A Web-based Secure System for the Distributed Printing of Documents and Images

Ping Wah Wong*, Daniel Tretter†, Thomas Kite§, Qian Lin† and Hugh Nguyen*

* Hewlett Packard Company, 11000 Wolfe Road, Cupertino, CA 95014
† Hewlett Packard Laboratories, 1501 Page Mill Road, Palo Alto, CA 94304
§ Dept. of Elect. and Comp. Engin., The Univ. of Texas at Austin, Austin, TX 78712

Abstract

We propose and consider a secure printing system for the distributed printing of documents and images over the World Wide Web. This system enables secure sharing, commerce, and collaboration using images and documents. The main feature of the system is that it allows a user authorized through an authentication mechanism to preview and print selected documents and images. The user can then print a certain number of hardcopies, based on an agreed payment. The security of the system resides in an aggregate of communication protocols, smartcard technologies, and cryptographic algorithms. The system prevents eavesdropping so that people who intercept the communication cannot generate copies of the document.

1 Introduction

Distributed computer systems such as the World Wide Web are excellent vehicles for the timely dissemination of documents and images over broad geographical areas. For example, documents and images may be shared among multiple offices of an organization in different cities. In this situation, the documents and images can be stored in a central repository, where they can be managed and updated easily. Users can access the repository via a computer network and obtain the desired hardcopies immediately. One of the primary considerations in the successful implementation of such a system is the pervasive security measures that protect the documents from unauthorized use.

In another possible scenario, a merchant is selling valuable images and documents over the Internet. In this case, not only do we need a secure way of delivering the material over the network, we also require a secure mechanism to control the number of hardcopies generated by a specific user. Our secure printing system solves both problems, and can therefore be interpreted as a mechanism for providing a "pay-per-print" service.

In this paper, we consider a secure printing system that protects the documents and images all the way from the server to the printer, so that

- users can be identified and authenticated before gaining access to a visibly watermarked document for previewing and selection purposes,
- a clean document (without a visible watermark) that is intercepted during transmission cannot be printed by an unauthorized user or printer, and
- the authorized user can only print the number of copies specified by the document server.

The security in our system resides in an aggregate of a secure communication protocol, smartcard technologies [1, 2], and the computational infeasibility of breaking a public key cryptographic system [3, 4, 5].

Secure devices have been designed in the past to perform some of the same functions as our secure printing system, although they all differ to some extent. Furthermore, the devices were not designed with an emphasis on secure printing. Chen and Wang propose a system based on shared secret keys to establish mutual authentication and secured communications across an open network [6]. Other user authentication techniques have been proposed that require the user (or smartcard) and the network to possess the same secret key for encryption and decryption [7, 8]. Our scheme uses a public key encryption technique [5] to protect the communication, so the private decryption key does not need to be known by a second party. Finally, our approach, which applies to the transfer and printing of documents, includes monitoring and acknowledging the printer operation, as well as limiting the number of copies printed. General communications schemes do not include such tasks.

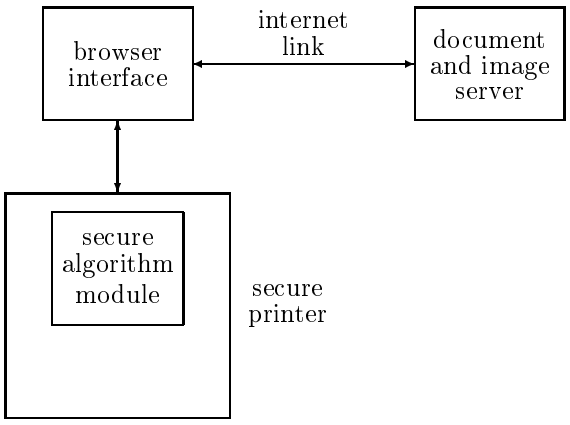

Figure 1: A secure printing system for sharing documents and images over the Internet, so that hardcopies can be generated in a secure and controlled manner. This system can also serve as a mechanism for a "pay-per-print" service.

2 Secure Printing System

Figure 1 shows a secure printing system that allows an authorized user to select and generate hardcopies in a controlled manner. The number of hardcopies that a user is permitted to generate is dependent on the agreement between the user and the document owner. This can be thought of as a type of "pay-per-print" service.

We have highlighted in Figure 1 the *secure algorithm module* inside the secure printer. The security of the system is fundamentally based on the secrecy of certain cryptographic keys. The required cryptographic keys reside in the secure algorithm module inside the secure printer, and cannot be accessed from outside it.

Our secure printing system consists of the following four major steps:

- user sign-on and verification
- document selection and payment negotiation
- document delivery and printing,
- client acknowledgment to server.

The communication steps that occur in a typical printing session using our secure printing system are represented graphically in Figure 2.

2.1 User Sign-on and Verification

To accomplish a "pay-per-print" service for documents and images over the Internet, we want to design the system so that any user can sign on to the system server without having to establish a pre-existing account. This can be accomplished with a smartcard that plugs into a slot in the secure printer, together with an authentication protocol. One reason that we require a smartcard is that it prevents someone from using purely software to imitate the communication protocol of the secure printing system, thereby gaining unlimited access to the content, as well as the ability to generate unlimited hardcopies.

Let $\{D(), E()\}$ denote the encryption and decryption functions of a public key encryption algorithm, respectively. The printer is authenticated through the use of a smartcard which implements a public key encryption algorithm. A smartcard user A inserts the card into a slot on the printer. Once a card is inserted, the printer becomes "active" and takes on the identity of the user A. The server can verify that A is a valid user through the validity of a public key K_A. Once the public key K_A has been verified as a valid smartcard key, the server proceeds to authenticate the identity of the user.

Because the list of all public keys is available as public information, any person B can implement a device in software, hardware, or both, to falsely claim the identity of A. An extra authentication step is therefore necessary. To authenticate the identity of A, the server generates a unique session token T, encrypts it using the public key K_A, and sends the encrypted result $U = E_{K_A}(T)$ to A. The printer, taking on the identity of A, passes U along to the smartcard. The smartcard obtains $T' = D_{K'_A}(U)$ by decrypting the message U with the private key K'_A stored in the smartcard, and passes T' back to the printer. The printer then sends the decrypted message T' back to the server for verification. Since only the smartcard knows the private key for decryption, the server verifies that the user is indeed A if $T = T'$. Note that the decryption procedure is performed within the smartcard, so that the private decryption key will never need to be revealed outside of the smartcard. This adds another level of security to the printing system.

2.2 Document Selection and Payment Negotiation

It is evident that a "pay-per-print" system must allow the user to preview the documents that are available on a server. One important feature of our system is that the server obtains a low resolution version of the document and adds a visible watermark [9, 10, 11] to it before transmitting to the user for preview and selection. The visible watermark and the small image size distinguish this preview document from the high

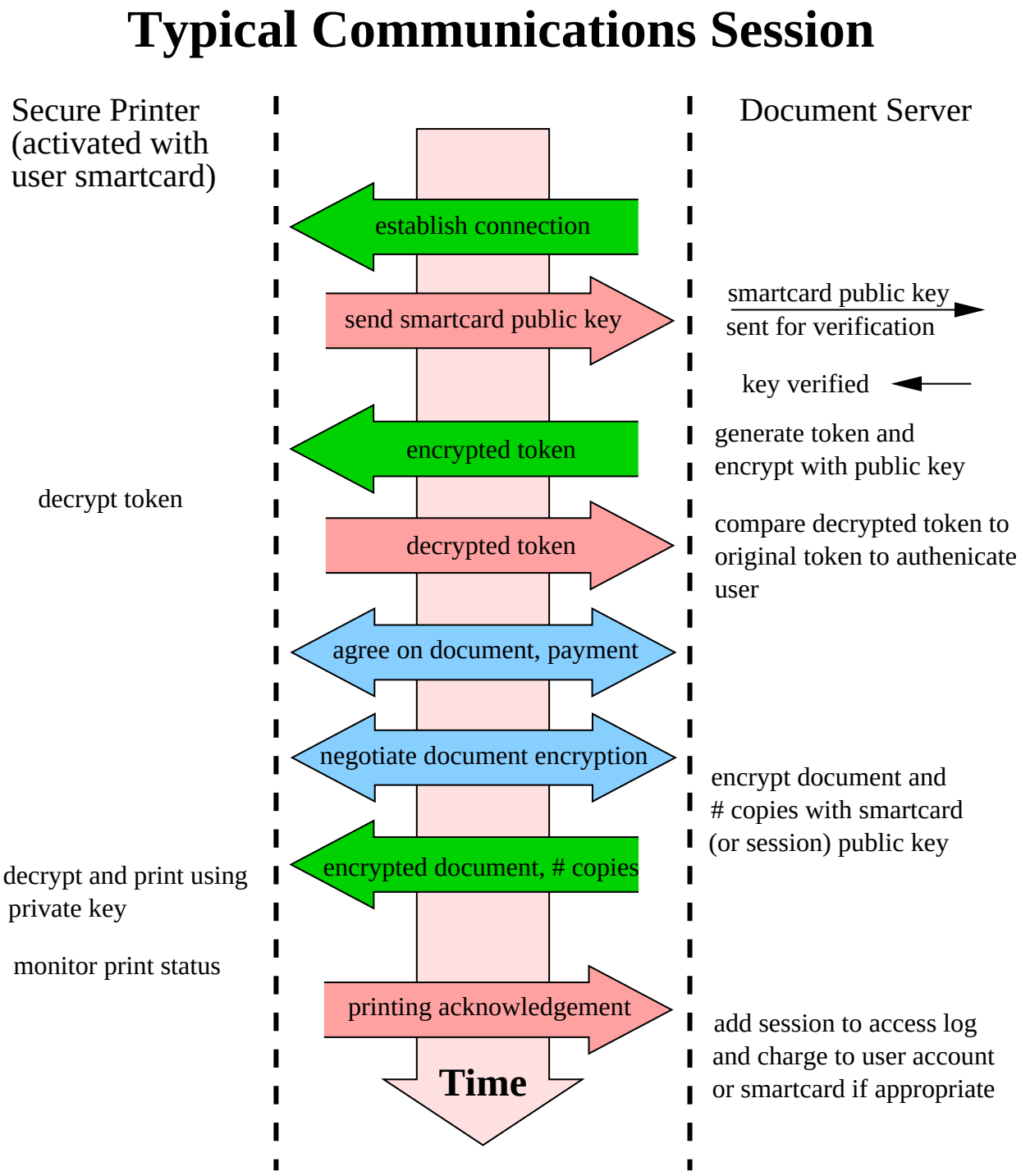

Figure 2: Communication steps in a typical secure printing session. The secure printer first identifies and authenticates itself. The server then encrypts the document before sending it, so only the secure printer can decrypt and print it.

quality original, and discourage the user from simply printing the preview document from the screen without payment.

2.3 Secure Document Delivery

After user A has agreed to pay for n copies of a specific document X, the high quality electronic document (without a visible watermark) must be transmitted to the "trusted" printer. To this end, the server encrypts the document and the permitted number of copies n using the public key K_A, and sends the result $Y = E_{K_A}(n, X)$ to the printer. Even if the data transmission is intercepted, an eavesdropper will not be able to generate high quality copies without knowing the decryption key $K_A^{'}$. Upon receiving Y, the printer streams the data to the smartcard, where it is decrypted using the private decryption key, recovering n and X. The printer then proceeds to print n copies of X. Since n (the number of copies) is also encrypted, it cannot be changed. The secure printer will therefore only print the number of copies authorized by the server. It is also not possible for user A to redirect the bit stream Y to an ordinary printer and generate hardcopies there, since the private decryption key is known only to the smartcard.

It is well known that the computational complexity of public key cryptographic systems is generally much higher than secret key systems with a similar level of security. Public key systems are therefore much slower than secret key systems. There are methods for improving on the speed of the system using combined public/secret key systems. Two approaches in this direction are described in [12].

2.4 Content Rendering

After decryption, the printer must render the document to generate high quality hardcopies, i.e., perform steps such as scaling, color correction and halftoning. Since the characteristics of printers vary a great deal, the optimum halftoning method depends on a variety of printer parameters such as print resolution [13]. As a result, the content provider is unlikely to send a prerendered document to the printer. Furthermore, the architectural design of printers also varies. In some printer designs, the rendering is performed inside the printer. In other designs, rendering is performed in a software module in a host computer; the printer simply performs the physical task of putting dots on paper according to the result produced by the host software. In our secure printing system, rendering must be performed inside the printer, so that the rendered data cannot be diverted to an insecure printer.

The optimum rendering strategy depends on the method by which the document was created. A typical document can contain various combinations of text, images and graphics. The optimum rendering algorithm for each of these data types (text, images or graphics) is usually distinct. For example, graphics are best rendered with vivid, high saturation color, and scattered-dot halftone [14]. Images, on the other hand, should be rendered with screen-matching color, and perhaps an adaptive type of halftoning [15, 16, 17]. If the document was generated using a word processor, for example, then the resulting file typically contains information about the various types of data in different areas of the page. One can then apply the optimum rendering strategy accordingly. If the document has been digitally scanned from existing hardcopy archives, one must perform segmentation to separate out the text, image, and graphics regions. The same data-dependent rendering methods can then be applied.

2.5 Acknowledgment from Client to Server

As the printing of X proceeds, the progress is monitored, and an acknowledgment is sent to the server indicating that the required printing has been performed. This triggers the payment process, billing a charge to the user.

3 Conclusion

We have proposed, constructed, and tested a secure printing system that allows a user to generate a specified number of hardcopies for a document, upon an agreed payment to the document owner. The security of our system resides in an aggregate of a communication protocol, smartcard technologies, and the computational infeasibility of breaking a public key cryptographic system. The secure printing system is useful in many business applications. One example is in trading valuable documents or images in which a user accesses the document server through the World Wide Web, and then purchases and generates hardcopies using a secure printer.

References

[1] J. J. Farrell III, "Smartcards become an international technology," in *Proceedings of* 13th *TRON Project International Symposium*, pp. 134–140, December 1996.

[2] C. H. Fancher, "In your pocket: smartcards," *IEEE Spectrum*, vol. 34, pp. 47–53, February 1997.

[3] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 67, pp. 644–654, November 1976.

[4] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, February 1978.

[5] B. Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C*. John Wiley & Sons, 1996.

[6] J. F. Chen and J.-S. Wang, "Application level security system and method." United States Patent 5602918, 1997.

[7] W. E. Bass, S. M. Matyas, and J. Oseas, "Method for establishing user authentication with composite session keys among cryptographically communicating nodes." United States Patent 4649233, 1987.

[8] H. Tsubakiyama, M. Oohashi, and K. Koga, "Mutual authentication/cipher key distribution system." United States Patent 5345506, 1994.

[9] G. W. Braudaway, K. A. Magerlein, and F. C. Mintzer, "Color correct digital watermarking of images." United States Patent 5530759, June 1996.

[10] P. W. Wong, "A watermark for image integrity and ownership verification," in *Proceedings of IS&T PIC Conference*, (Portland, OR), May 1998.

[11] P. W. Wong, "A public key watermark for image verification and authentication," in *Proceedings of ICIP*, (Chicago, IL), October 1998.

[12] P. W. Wong, D. Tretter, T. Kite, Q. Lin, and H. Nguyen, "A web-based secure system for the distributed printing of document and images," *Journal of Visual Communication and Image Representation*, 1998. submitted.

[13] H. Trontelj, J. Farrell, J. Wiseman, and J. Shu, "Optimal halftoning algorithm depends on printing resolution," in *SID Digest of Technical Papers*, pp. 749–752, 1992.

[14] B. E. Bayer, "An optimum method for two-level rendition of continuous-tone pictures," in *Proceedings of IEEE International Conference in Communications*, pp. 26.11–26.15, 1973.

[15] Z. Fan, "Halftoning by combining ordered dithering and error diffusion," in *Proceedings of IS&T's International Congress on Advances in Non-impact Printing Technologies*, (Williamsburg VA), pp. 277–279, October 1992.

[16] R. L. Levien, "Digital generation of halftone images with error diffusion and frequency matched periodic screen rulings." United States Patent 5331429, July 1994.

[17] P. W. Wong, "Adaptive error diffusion and its application in multiresolution rendering," *IEEE Transactions on Image Processing*, vol. 5, pp. 1184–1196, July 1996.