Securing Network Printers and Forever Ending Unwanted Print Jobs

Barbara McKinnon
Desktop Operations Manager, University of Pennsylvania
babney@upenn.edu

Session Description

Attacks on network printers throughout higher education reached an all-time high in 2016. In this case study-based session, Barbara McKinnon will share lessons learned and methods used at the University of Pennsylvania library, where they’ve achieved reliable junk-free cross-platform network printing. You’ll find out how the use of various print protocol settings, passwords, and features has resulted in increased productivity, reduced cost, and higher client satisfaction among faculty, staff, and students. You’ll walk away with an understanding of which print protocols to turn off, which ones can be managed by authentication methods, and how to the setup and support printing for Mac users in Windows Server printing environments.

Speaker Background

Barbara McKinnon is the desktop operations manager at the University of Pennsylvania library, where she manages all physical and virtual desktop and print devices, and is responsible for leading, coaching, and motivating teams to work together toward the achievement of a common goal. Barbara is currently working on her MS in project management at Drexel University, and she holds several industry certifications (Apple/A+/MCP). She previously served as VP of Programs for the HDI Philly local chapter.
Securing Network Print Devices
and forever ending unwanted print jobs

Barbara A. McKinnon
Desktop Operations Manager
University of Pennsylvania Library
Printing is a Big Deal

• Printing
  – Big business
  – Big deal
  – Personal
• Print device security
  – Not a new concept
  – Attacks spiked
    • Bold, disruptive, expensive
• Found
  – Multitier methods and solutions

Today’s Agenda

• University of Pennsylvania
• Library system
• Print cycle
• Case study scope
• Problem identification
• Solutions
• Best practice
• Appendix: How to’s
• References/sources
Penn Computing

• Distributed computing organization
  – Each school and center has separate IT structure and leadership
  – Enables customized support
Print cycle

- Four elements of print cycle:
  - Printer
    - Drivers
  - Print spooler
    - Windows service that instructs the drivers and hardware
  - Print monitor
    - Displays the status of print jobs
  - Print device
    - Physical hardware
- Print management menus:
  - Printer properties
  - Printing preferences
Background

• Case study scope
  – Failure to follow manufacturer recommendations to properly secure network print devices.

• Security recommendations
  – HP
  – Ricoh

Embedded Jetdirect Page

<table>
<thead>
<tr>
<th>General Information</th>
<th>TCP/IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status: I/O Card Ready</td>
<td>Enabled</td>
</tr>
<tr>
<td>Model Number: J8028E</td>
<td>IPv4: Hacked-By-Wild-soldier</td>
</tr>
<tr>
<td>Hardware Address: 204F010A8B8B</td>
<td>IPv6: Disabled</td>
</tr>
<tr>
<td>Firmware Version: JD123400000</td>
<td>IPv4 Domain Name: Hacked-By-Wild-soldier</td>
</tr>
<tr>
<td>IAA: 204F010A8B8B</td>
<td>IPv6 Domain Name: Not Specified</td>
</tr>
<tr>
<td>Port Config: 10T HALF</td>
<td>Primary DNS Server: 128.91.18.1</td>
</tr>
<tr>
<td>Auto Negotiation: On</td>
<td>Secondary DNS Server: 128.91.49.1</td>
</tr>
<tr>
<td>Manufacturing ID: 5321532100</td>
<td>DNS(IPv6): Not Specified</td>
</tr>
<tr>
<td>Date Manufactured: 05/2013</td>
<td>WINS Server: Not Specified</td>
</tr>
<tr>
<td>WS Registration: Registered</td>
<td>Idle Timeout: 278 sec</td>
</tr>
<tr>
<td>WS Status: Connected</td>
<td>Status: IPv4 Ready</td>
</tr>
<tr>
<td>ePrint: Allowed</td>
<td>Email: <a href="mailto:39oj1k9acfa@hpeprint.com">39oj1k9acfa@hpeprint.com</a></td>
</tr>
</tbody>
</table>
Attacked 1000 print devices per hour

The Daily Stormer

“I did not hack any printers. I sent them messages because they were configured to receive messages from the public.”

• Andrew Auernheimer (“Weev”)
Problem identification

- Printers attacked
- Open protocols
- Inventory control issues
- Lack of print management
- No passwords
- No restrictions

Solution – cost$

Look at cost$

Cost per month:
- $18,135 for all public facing
- $37,665 for all staff print devices
- Make the problem financial and solve using technology.
$how me the money$

<table>
<thead>
<tr>
<th>Item</th>
<th>Expense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Box of paper</td>
<td>$35.00</td>
</tr>
<tr>
<td>1 Ream of paper</td>
<td>$3.50</td>
</tr>
<tr>
<td>1 Sheet of paper</td>
<td>$0.01</td>
</tr>
<tr>
<td>Sheets p/ream</td>
<td>250</td>
</tr>
<tr>
<td>Reams per box</td>
<td>10</td>
</tr>
<tr>
<td>1 paper tray</td>
<td>500</td>
</tr>
<tr>
<td>3 paper trays</td>
<td>1500</td>
</tr>
<tr>
<td>Print devices</td>
<td>120</td>
</tr>
<tr>
<td>Public facing</td>
<td>39</td>
</tr>
<tr>
<td>Staff print devices</td>
<td>81</td>
</tr>
<tr>
<td>Cost per night p/print device</td>
<td>$15 = (1500*0.01)</td>
</tr>
<tr>
<td>Cost per month p/print device</td>
<td>$465 = (1500*0.01)*31</td>
</tr>
<tr>
<td>Cost per month all public facing print devices</td>
<td>$18,135 = (465*39)</td>
</tr>
<tr>
<td>Cost per month all staff print devices</td>
<td>$37,665 = (465*81)</td>
</tr>
</tbody>
</table>

Solution - technology

- Setup a print server
- Manage all print devices using your print server
Solution - policies

- Disable IPP
- Disable IPX/SPX
- Disable AppleTalk/Bonjour
- Set community name to: something meaningful
- Disable DLC/LLC
- Disable SLP
- Disable mDNS
- Disable 9100
- Disable Telnet
- Disable Multicast IPv4
- Disable FTP Printing
- Disable IPv6
- Disable HP XML Services
- Disable Web Services Print
- Disable WS-Discovery
- Set DNS: 000.000.000.000
- Disable control panel editing on the LCD

Solution – process

- Establish easy to follow procedures for desktop team. Make team your quality control inspector
- Use checklists
  - Unbox printer
  - Plug in
  - Set networking info
  - Add to print server
  - Secure
  - Publish to community
Best practice

1. Inventory your fleet
2. Setup a print server
3. Set administrative passwords
4. Set community name
5. Secure your LCD displays
6. Limit printing to your organization’s IP range
7. Gain support to secure devices
8. Turn off unneeded protocols
9. Disable remote administration and firmware updates
10. Use print server/ active directory / group policy / registry
11. Pull disks from devices before decommissioning

Appendix

- How to:
  - Screenshot of secured print device
  - IPP authentication screenshot
  - ACL interface screenshot
  - How to find your IP address range
  - Group policy to control print devices
  - Registry to control print devices
  - Active directory to control print devices
  - Install a print device onto print server
  - Add a print device on a PC and Mac
  - Setup and use web Jetadmin
  - Sample print device checklist
  - Glossary
  - Explanation of print protocols
Thank you …

My team
• Stephen Banks
• Richard King
• David Yu

My colleagues
• Grover McKenzie
• ISC Security
• Doug Smulens
• Richard Zak
• Ken Zeferes

References
• ADL. http://blog.adl.org/extremism/hacker-claims-credit-for-anti-semitic-flyer-sent-to-college-campus
• Microsoft.com. (n.d.). Understanding TCP/IP addressing and subnetting basics
  http://www.upenn.edu/computing/home/menu/organizations.html
Thank you for attending this session.

Please complete the short evaluation for this session on your mobile device. It is available in your email or through the conference app.