Global Information Assurance Certification Paper

Do You Copy? Security Issues With Digital Copiers
Kevin K. Smith
16 September 2000

OVERVIEW

Until recently, copy machines were not considered the responsibility of Information Technology Departments. They were relegated to the same department that handled office supplies, typewriters and calculators. The new breed of digital copiers change all that. With the ability to add network printing, scanning, e-mail and fax, copier dealers have realized that they need to make their pitches to directly to the IT Department or sneak one before IT realizes it is there. Whether you have inherited one of these units or are considering acquiring one, a closer look at the security issues is warranted.

The features available on these units are their selling point. A fully loaded digital copier can contain any combination of the following:

- Scan-Once - copy many, On Demand Reprint
- Scan to Fax, Scan to E-Mail, Scan to file
- Network Printing, IP Printing, FTP Printing
- Print to Fax, Print to E-Mail, Print to File
- E-Mail to Print, E-Mail to Fax
- SNMP, Telnet, HTTP based management
- E-Mail Diagnostics, Dial-In Diagnostics

After looking at this list, you begin to realize that this one unit may contain more access points and services than are available on some networks. Essentially these units are an embedded computer with a scanner and printer attached. As a result, you need to assess security just as you would for any other server or workstation in your organization. To illustrate the security issues with digital copiers, the Sharp AR-507 Imager [10] our office recently acquired will act as the backdrop. Let's start with a look at the management features available on digital copiers.

KEY OPERATOR CODE

The key operator code is the equivalent of the console password. It allows access to the configuration and status from the keypad on the machine. On the AR-507 this defaults to five zeros. This is the first vulnerability.

MANAGEMENT MODEM

Our AR-507 did not come with this option. The vendor assured us that it could only be used for diagnostic functions and not as a RAS server. However, it does provide an access point to possibly compromise the integrity of the copier. A possible vulnerability.

TELNET

One of the standard management options is through telnet. It uses the standard port and a lets you login as either SYSADM or GUEST. By default the password is the same as the user name. The GUEST login id will only let you view setting but will not let you change anything. The

SYSADM login brings up a menu option that allows you to change the IP settings, change the administrative password or enable other protocols such as IPX or AppleTalk. Here are our first two network vulnerabilities: a GUEST account that cannot be disabled and a system account where the username and password are the same.

FTP

The Sharp AR-507 uses FTP in both client and server functions. FTP in the server function is found on the standard port and is used by Sharp's Flash Update Utility to load new ROM BIOS images into the system. It also uses the default SYSADM password. Files can be submitted directly to the printer by using FTP with the username PORT1. No password is required. The client side is used as part of the Scan-to-File feature to post a scanned document to another server running FTP. This leaves the question of whether FTP is subject to buffer overflows as found in other FTP daemons. A fourth possible vulnerability.

SNMP

Sometimes you have to laugh to yourself as the salesman is expounding on the features of the printer management software. "…You can even control other network printers with it." The AR-507 uses the standard SNMP style management that is used on most network printers. A trace showed that SNMP is using the standard PUBLIC and PRIVATE community strings [12]. Sharp has not documented or provided a utility to change the community strings. Here is vulnerability five.

HTTP

The AR-507 also provides management through an embedded web server. It can be accessed through any of the current web browsers by using the copiers IP address as the URL. The HTTP management offers several more options than telnet. Through HTTP, you can view image counts and enable the Fax-to-File and Fax-to-E-Mail options if you have the network scanner option installed. It also allows you to set up the e-mail addresses of technical support or on-site staff to send copier status and counts. Several e-mail addresses can be programmed in.

Passwords are not required by default to access the management pages. When enabled, the standard administrative password is used to grant access. Any time a change to a setting is made, the standard SYSADM password is entered into a field on the page and posted along with new settings. Not directly vulnerability, but a portal to create others.

LOGGING

Logging on the AR507 is minimal. It keeps an internal log on paper jams and image counts. It is also able to e-mail alerts on jams, out of paper or other copier problems. However, it does not keep any kind of job log on when copies or prints were made. Not a real vulnerability, but it does make auditing more difficult.

WHAT ELSE?

It is now time to see if anything other than the published features is lurking about on the machine. NMap showed ports 21(ftp), 23(telnet), 129(pwdgen) and 515(printer) listening on the copier. Surprisingly, SMTP did not show up. However, since we did not have the Fax-to-Mail

or Mail-to-Print, all SMTP traffic would be outbound only. PWDGEN (port 129) was a little curious. It became clearer after the side effects of the port scan.

The port scan crashed FTP and HTTP. They did recover on their own after a half-hour. Telnet revealed something interesting. Instead of the expected login prompt, the line " HTTP 1.1/1.0 ROMPager by Allegro" briefly flashed by and telnet locked up. A search on the web revealed that ROMPager by AllegroSoft is a common package used to embed management services into network devices. Besides Sharp, 3Com has used it in their switches and Xerox has used it in their DocuCentre lines [2]. The web search also showed that certain versions of ROMPager are subject to denial of service attacks on FTP [8].

The ROMPager features page cleared up what PWDGEN was doing [3]. During HTTP management it looks like ROMPager sets a session cookie using a password from pwdgen and the system time for whenever the system administration password is used. However, this process doesn't make much sense. The administration password is sent as cleartext with the prefix http-pwd when the management web page is posted. There is vulnerability six.

The copier has six vulnerabilities, but what are we trying to protect that we care if integrity is compromised. We are trying to protect the confidentiality of the business information that is on every document that passes through the machine. It used to be that you fed paper into a copier and it spit paper back out. On top of that, you had to be at the machine to do it. The new breed of digital copiers can best be thought of as document transfer stations. Once the integrity of the copier has been compromised, it can become very easy to redirect documents using the features of the machine.

The essential feature that allows for breach of confidentiality is the demand reprint function. As pages are scanned or printed, they are buffered to the hard drive. Demand reprint allows you to reprint or redirect the copy to mail, fax or to a file. We protect confidentiality by turning this feature off. We protect the integrity to keep this feature turned off.

A second component we are trying to protect is the e-mail address book. The scan-to-email uses the address book to determine the destination. (It is very tedious to enter e-mail addresses with just a numeric pad.) Once integrity is compromised, a foreign e-mail address could be placed into the list.

A SOMEWHAT THEORETICAL SIDE TRIP

On a fully loaded digital copier, all the components are in place. The question is whether relaying e-mail can be turned on. The E-Mail-to-Print and Scan-To-E-mail option means that the copier is capable of accepting and sending out SMTP traffic. This becomes more of a concern as Linux works its way into the embedded market and brings along the standard daemons and their vulnerabilities [5]. It defeats the purpose to lock down the corporate mail server to have the spammer use your copier.

A HUMAN ISSUE

IT Staff are not usually responsible for maintaining copiers. This is usually provided by the vendor under the lease or maintenance contract. While trying not to overly stereotype, the copier

technician's concern is not security but getting the copier fixed and getting to the next assignment. The networking aspect is also new to many copier technicians. They either have minimal training in this area or rely on someone back in the shop with more experience. Consequently, the tendency is to keep default key operator and administrative passwords. This way they don't have to remember very many passwords or wait around for site personnel to let them into the machine. There may also be the tendency for technicians to turn features on or off during testing and not reset them. You will have to judge how serious an issue this is by your relationship with the vendors and technicians.

STEPS TO TAKE

- Verify what services are running. This will help determine what whether features need to be turned off; settings changed; or maybe identify a need to adjust settings on your firewall.
- Change the default Key Operator codes and administration passwords.
- If you can, change the default Public and Private SNMP community strings.
- Enable passwords for HTTP Management.
- Disable unused features and network protocols.
- If remote management through a modem is used:
    - Make sure it does not allow access to the network (i.e. act as a RAS server)
    - Do not make the telephone line directly accessible from the outside. Require the call be transferred through the company switchboard.
- Disable the demand reprint function. This is the key to keeping documents confidential.
- Verify whether the copier can relay e-mail. Disable it if you can.
- Consider routing all copier problems through IT or contacts trained to keep IT apprised of copier service calls. This allows you to verify that settings have been reset properly.
- Audit the configurations. Consider using IT Staff to gather the monthly copy counts. When gathering the counts, they can verify the configuration. (Vendors are usually nice enough to send you a fax to remind you they need the counts.)
- Know your vendor's technical staff. Knowing who is on your vendor's staff will help prevent a social-engineering ploy. Who really questions someone saying they are "here to fix the copier"?
- Find out what embedded management package is being used and check for vulnerabilities.
- Consider using a copier and/or printer control system. This provides you an audit trail of who used the copier when. They can be used in client situations for cost recovery as well.
- Scrub the copier when you dispose of it. The hard drive may still have a buffered image of the last document that could be retrieved if the hard drive was pulled out of the unit.

This is by no means all-inclusive considering the rate features are being added. However, it should give you the main points to use as a base to review and secure your own digital copier.

REFERENCES

[1] Agee, Bonita S. and Cowden, Jack. "Master IS Plan for Facsimile Devices and Digital Copiers" Fax/Digital Copiers. 1 December 1999. URL: http://cio.doe.gov/compsec/facsimile.htm (10 September 2000)

[2] Allegro Software Development Corporation. "Companies with Embedded Internet Products". 11 May 2000. URL: http://www.allegrosoft.com/innovators.html (13 September 2000)

[3] Allegro Software Development Corporation. "ROMPager Embedded Web Server Toolkit Features". 27 September 1999. URL: http://www.allegrosoft.com/pagerfeat.html (13 September 2000)

[4] Davidson, Peter. "Verge/FaxWire". 7 December 1999. URL: http://www.davidsonconsulting.com/MailVerge_Samples/120799.html (10 September 2000)

[5] Embedded Linux Consortium. "Embedding Linux? Start Here". URL: http://www.embedded-linux.org/linux.php3 (14 September 2000)

[6] Lebron, Roberto E. and Coletti, Noel. "CANON U.S.A. AND SIMPLIFY ANNOUNCE ENHANCED WINDOWS NT SCAN & E-MAIL SECURITY AND PERFORMANCE FOR CANON IMAGERUNNER DEVICES". 10 April 2000. URL: http://www.usa.canon.com/press/041000g.htm (10 September 2000)

[7] Lutz, Jason. "Xerox DocuColor 4 LP D.O.S." BugTraq Archives. 13 October 1999. URL: http://www.securityfocus.com/archive/1/30716 (10 September 2000)

[8] NetSec[davidv]. "ROMPager from Allegro software is vulnerable to DoS" SecuriTeam. 6 June 2000. URL: http://www.securiteam.com/securitynews/RomPager_from_Allegro_software_is_vulnerable_to_DoS.html (13 September 2000)

[9] Orvis, William J. and Van Lehn, Allan L. "Data Security Vulnerabilities of Facsimile Machines and Digital Copiers" UCRL-AR-118607/CIAC 2304. January 1995. URL: ftp://ftp.sunet.se/pub/security/csir/ciac/ciacdocs/ciac2304.txt (11 September 2000)

[10] SHARP. "AR-507 Copiers" Sharp Business Products. URL: http://www.sharpelectronics.com/products/ModelLanding/0,1058,150,00.html (10 Septmeber 2000)

[11] SecurityFocus. "J-019: Intelligent Peripherals Create Security Risk" UCRL-MI-119788. 8 December 1998. URL: http://www.securityfocus.com/advisories/1160 (11 September 2000)

[12] Zalewski, Michael. "Many network products have world-writable SNMP" SecuriTeam. 16 February 2000. URL: http://www.securiteam.com/securitynews/Many_network_products_have_world-writable_SNMP.html (12 September 2000)