INTERNET_DRAFT Printer Working Group
<draft-ietf-ipp-security-00.txt>

March 25, 1997 Expires September 25, 1997

Internet Printing Protocol/1.0: Security

Status of this memo

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

To learn the current status of any Internet-Draft, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

Abstract

This document is one of a set of documents which together describe all aspects of a new Internet Printing Protocol (IPP). IPP is an application level protocol that can be used for distributed printing on the Internet. The protocol is heavily influenced by the printing model introduced in the Document Printing Application (ISO/IEC 10175 DPA) standard, which describes a distributed printing service. The full set of IPP documents includes:

- Internet Printing Protocol/1.0: Requirements
- Internet Printing Protocol/1.0: Model and Semantics
- Internet Printing Protocol/1.0: Security
- Internet Printing Protocol/1.0: Protocol Specification
- Internet Printing Protocol/1.0: Directory Schema

This document deals with the security considerations for IPP.

Table of Contents

1.0 Introduction

2.0 Internet Printing Environments
- 2.1 Client, content and printer in the same security domain
- 2.2 Client and printer in one security domain, content in another
- 2.3 Client and content in one security domain, printer in another
- 2.4 Printer and content in one security domain, client in another

2.5 Printer, content and client all in different security domains
3.0 Security Services
3.1 Basic concepts
3.5 Miscellaneous
4.0 IPP Security threats and methods of attack
4.1 Threats
4.2 Methods of attack
4.3 Quality of service
5.0 Attacks vs. security services
6.0 Quality of service vs. security services
7.0 Required security services provided by current security methods
8.0 Further references.
9.0 Author's Address
10.0 Other Contributors

1.0 Introduction

It is required that the Internet Printing Protocol be able to operate within a secure environment. Wherever possible, IPP ought to make use of existing security protocols and services. IPP will not invent new security features when the requirements described in this document can be met by existing protocols and services. Examples of such services include Secure Sockets (SSL), Digest Access Authentication in HTTP, and the Content MD-5 Header Field in MIME.

It is difficult to anticipate the security risks that might exist in any given IPP environment. For example, if IPP is used within a given corporation over a private network, the risks of exposing print data may be low enough that the corporation will choose to not use encryption on that data. However, if the connection between the client and the Printer is over a public network, the client may wish to protect the content of the information during transmission through the network with encryption.

Furthermore, the value of the information being printed may vary from one use of the protocol to the next. Printing payroll checks, for example, might have a different value than printing public information from a file.

Since we cannot anticipate the security levels or the specific threats that any given IPP print administrator may be concerned with, IPP must be capable of operating with different security mechanisms and security policies as required by the individual installation. Security policies might vary from very strong, to very weak, to none at all, and corresponding security mechanisms will be required.

This document will describe the various environments within which IPP must operate. It will then introduce security related terminology used in this document, describe the various security services available and the possible threats and methods of attack. Finally, it will provide a mapping of threats to services and discuss how existing security methods address these requirements.

2.0 Internet Printing Environments

The printing environments described in this section must take into account the fact that the client, the Printer, and the document to be printed may all exist in separate security domains. This is complicated by the fact that IPP allows documents to be included in the print request or they may be printed by reference. When printing by reference a Printer may fetch the document from the client, but more often the document will be on another network node. Furthermore, there are at least two parties that have an interest in the value of the information being printed:

the client: the person asking to have the information printed

the author: the person who originated the information. This brings into the picture the need to worry about copyrights and protection of the content.

This requires consideration of the following Internet printing environments. Where examples are provided they should be considered illustrative of the environment and not an exhaustive set.

2.1 Client, Content and Printer in the same security domain

This environment would be typical of the traditional office where users print the output of office applications on shared work-group printers, or where batch applications print their output on large production printers. Documents may be included in a print request or printed by reference. Depending upon company policies security could range from none to very secure.

2.2 Client and Printer in one security domain, Content in another

In this environment, printing can only be done by reference (If the client has already obtained the content, then it is in the client's security domain). Examples of this environment include printing a document, such as software documentation, from a publicly available source on the Internet; or a copy of a contract or purchase order from a business partner, on a local Printer. Controlling access to content would be a major concern in this environment.

2.3 Client and Content in one security domain, Printer in another

Examples of this environment include printing a document created by the client on a publicly available printer, such as at a commercial print shop; or printing a contract on a business partner's printer. This latter operation would be functionally equivalent to sending the contract to the business partner as a facsimile. Documents may be included in the print request or printed by reference. Some credentials are required for the printer to fetch a document not in it's security domain.

2.4 Printer and Content in one security domain, Client in another

Printing in this environment is by reference only. Examples would include an employee at home connecting to his office through the Internet to print a document on a printer at work, or a student using the Internet to connect to the college library and asking

to have the results of a literature search printed on the library's printer. Authentication of the user and controlling access to print resources would be major concerns in this environment.

2.5 Printer, Content, and Client all in different security domains

Printing in this environment is by reference only. Examples include a person at home using the Internet to print a document from a remote site, at a commercial print shop. Authentication and controlling access to content and to print resources would be concerns in this environment.

3.0 Security Services

This section introduces common security terms used in this paper.

3.1 Basic Concepts

AAA: Overall term for security. The three A's are generally taken to be

Authentication, Authorization, and Auditing although it may mean Authentication, Authorization & Accounting in some contexts.

Security Domain: Security domain refers to the domain within which a specific set of security policies and mechanisms define access to resources within that domain.

Authentication: The process of reliably determining the identity of a communicating party. There are three classic ways of authenticating oneself: something you know, something you have and something you are. The two entities involved in the communication could use the following two ways to authenticate themselves.

Single entity authentication. Only one of the entities is authenticated by the other. In the case of IPP this may either by the end user or the Printer.

Mutual authentication. Both the parties authenticate each other.

Authorization: The granting of rights to a user, program or process to access a resource such as a Printer. Authorization may also apply to content being printed or to protect a resource from unauthorized use. This can be achieved by the use of access control lists (ACL) or capabilities.

Auditing: Keep a record of events that might have some significance, such as when a Printer is used and by whom. To record independently and later examine system activity. Audit data is generally used for security concerns (e.g. intrusion detection and consistency checks).

Accounting: Keep a record of events that might have some significance, such as when access to a Printer occurred, who accessed it, what print resources were used. Accounting data is generally used for commercial concerns (e.g. billing and charges).

3.2 Security Service Attributes

Anonymity: The ability to communicate so that the other principal can't find out the identity of the sender.

Integrity: Keeping information from corruption or unauthorized modification either maliciously or accidentally. Integrity protects against forgery or tampering. Many document printing applications, such as payroll, absolutely require integrity.

Non-Repudiation: There is proof who sent a message that a recipient can show to a third party and the third party can independently verify the source.

Confidentiality: Protection from the unauthorized disclosure of print data, both during transport, in storage, and on the printer.

3.3 Encryption Concepts

Encryption: To scramble information so that only someone knowing the appropriate secret can obtain the original information. This might apply to the document being printed, or to the entire print request.

Nonce: In order to prevent an attacker from launching a replay attack, a very large random number or sequence number that is different every time the cryptographic protocol is run is used. A nonce can also be created from a time stamp that indicates the current date and time up to milliseconds accuracy.

Public Key: Dual key (RSA/PGP style) cryptography. Uses two different keys, either one for encryption and the other for decryption. Also called a asymmetric cryptography.

Secret Key: Single key cryptography. Also called symmetric cryptography.

Session Key: A short lived Secret Key used by two principals for the purpose of secure communications between them.

3.4 Authorization Concepts

ACL: Access Control List. A list of the subjects authorized to access a Printer, a print resource, or a document. The list usually indicates what type of access is allowed for each user.

Groups: A named set of users, created for convenience in stating authorization policy.

Roles: A specific function a principal plays with respect to another principal. Examples include a print administrator, a printer operator, or an end-user. If a principal has multiple functions with respect to another principal, it has multiple roles (e.g. A person can have both administrator and operator roles for a Printer).

Capability: An identifier that specifies an object, such as a Printer, and the access rights for the subject who possess the capability. See also "Certificate / Ticket / Token"

Proxy Agent: A principal that has been authorized to work on the behalf of another.

Proxy: A token that grants the rights of a principal to another.

Restricted Proxy: A token that grants the rights of a principal to another while placing restrictions on the privileges granted.

Certificate / Ticket / Token: Different names for a object used to grant privileges. While these terms have individual meanings in specific contexts (Kerberos generates tickets, physical objects are tokens), there is no general agreement on how they differ. We will use Certificate / Ticket / Token largely interchangeably. Capability & Proxy are related terms, but with narrower focus.

CRL: Certificate Revocation List. A list of revoked certificates.

3.5 Miscellaneous

Denial of Service: An action that prevents a system or its resources from functioning efficiently and reliably.

4.0 IPP Security Threats and Methods of Attack

The purpose of a security system is to restrict access to information and resources to just those users which are authorized to have access. To produce a system that is demonstrably secure against specific threats, it is useful to classify the threats and methods of attack by which each of them may be achieved.

4.1 Threats

Security threats for IPP fall into the following broad categories:

Resource stealing: The unauthorized use of facilities, such as printers, specific printer features, media, fonts, or logos etc. resulting in some value to the perpetrator.

Vandalism: Similar to resource stealing, but usually without gain to the perpetrator. Often results in denial of service to other authorized users.

Leakage: The acquisition of information by unauthorized interceptors during transmission.

Tampering: The interception and altering of information during transmission.

4.2 Methods of Attack

The methods by which security violations can be perpetrated in the IPP environment depend upon obtaining access to existing communication channels or establishing channels that masquerade as connections to a user with some desired authority. These methods are:

Masquerading: Submission of print jobs or performing other IPP operations using the identity and password of another user without their authority, or by using an access token or capability after the

authorization to use it has expired.

Eavesdropping: Obtaining copies of documents and job instructions without authority, either directly from the network or by examining information that is inadequately protected in storage.

Document tampering: Interception documents or other print job related information and altering their contents before passing them on to the printer or print server.

Replaying: Intercepting and storing print jobs or documents, and have them submitted again later. Example: Stock Certificate Printing.

Spamming: Sending irrelevant or nonsensical print jobs or other IPP operations to a printer or print server with the objective of overloading the system and prevent legal users to get service.

Malicious Document Content Code: Sending documents that contain malicious code which will bring the printer software into a loop or even ruin hardware components in the print device. Example: Using PostScript as a programming language to run the printer into an infinite loop.

4.3 Quality of Service

Liability: Responsibility of the user for the printed content. This holds the user accountable for making payments, usage of special resources like transparencies, color printing, etc. The printer is also responsible for the services performed and will be held responsible for it.

Provability of Service: The printer should be able to prove that it performed correctly according to the job attributes which the client/user had indeed issued. Example: The printer should be able to prove that the job request was indeed a monochrome when the user claims it issued a color copy.

Payment and Accounting System: It is a mistake to charge the wrong person when someone has issued a print request.

5.0 Attacks Vs. Security Services

The following table defines how the services described here address security attacks. A (C) in the table refers to client side services, an (S) server side services. CA = Client Authentication, SA = Server Authentication, DC = Data Confidentiality, DI = Data Integrity, NR = Non-repudiation, TS = Time Stamp and Nonce.

Attacks\Services	CA	SA	DC	DI	NR	TS
Masquerading						
1. User/Client (Incorrect source - misuse of resources)	Yes					
2. Printer/Server (Incorrect destination)		Yes	Yes		Yes (S)	
Eavesdropping		Yes				
Document Tampering						
1. incorrect rendering of data and job attributes				Yes		
2. guarantee security marks (watermarking, fingerprinting, security banners)			Yes			Yes
Replaying					Yes	
Denial of Service (Spamming)	Yes				Yes(C)	Yes
Document Malicious Content Code						
1. corruption of hardware resources	Yes	Yes	Yes			
2. corruption of printer software	Yes		Yes			

6.0 Quality of Service vs. Security Services

The following table defines how the services described here address security attacks. A (C) in the table refers to client side services, an (S) server side services. CA = Client Authentication, SA = Server Authentication, DC = Data Confidentiality, DI = Data Integrity, NR = Non-repudiation, TS = Time Stamp and Nonce.

Qual of Service/Services	CA	SA	DC	DI	NR	TS
Liability for						
1. printed content	Yes					Yes
2. for services performed		Yes				Yes
Provability of service					Yes(S)	Yes
Defeating payment or accounting system	Yes				Yes(C)	Yes

7.0 Required Security Services provided by current security methods

The following table describes how current security methods address the requirements discussed in this paper. Security methods would be invoked by standard means, i.e. IPP would use the URL https://www.xyz.com/printer-1 to name a printer that requires SSL.

Requirements	HTTP/1.1	SSL (V2)	SSL (V3)	LDAP
Authentication				
single entity	Yes	Yes	No	
mutual	No	No	Yes	
Authorization				
ACL	--	--	--	
Capability	--	--	--	
Non-repudiation				
Integrity	--	Yes	Yes	
Confidentiality	--	Yes	Yes	
Administration				
Certificate Mgmt.	--	--	--	Yes
Secure Comm.				

8.0 References

[1] C. Kaufmann, R. Perlman and M. Speciner, Network Security

[2] D. Russell and G.T. Gabgemi Sr., Computer Security Basics

[3] A. Freier, P. Karlton and P. Kocher, The SSL Protocol Version 3.0, Internet Draft <draft-freier-ssl-version3-01.txt>, March 1996

[4] K. Hickman and T. Elgamal, The SSL Protocol, Internet Draft < draft-hickman-netscape-ssl-01.txt> (deleted), February 1995

[5] X.500: The Directory -- Overview of Concepts, Models, and Service, CCITT Recommendation X.500, December 1988

[6] W. Yeoung, T. Howes, and S. Kille, Lightweight Directory Access Protocol, RFC 1777, 03/28/1995. (Work is alos underway in the IETF to produce an extended version of LDAP.)

[7] R. Rivest, The MD5 Message Digest Algorithm, RFC 1321, April 1992

[8] M. Mahl, T. Howes, S. Kille, Lightweight Directory Access Protocol (v3), Work in progress, Internet Draft <draft-ietf-asid-ldapv3-protocol-03.txt>, October 22, 1996

[9] J, Franks, P. Hallam-Baker, J. Hostetler, P. Leach, A. Luotonen, E. Sink, and L. Stewart, An Extension to HTTP: Digest Access Authentication, RFC 2069, January 1997

[10] J. Myers and M. Rose, The Content MD-5 Header Field, RFC 1864, October 1995

9.0 Author's Address

Roger deBry
HUC/003G
IBM Corporation
P.O. Box 1900
Boulder, CO 80301-9191

Jerry Hadsell
1130
IBM Corporation
Rt. 100
Somers, N.Y. 10589

Daniel Manchala
Xerox Corporation
701 Aviation Blvd.
El Segundo, CA 90245

Xavier Riley
Xerox Corporation
701 Aviation Blvd.
El Segundo, CA 90245

10.0 Other Contributors

Scott Isaacson
Carl-Uno Manros