Network Access Control of Multifunction Hardcopy Devices

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

Comment [JBM1]: Given the new introduction do we still need this?

Executive Summary

In these days of security consciousness, one area of increasing concern is the security of multifunction hardcopy devices and the storage of digital documents.

Add links to printer security articles...

Please take the survey

Introduction

Enterprise class networks deploy network security protocols and tools for asset management and access control of systems on the network. Network Access control goes beyond simply checking credentials of a system by gathering and assessing a system's health and security before allowing it to interoperate on the network. Providing health assessment for modern multifunction hardcopy devices enables these devices to participate in this asset management process and provide more complete network security.

Multifunction Hardcopy Device Threat Exposure

As multifunction hardcopy devices have evolved, their 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. The following are existing threat exposures for multifunction hardcopy devices:

- **Document Repository**
  Modern multifunction hardcopy devices also function as file servers and are used to store sensitive company documents and information for later retrieval.
- **Email Client and Server**
  Scanned confidential documents can be sent to arbitrary email destinations, while an email containing potentially dangerous binary data could be received by a device.
- **FTP Client and Server**
  Confidential documents can be transferred to arbitrary FTP destinations.
- **HTTP Web Server**
  An unprotected web server exposes a device to a potentially insecure reconfiguration and can allow the transfer of confidential documents out of the corporate network.
- **HTTP Web Browser**

Web access can used to send confidential documents outside a corporate network and to retrieve infected files from outside the corporate network.

- **Fax Modem**
  The fax modem can transmit confidential documents out of the corporate environment.
- **User Authentication**
  The enabling of user login and accounting information provides multifunction hardcopy devices with access to corporate authentication services such as Active Directory and LDAP servers.
- **Downloadable Applications**
  The execution of downloaded applications presents a security threat to the system and network.

With these capabilities, it is no longer possible for network and security administrators to assume that a typical multifunction hardcopy device is a localized stand-alone device that does not warrant excessive concern. These devices present as much of a threat exposure as a user's desktop system or a corporate server.

Overview of Network Access Control

Network Access Control (NAC) systems are deployed in companies the world, from large enterprises networks to small branch offices. NAC protocols and systems provide a method for evaluating systems and devices, and restricting network access to those devices that do not comply with security policy. Devices (such as current multifunction hardcopy devices) that do not support NAC assessment also are quarantined and must be manually configured to use the network.

Health Assessment Concepts

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 such as OS version, patch level, anti-virus software, etc.
- **Quarantine**
  System and devices will be quarantined if they fail to or cannot be assessed. A system will remain quarantined until it is fixed or manually allowed onto the network (the behavior for current multifunction hardcopy devices).
- **Remediation**
  Is most NAC systems, provision can be made for a quarantined system to be made healthy through a process of health remediation. Once a quarantined device has been through the remediation process, is reassessed and, if found to be health, allowed onto the network.

Asset Management

In addition to evaluating the health of systems and devices, NAC tools provide useful network asset management functionality. However, current multifunction hardcopy devices cannot participate in the process and are not identified in the network asset collection unless they are manually entered. This

requirement for manual configuration makes it difficult for network administrators and service technicians to find and manage multifunction hardcopy devices that may be inserted in their network by users.

Network Access protocols

- **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.
- **NEA (Cisco)**

NAC Vendors

- **Microsoft System Center Configuration Manager**
- **Symantec Endpoint Assessment**
- **IBM Tivoli**
- **HP Open View**
- **CA Unicenter**
- **Network Access Points and Routers (Cisco, Juniper, etc.)**

Multifunction Hardcopy Devices and NAC

Device Assessment

To facilitate a unified approach to ensuring the network health of a multifunction 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 allowing a company to monitor and assess the multifunction hardcopy devices on their network in the same manner as they assess their user systems and servers.

The PWG has defined attributes useful for Asset Management such as:

- Machine Type and Model
- Vendor Name

Areas that the PWG has identified as 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)

Device Remediation

Once a device has been quarantined, it must be attended to in order to make it healthy and accessible for use. To facilitate this, the PWG is defining specifications for providing automatic correction of multifunction hardcopy device health issues, regardless of device vendor.

Some of the areas where automatic remediation of multifunction hardcopy devices is being defined 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)

Reference Links:

Digital Photocopiers Loaded With Secrets

http://www.cbsnews.com/stories/2010/04/19/eveningnews/main6412439.shtml

http://www.youtube.com/watch?v=6pIFUOav2xE

Digital photocopiers security

http://www.wral.com/news/local/story/7617322/

http://itknowledgeexchange.techtarget.com/security-corner/security-risk-of-digital-copiers/

http://www.tgdaily.com/security-features/49823-ftc-to-investigate-photocopier-security-risks

http://security.arizona.edu/copiers

Digital multifunction device security

http://portal.acm.org/citation.cfm?id=1456625.1456640

http://www.digitaloutput.net/content/contentct.asp?p=76

IEEE P2600 Home Page

http://grouper.ieee.org/groups/2600/

Survey questions

1. Do your clients use NAC to manage network access?
    a. Are your client's multifunction hardcopy devices manually configured in their NAC system?
    b. Is it important that your client's multifunction hardcopy devices support NAC?
2. Do your clients use network asset management tools
    a. Which tools
        i. Microsoft System Center Configuration Manager?
        ii. Symantec Endpoint Assessment
        iii. IBM Tivoli
        iv. HP OpenView
        v. CA Unicenter
        vi. Network Access Points and Routers (Cisco, Juniper, etc.)
        vii. other
3. Would limited support for existing NAC tools such as Microsoft SCCM help you clients?
4. Would automatic remediation of device security failures help your clients?
    a. Automatic firmware updates
    b. Device application control
    c. Firewall policy configuration
5. What are other hardcopy security issues that your clients are concerned with?
    a. Device Authentication
    b. User Authorization
    c. Security Compliance Logging
    d. other
6. Are you or your clients aware of the IEEE 2600 series of hardcopy security standards?
7. Are you or your clients aware of the PWG Imaging Device Security projects?
8.