Investigating Machine Identification Code Technology in Color Laser Printers

Note: *As of October 13th, 2005, some information in this paper is out of date. Please visit http://eff.org/Privacy/printers for the most up-to-date information on this project.*

Introduction

On Nov. 22, 2004, PC World published an article stating that "several printer companies quietly encode the serial number and the manufacturing code of their color laser printers and color copiers on every document those machines produce. Governments, including the United States, already use the hidden markings to track counterfeiters." According to the article, the high fidelity of outputs from color machines to their original documents suggests that counterfeiters can potentially succeed in creating high-quality counterfeited currency and government documents using these machines. At the request of the United States Secret Service, manufacturers developed mechanisms that print in an encoded form the serial number and the manufacturer's name as indiscernible markings on color documents. The Secret Service and manufacturers would be able to decode these values from the markings and in the event a color machine was used to print a suspected counterfeited document, these values would be used with customer information to discover the identity of the machine's owner.

The U.S. government is not the only national government using the marking technology to deter counterfeiting activities. An Oct. 26, 2004, PC World article entitled "Dutch Track Counterfeits Via Printer Serial Numbers" explained that Dutch railway law enforcement officials were employing this same technology to investigate a large-scale railway ticket counterfeiting operation. According to the article, since information about a user is not encoded into the arrangement of markings, law enforcement agencies work with manufacturers to obtain the identities of the persons to whom the printers were sold. In a typical scenario, when distributors sell printers, they obtain information about the purchaser, which is maintained in a database. The purchaser's identity is then associated with the serial number and the manufacturer's name of the machine. A document whose author a governmental agency wants to discover contains only the serial number and the manufacturer's name of the machine on which it was printed, so upon extracting this information from a document, it must consult the distributor responsible for selling the machine. The distributor performs a database query to match the serial number with a purchaser; manufacturers can also do searches if they have access to the database.

Motivations

In the PC World article, manufacturers and the Secret Service claim that the marking technology was developed to deter counterfeiting activities using color machines. While they may actually use it for legitimate anticounterfeiting purposes, currently no law prevents them from exploiting the technology in ways that could infringe on the privacy and anonymity of Americans. This means that we have no way to require them to adhere to these purposes or even verify that they are the only purposes. We also have no way of knowing whether the Secret Service is the only governmental agency using this technology.

Enter search terms
Search EFF

Contents

EFF in the News
miniLinks
Pioneer Awards
EFF Victories
EFF White Papers

EFFector

Subscribe to EFFector!
[our free email newsletter]

Email:

Zip / Postal Code
(*optional*)

Subscribe!

» EFFector Archive

Topics

Anonymity
Biometrics
Bloggers' Rights
Broadcast Flag
CALEA
CAPPS II
Censorship
Copyright Law
Digital Rights Management
DMCA
Domain names

The possible misuses of this marking technology are frightening--individuals using printers to create political pamphlets, organize legal protest activities, or even discuss private medical conditions or sensitive personal topics can be identified by the government with no legal process, no judicial oversight, and no notice to the person spied upon. If the Secret Service or any other governmental body wanted to identify the author of an anonymously printed political pamphlet, it could use the markings on the document to at least determine the serial number and the manufacturer of the machine on which it was printed. Then, with the cooperation of distributors and manufacturers, it could identify who purchased the machine. We do not even know if the government actually needs to consult manufacturers each time it seeks to identify document authors; it could obtain a complete customer database from the manufacturer and simply access the specific information on its own for any purpose it chooses.

Xerox senior research fellow Peter Crean has informed us that each document identification request that Xerox's security department receives from the Secret Service is handled on a case-by-case basis, that Xerox identifies only suspected currency documents, and that identification of machines used to print pamphlets, letters, and other non-currency documents does not occur. If true, these statements are somewhat comforting, but a clear risk remains due to the absence of legislation regulating the use of the marking technology. Color printers are regularly used for anonymous printing and pamphleteering; they are an important tool of speech. Without appropriate legal protections against the misuse of identifying technologies, these long-protected forms of expression may be in danger, as the government has easy and secret ways to identify the authors, or at least the printer purchaser, of any speech printed on color printers.

Furthermore, what assurance does an author have that foreign governments, or even private entities, are not also using or misusing these marking technologies to identify speakers? We're aware of no laws regulating the distribution or reuse of information obtained through the use of marking technologies and customer databases. The Secret Service could share with foreign governments knowledge about interpreting the markings, which would mean that they could identify color documents printed in the United States. Similarly, no law prevents individuals or organizations from using this technology for their own purposes, which means that malicious parties who understand how it works can misuse it.

It is especially worrisome that the Secret Service was able to coordinate with private-sector manufacturers on the development of this technology since at least the early 1990s with no public awareness, much less public discussion, of the privacy and anonymity risks for users of this technology. This raises the general concern that the U.S. government might have promoted the development of identification mechanisms in other devices and might do so in the future with new technologies. The marking technology is possibly one of many instances of the federal government's unwillingness to be forthright with questionable law enforcement techniques. In addition to the serious privacy concerns, we must consider the implications of the government's possible lack of accountability to the public on matters affecting technology use and development.

Through this project, we want to inform current and prospective color laser printer owners, purchasers, and users of this potential privacy risk so that they can make educated consumer decisions. It does not necessarily follow from the presentation of this material that members of the general public should never use color laser printers containing marking technology. We recognize that some consumers, upon being informed, will still choose to use these machines; such a decision is within their discretion. We simply want to ensure that current and prospective owners, purchasers, and users of these machines know that they can be identified using this technology and consider the potential risks. We also want to continue to gather information to make this technology better understood over time.

E-voting
File-sharing
Filtering
FTAA
Intellectual Property
International
Internet governance
ISP legalities
Licensing/UCITA
Linking
Patents
Pending legislation
Privacy
Public records/FOIA
Reverse engineering
RFID
Spam
States
Surveillance
USA PATRIOT Act
Wireless
WIPO

EFF en Español

Recursos e información de EFF en Español

Methodology

We visited numerous local print stores and printed eight speciallydesigned 8.5" by 11" test sheets, each with a resolution of 600 dpi (see right for two of these test sheets). We initially examined the printed test sheets using a Digital Blue QX5 computer light microscope, but later determined that a blue LED flashlight and a magnifying glass were sufficient to detect the markings, confirming the efficacy of the technique suggested by Xerox senior research fellow Peter Crean.

Upon detecting markings on a test sheet, we attempted to describe their arrangement. With Xerox documents, the markings consisted of minuscule yellow dots positioned within a 0.5" by 1.0" rectangular space. The arrangement of dots was repeatedly printed over the entire printed side. These dots were transcribed onto paper and text files. We wrote simple Linux shell scripts and C programs to analyze the arrangements.

With Canon documents, the markings also consisted of tiny yellow dots. However, they were not arranged within a rectangular space, which made analyzing them more challenging. As of this writing, we haven't developed a protocol for analyzing Canon markings, which may require an interpreting scheme different from the one needed to interpret Xerox's. There may be multiple marking systems in use by different manufacturers or in connection with different generations of color printing technology.

Results

Here are images of yellow tracking dots printed by Canon and Xerox printers:

Printed side of test01 sheet
Machine: Canon Color imageRUNNER C3200. Magnified: 60 times.

Unprinted side of test01 sheet
Machine: Canon Color imageRUNNER C3200. Magnified: 60 times.

Printed side of test01 sheet
Machine: Xerox DocuColor 12. Magnified: 60 times.

Yellow dots on blue color box background, test07
Machine: Xerox DocuColor 12. Magnfied: 60 times.

Yellow dots on edge of test09 sheet with blue LED light
Machine: Xerox DocuColor 12. Magnified: 10 times.

Yellow dots on test07 sheet
Machine: Xerox DocuColor 12. Magnified: 60 times.

Below is a list of transcribed dot patterns for Xerox printers in text file format. Pattern pXY refers to the pattern found on test sheet testXY, pattern pXY1_XY2 refers to the shared pattern found on test sheets testXY1 and testXY2, and pattern pXY1-XY2 refers to the shared pattern found on test sheets testXY1 to XY2, inclusive.

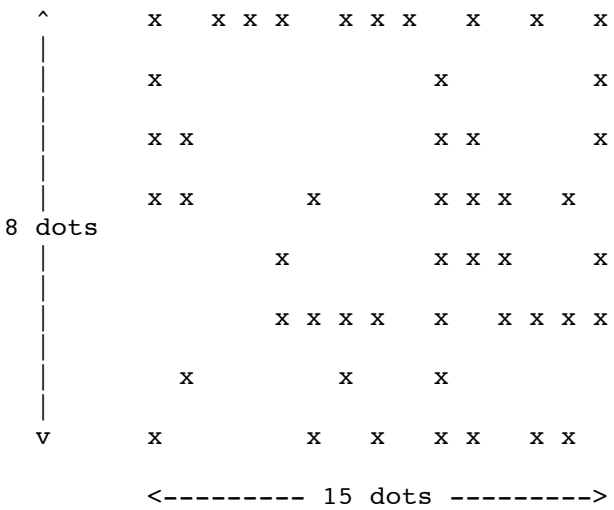
Aftering unzipping these files, use WordPad or another text editor to examine them.

1. DocuColor 12 (FedEx Kinko's, 201 Sacramento Street, San Francisco, CA)
2. DocuColor 12 (FedEx Kinko's, 303 2nd Street, San Francisco, CA)
3. DocuColor 12 (FedEx Kinko's, 369 Pine Street)
4. DocuColor 40 (Let Us! Copy, 565 Commercial Street, San Francisco, CA)
5. DocuColor 2045 (FedEx Kinko's, 369 Pine Street, San Francisco, CA)

6. DocuColor 6060 (FedEx Kinko's, 201 Sacramento Street, San Francisco, CA)
7. DocuColor 6060 (FedEx Kinko's, 1800 Van Ness Avenue, San Francisco, CA)

Analysis

For Xerox documents, within the 0.5" by 1" rectangular space, 8 x 15 = 120 locations exist for printers to print yellow tracking dots. Consider the following pattern found on test00-template, printed on a Xerox DocuColor 12 located at FedEx Kinko's, 201 Sacramento Street, San Francisco, CA.



We hypothesized that the patterns should be interpreted as binary values of fifteen bytes, where one byte was eight bits long and the more significant bits were written near the top of the pattern. We further postulated that the presence of a yellow tracking dot was equivalent to a "1" and the absence thereof was equivalent to a "0." We used shell scripts to translate these binary values into hexadecimal numbers, reading each column from top to bottom as a byte and taking columns in order from left to right. Below are the fifteen hexadecimal representations generated for the above Xerox DocuColor 12 pattern:

```
F1 32 80 80 8C 15 86 85 80 7F B9 1C 85 15 EC
```

It is difficult to discover their significance without printer information such as a serial number. These values could be encrypted, which could thwart analysis. When we obtain more data, including the serial numbers of machines, we look forward to determining the meaning of the bit fields in this pattern. Our analysis could be enhanced when we obtain the serial numbers of color machines.

List of Printers

Click here for an updated list of printers which do or not print tracking dots

FOIA Request

EFF is also trying to discover information on this subject through a Freedom of Information Act (FOIA) request [PDF] to the United States Secret Service.

Conclusions

Our project's work confirms that one form of marking technology is being used in color laser printers. There could certainly be other forms of marking involved. Consumers can easily test whether printers are printing yellow tracking dots on their documents by flashing a blue LED

light onto the white parts of their document. If numerous black dots appear (yellow becomes black under a blue LED light) with a semblance of structure, it is likely that the document contains tracking dots.

What You Can Do to Help EFF

We always appreciate the help of our members and supporters. You can help us make further progress with this project. Ask manufacturers of color laser printers and color photocopiers to disclose information on this technology and to explain why it is not publicized or brought to the consumer's attention at the point of sale.

You can also help us through a more hands-on approach. If you own, operate, or have legitimate access to color laser printers or color photocopiers, please print the eight test sheets provided below on each of the machines to which you have access and send them to EFF (see address below). If there are printing stores near where you live or work, please print the eight test sheets there and send them to us. Please also print a configuration page, which will tell us information about the printer. If you cannot obtain a configuration page, please obtain the name of the manufacturer, the model type, and, if you can, the serial number. Unfortunately, EFF cannot reimburse costs incurred in printing these documents. In the event that all eight test sheets cannot be printed, please try to print as many as you can. Please print or request printing of these test sheets on normal laser printer paper and in consecutive order based on their filenames' numbering. If you plan to send us more than one machine's test sheets, please keep them separated (preferably in folders) to prevent data mixing.

Please include this information form (PDF) within each folder, to help EFF identify whence the test sheets came.

Test sheets printed in foreign countries are welcome. Please send test sheets until Nov. 1, 2005.

Test sheets:

Use either the .pdf or the .png versions of each - no need to print both.
You can also download a compressed file [tar.gz, 8.7M] of all the sheets.

1. test00-template.pdf (1M) | test00-template.png (246K)
2. test01-eff_white.pdf (1.6M) | test01-eff_white.png (377K)
3. test02-eff_blue.pdf (1.6M) | test02-eff_blue.png (1.6M)
4. test03-black_square.pdf (1.1M) | test03-black_square.png (264K)
5. test04-blue_square.pdf (1.1M) | test04-blue_square.png (264K)
6. test05-pale_green_square_008857.pdf (1.1MB) | test05-pale_green_square_008857.png (295K)
7. test06-text.pdf (3.3M) | test06-text.png (918K)
8. test07-checkerboard.pdf (1.1M) | test07-checkerboard.png (354K)

Send test sheets to:

Electronic Frontier Foundation
Machine Identification Code Technology Project
454 Shotwell Street
San Francisco, CA 94110-1914
U.S.A.

References

De Vries, Wilbert. "Dutch Track Counterfeits Via Printer Serial Numbers." *PC World*. Published 26 Oct. 2004, accessed 06 Jun. 2005. http://www.pcworld.idg.com.au/index.php/id;1002274598

Katzenbeisser, Stefan, and Fabien A.P. Petitcolas, eds. *Information Hiding Techniques for Steganography and Digital Watermarking*. Boston: Artech House, 2000.

Tuohey, Jason. "Government Uses Color Laser Printer Technology to Track Documents." *PC World*. Published 22 Nov. 2004, accessed 06 Jun. 2005. http://www.pcworld.com/news/article/0,aid,118664,00.asp