imageRUNNER Security White Paper
AFD Response

2010 07 28

Introduction:

This paper is a response to the Canon White Paper: Canon imageRUNNER/imagePRESS Security. This is a response from ANTS on what we are doing today and what we feel we need to investigate more.
When a setting is applicable to network printers it will be noted.
It should be noted that some of the features cannot be accessed from the RUI (Remote User Interface) and must be done at the printer console.

Canon Security Recommendations Quick Reference

On page 19 of the white paper Canon Recommends the following.

> The following actions are recommended by Canon as appropriate first steps in securing the Canon imageRUNNER or imagePRESS device for most environments. While these suggestions assist in enhancing device security, internal company security policies should ultimately dictate which security measures are appropriate for implementation within a specific environment.

1. Set the system administrator ID and password
2. Disable unused ports and applications (e.g. FTP, RUI)
3. Set passwords for MailBoxes
4. Restrict printing and RUI access to specific IP or MAC addresses
5. Set passwords for Address Book management
6. Change the SNMP community strings
7. Disable the USB port if unused
8. Utilize Optional Hard Disk Drive Erase Kit or Hard Disk Drive Encryption Kit to ensure integrity of data stored on internal imageRUNNER/imagePRESS Hard Disk Drives
9. Enable and configure Department ID to manage user device access permissions on a departmental or user level
10. Monitor the devices using imageWARE EMC

What AFD is Doing

1. Set the system administrator ID and password
   Section 2.1 Password-Protection System Settings Page 7
   AFD sets a System user and password on all Copiers and printers to protect the system settings. This restricts access to the copier/printer setup.
   a. Pros – Our copiers and printers are protected from having the system settings changed.
   b. Cons – More Office Systems has to arrange for help from ANTS when they come to service any AFD copier. More does not have our username and password.
2. Disable unused ports and applications (e.g. FTP, RUI)
   Section 2.2 Network Security Page 9
   ANTS disables all unused protocols or feature on all copiers and printers. Example, ANTS does not support Novell or Apple Computers so we disable these protocols on all our copiers and printers.
3. Set passwords for Mail Boxes
   Section 2.2 Mail Box Password Protection Page 8
   ANTS offers this as an option to end users. ANTS will help an end user add a password to a mail box for confidential printer. ANTS does not require it.
4. Restrict printing and RUI access to specific IP or MAC addresses
   Section 2.2 IP Address Range Settings Page 10
   ANTS does not restrict access to the printers by IP Address. We have users in many different buildings on campus and in many different subnets. Our goal is to allow any user in any location to have the ability to print to any of our Copiers or Printers.
5. Set passwords for Address Book management
   Section 2.2 Access Code for Address Books Page15
   ANTS does not restrict access to address books.
6. Change the SNMP community strings
   ANTS changes the community string for all printers. The software that More Office Systems uses to collect copier counts for billing uses SNMP. The Community Name for all copiers on campus have to use the same community name, currently they are using public.
7. Disable the USB port if unused
   ANTS disables the USB ports on our copiers.
8. Utilize Optional Hard Disk Drive Erase Kit or Hard Disk Drive Encryption Kit to ensure integrity of data stored on internal imageRUNNER/imagePRESS Hard Disk Drives
   Section 3.1 Canon Advanced imageRUNNER Security Solutions Page 21

AFD has purchased the option HDD security kits for our copiers that are in areas that deal with high volumes of level 1 data. See note 1 at the bottom of this document for instructions on how to tell if you have the HDD Security kit installed.

9. Enable and configure Department ID to manage user device access permissions on a departmental or user level
   Section 2.1 Device Security, Department ID Mode
   ANTS offers this as an option. Department ID Mode does multiple things.
   a. It enables job accounting. With job accounting you can track how many clicks each ID uses.
   b. It secures the copier from use. You have to have a code to use the copier.
   c. With Department ID mode enabled you have many choices as to what requires a code from mail boxes to B&W printing to Color Printing.
   d. ITS WTS does not support Department ID Mode when printing to Copiers from ITS WTS.
10. Monitor the devices using imageWARE EMC
    Section 2 Access Management System Kit Page 19
    ANTS has a copy of the Canon imageWARE Enterprise Management Console. We have not yet installed and tested it. After talking with Marty at More Office Solutions, I do not think this will do much to help us with security. This is more like the HP Jet Admin.

NOTE 1:

To determine if you have a HDD Security Kit installed on your Canon copier:

- A symbol of a lock will show on the copy screen in one of the corners.
  In the AFD machines this is true on some but not all of the copiers that have the HDD Security Kits.
- On any machine if you
  - Press the counter button.
  - In the lower right corner of the touch screen: touch the device config key
  - All features of that machine will show in a list.
    ANTS has not yet determined what will show up in this list. It appears that the HDD Security Kits is listed differently for models of copiers.

NOTE 2:

HDD Security Kit and HDD Erase Kit are two different items.

- HDD Security Kit – Will have a lock on the screen – encryption
- HDD Erase Kit – Will not have a lock on the screen.

- If you watch the screen when the machine is powered on, on the screen you will see the machine go through a HDD erase cycle.

All the copiers have an erase feature from the front panel. The will reset configuration to factory defaults. The copier will also go through a HDD cleaning cycle, one pass zeros overwrite.

1. Press the Additional Features Button
2. System Settings
3. Initialize all data / settings

NOTE 3:
The Tech at More Office Systems have been instructed that if they need to do a HDD replacement on a machine at Cal Poly, they are to leave the old hard drive behind for Cal Poly to dispose of.