man in the middle" attacks
- Media players should be behind a NAT (Network Address Translation) firewall that only allows outbound connections to be established

Software Security

The user interface software of digital signage platforms are either web-based systems that leverage a browser to access and execute logic over the network at a hosted facility or client-side software where the logic and executions are conducted locally. Although it is unlikely a local virus would be smart enough to perform damage to a web-based, hosted application, both web-based and client-side approaches inherit the security risks associated with viruses and spyware that can attack a local machine. Anti-spyware and virus protection systems, therefore, are a must at the local level.

Assuming the local machine assessing the digital signage network is secure, the user software should have a robust personalization engine to create and enforce role based security and authentication. Each user that is created in the system should be able to create a unique password that is tested for strength during the creation process. This ensures appropriate security measures are taken at the user level.

Questions about the software security that you want to ask include:

- Is the software web-based or client-side?
- How are passwords implemented and is strength checked?
- Does the software have a robust personalization engine to restrict access?
- Is two factor authentication implemented locally?
- Are all important communications with the server software encrypted (e.g. HTTPS)?

Operational Security

Lastly, having operational protocols in place will go a long way to ensuring sound security for your digital signage network. Even though you have the physical, technical and networking security solutions in place, most security breaches occur simply because users share their passwords with co-workers, old passwords are not deactivated, or vendors don't maintain compliance with the latest software upgrades.

Network operators must consider employees and vendor's employees as part of the security fabric. Many attacks come from what are known as social engineering rather than technical engineering. Ensure that vendors are verifying the identity of those who are requesting changes to be made to operational software and systems. Passwords, access codes, media and software should never be made available without verification of identity.

Employing simple operational practices go a long way to ensuring those that use your system don't inadvertently or intentionally put your digital signage network at risk. Some suggestions for operational security measures include:

- Change your passwords regularly
- Using normal IT precautions such as patching servers with software updates for security issues
- Monitor your servers and have intrusion detection systems in place
- Run routine security audits
- Have media players report on their health
- Check your play affidavits carefully for anomalies

Summary

Digital signage networks are complex projects that stand to deliver tremendous competitive advantages to organizations across a number of industries. These networks may span thousands of locations, delivering timely and relevant messages that educate, inform and motivate employees and customers alike. Securing them is essential, and most organizations have IT staff ready, able and motivated to assist with outlining security precautions and measures.

While security is a complex domain outside the daily demands of most marketers, these professionals should invest time in understanding the host of variables associated with digital signage security. Understanding these security variables upfront will only help in the decision on what digital signage architecture is best for your organization.

About Real Digital Media

Real Digital Media is the provider of NEOCAST®, an enterprise class digital signage platform for managing the efficient distribution of place-based targeted messages and branded experiences across networked displays. Designed intelligently to scale with the growing demands of the digital out-of-home (DOOH) industry, NEOCAST® is a standards-based platform that offers certainty to marketing and advertising professionals seeking a viable long-term solution to meet the current and future demands of their digital signage deployments.

Real Digital Media is a founding member of the Digital Signage Federation.

Real Digital Media
941.951.0150
info@realdigitalmedia.com

NEOCAST®