Multi-function Devices and Printers

Fear and Loathing in JetDirect
Agenda

What They Are
What We Have Today
Problems with Printers and MFDs
Managing These Devices
Securing These Devices
How can the ITSO Help
Questions
Show of Hands

Up with them
When Copiers Attack

“I found him lifeless on the floor, covered in toner.”
May 17, 2010 5:08 PM

Photocopier Fallout: FTC "Concerned" About Copier Security

Posted by Michael Rey  1 comments

Three weeks after Congressman Ed Markey (D-MA) watched our investigation into the dangers of digital copiers and called for an investigation, the Federal Trade Commission (FTC) responded to him today with a letter saying it shares his, "concerned that personal information can be so easily retrieved from copiers."

Stopping short of announcing a full investigation, the FTC did say it is, "now reaching out to copier manufacturers, resellers and retail chains and office supply..."
PDAs, smart phones making ID thefts from copiers easier

By Jim DeBrosse, Staff Writer

Updated 11:36 PM Monday, May 31, 2010

A CBS news report in April exposed the risks of identity theft posed by just one of today’s electronic conveniences — high-speed office copiers that store images of every document or photograph they process.

But with memory chips getting smaller and cheaper all the time, even hand-held electronic devices, such as PDAs and...
June 1, 2010, 3:00 PM

Why Photocopiers Have Hard Drives
By JENNIFER SARANOW SCHULTZ

In a Bucks post last month, “The Identity Theft Threat from Copiers,” we highlighted the risks associated with copying sensitive information on copy machines that have hard drives and provided some information to help consumers better understand the risks and protect themselves.

One reader wrote in, however, questioning why copiers have hard drives storing images to begin with. To find out, we turned to the copier manufacturers, and here’s what we found out.
This started as an espionage thing in the 1970s, when the US Government had Xerox put a hard drive in the copier leased to the Russian Embassy. This information is public now, not classified. We got a LOT of information, as the drive was dumped every time Xerox went to service the copier, which, back then, was regularly, either weekly or monthly. Guess they just went ahead and added them to their other products. They did not hide this info, one of the selling points was that a lost copy could be regenerated from the image on the drive. Seems that most people did not consider the fact that this information would remain.
Printers
What is an MFD?

- Multi-function Devices
  - Free-standing Copier-style
    - Scan
    - Fax
    - Print
    - Copy
  - Desktop PC-attached AIO
    - Scan
    - Fax
    - Print
    - Copy
How We Use Them

- UI network via Ethernet
- Workstations via USB
- Workstations via Parallel ports (legacy)
They Aren’t “Just Printers”

- Limited, but usable operating systems
- As many as two dozen services
- Flash, optical, and magnetic drives
- Some can act as file servers (don’t laugh)
- Can be used to perform reconnaissance scans by remote attackers
They Aren’t “Just Copiers” Either!

- Flash, optical, and magnetic drives
- As many as two dozen services
- Archival storage that may or may not be secure or safe
- Even more capacity
- **What devices do you have that store documents?**
  - If you don’t know, find out!
  - Vendor and service company can do this for you
They Are Protocol Droids!

“I’m fluent in over six million forms of communication.”
Robots are Dangerous!

Doom and Gloom

- Can be used by remote attackers to mask scans
- Good target for identity thieves
- Storage and web services make them possible C&C hosts for malware
What Kind of Printers and MFDs are Deployed?

- HP: 1066
- Xerox: 72
- Lanier: 68
- Dell: 91
- Ricoh: 65
Show of Hands

Up with them
Printers and MFDs are Great Candidates for LSA!

Get those devices off the public internet!
(Maybe when you purchase your new Dell printer?)
Local-Scoped Addressing

- Public Addresses
- LSA

Pie chart showing 1770 Public Addresses and 56 LSA.
Show of Hands

Up with them
Problems with MFDs

• Many offer a lot of services that you don’t want active (Just like ‘3PO)

• Many are configured with publicly-accessible interfaces
  o Confidential documents readily available
  o Data-mining for usernames and other interesting data
More Problems

- Many archive jobs short-term or long-term
- Poor physical security (and they’re everywhere)
- Trivial to access from campus or off-campus (unless they’re on LSA!)
Things I Learned in 3 Exciting Days

• Open file systems via NFS (NFS!) on ~600 devices

• Open telnet interfaces on ~800 devices

• Open Web interfaces on most devices
Things I Found in 3 Exciting Days

• Copies of old and new purchase orders
• Contracts and proposals, responses to RFPs
• Order forms with credit card information
• Personal copies/faxes
• Other terrible things: medical and HR related
What You Can Find

- Even using the web interface of your printer or MFD
  - “Document Server”
  - “Saved Scans”
  - “Print Jobs”
  - “Queue Manager”
  - “File Server”
  - …these are all dangerous, Will Robinson!
Tools for Management of Printers and MFDs

• HP Web JetAdmin
    • Works via JetDirect protocol, supporting most printers

• Ricoh SmartDevice Monitor
  o [http://support.ricoh.com/html_gen/util/SDM/SDM.html](http://support.ricoh.com/html_gen/util/SDM/SDM.html)

• The LCD Panel on the device

• Other SNMP-based management software

• A Web Browser

• Telnet client and a manual
How to Get Started
Securing Printers and MFDs

It’s easier than you think
Show of Hands

Up with them
First Steps

• **Change the passwords**
  - Most devices polled on the UI internet don’t require authentication

• **Start planning to move them to LSA**
  - Immediate reduction in attack surface and smarter utilization of resources like IP addresses!
  - Get a device count and talk to TNS about next steps
Actual Device Hardening

• Disable services you don’t care about
  o Disable things like telnet, NFS and other network filesystems, and web interfaces if you don’t need them

• Create ACLs
  o Via management software or web interface/telnet to limit access to UI networks or your workgroup(s)
HP’s Guidelines

1. Ensure you have current firmware for your devices
2. Specify a telnet password other than the factory default
3. Require authentication
4. Protect the LCD panel as best you can
5. Disable all unused protocols and services
6. Disable all unused print services
7. Set an SNMP community name other than “public”
   1. Consider only using SNMPv3
8. Specify and activate an access control list
Configure via Browser

• Web Configuration
Configure via Web JetAdmin
Configure via Telnet

- Easily scriptable

Trying 192.168.1.2...
Connected to 192.168.1.2.
Escape character is '^]'.

HP JetDirect

Please type "?" for HELP, or "/" for current settings
> HALP
Access Lists via Telnet

- Single hosts or masks, 10 ACLs max on most devices
- Restricts access to all network services (telnet, www, ftp, printing, etc.)

Please type '?' for HELP, or '/' for current settings
> allow:172.30.0.0 255.255.0.0
> allow:128.255.0.0 255.255.0.0

> allow:list
Access Control List:
IP: 172.30.0.0 Mask: 255.255.0.0
IP: 128.255.0.0 Mask: 255.255.0.0
> quit
Disable Print Protocols via Telnet

- Show current config with `/` and enable or disable accordingly using "`:1" for enable and "`:0" to disable
- Disable the ones you don't need, such as "ftp-printing:0"

1. ipp-printing
2. ftp-printing
3. ftp-config
4. lpd-printing
5. 9100-printing
6. slp-config
7. ipx/spx
8. dlc/llc
9. appletalk
Harden SNMP or Disable it Entirely

- Change community string from default `public` or disable SNMP entirely if you don’t need it
  - `set-cmnty-name: $passphrase`
  - `snmp-config:0` to disable `snmp-config:1` to enable
Your Printers Have Logs!

- Configure syslog and aim logs at your log server or a host that has OSSEC HIDS ;)
  - `syslog-svr:128.255.n.n`

- Max Messages
  - `syslog-max:1-1000` (max messages per minute, 0 disables)

- Syslog Priority (not facility)
  - `syslog-priority:0-7` (zero through seven, 8 disables)

- Actively reviewing your logs is a prudent activity, even for MFDs
What can the ITSO do to help me?

- We can scan your printers for available services and assess your exposure and evaluate any possible information disclosures.

- Test the security of your printers after you’ve hardened them – on-campus and off-campus.
What else can the ITSO do for me?

• Help with creation of appropriate ACLs to protect your MFDs and other assets

• We can work with you to answer questions your users may bring you (i.e. how can I use CUPS instead of LP on my Linux workstations?)
Hardening Guides

- [http://security.utexas.edu/admin/mfdevice.html](http://security.utexas.edu/admin/mfdevice.html)
  - Nice checklist for secure setup of MFDs
- [http://security.yale.edu/sysadmin/mfd.html](http://security.yale.edu/sysadmin/mfd.html)
  - Hardening steps and reasons
- [http://informationsecurity.iu.edu/articles/Copiers_and_Multifunction_Devices](http://informationsecurity.iu.edu/articles/Copiers_and_Multifunction_Devices)
  - Including special considerations for retiring equipment and acquiring new devices!
Your Opportunities for Excellence!

When you are participating in purchasing, administration, or decommissioning, your responsibilities may include:

- Asking about disposal procedures for equipment
- If you review service contracts or purchasing agreements, keeping pressure on your vendors to provide adequate protection for the University and our users and students!
- Asking for and requiring strict standards – for example, view Brown’s ISG Security Standard for MFDs here: http://www.brown.edu/cis/policy/mfd_stnds.php (They have a very severe one)
- CpC program is getting language added to contracts (Purchasing & OGC)
Warren Says

- Warren couldn’t be here but he had some thoughts on this matter that I couldn’t paraphrase:

  “Legal advises any units (decision makers and techs in an advisory capacity) entering into contractual agreements either with a purchasing agent or directly with any vendor, to try to anticipate what kind of data may traverse the equipment. Because this may be difficult to ascertain they (units) should work on a worst-case disclosure scenario.”

- Tell your purchasing agent about your needs for confidentiality. There may be an added cost.
Getting a Dell?

• The default landing for purchasing a Dell Printer allows you to opt-out of keeping the drive

• Consider not opting-out

• Talk to TNS about implementing LSA networking
Q&A

All are welcome to ask questions, except for Carl