MICROSOFT EXCEL SPREADSHEETS EXPOSE USER PIN USED FOR CONFIDENTIAL/SECURE PRINTING

Written in February 2009
Last updated with vendor feedback in November 2010
Published on 15 January 2011 at the web site http://www.insecureprinting.com

EXECUTIVE SUMMARY

Confidential/Secure Print is a feature common to printers used in corporate environments. This feature is designed to avoid exposing sensitive printouts to other people who also have access to the printer. Print jobs are delayed until the owner is physically present at the printer to enter their Personal Identification Number (PIN).

This document discusses a design feature of Microsoft Excel created twelve years ago, which in more recent times has the undesired consequence of storing the user's Confidential/Secure Print PIN inside the spreadsheet. This defeats the whole concept of the Confidential/Secure Print feature especially when some less sensitive spreadsheets using the same PIN are available to potential adversaries, for example stored in a network shared directory.

The Confidential/Secure Print feature is enabled at the printer driver level to conveniently and automatically apply the user PIN protection to all files printed by the user. An adversary can use Windows Explorer to search network shared drives for Excel spreadsheets, and view them in Microsoft Notepad to reveal user PIN information. The adversary can then gain access to any file (e.g. Word, Excel, PowerPoint, PDF) printed by the victim, if the adversary beats the victim to the printer. The adversary can then either print two copies of the victim's file and leave one on the printer for the victim, or print one copy of the victim's file and photocopy it before leaving the original on the printer for the victim, or print one copy of the victim's file and take it resulting in the victim thinking that perhaps they didn't click the print icon after all.

EXCEL DESIGN FEATURE

Microsoft has made the specifications publicly available for the proprietary binary file formats used by Microsoft Word, Microsoft Excel and Microsoft PowerPoint [1].

A quick skim of the 349 page Microsoft Excel specifications reveals that spreadsheets contain

"*PLS: Environment-Specific Print Record (4Dh)*
The PLS record saves printer settings and printer driver information." [2]

This includes a "*DEVMODE structure*" which contains a field called "*dmDriverExtra*" which has the following definition

"*Contains the number of bytes of private driver-data that follow this structure. If a device driver does not use device-specific information, set this member to zero. The private data for a device driver follows the public portion of the DEVMODE structure.*" [3]

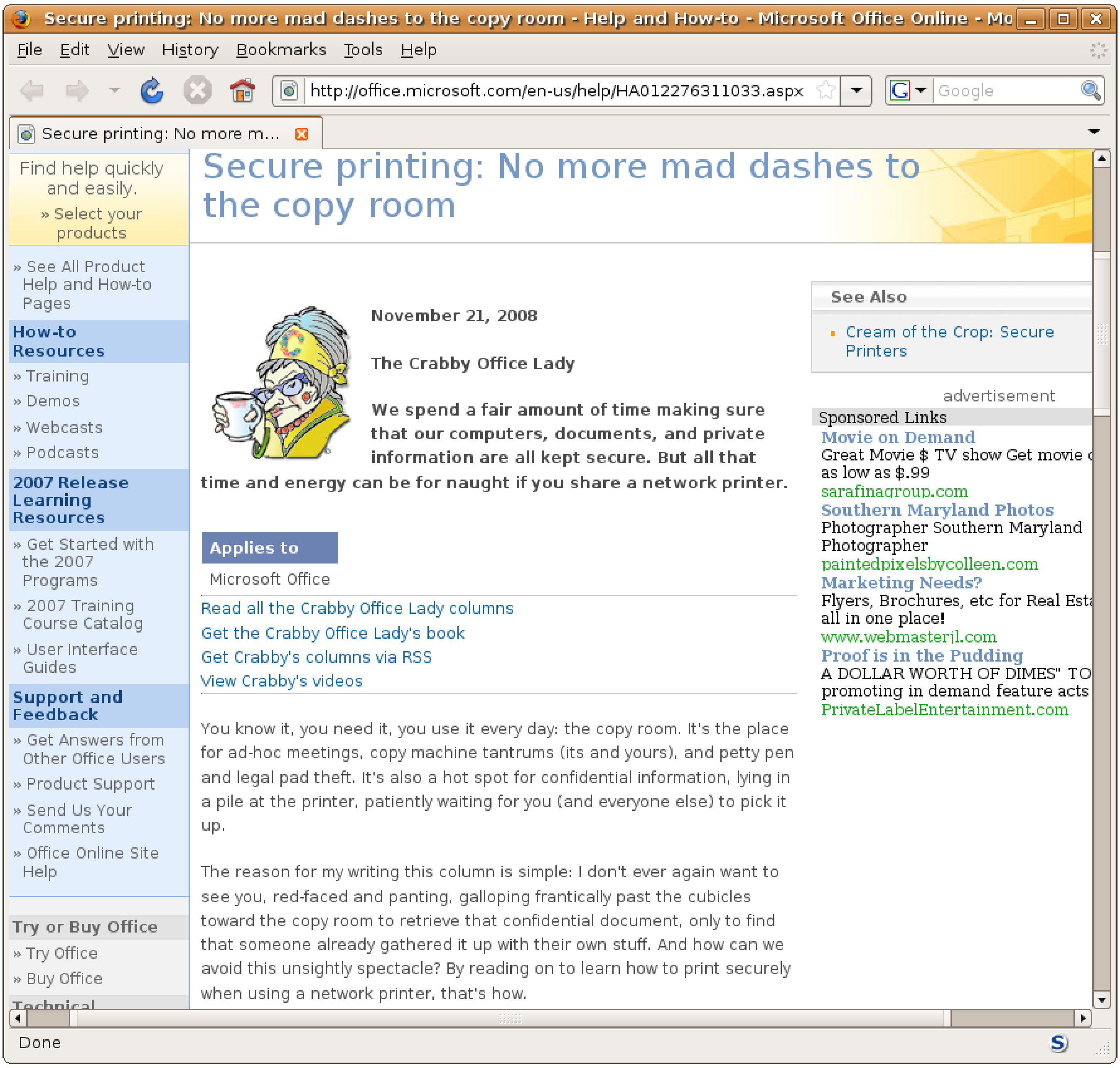
EXAMPLE PRIVATE DEVICE-SPECIFIC INFORMATION

Corporate Xerox printers typically have a Secure Print feature which Xerox describe as

"*Jobs are safely stored at the device until the owner enters a PIN to release them. This controls unauthorized viewing of documents sent to the printer.*" [4]

Corporate Lexmark Multifunction Products/Printers (MFP) typically have a Confidential Print feature which Lexmark describe as

"*The Confidential Print feature addresses the basic concern of printed pages lying on the MFP for any-one to pick up. With Confidential Print, the MFP holds submitted jobs until the intended recipient is present at the device. By producing the printed job only when the proper PIN code is entered on the MFP's operator panel, the job is delivered securely into the right hands.*
The features and benefits of Confidential Print include:
 ** An intuitive and effective means to deliver print jobs only when the recipient is at the MFP.*" [5]


Secure printing: No more mad dashes to the copy room - Help and How-to - Microsoft Office Online - Mo
File Edit View History Bookmarks Tools Help
http://office.microsoft.com/en-us/help/HA012276311033.aspx
Google
Secure printing: No more m...
Find help quickly and easily.
» Select your products
» See All Product Help and How-to Pages
How-to Resources
» Training
» Demos
» Webcasts
» Podcasts
2007 Release Learning Resources
» Get Started with the 2007 Programs
» 2007 Training Course Catalog
» User Interface Guides
Support and Feedback
» Get Answers from Other Office Users
» Product Support
» Send Us Your Comments
» Office Online Site Help
Try or Buy Office
» Try Office
» Buy Office
Technical
Done

Secure printing: No more mad dashes to the copy room

November 21, 2008

The Crabby Office Lady

We spend a fair amount of time making sure that our computers, documents, and private information are all kept secure. But all that time and energy can be for naught if you share a network printer.

Applies to

Microsoft Office

Read all the Crabby Office Lady columns
Get the Crabby Office Lady's book
Get Crabby's columns via RSS
View Crabby's videos

You know it, you need it, you use it every day: the copy room. It's the place for ad-hoc meetings, copy machine tantrums (its and yours), and petty pen and legal pad theft. It's also a hot spot for confidential information, lying in a pile at the printer, patiently waiting for you (and everyone else) to pick it up.

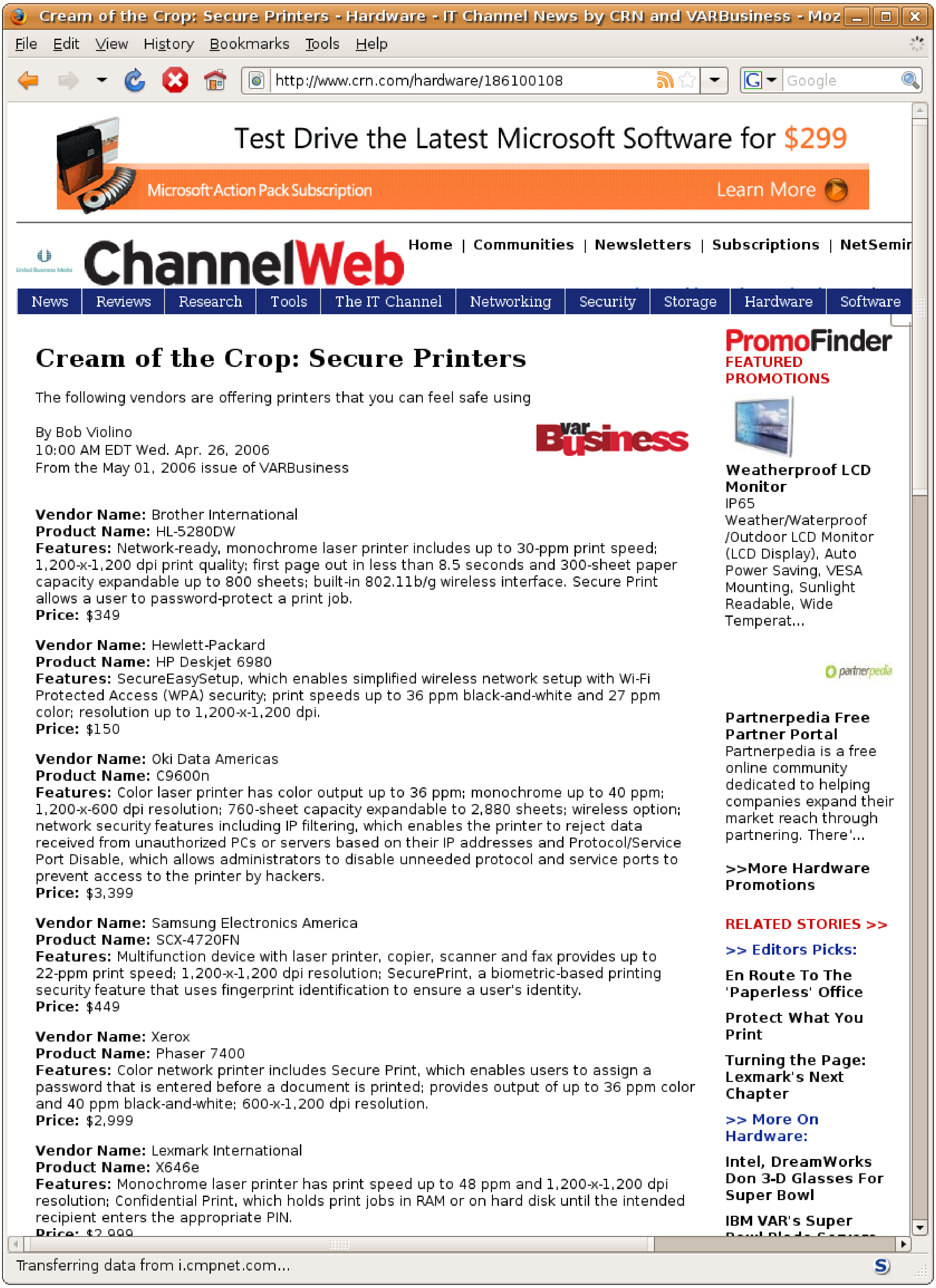
The reason for my writing this column is simple: I don't ever again want to see you, red-faced and panting, galloping frantically past the cubicles toward the copy room to retrieve that confidential document, only to find that someone already gathered it up with their own stuff. And how can we avoid this unsightly spectacle? By reading on to learn how to print securely when using a network printer, that's how.

See Also

- Cream of the Crop: Secure Printers

Microsoft highlights the benefits of using the Confidential/Secure Print feature to print sensitive Excel spreadsheets and other Microsoft Office files to shared Xerox and other printers [6]. This Microsoft article links to a list of "*which printers offer the best security*" which includes the corporate printers Xerox Phaser 7400 and the Lexmark X646e [7].

FEEL SAFE USING XEROX PHASER 7400 AND LEXMARK X646E ?


Cream of the Crop: Secure Printers - Hardware - IT Channel News by CRN and VARBusiness - Moz
File Edit View History Bookmarks Tools Help
http://www.crn.com/hardware/186100108
Google

ChannelWeb
Home | Communities | Newsletters | Subscriptions | NetSemir
News Reviews Research Tools The IT Channel Networking Security Storage Hardware Software

Cream of the Crop: Secure Printers

The following vendors are offering printers that you can feel safe using

By Bob Violino
10:00 AM EDT Wed. Apr. 26, 2006
From the May 01, 2006 issue of VARBusiness

Vendor Name: Brother International
Product Name: HL-5280DW
Features: Network-ready, monochrome laser printer includes up to 30-ppm print speed; 1,200-x-1,200 dpi print quality; first page out in less than 8.5 seconds and 300-sheet paper capacity expandable up to 800 sheets; built-in 802.11b/g wireless interface. Secure Print allows a user to password-protect a print job.
Price: $349

Vendor Name: Hewlett-Packard
Product Name: HP Deskjet 6980
Features: SecureEasySetup, which enables simplified wireless network setup with Wi-Fi Protected Access (WPA) security; print speeds up to 36 ppm black-and-white and 27 ppm color; resolution up to 1,200-x-1,200 dpi.
Price: $150

Vendor Name: Oki Data Americas
Product Name: C9600n
Features: Color laser printer has color output up to 36 ppm; monochrome up to 40 ppm; 1,200-x-600 dpi resolution; 760-sheet capacity expandable to 2,880 sheets; wireless option; network security features including IP filtering, which enables the printer to reject data received from unauthorized PCs or servers based on their IP addresses and Protocol/Service Port Disable, which allows administrators to disable unneeded protocol and service ports to prevent access to the printer by hackers.
Price: $3,399

Vendor Name: Samsung Electronics America
Product Name: SCX-4720FN
Features: Multifunction device with laser printer, copier, scanner and fax provides up to 22-ppm print speed; 1,200-x-1,200 dpi resolution; SecurePrint, a biometric-based printing security feature that uses fingerprint identification to ensure a user's identity.
Price: $449

Vendor Name: Xerox
Product Name: Phaser 7400
Features: Color network printer includes Secure Print, which enables users to assign a password that is entered before a document is printed; provides output of up to 36 ppm color and 40 ppm black-and-white; 600-x-1,200 dpi resolution.
Price: $2,999

Vendor Name: Lexmark International
Product Name: X646e
Features: Monochrome laser printer has print speed up to 48 ppm and 1,200-x-1,200 dpi resolution; Confidential Print, which holds print jobs in RAM or on hard disk until the intended recipient enters the appropriate PIN.
Price: $2,999

RELATED STORIES >>

>> Editors Picks:

En Route To The 'Paperless' Office

Protect What You Print

Turning the Page: Lexmark's Next Chapter

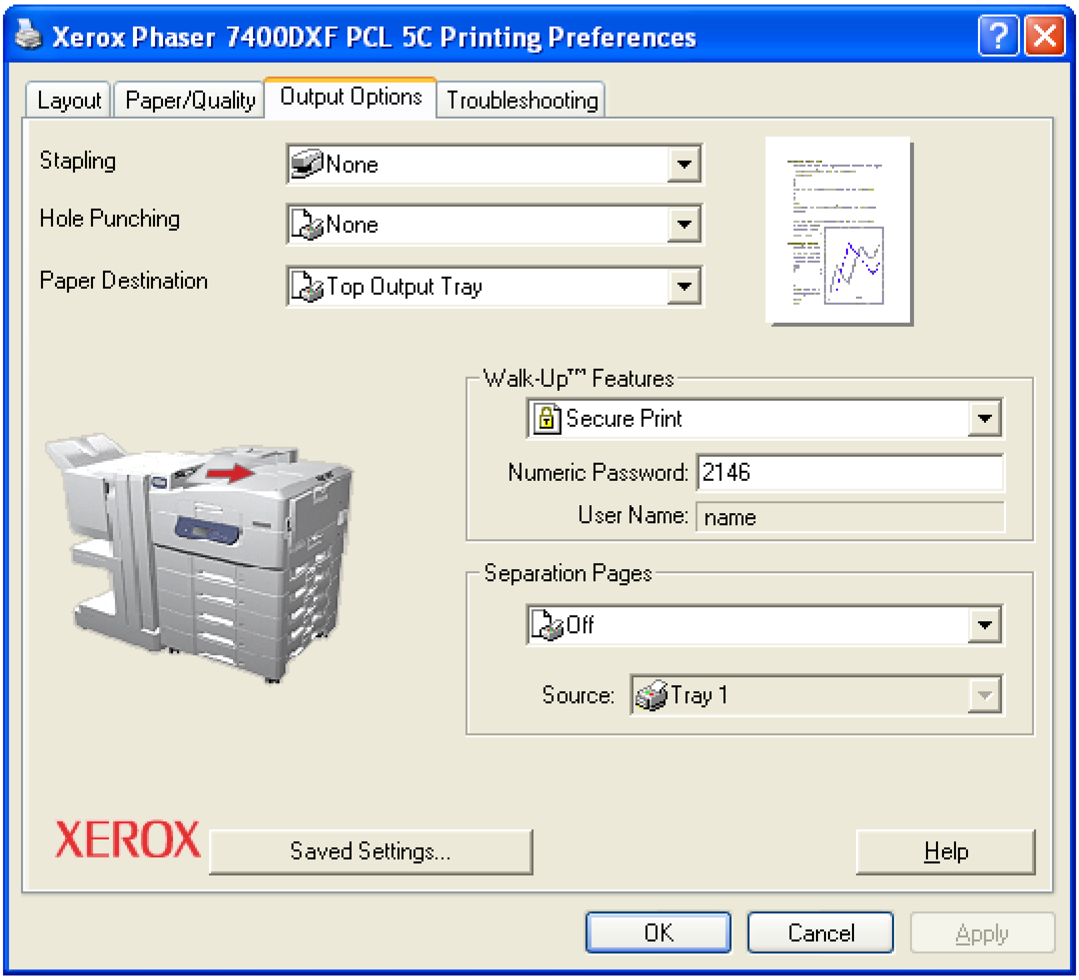
>> More On Hardware:

Intel, DreamWorks Don 3-D Glasses For Super Bowl

IBM VAR's Super

The Xerox Phaser 7400 and Lexmark X646e are listed as “*printers that you can feel safe using*”.

The following screenshots illustrate Excel spreadsheets storing the Confidential/Secure Print user PIN when the spreadsheets were printed and saved.



Xerox Phaser 7400DXF PCL 5C Printing Preferences

Stapling: None

Hole Punching: None

Paper Destination: Top Output Tray

Walk-Up™ Features: Secure Print

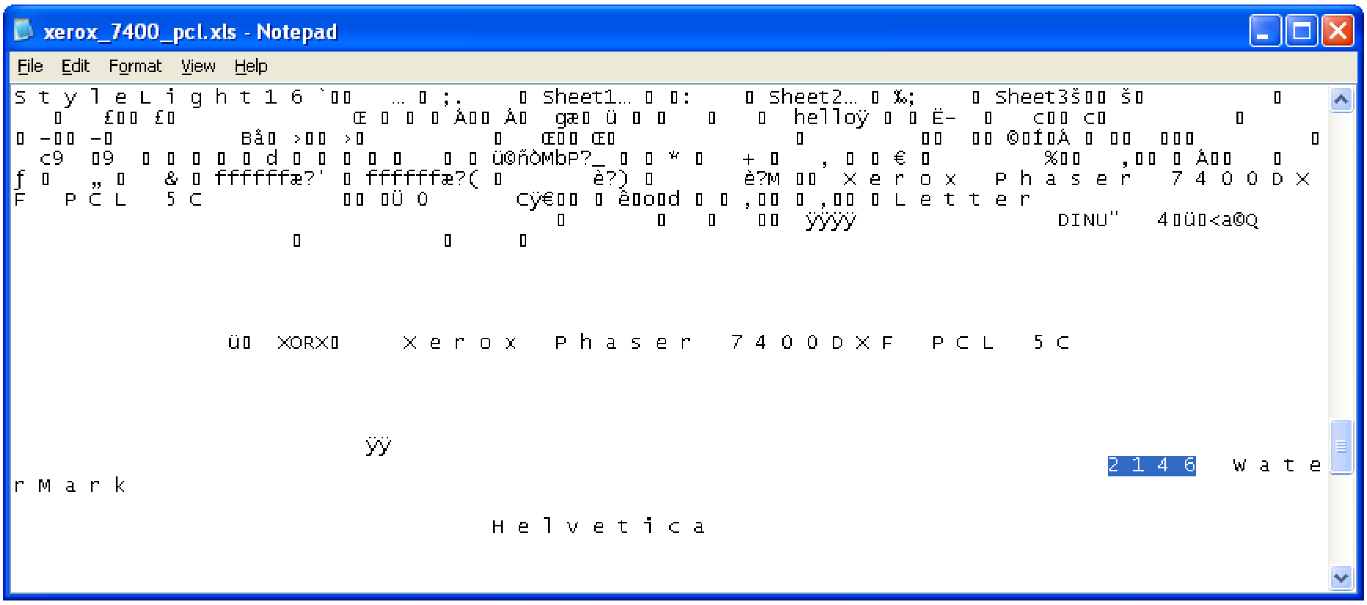
Numeric Password: 2146

User Name: name

Separation Pages: Off

Source: Tray 1

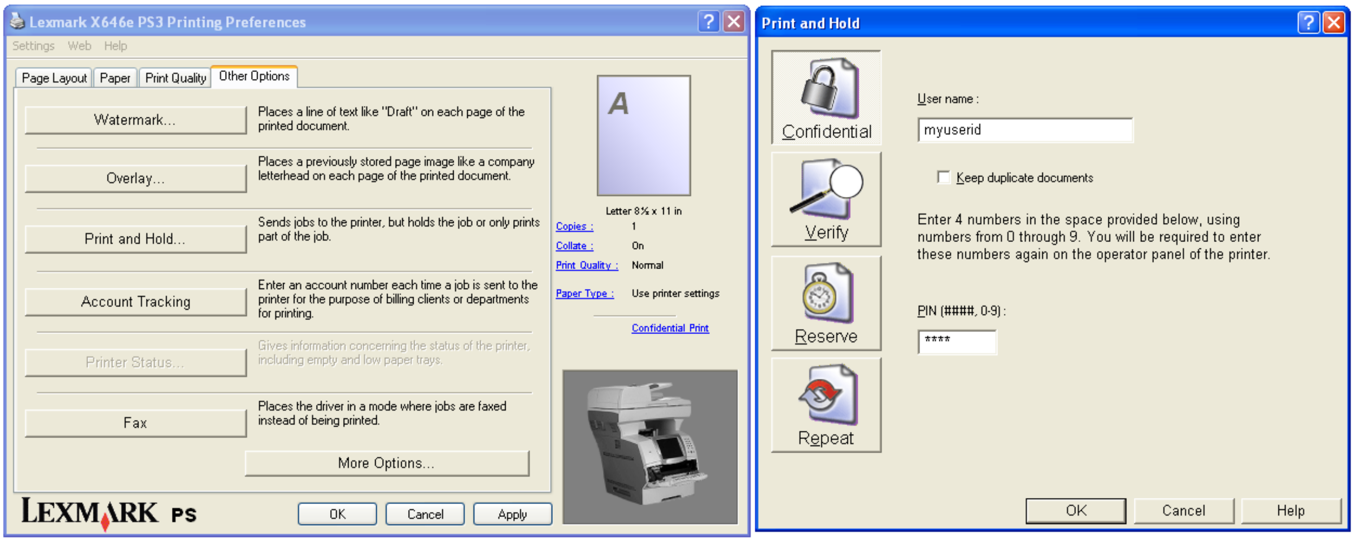
The Secure Print feature is configured with a PIN of 2146 using the latest Xerox Phaser 7400 Printer Command Language (PCL) printer driver from the Xerox web site as of 1 Feb 2009.



xerox_7400_pcl.xls - Notepad

```
S t y l e L i g h t 1 6 `▯▯   … ▯ ;.    ▯ Sheet1… ▯ ▯:    ▯ Sheet2… ▯ ‰;    ▯ Sheet3š▯▯ š▯         ▯
  ▯   £▯▯ £▯           Œ ▯ ▯ ▯ À▯▯ À▯  gæ▯ ü ▯ ▯   ▯   ▯ helloÿ ▯ ▯ Ë–  ▯   c▯▯ c▯        ▯
▯ –▯▯ –▯        Bå▯ ›▯▯ ›▯       ▯   Œ▯▯ Œ▯        ▯       ▯▯  ▯▯ ©▯Í▯À ▯ ▯▯  ▯▯▯          ▯
 c9  ▯9  ▯ ▯ ▯ ▯ ▯ d ▯ ▯ ▯ ▯ ▯   ▯ ▯ ü©ñÒMbP?_ ▯ ▯ * ▯  + ▯   , ▯ ▯ € ▯       %▯▯   ,▯▯ ▯ À▯▯   ▯
ƒ ▯  „ ▯  & ▯ ffffffæ?' ▯ ffffffæ?( ▯    è?) ▯    è?M ▯▯ X e r o x  P h a s e r  7 4 0 0 D X
F  P C L  5 C         ▯▯ ▯Ü 0     cÿ€▯▯ ▯ ê▯o▯d ▯ ▯ ,▯▯ ▯ ,▯▯ ▯ L e t t e r
                             ▯     ▯   ▯   ▯▯  ÿÿÿÿ            DINU"   4▯Ü▯<a©Q
                ▯          ▯    ▯




            ü▯  XORX▯    X e r o x  P h a s e r  7 4 0 0 D X F  P C L  5 C



                       ÿÿ
                                                                              2 1 4 6   W a t e
r M a r k

                                  H e l v e t i c a
```

The readily available Microsoft Notepad works as a substitute for a hex editor to reveal the user PIN of 2146, highlighted by the author of this document for the reader’s convenience.



Lexmark X646e PS3 Printing Preferences

Watermark...

Places a line of text like "Draft" on each page of the printed document.

Overlay...

Places a previously stored page image like a company letterhead on each page of the printed document.

Print and Hold...

Sends jobs to the printer, but holds the job or only prints part of the job.

Account Tracking

Enter an account number each time a job is sent to the printer for the purpose of billing clients or departments for printing.

Printer Status...

Gives information concerning the status of the printer, including empty and low paper trays.

Fax

Places the driver in a mode where jobs are faxed instead of being printed.

More Options...

Letter 8½ x 11 in

Copies : 1

Collate : On

Print Quality : Normal

Paper Type : Use printer settings

Confidential Print

Print and Hold

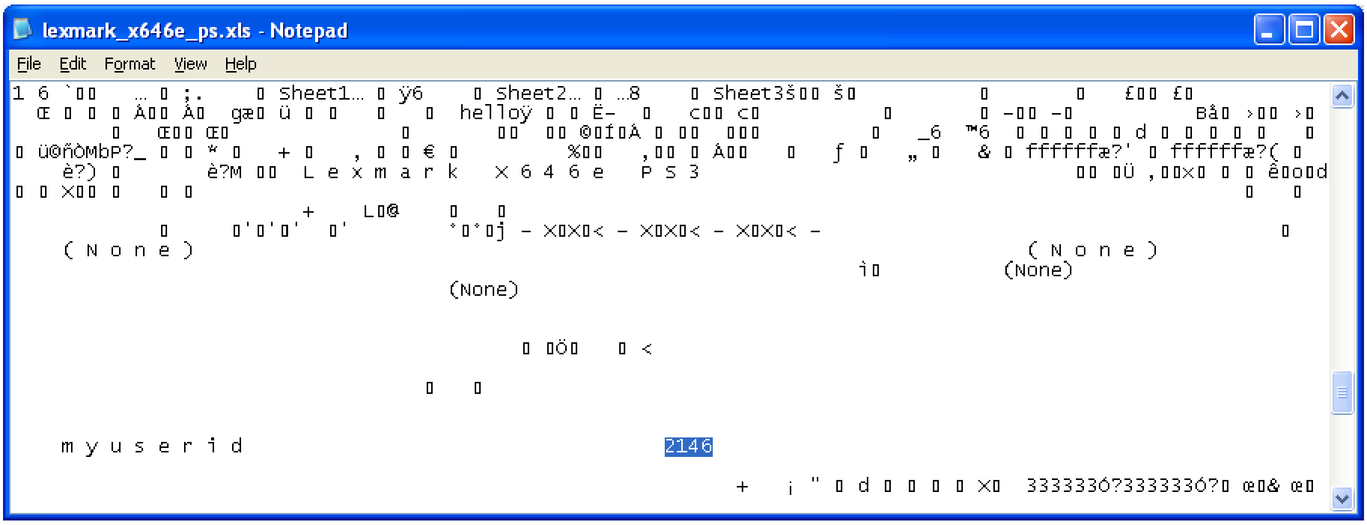
User name : myuserid

☐ Keep duplicate documents

Enter 4 numbers in the space provided below, using numbers from 0 through 9. You will be required to enter these numbers again on the operator panel of the printer.

PIN (####, 0-9) : ****

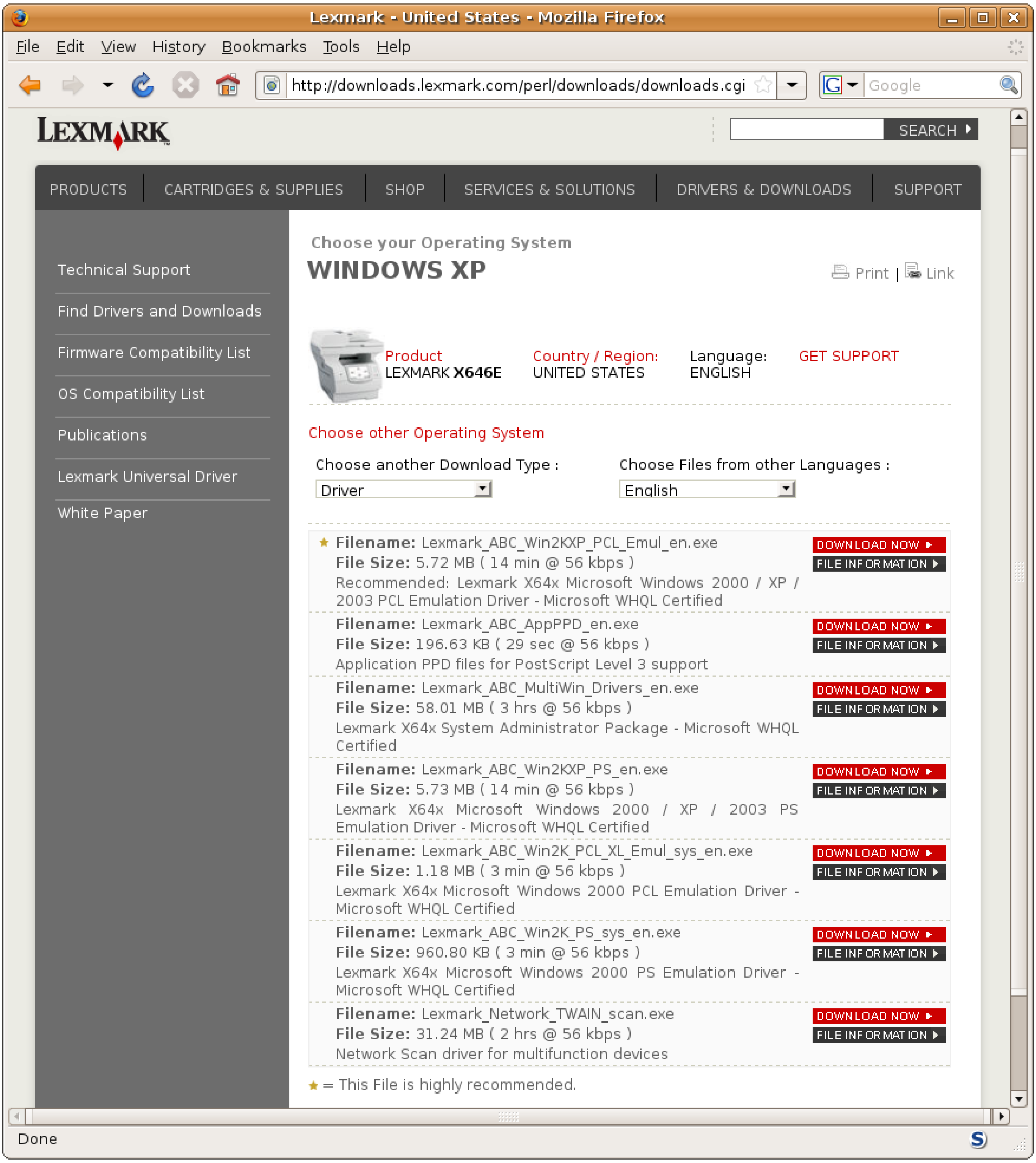
The Confidential Print feature is configured with a PIN of 2146 using the latest Lexmark X646e PostScript (PS) printer driver from the Lexmark web site as of 1 Feb 2009.



lexmark_x646e_ps.xls - Notepad

```
1 6 `▯▯    … ▯ ;.     ▯ Sheet1… ▯ ÿ6    ▯ Sheet2… ▯ …8    ▯ Sheet3šƒ▯ š▯          ▯        ▯    £▯▯ £▯
  Œ ▯ ▯ ▯ À▯▯ À▯  gæ▯ ü ▯ ▯    ▯    ▯  helloÿ ▯ ▯ Ë–   ▯    c▯▯ c▯          ▯              ▯ –▯▯ –▯          Bå▯ ›▯▯ ›▯
         ▯    Œ▯▯ Œ▯            ▯            ▯▯   ▯▯ ®▯Í▯À ▯ ▯▯  ▯▯▯         ▯    _6   ™6  ▯ ▯ ▯ ▯ ▯ d ▯ ▯ ▯ ▯ ▯    ▯
▯ ü@ñÒMbP?_ ▯ ▯ * ▯   + ▯   , ▯ ▯ € ▯       %▯▯   ,▯▯ ▯ À▯▯    ▯   ƒ ▯   „ ▯   & ▯ ffffffæ?' ▯ ffffffæ?( ▯
   è?) ▯      è?M ▯▯  L e x m a r k   X 6 4 6 e   P S 3                                 ▯▯ ▯Ü ,▯▯×▯ ▯ ▯ ê▯o▯d
▯ ▯ X▯▯ ▯    ▯ ▯                                                                                          ▯    ▯
                      +    L▯@      ▯    ▯
          ▯     ▯'▯'▯'  ▯'        ˆ▯ˆ▯j – X▯X▯< – X▯X▯< – X▯X▯< –                                        ▯
  ( N o n e )                                                                         ( N o n e )
                                                                           ì▯           (None)
                                    (None)

                                          ▯ ▯Ö▯    ▯ <

                                 ▯   ▯


  m y u s e r i d                                   2146

                                                       +   ¡ " ▯ d ▯ ▯ ▯ ▯ X▯   333333ó?333333ó?▯ œ▯& œ▯
```

After printing and saving an Excel spreadsheet, Notepad reveals the user PIN of 2146.



Choose your Operating System

WINDOWS XP

Product: LEXMARK **X646E**
Country / Region: UNITED STATES
Language: ENGLISH

Choose other Operating System

Choose another Download Type : Driver

Choose Files from other Languages : English

★ **Filename:** Lexmark_ABC_Win2KXP_PCL_Emul_en.exe
File Size: 5.72 MB (14 min @ 56 kbps)
Recommended: Lexmark X64x Microsoft Windows 2000 / XP / 2003 PCL Emulation Driver - Microsoft WHQL Certified
DOWNLOAD NOW ▸ FILE INFORMATION ▸

Filename: Lexmark_ABC_AppPPD_en.exe
File Size: 196.63 KB (29 sec @ 56 kbps)
Application PPD files for PostScript Level 3 support
DOWNLOAD NOW ▸ FILE INFORMATION ▸

Filename: Lexmark_ABC_MultiWin_Drivers_en.exe
File Size: 58.01 MB (3 hrs @ 56 kbps)
Lexmark X64x System Administrator Package - Microsoft WHQL Certified
DOWNLOAD NOW ▸ FILE INFORMATION ▸

Filename: Lexmark_ABC_Win2KXP_PS_en.exe
File Size: 5.73 MB (14 min @ 56 kbps)
Lexmark X64x Microsoft Windows 2000 / XP / 2003 PS Emulation Driver - Microsoft WHQL Certified
DOWNLOAD NOW ▸ FILE INFORMATION ▸

Filename: Lexmark_ABC_Win2K_PCL_XL_Emul_sys_en.exe
File Size: 1.18 MB (3 min @ 56 kbps)
Lexmark X64x Microsoft Windows 2000 PCL Emulation Driver - Microsoft WHQL Certified
DOWNLOAD NOW ▸ FILE INFORMATION ▸

Filename: Lexmark_ABC_Win2K_PS_sys_en.exe
File Size: 960.80 KB (3 min @ 56 kbps)
Lexmark X64x Microsoft Windows 2000 PS Emulation Driver - Microsoft WHQL Certified
DOWNLOAD NOW ▸ FILE INFORMATION ▸

Filename: Lexmark_Network_TWAIN_scan.exe
File Size: 31.24 MB (2 hrs @ 56 kbps)
Network Scan driver for multifunction devices
DOWNLOAD NOW ▸ FILE INFORMATION ▸

★ = This File is highly recommended.

The user PIN was visibly stored in Excel spreadsheets when using any of the four (two PS and two PCL) printer drivers, including when using the "*highly recommended*" PCL driver.

FEEL SAFER WITH UPDATED/UNIVERSAL PRINTER DRIVERS?

Some printer driver vendors are producing generic universal printer drivers which

"*provide users and administrators with a standardized, one-driver solution for their printing needs. Instead of installing and managing individual drivers for each printer model, administrators can install the Lexmark Universal Print Drivers for use with a variety of both mono and color laser printers. The Lexmark Universal Drivers are available in 19 languages, supporting more than 100 printer models*" [8].

Some of these newer printer drivers appear to use data compression or other mechanisms which have the side effect of avoiding storing the user PIN in the clear in Excel spreadsheets.

The author of this document will assume that this attempted mitigation is an accidental side effect. It is unlikely that the printer driver vendors were already aware of this Excel information disclosure vulnerability, otherwise (hopefully) they would have fixed or removed affected printer drivers from their web site and publicly informed their customers.

Lexmark deserve some kudos for their Oct 2008 version universal printer driver avoiding storing the user PIN in the clear in Excel spreadsheets. However, the following extracts from the Lexmark Universal Print Driver Technical White Paper [8] indicate that the updated and perhaps more secure universal printer driver is not designed to replace model-specific printer drivers

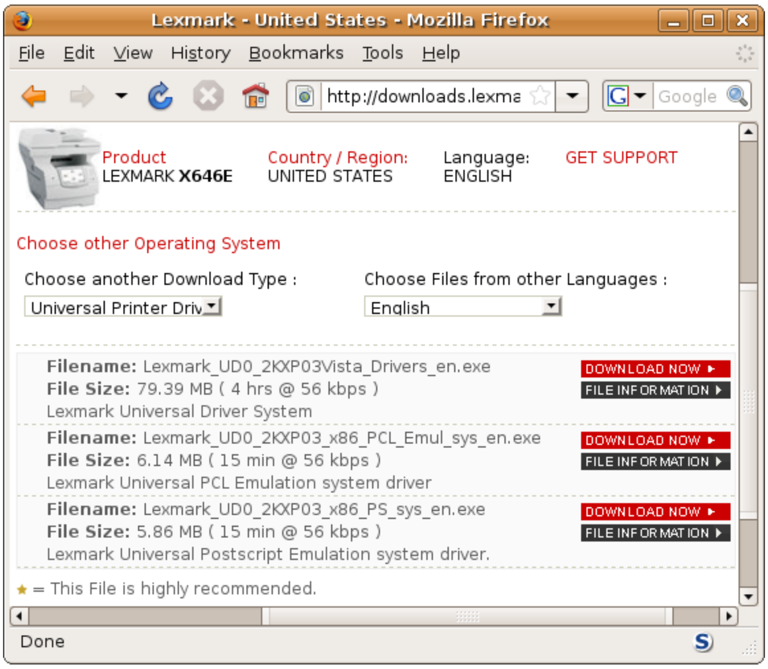
"Frequently asked questions

Will Lexmark stop providing model-specific drivers?

There are no plans for the Universal Print Drivers to replace model-specific drivers.

When should I use a model-specific print driver instead of the UPD?

Use a model-specific driver if you need a PCL-XL (PCL 6) emulation driver or if your printer is not in the list of supported printers. Use model-specific drivers if you need resolutions other than 600 dpi."



http://downloads.lexma

Product
LEXMARK **X646E**

Country / Region:
UNITED STATES

Language:
ENGLISH

Choose other Operating System

Choose another Download Type : Universal Printer Driv

Choose Files from other Languages : English

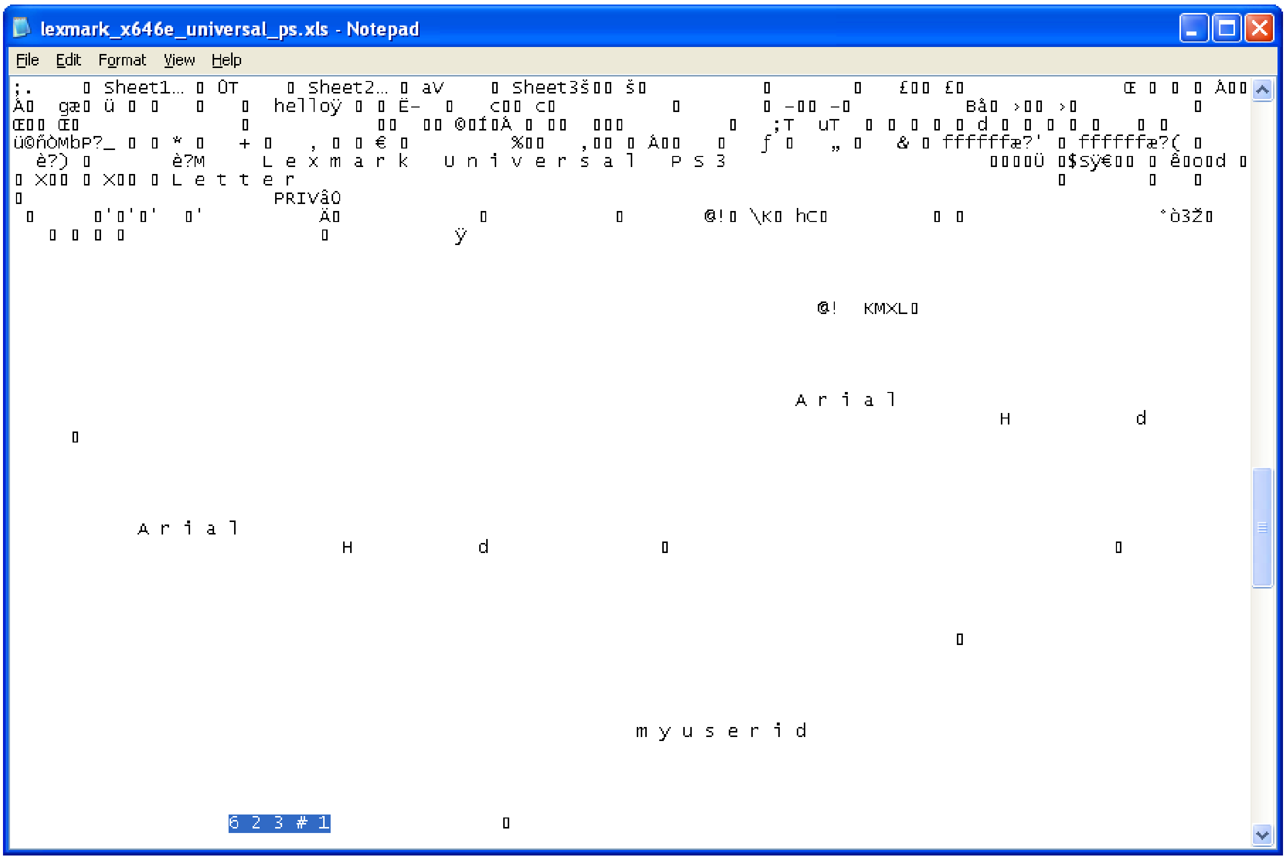
Filename: Lexmark_UD0_2KXP03Vista_Drivers_en.exe
File Size: 79.39 MB (4 hrs @ 56 kbps)
Lexmark Universal Driver System

Filename: Lexmark_UD0_2KXP03_x86_PCL_Emul_sys_en.exe
File Size: 6.14 MB (15 min @ 56 kbps)
Lexmark Universal PCL Emulation system driver

Filename: Lexmark_UD0_2KXP03_x86_PS_sys_en.exe
File Size: 5.86 MB (15 min @ 56 kbps)
Lexmark Universal Postscript Emulation system driver.

★ = This File is highly recommended.

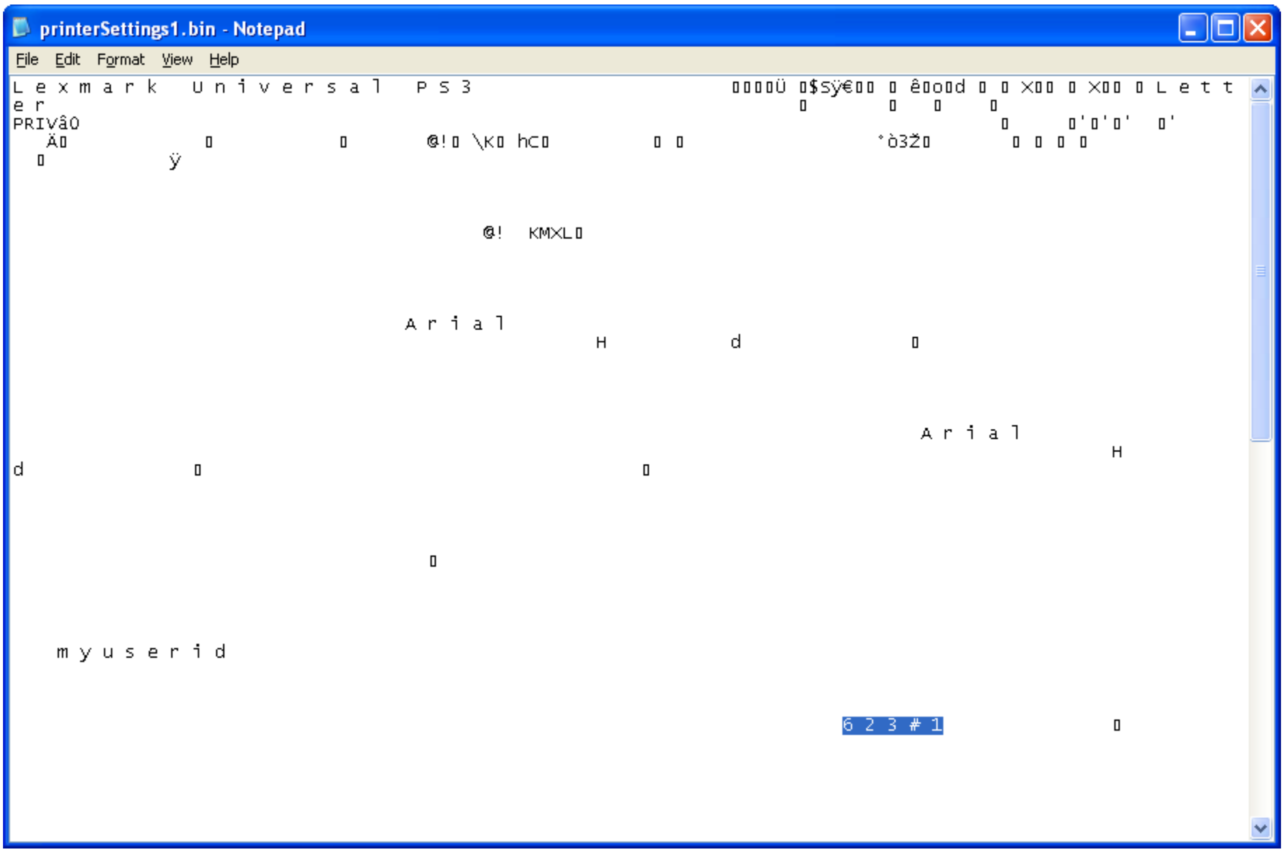
The universal printer driver version 1.3 released in Oct 2008 is available, although strangely the Lexmark web site recommends using the older model-specific X646e PCL printer driver instead.



lexmark_x646e_universal_ps.xls - Notepad

```
;.     ▯ Sheet1… ▯ ÒT     ▯ Sheet2… ▯ aV     ▯ Sheet3š▯▯ š▯        ▯        ▯    £▯▯ £▯              Œ ▯ ▯ ▯ À▯▯
À▯   gæ▯ ü ▯ ▯     ▯    ▯  helloÿ ▯ ▯ Ë-   ▯     c▯▯ c▯        ▯        ▯ -▯▯ -▯           Bå▯ ›▯▯ ›▯           ▯
Œ▯▯ Œ▯              ▯              ▯▯  ▯▯ ©▯í▯À ▯ ▯▯  ▯▯▯        ▯   ;T  uT  ▯ ▯ ▯ ▯ ▯ d ▯ ▯ ▯ ▯ ▯  ▯ ▯
ü©ñÒMbP?_ ▯ ▯ * ▯   + ▯   , ▯ ▯ € ▯         %▯▯   ,▯▯ ▯ À▯▯   ▯  ƒ ▯   „ ▯   & ▯ ffffffæ?' ▯ ffffffæ?( ▯
  è?) ▯      è?M     L e x m a r k   U n i v e r s a l   P S 3                 ▯▯▯▯Ü ▯$sÿ€▯▯ ▯ ê▯o▯d ▯
▯ X▯▯ ▯ X▯▯ ▯ L e t t e r                                                                   ▯       ▯   ▯
▯                      PRIVâ0
 ▯     ▯'▯'▯'  ▯'          Ä▯           ▯           ▯       @!▯ \K▯ hC▯        ▯ ▯               ˚ò3Ž▯
   ▯ ▯ ▯ ▯                 ▯           ÿ

                                                                             @!  KMXL▯

                                                                           A r i a l
                                                                                          H          d
   ▯

          A r i a l
                         H          d             ▯                                  ▯

                                                                                    ▯

                                                     m y u s e r i d

                  6 2 3 # 1           ▯
```

Kudos to Lexmark's proactive security by applying (basic) mathematical obfuscation to store the user PIN as 623#1 instead of 2146.



printerSettings1.bin - Notepad

```
L e x m a r k   U n i v e r s a l   P S 3                 ▯▯▯▯Ü ▯$sÿ€▯▯ ▯ ê▯o▯d ▯ ▯ X▯▯ ▯ X▯▯ ▯ L e t t
e r                                                            ▯       ▯   ▯    ▯
PRIVâ0                                                                                  ▯    ▯'▯'▯'  ▯'
   Ä▯           ▯           ▯       @!▯ \K▯ hC▯        ▯ ▯               ˚ò3Ž▯       ▯ ▯ ▯ ▯
  ▯           ÿ

                                        @!  KMXL▯

                                  A r i a l
                                                 H          d             ▯

                                                                                      A r i a l
d              ▯                                   ▯                                                 H

                                     ▯

   m y u s e r i d

                                                                                  6 2 3 # 1           ▯
```

The Open XML 2007 .xlsx format also appears to store private device specific information such as the user PIN. After printing and saving a spreadsheet in this format, the (slightly obfuscated) user PIN was stored in the *printerSettings1.bin* file inside the .xlsx container.

POTENTIAL MITIGATION

In the absence of Microsoft changing the Excel file format specification which has been in use for over 12 years, or modifying the Excel executable to store blank spaces instead of private data in the spreadsheet, the following steps can help mitigate exploitation of this information disclosure vulnerability:

- Printer driver vendors could update their printer drivers to ensure the user PIN is not stored in the clear in Excel spreadsheets.
- Users should ensure they are using a recent printer driver which does not store the user PIN in the clear in Excel spreadsheets. This may mean using a recently produced universal printer driver, since printer driver manufacturers are unlikely to fix all of their hundreds or thousands of printer drivers (and perhaps associated printer firmware).
- Users could manually disable the Confidential/Secure Print feature when working on Excel spreadsheets which other users have access to. However, this mitigation step would involve effort and consistent discipline since the Confidential/Secure Print feature is enabled at the printer driver level to conveniently and automatically apply the user PIN protection to all files printed by the user.
- Users could attempt to justify acquiring a printer to be located in their line of sight, or otherwise run to the printer as soon as they print a sensitive file.
- Users should be suspicious if they are certain they printed their file, yet when they arrive at the printer, the printer is not waiting for the user to enter their PIN. Perhaps somebody else entered the PIN and printed the file. Note however that these symptoms may occur legitimately since
  "*Jobs stored in the MFP's RAM memory will be deleted if the MFP is powered off, and can be deleted automatically by the MFP if a memory shortage is encountered.*" [5]
- Users should be suspicious if they printed their file, yet when they arrive at the printer, their printout is already sitting on the printer without requiring the user to enter their PIN. Perhaps somebody else entered the PIN, printed and photocopied the file, or selected "*2 copies*" and kept one copy for themselves and left the other copy on the printer.

VENDOR CONTACT

Relevant vendors were contacted prior to the public release of this document, as per the principles of responsible and coordinated disclosure. Since this document mentions Microsoft, Lexmark and Xerox, they were initially contacted to confirm the technical accuracy of this document, with subsequent attempts to contact other printer driver vendors.

This document was provided to the Microsoft Security Response Center in April 2009. Microsoft agreed that this is an information disclosure vulnerability, and after spending many months investigating and contemplating remediation options, eventually concluded that "*the best way to address this issue is through documentation, and suitable changes to the WHQL (Windows Hardware Quality Labs) logo program that help foster a conscious decision on the side of the driver manufacturer, with respect to the nature of information they store in the DEVMODE.*"

This document was provided to Lexmark for comment in September 2010. Lexmark responded in a timely and positive manner. Lexmark engaged in a constructive dialogue, expressed appreciation for the opportunity to review this document and stated "*It is a well written and informative piece of work*".

Lexmark noted the steps they have already proactively taken to help mitigate this information disclosure vulnerability, including masking the user PIN, and mentioned their plan to further enhance this masking feature for both device specific printer drivers as well as for future versions of their Universal Print Driver.

For users requiring increased levels of printing security, Lexmark noted their variety of Print Protection capabilities, ranging from additional layers of authentication such as card readers, to full encryption of the data stream between the host computer and the printing device using features such as Lexmark's IPsec and PrintCryption capabilities discussed in more detail at the web page

http://www1.lexmark.com/content/en_us/solutions/business_solutions/security/standard_security_features.shtml

This document was provided to Xerox for comment in September 2010. Xerox expressed appreciation for being informed about this new information disclosure vulnerability.

Xerox confirmed the flaw in a number of older printer drivers, and recommended that customers should download and install newer printer drivers such as the Global Print Driver and the Mobile Express Driver available at the web pages

http://www.support.xerox.com/go/results.asp?Xtype=download&prodID=GLOBALPRINTDRIVER&Xlang=en_US&Xcntry=USA

http://www.support.xerox.com/go/results.asp?Xtype=download&prodID=MOBILEEXPRESSDRIVER&Xlang=en_US&Xcntry=USA

For users requiring increased levels of printing security, Xerox noted their more secure methods to prevent the exposure of printed information, including techniques such as strong encryption, tokens and authentication. Xerox noted that features like this are already shipping in their advanced multifunction devices and will be incorporated into more Xerox devices over time.

This document was provided to US-CERT and CERT/CC in October 2010 for them to liaise with printer driver vendors prior to public release of this document. CERT/CC replied that "*due to our current case load we will not be able to follow up with the coordination at this time. Please continue to work with affected vendors before disclosing the details to the public.*" Therefore, as per the principles of responsible and coordinated disclosure, the author of this document attempted to perform coordination by sending a copy of this document on 13 November 2010 to readily available email addresses at the following readily available list of printer vendors: Brother, Canon, Epson, HP, Konica Minolta, Kyocera, Oki, Ricoh and Samsung. Some of these vendors did not disclose readily available email addresses, so a copy of this document was sent to the following email addresses for all of these vendors: secure@, security@ and postmaster@ These vendors were also notified that this document would be publicly released on 15 January 2011 (or beforehand if publicly leaked).

HP should be applauded for taking security seriously enough to have established a dedicated and contactable security team. The HP Software Security Response Team replied quickly with the statement "*Thanks for the advance notice. We can find no HP printers that are vulnerable.*"

REFERENCES

[1] Title: Microsoft Office Binary (doc, xls, ppt) File Formats
Publication Date: 15 Feb 2008
URL: http://www.microsoft.com/interop/docs/OfficeBinaryFormats.mspx
Access Date: 1 Feb 2009

[2] Title: Microsoft Office Excel 97-2007 Binary File Format (.xls) Specification
URL: http://download.microsoft.com/download/0/B/E/0BE8BDD7-E5E8-422A-ABFD-4342ED7AD886/Excel97-2007BinaryFileFormat(xls)Specification.pdf
Access Date: 1 Feb 2009

[3] Title: DEVMODE
URL: http://msdn.microsoft.com/en-us/library/aa927408.aspx
Access Date: 1 Feb 2009

[4] Title: Xerox Product Security for Information Security and Document Control
URL: http://www.xerox.com/information-security/product-security/enus.html
Access Date: 1 Feb 2009

[5] Title: Security and Lexmark Multifunction Products: Overview of Features
Author: Rich Russell
Publication Date: Feb 2006
URL: http://www.lexmark.com/vgn/images/portal/Security%20Features%20of%20Lexmark%20MFPs%20v1_1.pdf
Access Date: 1 Feb 2009

[6] Title: Secure printing: No more mad dashes to the copy room
Author: Annik Stahl
Publication Date: 21 Nov 2008
URL: http://office.microsoft.com/en-us/help/HA012276311033.aspx
Access Date: 1 Feb 2009

[7] Title: Cream of the Crop: Secure Printers
Author: Bob Violino
Publication Date: 26 Apr 2006
URL: http://www.crn.com/hardware/186100108
Access Date: 1 Feb 2009

[8] Title: Universal Print Driver Technical White Paper
Publication Date: Dec 2008 (according to metadata)
URL: http://www.downloaddelivery.com/downloads/documentation/Lexmark-Universal-Driver-v1.3-White-Paper.pdf
Access Date: 1 Feb 2009