Management, Accounting and Device Utilization Issues

Who is accessing your printers and what are they doing?

Introduction

Security issues are of concern to the Managed Print Services users because they relate to the functioning of the network and network services and the privacy and integrity of data. Security issues, and the methods used to insure security, also affect the ability of Managed Print Services providers to reliably and profitably manage their fleets. A previous PWG article discussed Network Access Control, which manages the devices' access to networks. This article discusses User Access Control, the management and logging of who is accessing the devices, what they are doing and what is happening to their data. Future articles will deal with some of the other security issues applicable to the use, maintenance and billing for hardcopy devices,

Various User Access Control methods may be used to protect against improper access to or use of the devices. Such access may impact device configuration and accessibility to others, accounting for services used and the security of information processed by the hardcopy imaging services. Although some of these methods are largely the same as those used for servers and personal computers, others address the unique nature of hardcopy devices. User Access Control methods may be grouped into:
Identification, Authentication and Authorization, controlling who has what level of access.
Logging, to record user access for tracing problems (Audit trail) and for billing/accounting purposes.

The IEEE 2600-2008 standard describes the security vulnerabilities and requirements applicable to the hardcopy device itself. The document also identifies possible countermeasures to be used by equipment manufacturers, administrators, and others in the selection, installation, configuration, and usage of hardcopy devices. (Note that the associated IEEE-2600.1, IEEE-2600.2, IEEE- 2600.3, and IEEE-2600.4 standards are constructed as Protection Profiles, suitable to assist in Common Criteria Certification of devices which certain customers, such as US government agencies and certain enterprises, require to have confidence in device compliance to the manufacturer's stated security provisions.)

In addition to the Identification, Authentication and Authorization and Logging capabilities discussed in this article, IEEE 2600 addresses other security measures including:

a. Use of a standard network time server for reliable time stamp generation for event or log records.
b. Secure erase of residual data stored in the device.
c. Running device self-tests at designated times or under designated error conditions.
d. Time out of an interactive session after a designated time period of inactivity.
e. A whole set of User and Configuration Data security measures (which will be the subject of the next PWG article.)

The PWG Imaging Device Security (IDS) working group is currently developing specific standards for addressing the threat issues identified in IEEE-2600 and its associated Protection Profile documents. These efforts, for the most part, are concerned with applying standard security practices to hardcopy devices.

As with any protection mechanisms, there are costs in terms of efficiency and convenience. One of these costs is the difficulty in assuring protection of the device use and configuration data, and the information sent for processing while still permitting effective remote management and service of the device.

Access Control According to User Roles

Hardcopy device operations allow users to access device configuration, setup and usage information as well as job and document data. Without user access control, anyone could access the device and use these operations to disrupt service, avoid proper billing, or gain inappropriate access to the job and document information of other users (which is often retained in the device after a job has been completed.) Configuration capability must be restricted to those with administration rights, service access to device maintenance people, billing information to designated accounting personnel and job/document data to the job owner (and perhaps the device administrator), according to site security policy. Controlling access means identifying those who wish to access the device, authenticating their identity, determining the types of access for which they are authorized, and limiting their access accordingly.

In addition to controlling user access to device configuration, management and job information, an access control system can provide fine grained control over user access and use of hardcopy device features and resources. For example, User Access Control can be used to allow a visiting guest to print to a hardcopy device, but control their access to device resources, such as certain paper types (letter head) or document storage.

Identification, Authentication and Authorization

To ensure proper access control, a set of administrator-configurable access control policies must be available. These policies must follow the local site security policy and must be based on which accesses to user data and device operations can be controlled. To enforce these access control policies, users must be properly identified (who are you?) and authenticated (prove it!). Once a user has been identified and the identity has been authenticated, specific access authorization can be provided to control the use of device resources and capabilities.

Identification and Authentication

General security practice recognizes three categories of information that can be used for identification and authentication.

1) Something you know — This category covers information known to the user, such as a User Name, User ID, email address, phone number, or some other piece of unique information. Generally this information will be combined with some form of password or passphrase information.

2) Something you have — This covers the areas of physical identification content such as Common Access Cards, passports, driver's license, etc.

3) Something you are — While generally referring to user biometric information such as finger prints, or retinal scans, this category could also include information such as the user's physical location (proximity detection, etc.).

The provided identity information can be authenticated against a trusted access database, such an Active Directory or LDAP server, or a Trusted Certificate Authority.

Authorization

A method of defining and providing authorization and usage rights must be provided to enable control over user operations. By defining a set of Access Control Policies, an administrator can exercise various levels of management over user and device permissions.

The access control policies should be configurable only by an authorized local site Administrator or Operator according to the local site's security policies. In general, the access control policies should observe the following access control principles:

1. A User's Job data and the associated document data should only be accessible to the Job Owner, or an Administrator or Operator who has higher privilege than the Owner.
2. Any status data including System Status, Subunit Status, Service Status, Job or Document Status, Job or Document Receipt, and Job History are automatically generated and maintained by the device. Once generated, these data must never be modified by anybody and must be retained or deleted according to local administrative or regulatory policy.
3. User (or Basic) operations are mainly Job-oriented operations, available to Users including Job Owner, Administrator, and Operator; although any operation affecting a Job or Document is restricted to Job Owner, or an Administrator or Operator. The local site policy may cause a Service to restrict information provided to a User who is not an Administrator or Operator.
4. Administrative operations must be restricted to Administrators and Operators. For some Services such as Copy, certain operations may consider any User that is present at the device as having Administrator access.

The access control policies should assign access rights to the operations and stored data in accordance with the User's specific roles, assigned groups, and the local site's security policy. The access control policies for Users may be stored or configured in an external central user database such as an Active Directory or LDAP server along with a network domain user's identification and authentication information. The device should use the authentication protocols that perform authentication of a User's identification as well as access control policies against the central user database in the user's enterprise authentication framework before granting the user access to any device stored data or Service operation.

Log Generation and Availability

Usage is often the basis for billing or attributing charges. It is also useful for maintenance and resource planning purposes. Keeping proper records of who uses how much of what services when is a necessary consideration in any managed print services installation. Further, because even properly authenticated and authorized users may intentionally or unintentionally abuse their access rights, logging who does what when is often required for security purposes, (audit log), sometimes with alerts sent out when actions contrary to security policy are attempted.

Hardcopy devices generally are capable of generating a great deal of information such as the number of pages printed for a given job, when a facsimile was received along with the sender's phone number and the number of pages, printer maintenance alerts, security issues like unauthorized access, and so forth. The "syslog" protocol (RFC 5424) is a common standard used for logging this information. This standard is already supported by many printers and all major operating systems to allow for centralized logging and analysis. The PWG's Imaging Device Security working group is currently developing an extension to the syslog protocol that defines standard keywords, values, and events so that printers from multiple vendors can log this information in a common format, greatly simplifying log analysis.

Although the most secure approach is for devices to continually send out log information to an external repository as events occur. Often however, this is neither practical nor justifiable. In many cases, log information is accumulated in the device with the external log updated periodically. In some cases, the log is maintained in the device itself, with log content being accessed by a remote call. Sometimes, log information can be locally accessed, perhaps by being printed out. In any case, Log data must be considered privileged information with special care taken so that this data cannot be altered.

Audit Logs

The primary purpose of audit logs is to support site security requirements and regulatory compliance. Audit logs provide forensic information about access to the hardcopy device - when jobs were printed/faxed/copied, when software updates are applied, what computer(s) accessed the device and

when, what information was requested from the device and when, and whether the access was allowed. The IEEE Standard 2600 series of Protection Profiles define standard events and information that must be part of an audit log. The PWG IDS work group is also working to define additional events specific to secure networks and health assessment.

Generating audit log records and making them available for review and analysis by Administrators or Auditors is the most basic of common security requirements for all device operational environments. The types of security events that must be logged vary for different operational environments, as identified in the IEEE Standard 2600 series. Since the log records generated must be available for review and analysis by Administrators or Auditors who may not conveniently collocated with the distributed devices across the network, devices are often capable of sending the log records to an Administrator designated central log aggregation server. The log records are typically in a standard format using the IETF standard syslog protocol so that the logs can be integrated, audited, correlated and analyzed centrally across different log management applications.

Log records sent across the network must be protected for their authenticity and integrity. Typically, encryption of the syslog protocol information is used to mitigate the risk of device spoofing and man-in-the-middle attack,as required by the local site security policy.

Accounting Logs

The primary purpose of accounting logs is to support accurate usage information for billing and/or expense analysis. Accounting logs may also be required for regulatory compliance.

Accounting logs provide a snapshot of print/fax/copy job activity - the owners of the jobs, billing information such as account numbers, the printer(s) used for the jobs, the number of pages in the job, the type of media used, and so forth. Detailed consumable information (how much cyan toner was used for each job) is generally not available, however. ISO 10175 (Document Printing Application or DPA) defines the baseline information necessary for accounting logs and is used as the basis of all IETF and PWG printing standards.

Maintenance Logs

The primary purpose of maintenance logs is to support site planning and response. Maintenance logs provide information about the hardcopy device - when consumables are replaced, when paper jams or other error conditions occur and are resolved, when the device detects faults in external connections such as power or networking, and when the device is in specific operating modes such as sleep, power down, servicing, etc. Much of this information is also available via SNMP in various standard (RFC 3805, PWG Power MIB) and vendor proprietary MIBs.

References:

“IEEE Std. 2600™-2008, Information Technology: Hardcopy Device and System Security”, IEEE, 2008

"IEEE Std. 2600.1™-2009, IEEE Standard for a Protection Profile in Operational Environment A", IEEE, 2009

"IEEE Std. 2600.2™-2009, IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std. 2600™-2008 Operational Environment B", IEEE, 2010

"IEEE Std. 2600.3™-2009, IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std. 2600™-2008 Operational Environment C", IEEE, 2010

"IEEE Std. 2600.4™-2010, IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std. 2600™-2008 Operational Environment D", IEEE, 2010

“Transmission of Syslog Messages over UDP”

RFC5424 The Syslog Protocol, R. Gerhards March 2009

RFC5425 Transport Layer Security (TLS) Transport Mapping for Syslog, F. Miao, Ed., Y. Ma, Ed., J. Salowey, Ed., March 2009

RFC5426 Transmission of Syslog Messages over UDP, A. Okmiansk,i March 2009

RFC5427 Textual Conventions for Syslog Management, G. Keeni March, 2009

Common Criteria http://www.commoncriteriaportal.org/

IT Baseline Protection for Hardcopy Equipment
https://www.bsi.bund.de/cae/servlet/contentblob/479612/publicationFile/28017/moduleb03406_pdf.pdf

Background on Identification_Authentication_and_Authorization
http://www.windowsecurity.com/whitepapers/Identification_Authentication_and_Authorization_on_the_World_Wide_Web.html

Identification, Authentication and Authorization and Logging Survey Questions

1. Do you or your clients have a security policy that includes user access control for printers or multi function imaging device functions or capabilities?
    a. No, there appears to be no need..
    b. Not yet but the need is recognized.
    c. Yes, via an external server,
    d. Yes, using features in the device.
2. Are you or your clients implementing access control methods with respect to device configuration and/or access to user data (such as recently printed jobs)

    a. No, there appears to be no need..
    b. Not yet but the need is recognized.
    c. Yes, via an external server,
    d. Yes, using features in the device.

3. Are you or your clients implementing access control methods with respect to device functions limiting access to some features(e.g., color printing, fax message transmission) to only privileged users
    a. No, there appears to be no need..
    b. Not yet but the need is recognized.
    c. Yes, via an external server,
    d. Yes, using features in the device.

4. In your opinion, are currently available hardcopy devices equipped to support user access control?
    a. Yes, adequate features are currently available.
    b. No, support is needed but not yet available.
    c. Such support is not needed.

5. Please indicate your opinion with respect to the following roles:

    A. Guest User
        a. In my experience, this is a reasonable and necessary role
        b. In my experience, this is not a distinct role requirement
        c. In my experience, it would be very difficult supporting this as a role since it is too restrictive

    B. Basic user
        a. In my experience, this is a reasonable and necessary role
        b. In my experience, this is not a distinct role requirement
        c. In my experience, it would be very difficult supporting this as a role since it is too restrictive

    C. Privileged user
        a. In my experience, this is a reasonable and necessary role
        b. In my experience, this is not a distinct role requirement
        c. In my experience, it would be very difficult supporting this as a role since it is too restrictive

    D. Local manager (manages guest, basic and privileged user accounts, but cannot affect higher level accounts and has limited control over configuration; may have control over software “applications” in device)
        a. In my experience, this is a reasonable and necessary role

b. In my experience, this is not a distinct role requirement
c. In my experience, it would be very difficult supporting this as a role since it is too restrictive

E. Local Maintenance (can replenish paper and simple supplies, clear simple paper jams but cannot configure device nor have access to any user data.)
   a. In my experience, this is a reasonable and necessary role
   b. In my experience, this is not a distinct role requirement
   c. In my experience, it would be very difficult supporting this as a role since it is too restrictive

F. Network Manager (responsible for overall network including network security (can disconnect unit from network and possibly reconfigure network interfaces and security provisions. May have control over software/firmware updates.)
   a. In my experience, this is a reasonable and necessary role
   b. In my experience, this is not a distinct role requirement
   c. In my experience, it would be very difficult supporting this as a role since it is too restrictive

G. Accounting manager(has access to usage log information including who used what amount of which service and when, for billing/accounting/chargeback, but not access to user data)
   a. In my experience, this is a reasonable and necessary role
   b. In my experience, this is not a distinct role requirement
   c. In my experience, it would be very difficult supporting this as a role since it is too restrictive

H. Maintenance and Service (responsible keeping unit operating, including configuration, firmware update, corrective and preventive maintenance, parts replacement. Probably can run tests, status and configuration queries)
   a. In my experience, this is a reasonable and necessary role
   b. In my experience, this is not a distinct role requirement
   c. In my experience, it would be very difficult supporting this as a role since it is too restrictive

6. Are you or your clients implementing logging ?
   a. For security purposes.
   b. For billing or accounting.
   c. For other reasons.

7. If you or your clients are implementing logging, is the log kept:
   a. In the device
   b. In a local server
   c. Remotely
   d. No logging. Billing is done by simple copy count or other method.

8. What problems with respect to access are you experiencing/anticipating? (Check all that apply)
   a. Unauthorized users gaining access to other users' job data (including violation of regulations such as HIPAA, Sarbanes-Oxley etc.)
   b. Users modifying device characteristics, or rending device inappropriate for or inaccessible to other users.
   c. Users abusing access for unauthorized use of services (e.g., unnecessary use of higher cost services, such as color; private use, etc)
   d. Users not being allowed proper access to perform their jobs.
   e. Other

9. With respect to user access control and logging:

a. What additional information would you like to know about these techniques?
b. What access threats are you aware of that are not addressed by the capabilities outline in the article?
c. What features would you like to see standardized to allow more effective implementation?