社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2003－UBI－2 (29)
2003／11／19

セキュアなネットワーク印刷機構の実現

鈴木源太[†] 松宮健太[†]
高汐一紀[†] 徳田英幸[†,††]

本稿では，セキュアなネットワーク印刷機構である SCPS (Secure Campus Printing System) について述べる．遠隔のネットワークプリンタを用いてファイルを印刷する際，印刷物がプリンタのまわりにいる第三者に見られることがある．そのため，多くのユーザにとってメール等のプライベートな印刷物や機密書類は遠隔のプリンタから印刷しずらい．SCPS では，ユーザは安全に印刷したいファイルを一時的に SCPS サーバに登録する．その後，ユーザが任意のプリンタの傍で，Java カードや PDA から SCPS サーバに登録したファイルへの印刷命令を発行する． これにより，ユーザがプリンタの傍にいるときにのみ印刷作業が開始され，印刷物が第三者に見られることを防ぐ．加えて，SCPS はネットワークデータの暗号化技術やユーザ認証によって印刷するファイルデータの安全性も保証する．また，本稿では SCPS の想定するユーザインタフェースの一つである PDA をとりあげ，これを使用してユーザ付近のプリンタを自動検知する PDA SCPS を設計し，実装した．

Secure Printing System for Shared Network Printers

Genta Suzuki[†], Kenta Matsumiya[†], Kazunori Takashio[†] and Hideyuki Tokuda[†,††]

In this paper, we describe the use of the *Secure Campus Printing System* (SCPS) that protects sensitive documents such as private mails printed on shared network printers from being underlooked by others. We developed SCPS where sensitive documents are printed only when their owner stands by the printer. In our system, a user registers a document (which the user wants to print securely) in a SCPS server from any computer in the campus. Afterward, when he/she comes close to one of the printers he/she can use, he/she triggers printing on the printer using multiple interfaces (e.g. touch panel beside the printer, PDA, Java card). SCPS is flexible to use multiple interfaces and can coexist with general printing mechanisms. We also demonstrated PDA-based SCPS that can provide automatic detection of a printer nearby and notification of queued jobs.

1. Introduction

Today, wired and wireless network infrastructures are widely pervasive. Shared network resources are ready for use for daily work in offices and even in public spaces. This enables us to work with network file systems, printers, scanners, and cameras, in the same fashion as our own resources.

In campus environment, there are also large number of shared devices, and students are able to use them in many places. In this kind of environment, generally, inherent privacy problem exists because of the *collision* on devices. For example, if a student who used a shared desktop computer leaves his/her seat for a moment, another student can enter the room and use the same computer. The latter student may read the other's mail on the desktop. In another case, a student who left photos of himself at a shared scanner one weeks ago, can become famous on the internet.

Focusing on shared network printers, there are similar privacy problems, such as misplacement of a document. In addition, network printing is a kind of remote operation where users start printing jobs on the remote host and afterward pick up printed documents.

Therefore, network printer-specific problem will occur. For instance, a user beside a printer can accidentally see other's printings mistaking them for his/her own printings. This problem of others seeing a printed document is more serious when the printed documents are the kind of "sensitive documents", such as private mails. Sometimes users

† 慶應義塾大学大学院 政策・メディア研究科
Graduate School of Media and Governance, Keio University
†† 慶應義塾大学 環境情報学部
Faculty of Environmental Information, Keio University

start jobs from the desktop computer, and then run to pick their documents up.

The goal of our research is to develop a printing system that can print sensitive documents safely. We describe the design and implementation of the *Secure Campus Printing System* (SCPS) to print documents only when their owner come close to the printer, if they are sensitive documents.

The rest of the paper is organized as follows. Next section analyzes actual condition of network printing in our campus. And third section illustrates scenarios. Fourth section discusses design issues of SCPS. Fifth section describes a system model of SCPS. Then in sixth section, we propose PDA SCPS which highlights advantages of our architecture. In seventh section, we discuss related works. Eighth section remarks future work and final section concludes our paper.

2. Analysis of Actual Campus Printings

Let us now look at the actual condition of network printing in our campus, Keio University Shonan Fujisawa Campus[1]. We first explain our campus network environments. Then we analyze the present condition of network printings ☆.

2.1 Campus Networks

In our campus, wired and wireless LAN infrastructures are widely pervasive. The common bandwidth of wired network is at least 100Mbps. The wireless network infrastructure conforms to 802.11b. More than 150 wireless LAN access points are allocated and their signal covers the whole indoor areas in the campus. Furthermore, no wireless data are encrypted by WEP. These features and single IP subnet assigned to the wireless connection enable us to connect to LAN seamlessly even on the move.

2.2 Printing Environment

Eleven printers actually operate in our campus. Printers whose names are nps1, nps2, nps3, nps4, nps5, nps10 are located with shared desktop computers in working rooms, shown in Figure 2. Nps6 and nps8 are in copy rooms where they are located with copy and fax machines. Nps12, nps13, nps14 are in a Media Center where larger number of computers than working rooms are located with printers. Students use them from individual laptop computers or shared desktop computers in which Windows, FreeBSD or Mac operating system is installed. A printer name is labeled on the printer, therefore if a student wishes to print documents on a printer, he/she goes to see the label, returns to his/her seat and issues print jobs on the printer.

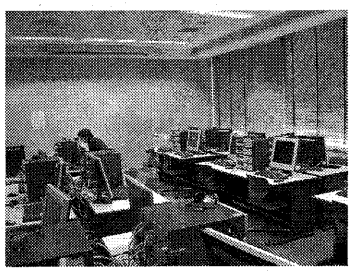

Fig. 2 Working room

The printer's actual workload between April 1 and August 1 of year 2003 is shown in Figure 1. Left graph shows the total number of pages printed on each printer a day. This denotes that most of printed literature are printed at working rooms and the Media Center. Right graph shows the average printed pages on individual printers per queue. This denotes that between 3.5 and 4 pages are printed per one queue. Our printers require two seconds to print a page at the minimum. Therefore, if a user issues 4 pages of a document to be printed on a printer from a desktop computer far from the printer, all of his/her documents could be stolen unless he/she arrives on the printer in eight seconds. In addition, we found that there are a lot of documents which are left or misplaced on printers.

3. Scenarios

We describe two scenarios which represent the most common cases in our system.

Scenario 1:

Ann, a student, works at a shared desktop computer in a working room. She reads the mail about tonight's party and wants to print it to remember when and where it is being held. But a printer is far from her seat and there are several unfamiliar students in the same room.

For this reason, Ann uses secure printing command and walks to the printer. She reached there and swipe her student card through a reader besides a printer. After this operation,

☆ All of our researches about our campus does *not* include subnet environment assigned to individual laboratories.

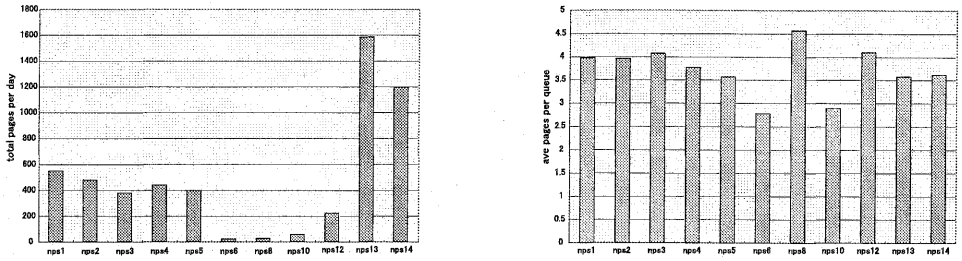

Fig. 1 Actual printing conditions in our campus; left graph denotes total number of pages printed on individual printers per day and right graph denotes average pages per queue

the mail is printed. She finally picks it up without it being seen by others.

Scenario 2:

Bob wrote a term paper that he should hand in to a professor on his laptop computer. He completes it, but there are no printers in the room where he is. Then, he presses "Secure Printing" button at his editor. After this operation, he shutdowns his computer.

Bob begins walking to the professor's room. On the way to the professor's room, his PDA beeps. He sees PDA's display and there is a message that tells "Print the report on this printer B?" He looks around and finds the printer B, but it isn't a color printer he wants. Therefore, he answers "No." He walks for a while and his PDA beeps once again. He saw his PDA's display, and there is a message that tells "Print the report on this printer C?" He finds that the printer is a color printer. Therefore, he answers "Yes" with joy.

Finally, he gets his paper and hand it in to the professor.

4. Design Issues

One of the reliable ways to protect sensitive documents from other's seeing is that their owner stands before a printer and monitors whenever it outputs them. Therefore, our system should be able to access to the documents and execute printing jobs beside the printer. We summarized the design issues as follows.

(1) ***Low interaction system with consensus.*** It is desired that the system is a low-interaction system meaning that the number of users' input are low. For example, not making users to input the printer name. Although low-interaction printing is convenient, no-interaction printing is no more useful. It is difficult to decide what documents to print, when to print or where to print without consensus. The first issue of the system is the *balance* between degree of interaction and consensus with the users.

(2) ***Flexible system with multiple user interfaces.*** A system that can be accessed from multiple devices, such as Personal Digital Assistant (PDA), touch panel beside a printer and Java Card is preferable. A user who has a PDA can use it for SCPS, and another user can use his/her Java Card and a touch panel beside the printer in the same framework.

(3) ***Hybrid system with general printing strategies.*** We believe that the system to make *all* printed documents secure is not needed. It is sensible to print public documents using regular printing systems, since it is likely to be faster. Therefore, our system should co-exist with the existing printing systems and require less modification to the existing mechanism.

5. SCPS Design

We propose SCPS architecture, shown in Figure 3, which is based on the client-server model. Left elements in the figure is a *data register*. User's working computer such as shared desktop computers in working room or his/her laptop computer works as a data register. Instead of clicking "Print" button, the user clicks "SCPS" button, or execute SCPS command. The document registers to a *SCPS server* in this sequence. The cashed documents are counted as queued job in SCPS server and the print commands are published there. At

SCPS client, a user obtains information on queued jobs and he/she decides to print a document beside the printer. Terminals where clients work in can be classified into two; *placed* and *portable*. For example, terminals which connects to Java Card reader are placed terminals and they are located beside printers. In contrast, PDA and cellular phone are portable terminals.

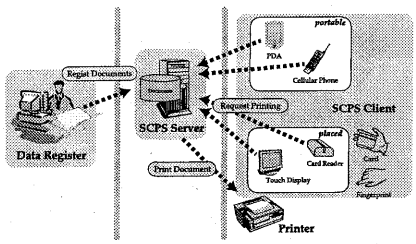

Fig. 3 SCPS architecture

5.1 Two Phase Printing

In general, when a user issues a printing job, the document will soon be outputted on a certain printer. Decision to print a file and actual printing are synchronous. In contrast, they are asynchronous in SCPS. We make printing sequence be divided into two phases. In the first phase, which we call *data registration phase*, is executed on the data register where we normally start a printing job. A user issues a printing job and documents to print are copied to a SCPS server in this phase.

The second phase is *print phase*, where the user decides when to print and where to print. SCPS server and SCPS client are involved in this phase. The work flow of this phase is shown in Figure 4. First, a SCPS client asks to a SCPS server

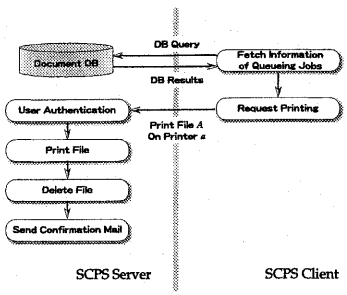

Fig. 4 Generic work flow of the SCPS server and SCPS client

whether the user's jobs are queued or not. If the user starts the print phase, for example by swiping his/her card through a card reader beside a printer, the SCPS client searches for the user's queueing jobs. In the case the jobs are available, the printer and documents to print are selected on the SCPS client. Then, the request which includes the selected printer name and the document name is sent to the SCPS server. When the SCPS server receive this request, it starts printing the document on the printer. After printing, documents which were printed are removed from the data server. As a certification of deletion of a file, confirmation mail is published. Confirmation mail may state "File *A* was printed and remove from the SCPS server."

5.2 Other Security Issues

We propose our system to protect sensitive documents from underlooking. However, these systems could cause spoofing and eavesdropping. Our system also cope with these problems. Following are our measures.

- **Network Data Encryption.** In our system, network data between the data register, the data server and the portable client are encrypted by Secure Socket Layer (SSL)[2].
- **Permission of Data in SCPS Server.** Sensitive documents copied to a server can be looked by other users accessible to the server. When copying to the SCPS server, permissions to access the file are set so only the user can read or write files. When using a database, permissions to the database access are also limited.
- **User Authentication.** The user should be authenticated with the SCPS server to print his/her documents. When accessing a document database or issuing to print, he/she should be authenticated.
- **Confidence in SCPS Server.** If data servers are unreliable, their administrators may suddenly shutdown data servers or obtain our sensitive documents. We assume every SCPS servers are operated by reliable administrator such as the network administrator of a university.

6. PDA SCPS

We developed "PDA SCPS," which uses PDA that connects to the campus wireless network. In scenario 2 we mentioned above, a PDA detects the owner coming close to one of the printers, and informs him/her about it. If the user wants to print

documents on the printer, he/she operates printing with GUI on his/her PDA. This approach is intelligent in respect to automatic printer lookup compared with other approaches.

6.1 Proximity Detection

To realize the scenario, proximity detection between a user and a printer is needed. This gives us notification of the printers available, in other words, low interaction for selecting a printer.

There are several approaches to detect proximity. Some uses Infrared[3] , and others adopt Ultrasound[4)5)], Radio Frequency(RF) or radio field intensity of wireless LAN[6)7)]. The Infrared, Ultrasound and RF approach require specific sensor devices only for detecting distance or location. On the other hand, by using signal of wireless LAN, user's PDA can detect proximity to a printer itself. Therefore, we adopted this approach.

When wireless access point (AP) and computers are connected wireless, there is a implication between signal strength (SS) of wireless connections and distance between them[7)].
SS is in inverse proportion to the square of the distance. This research shows that the distance calculated with SS is capable of precision within 5 meters from AP.

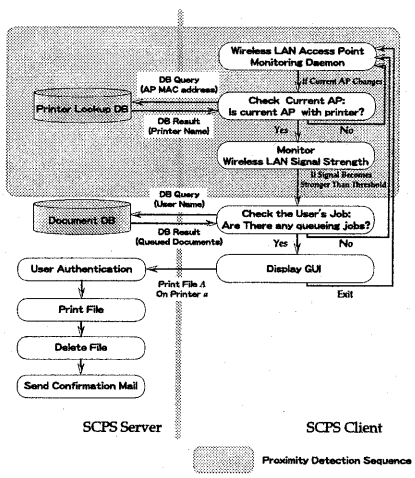

Fig. 5 Work flow of PDA SCPS

In PDA SCPS, We allocate an AP beside a printer. We call the AP beside a printer APBP in distinction from normal AP. We set up each APBP so that it has about 2 meter of *printing area* around it and SS threshold for proximity detection are set

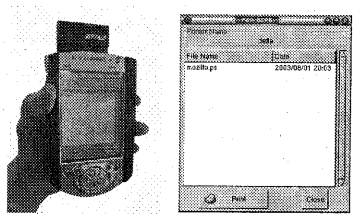

Fig. 6 PDA SCPS: Screen dump of PDA when proximity is detected and queued jobs are available

to detect printing area in a heuristic method. Basic procedure of proximity detection at SCPS client is

(1) Acquire the name of current AP.
(2) Lookup the printer name and the threshold of SS with the current AP as a key.
(3) If current AP is APBP, set the result as a SCPS default printer name and its threshold.
(4) If SS of current APBP is over the threshold, the proximity is detected.

After the proximity detection, SCPS client checks whether the user's queueing jobs are available or not. If queueing jobs are available, it display a GUI which include current printer name and the queueing job's name. All the work flow is shown in Figure 5.

6.2 Prototype Implementations

We prototyped PDA SCPS. Table 1 shows the computing devices we have used. In addition, a printer and a wireless LAN access point have been used. Our prototyped system works in the same procedure as in Figure 5. Databases are based on PostgreSQL and each SCPS client should be authenticated using password to access these databases. All communication links including database access are protected by SSL. The behavior of the PDA client is shown in Figure 6.

item	Desktop PC	ThinkPAD	iPAQ
Type	Data Register	SCPS Server	SCPS Client
CPU	Athron 2000+	Intel PentiumIII 1200MHz	StrongARM 206MHz
Memory	256MB	640MB	64MB
OS	FreeBSD 4.8-Release	FreeBSD 4.8-Stable	Familiar Linux v0.5.1

Table 1 Computing devices used in prototype implementation

7. Related Work

There are several researches that deal with a similar problem addressed by SCPS. In[8)], Personal Interaction Points (PIPs) give smart access, that is "low interaction", to user's file at shared devices.

In the "printer PIP," they apply it in a mailroom that is exclusive for print, copy, scan, and fax functions. If a user enters the mailroom, PIP accesses the user's most recently edited documents and enquire whether to print them. Entering the mailroom implies that the user is going to print. For this reason, PIP is useful in mailrooms. In our targeted printing environment, however, most of the shared printers are located with shared desktop computers in a working room, and users close to the printer does not necessarily wish to print. In this case, self-active inquiry can be disturbing.

In PrinterOn[9], the company of Internet Printing service, they developed a system where a user or company who does not have printers can use public printers or other company's printer registered to PrinterOn membership. They also dealt with the following three security issues; confidentiality of customer and user information, transmission of the printed information, and maintaining user's existing corporate network security standards. If a user registers a document to PrinterOn server and he/she encounters a printer afterward, he/she can use the printer by inputting his/her ID or job number to the terminal which is in front of the printer. They did not deal with multiple interface support, such as PDAs, cards, or touch panels. In addition, their interface are not intelligent, which requires users to input their ID or queueing jobs and do not notify that a printer is in front of a user.

8. Future Work

Currently, we assume SCPS is applied to a campus environment. We wish to apply our system to "open" environment such as cross-company environments. In such a situation, other security issues will arise. For example, there is a difference of security policy between individual companies. SCPS needs to deal with this difference.

9. Conclusion

In this paper, we proposed SCPS, an architecture for printing sensitive documents safely in campus environment. SCPS can print sensitive documents only when their owner stands before a printer. SCPS also aims to provide multiple interfaces, coexist with general printing strategies and decrease user's input. In addition, our system copes with generic security issues such as unsecure data transmission in the network.

We also designed and implemented "PDA SCPS" which applies PDA as SCPS interface. In PDA SCPS, when a user comes close to one of the printers, his/her PDA detects it, checks his/her queueing jobs and asks him/her whether to print the documentsor not. PDA SCPS is not only proactive but also acceptable.

Acknowledgments We wish to express our special gratitude to staffs of Information Technology Center (ITC) of Keio University Shonan Fujisawa Campus to offer necessary datas about printings in our campus.

References

1) Keio University Shonan Fujisawa Campus, http://www.sfc.keio.ac.jp/english/

2) Alan O. Freier, Philip Karlton, and Paul C. Kocher. "The SSL Protocol Version 3.0.," Work in progress, Netscape Communications, November 1996.

3) Roy Want, Andy Hopper, Veronica Falcao and Jon Gibsons, "The Active Badge Location System," *ACM Transaction on Information Systems*, vol.10, no.1, pp.91-102, January 1992.

4) Andy Harter, Andy Hopper, Pete Steggles, Andy Ward, and Paul Webster, "The Anatomy of a Context-aware Application," *Mobicom '99*, ACM, 8, 1999.

5) Nissanka B. Priyantha, Anit Chakraborty and Hari Balakrishnan, "The Cricket Location-supoprt System," *6th ACM International Conference on Mobile Computing and Networking (ACM MOBICOM)*, Boston, MA, 2000, ACM

6) Andrew M. Ladd, Kostas E. Bekris, Guillaume Marceau, Algis Rudys, Dan S. Wallach and Lydia E. Kavraki, "Using Wireless Ethernet for Localization," *Proceedings of the 2002 IEEE/RSJ International Conference on Intelligent Robots and Systems* September 2002.

7) Paramvir Bahl annd Venkata N. Padmanabha, "RADAR: An In-Building RF-based User Location and Tracking System," *IEEE INFOCOM 2000*, Tel Aviv, Israel, 2000.

8) Jonathan Trevor, David M. Hilbert, Bill N, Schilit, "Issues in Pernonalizing Shared Ubiquitous Devices," *Proceedings of Ubicomp 2002*, pp. 56-72, 2002.

9) PrinterOn Corporation, http://www.printeron.net