Hardcopy Security and Network Access Control

Do you know where your printers are and who they're talking to?

Introduction

Enterprise class networks are beginning to deploy new network security protocols and tools designed to gather and assess the health of client computers and other devices on the network. These assessment protocols go beyond simply checking that the device or user possesses the correct credentials to access the network. Instead they validate the network health of a system by gathering and assessing health attributes such as operating system version, security patch levels, antivirus definition levels, system configuration, etc.

Modern hardcopy devices (e.g. MFPs) behave as complex servers and clients running multiple applications. By standardizing common Health Assessment attributes for these powerful devices (Network Printers, Multi-Function Devices, Network Scanners, etc.) should be incorporated into commercial network security tools. When health assessment support is provided for modern imaging devices, commercial network security tools will be able to offer more complete network security.

Hardcopy Device Security Threat Exposure

As hardcopy devices have evolved, they have gained increasing levels of communications and file handling capabilities. These capabilities are no longer limited to just local document printing, scanning and copying. Increasingly, these devices are connected to corporate networks and use these networks to receive and transmit corporate data and documents and perform user activities.

- **Document Repository**
  Modern hardcopy devices also function as file servers and are used to store sensitive company documents and information for later retrieval. File access may be limited to non-accessible local storage or the device storage may be network accessible through various network file server protocols such as CIFS, SMB, NFS, etc.
- **Email Client and Server**
  Corporate documents can be sent from and received by hardcopy devices using standard email protocols. Scanned documents can potentially be sent to arbitrary email destinations, while an email containing potentially dangerous binary data could be received by a device.
- **FTP Client and Server**
  In the same manner as dangerous emails, potentially dangerous files could be sent to a device that provides an FTP server. Corporate documents could be transferred to arbitrary FTP destinations.
- **HTTP Web Server**

Many hardcopy devices provide an embedded HTTP Web Server to allow remote configuration of the device and transfer of files. If unprotected, this capability could expose the device to a potentially insecure reconfiguration. Since some devices allow the transfer of documents through the web server potentially dangerous files could be transferred out of the corporate network.

- **HTTP Web Browser**
  In addition to file and document server functionality, hardcopy devices can include web browsers to allow user to access local and remote web sites and services. Web access can used to send documents outside a corporate network and to retrieve documents from outside the corporate network.
- **Fax Modem**
  The fax modem provided by some hardcopy devices also presents a potentially insecure method of transmitting documents into and out of the corporate environment.
- **User Authentication**
  The enabling of user login and accounting information means that hardcopy devices now have access to corporate authentication services such as Active Directory and LDAP servers.
- **Downloadable Applications**
  Some advanced hardcopy devices provide a mechanism for user and system applications to be downloaded and executed on the device. Each of these applications presents a potential security threat to the system and network. Some method of monitoring and restricting the use of these applications is necessary.

As a result of this increased functionality the level of potential susceptibility of modern hardcopy devices to security threats and network attacks has greatly increased. It is no longer possible for network and security administrators to assume that a typical hardcopy device is a safe, localized stand-alone device that does not warrant excessive concern. Rather, these devices are just as capable of providing remote data transmission and the resulting exposure to threats as a user's desktop system or a corporate server.

Network Access Control

Network Access Control (NAC) protocols and systems provide a method for restricting network access to systems and devices, based on a set of health criteria, such as OS version, anti-virus status, application support, patch level, etc. Based on the values of these criteria, a system or device may be restricted to a non-trusted network zone, pending resolution of problems.

Health assessment can be a distinct process to validate systems, or it may be as an integral function of network asset management. It may be handled by network hardware such as an access point or switch, or it may be a function of a general system management tool such as in the Microsoft System Center product line.

Regardless of how the assent is performed, non-assessable devices such as MFPs and Printers typically must be manually excluded from the health assessment and asset management process, relegated then as unmanageable devices.

The basic operation involved with evaluating a system or device for admission to a network are:

- **Assessment**
  A system or device is first assessed to determine if it is safe to be allowed on the network. This assessment is performed by evaluating a set of factors referred to as Health Assessment Attributes. Health Assessment Attributes used to determine the safeness or health of a system or divide may vary from site to site, but include such information as OS or firmware version, OS patch level, status of anti-virus software, etc. If a system or device is determined to be healthy, it is allowed onto the secure or non-quarantined portion of a network. If a system is determined to be unhealthy, or cannot be assessed by the tool, it will be quarantined from the network.
- **Quarantine**
  If a system or device is determined to be un-healthy, it is quarantined from the rest of the network. A quarantined system may be logically removed from the network (e.g. not given a DHCP-assigned IP address or a security certificate) or may be restricted to a quarantine area (subnet) of the network
- **Remediation**
  Is most NAC systems, provision can be made for a quarantined system to be made healthy through a process of health remediation. This process may involve such steps as automatically applying a series of OS or anti-virus updates and patches. Once a quarantined device has been through the remediation process, is reassessed and, if found to be health, allowed onto the network.

The major Network Access protocols include:

- **Microsoft Network Access Protection (MS NAP)**
  Defined by Microsoft, Network Access Protection is the protocol used by Microsoft management tools such as System Center Configuration Manager and the Forefront family of security products, as well as tools from vendors such as Symantec. The primary orientation of NAP is to assess the health of Windows desktop and server system Operating systems and provide a measure of automatic correction of unhealthy systems through a health remediation process. Microsoft ships NAP client functionality in the Windows Vista, Windows 7 and Server 2008/2008R2 operating systems. Other vendors provide NAP support for other Operating Systems and devices.
- **Trusted Computing Group's Trusted Network Connect (TCG TNC)**
  Trusted Network Connect is an open standard for providing Network Access Control for a variety of clients and security tools from multiple vendors such as Juniper Network, IBM, SUN, Symantec, etc.

Hardcopy device assessment

Currently, it is not possible for a network or system administrator to detect or monitor all of the hardcopy devices that reside on the network, nor automatically determine whether they present potential security threats. While it is possible to monitor and validate devices on an individual basis, having hardcopy devices incorporated within an organization's network security tools can provide immense benefits to the network and system administrator. If a network access tool is used to perform asset management tasks such as validation and mapping all devices inserted on a secure network, it is currently not possible for hardcopy devices to be detected and displayed in a secure asset map.

To facilitate a unified approach to ensuring the network health of a hardcopy device, the PWG has defined a set of Health Assessment Attributes designed to enable device security assessment. By incorporating support for these Health Attributes in their security tools, a security vender can provide tools that present a more complete picture of network and device security. By using the security tools that provide hardcopy device support, a company can monitor and assess the hardcopy devices on their network in the same manner as they assess their user systems and servers. The level of this assessment may range from locating and identifying devices on the network to actively assessing the threat level of a device, and either remediating potential issues or isolating the device from the corporate network, thus eliminating the potential security threat.

To help incorporate the PWG Health Assessment standards with existing NAC protocols, the PWG has modeled the PWG Hard Copy Device Health Attributes to align with the existing models used for PCs and other systems, yet still allow for the evaluation of the unique security issues of hardcopy devices. The PWG Health attributes can be divided into two areas of information: Attributes for Asset Management and Health Assessment Attributes. In this manner, it may be possible to provide partial assement and management of hardcopy devices without a security vendor being required to update existing tools. Of course, for a hardcopy device to participate fully in the network assessment process, security tools will need to be updated to recognize and support the PWG Health Attributes

Attributes mainly useful for Asset Management include:

- Machine Type and Model
- Vendor Name

The areas that the PWG has identified as potential security and health factors include:

- Device Firmware version and patch level
- Device Firewall settings
- Device Admin password settings
- System Applications enabled on the device
- User Applications enabled on the device
- Configuration settings (configuration change)

Hardcopy Device Registration

Hardcopy Device Remediation

Performing proper Health assessment and potential quarantining of hardcopy devices is useful in assuring that a potentially dangerous device is not allowed on a network. However, once a device has been quarantined, it must be attended to in order to make it healthy and accessible for use. Unless a quarantined device can participate in an automatic remediation process, it must be examined by an administrator or service technician and any corrections applied manually. This can be an expensive process, particularly for hardcopy devices where the examination and correction process may involve a trip to a client site by a service technician.

For this reason, the PWG is defining specifications for providing automatic correction of hardcopy health issues, regardless of device vendor, where possible. While it is not possible to automatically repair all health problems, it may be that's a system can be automatically configured enough to able to function on the network in a safe manner.

Some of the areas where vendor agnostic automatic remediation of hardcopy devices is possible include:

- Device Firewall settings
- Device port forwarding
- System Applications enabled on the device
- User Applications enabled on the device
- Fax control
- Firmware version (limited updating capability)

Survey questions

1. Do you or your clients use NAC protocol to control network access
    a. Are your hardcopy devices regressed as unmanageable?
    b. Do you perceive value in a manageable MFP?
2. Do you or your clients use network asset management tools such as System Center Configuration Manager?