Security for Printing Data and Printed Materials

Yoshitaka Nishiyama Nobuyuki Yokoyama
Kunio Kanai Taisuke Watanabe

Interest in security functions for electronic data and a communication protocol, as well as for preventing information leaks, has been rising in recent years due to a rapid increase in the number of devices connected to networks represented by broadband connections to the Internet, an epidemic propagation of computer viruses and also legal systems relating to the protection of personal information in various countries (refer to Reference Document 1).

Theft of hard disks from printing devices, such as printers, MFPs[*1)] and copy machines in which printing data is stored, or unauthorized persons sneaking a glance at material during printing or even stealing printed materials from these devices, is becoming an issue of concern with regards to the leaking of information. For this reason, there is demand for security functions to be provided through such information leaking preventative measures as encryption of data stored on printing devices or the clearing of such data by overwriting it, as well as the superimposition of a user ID and printing device information onto printed materials.

This paper will introduce the functions of encrypted authenticated printing, disk clearing and the forced printing of logon information available with printers in order to prevent information leaks.

Encrypted Authenticated Printing Function

The encrypted authenticated printing function described in this chapter is an effective strategy against information leaks and the tampering of printed data, which can occur through the interception of printing data transmitted from personal computers to printers during printing, as well as the theft of printed materials.

(1) Security threats and countermeasures during printing

Security threats, such as the tampering of printing data or the leaking of confidential information as shown in **Figure 1**, are generally present when shared printers are connected to a network for printing documents that include confidential information, which should not be disclosed to third parties. For this reason it is necessary to ensure that the contents are indecipherable to any third parties if the printing data is intercepted (interception countermeasures), as well as to verify whether the printing data has been tampered with or not (tampering countermeasures). Furthermore, it is also necessary to ensure that printed materials are not accessible to third parties (printed matter sneak glancing and theft countermeasures).

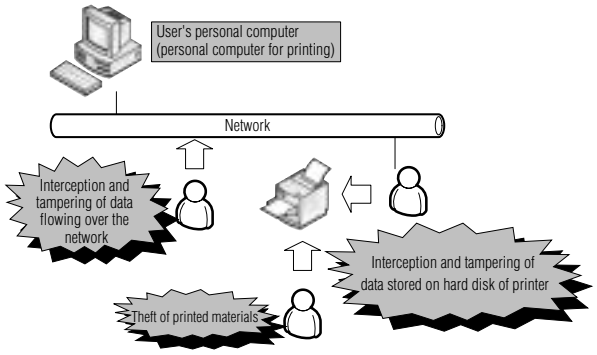

Fig. 1 Security threats during printing

Printers are equipped with the functions described below for the purpose of implementing such security strategies:

- Encrypting printing data as an interception countermeasure
- Addition and verification of Message Authentication Code (MAC) as a tampering countermeasure
- Authenticated printing using a password as a countermeasure against sneak views and theft of printed materials

More detailed descriptions of these three security functions are provided below.

Printing data is encrypted to ensure that the contents cannot be deciphered, even when the printing data being transmitted over a network or stored on a hard disk built into a printer is seen by a third party. Encryption is performed through the personal computer of the user who is transmitting the printing data. The encryption algorithm adopted for this purpose is the Advanced Encryption Standard (AES), a common key encryption system. With this an encryption key is generated based on the password entered by the user. The method used for generating the key is in accordance with the Public Key Cryptography Standard #5 (PKCS#5), which is an encryption standard. Refer to Reference Document 2 for details regarding this matter.

MAC is a hash value calculated from the aforementioned encryption key and the encrypted authenticated printing data. It is not possible to calculate

*1) MFP: An abbreviation used for multi-functional devices (multi-function products, printers or peripherals), which have at least two scanning, printing, faxing or copying functions.

the MAC that corresponds to data for which the encryption key is unknown. The MAC is calculated on the personal computer of the user and transmitted to the printer when printing. To detect any tampering of the printing data the printer calculates the MAC based on the encrypted printing data and verifies the value against the MAC value transmitted by the personal computer to see if they match. If the MAC values match then it is determined that no tampering of data has taken place.

Authenticated printing is a function with which printing is performed only when the password of the printing data matches the password entered by the user on the operation panel of the printer. Printing data transmitted from personal computers of users are initially stored on the hard disk built in the printer and are not printed until the matching passwords are entered. This means that data is printed only if the correct password, previously set by the user at the time printing was initiated, is entered into the operation panel of the printer when the user physically relocates to the location of the printer. Due to the procedure involved the risk of a third party sneaking a look at the printed documents or having those printed documents stolen is relatively slim.

(2) Encrypted Authenticated Printing

Encrypted authenticated printing is a combination of the three aforementioned security functions. The flow of operation of the user, as well as the processing performed by the personal computer of the user and processing carried out internally in the printer, are shown in **Figure 2**.

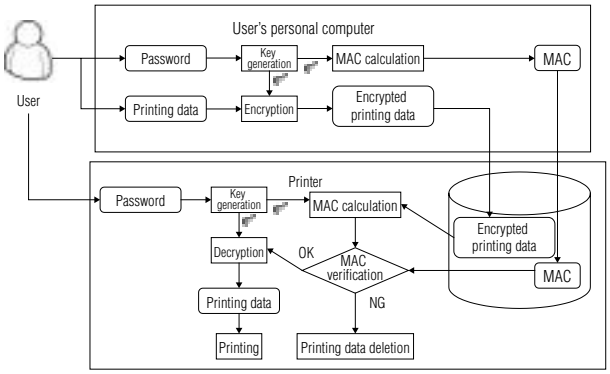

Fig. 2 Process for encrypted authenticated printing

The user of encrypted authenticated printing must first enter the password on the screen of the printer driver when printing a document from a personal computer. A screen used to specify encrypted authenticated printing from the printer driver is shown in **Figure 3**.

The printer driver generates an encryption key using the entered password and encrypts the printing data using the key before transmitting the printing data. The MAC is also calculated and transmitted to the printer at the same time, but the password is not transmitted. Therefore, since the printing data is encrypted leaking information from the contents of the printing is not a concern even if the printing data is intercepted on the network.

The printer initially stores the encrypted printing data

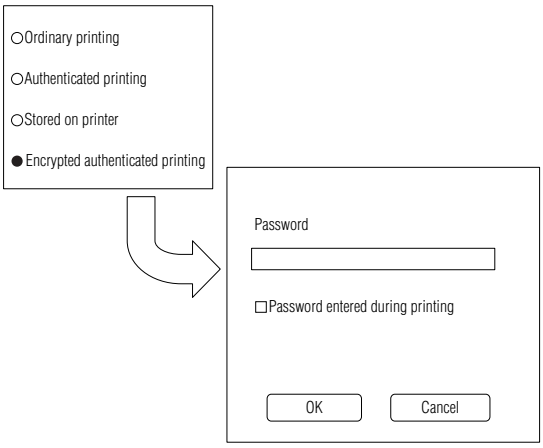

Fig. 3 Screen for specifying encrypted authenticated printing

and MAC on the hard disk built into the printer. Because the printing data stored on the hard disk in the printer is in an encrypted form at this stage, leaking information from the contents of the printing is not a concern, even if the hard disk is stolen by a third party or if the printing data is read from the hard disk.

Next, in order to start the printing of the transmitted data the user relocates to the place where the printer is installed and to which the printing data has been transmitted. He then enters into the operation panel of the printer the password that is identical to the one entered on the personal computer when the printing data was transmitted. The printer generates the encryption key based on the entered password. The printer then uses the encryption key to calculate the MAC based on the encrypted printing data read from the hard disk to verify whether it matches the MAC transmitted by the personal computer of the user. The encrypted printing data is decrypted and printed by the printer whenever the MAC values match. Whenever the MAC values do not match the printer determines that the printing data has been tampered with and deletes the data without printing it.

In this manner it is possible to prevent information leaks arising from the theft of printed materials or sneak views of the printed contents with encrypted authenticated printing, since the printing starts only after the password is entered into the printer by the user.

Disk Clearing Function

The hard disk built into the printer contains not only the aforementioned encrypted authenticated printing data but also other data, such as ordinary printing data that has not been encrypted, as well as data on user information. For this reason it is potentially possible for user information or printing data to be read from the hard disk through theft of the hard disk or when the password for encryption data has been leaked.

The disk clearing function, which positively deletes data by overwriting it when data stored on the hard disk becomes unnecessary in order to prevent information leaks, is described in this chapter. This disk clearing function can be used to delete data in units of individual files or for the entire hard disk.

(1) Threats and countermeasures for leakage of data stored on hard disks

The data on hard disks is generally managed by file systems. Files containing data are stored separately either as management information or data for storing.

When data stored on a hard disk (or a file) is deleted only the management information for that file is ordinarily deleted, whereas the data itself remains on the hard disk. For this reason it is possible for individuals who are technically familiar with hard disks and file systems to read the deleted data from the hard disk in such a condition.

Deletion combined with overwriting by another set of data is an effective strategy against such reading of data. If the data is overwritten only once, however, it is still potentially possible to restore the original data by using special equipment to read the magnetic traces of data that remains on the recording media of the hard disk. Overwriting data multiple times is an effective means to prevent such restoration of data from magnetic traces.

(2) Data clearing method

The three methods described below are for deleting data using a disk clearing function.

- **Simple data deletion**

This method rewrites only the management information of the file, without overwriting the actual data. This is a high-speed process, since only the management information is overwritten. The actual contents of the data, however, remain on the hard disk.

- **Data clearing (Clear)**

This is one of the data deleting methods stipulated by the United States Department of Defense in their standard, DoD 5220.22-M. The deleted data is overwritten once with fixed data, “0x00”. Unlike the method for simply deleting the management information, additional time comparable with the size of the data to be deleted is required for processing (writing a set of data on the hard disk) since the entire data for deletion is overwritten. Refer to Reference Document 3 for details concerning the deletion method stipulated in DoD 5220.22-M.

- **Data sanitizing (Sanitize)**

This is another data deleting method stipulated by the United States Department of Defense in their standard, DoD 5220.22-M. The deleted data is overwritten three times with fixed data of “0x00” and “0xFF”, and then random numbers. Verification is then performed to ensure that the data written last can be read correctly. Of the three data deleting methods this has the highest degree of security rendering an extremely small potential for restoring the original data from magnetic traces. Since verification is performed through data reading after data has been overwritten three times, this method requires the most processing time out of the three data deleting methods.

(3) Automatic data deletion function for encrypted authenticated printing data

Data deleting methods for the printing of data (encrypted) stored on hard disks that are built in printers can be specified with encrypted authenticated printing, although this was not mentioned in the descriptions provided previously. The data deleting method can be specified using the printer driver. The method for deleting printing data is selected from the aforementioned simple data deletion, data clearing (overwritten once) and data sanitizing (overwritten three times) once printing has been completed. The potential for confidential data leaks arising from magnetic traces remaining on a hard disk can be rendered extremely slim particularly when data sanitizing is selected.

(4) Deleting all data on hard disks built in printers

The function for deleting all the data on hard disks built into printers is a feature used if all the data remaining on hard disks built into printers is to be deleted, such as for printers used for rental services or when disposing of printers. Confidential information leaks arising from magnetic traces can be prevented with the use of this function.

Logon information forced printing function

Strategies for the prevention of information leaks from electronic files, such as printing data, can be realized with a thorough implementation of security management on servers and personal computers of all users, as well as by preventing the copying and encryption of electronic files. However, all relevant companies are searching for strategies to prevent information leaks once the data is printed onto a paper medium (printed materials), through theft or the making of unauthorized copies.

Logon information forced printing function, which can raise the security consciousness of users and inhibit the leaking of information through theft of printed materials by embedding information, such as user IDs and printed document names, is described in this chapter.

(1) Functional summary

The logon information forced printing function is comprised of the printer driver and configuration utility.

The dedicated printer driver prints additional information forcibly adding watermarks onto the printed document. The additional information can include IDs used for logging onto the systems, document names of the printed materials, as well as printing times. The additional information is superimposed onto the image of the printing data as a background. An example of printed material obtained using the logon information forced printing function is shown in **Figure 4**.

Fig. 4 An example of printed material obtained using logon information forced printing function

It is possible to psychologically boost the consciousness of users regarding the management of printed materials, as well as offer a deterrent against information leaks through the theft of printed materials due to visibly verifiable additional information on the image of printed materials, such as the user ID of the person performing the printing. Furthermore, in the unlikely event the printed materials are leaked, it is possible to easily determine the source of the leak based on the additional information.

(2) Use environment

This function can be made available simply by setting up the printer driver and configuration utility on the system, which makes it possible to build an environment for keeping a check on information leaks with the utmost ease and at affordable prices.

(3) Additional information setting method

Items included in the printed additional information as well as the format used can be set arbitrarily by the system administrator through the use of the configuration utility **(Figure 5**). Doing so sets the system with the printer driver enabled to superimpose additional information on all printing data for all printed materials at all times, without any special operations. Users, however, will not be able to disable this function.

Furthermore, it is also possible to output printed materials without additional information, such as documents submitted to customers or official documents used in meetings, by assigning an authority to specific users This setting can also be changed arbitrarily by the system administrator through the use of the configuration utility (**Figure 5**).

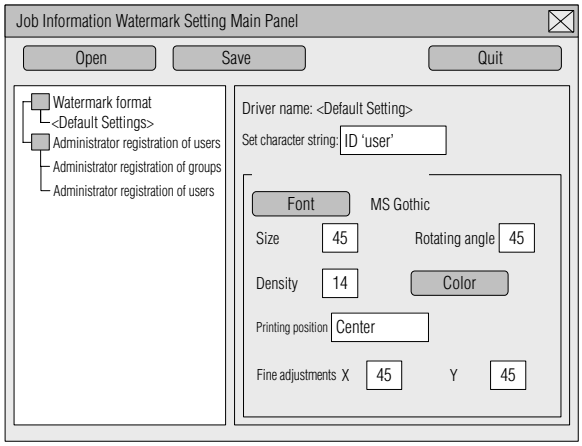

Fig. 5 Job information setting screen of utility

Conclusion

A number of functions available in printers for preventing the leaking of information from printing data and printed materials have thus far been introduced. With the advancement of sophisticated functions, printing devices are becoming a major constituent component of document management systems and business systems, along with various servers as well as the personal computers of users. For this reason, sophisticated security functions linked with authentication servers and log servers are prerequisites for printing devices also. We intend to develop security functions for such system linkups in the future.

References

1) Hirohiko Nakazato et al: "Printing Solutions for Era of Ubiquitous Networks", Oki Technical Review, Issue 204, Vol. 72, No. 2, pp. 28 to 31, October 2005.
2) PKCS#5: http://www.rsasecurity.com/rsalabs/node.asp?id=2127.
3) DoD 5220.22-M: http://www.dtic.mil/whs/directives/corres/html/522022ms.htm, chapter 8.

Authors

Yoshitaka Nishiyama: Oki Data Corporation, Software Development Center, Software Development Dept.-2, General Manager.

Nobuyuki Yokoyama: Oki Data Corporation, Software Development Center, Software Development Dept.-1, Team Leader.

Kunio Kanai: Oki Data Corporation, Software Development Center, Software Development Dept.-1.

Taisuke Watanabe: Oki Data Corporation, Software Development Center, Software Development Dept.-2.