Roger deBry
IBM Corporation
Jerry Hadsell
IBM Corporation
Daniel Manchala
Xerox Corporation
Xavier Riley
Xerox Corporation
John Wenn
Xerox Corporation
July 29, 1997

Internet Printing Protocol/1.0: Security
draft-ietf-ipp-security-01.txt

Status of this memo

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:

Requirements for an Internet Printing Protocol
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 is the `Internet Printing Protocol/1.0: Security' document.

Table of Contents

1.0 Introduction

The purpose of this document is to describe security considerations for the Internet Printing Protocol (IPP). Internet Printing is the application of Internet technology to network printing. Using Internet technology, users want to be able to locate printers, install and configure printer software, query printers for capabilities and status, and submit and track print jobs. The Internet Printing Protocol defines the network interface for many of these functions.

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 Transport Layer Security (TLS)[1] and Basic Authentication[2] and Digest Access Authentication[3]in HTTP.

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 not to 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, would 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.

2.0 Security Threats and Attacks

Before discussing security services specifically as they relate to IPP, it will be useful to quickly discuss and categorize security threats in a general way and discuss the means by which these threats are carried out.

2.1 Threats

Security threats 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.

2.2 Methods of Attack

The methods by which security violations can be perpetrated 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: Intercepting 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. Protection against replaying requires the use of a nonce and/or time stamp.

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 preventing legal users from getting 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.

3.0 Internet Printing Environments

It is now important to understand how the threats and attacks we have discussed above apply to the various environments in which IPP will operate.

The IPP Model encapsulates the important elements required for printing into three simple objects, the Printer, the Job, and the Document. The Printer represents the functions associated with a physical output device along with the spooling, scheduling, and multiple output device management often associated with a print server. An IPP client uses the IPP protocol to invoke operations on IPP objects on other network nodes.

The initial security needs of IPP are derived from two primary considerations. First, the printing environments described in this document take into account the fact that the client, the Printer, and the document to be printed may all exist in different security domains. When objects are in different security domains the requirements for authentication and message protection are much stronger than when they are in the same domain.

Secondly, the sensitivity and value of the content being printed will vary. For example, a publicly available document does not require the same level of privacy that a payroll document requires. There are at least two parties that have an interest in the value of the information being printed, the person asking to

have the information printed and the person who originated the

information. This brings into the picture the need to worry about copyrights and protection of the content.

Security attacks are now described for the following IPP environments. Where examples are provided they should be considered illustrative of the environment and not an exhaustive set. Not all of these environments will necessarily be addressed in initial implementations of IPP.

3.1 Client and Printer in the Same Security Domain

This environment is typical of internal networks where traditional office workers print the output of personal productivity applications on shared work-group printers, or where batch applications print their output on large production printers. Although the identity of the user may be trusted in this environment, a user might want to protect the content of a document against such attacks as eavesdropping, replaying or tampering.

3.2 Client and Printer in Different Security Domains

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 document remotely on a business partner's printer. This latter operation is functionally equivalent to sending the document to the business partner as a facsimile. Printing sensitive information on a Printer in a different security domain requires strong security measures. In this environment authentication of the printer is required as well as protection against unauthorized use of print resources. Since the document crosses security domains, protection against eavesdropping and document tampering are also required. It will also be important in this environment to protect Printers against spamming and malicious document content code.

3.3 Print by Reference

When the document is not stored on the client, printing can be done by reference. That is, the print request can contain a reference, or pointer, to the document instead of the actual document itself. If the client physically gets the document before it prints it, then this defaults to one of the previous cases.

3.3.1 Unprotected Documents

In many cases, documents to be printed are literally available to anyone. Documents, such as this Internet Draft which are stored on anonymous FTP sites, are good examples of this. No security mechanisms are required to protect access to these documents.

3.3.2 Protected Documents

Clearly, there are cases where the nature of a document requires that access to it be protected by some authentication and/or authorization mechanism, or where the right to print the document must be paid for. This would be the case for sensitive or confidential information, or where documents are copyrighted or sold for profit. Unauthorized access to content is a major concern in this environment. Protection against eavesdropping, document tampering and unauthorized access to the document are also concerns if the content is sensitive.

3.4 Common Security Scenarios

As discussed earlier in this document, we cannot anticipate the security levels or the specific threats that any given IPP print administrator may be concerned with. Security policies might vary from very strong, to very weak, to none at all, and corresponding security mechanisms will be required. In this section we will describe what we believe to be four common usage scenarios.

1) No security at all
2) Message protection during transmission
3) Client authentication and authorization
4) Mutual authentication, authorization, and message protection

3.4.1 No Security

If the server requires no authorization and the client wants no message protection the client can send the print job, i.e., the job content and the job attributes without invoking any security mechanisms. The printer will print the job for the client. Print by reference also works well in this environment as long as no security mechanisms are required to access the documents to be printed.

3.4.2 Message Protection During Transmission

There are two types of security that could be used to provide message protection. These are channel security and object security. In the first case, the transport medium must be made secure by mutual authentication. Then everything between the client and server is encrypted by the transport medium. The transport medium can be either of the following: transport layer security (TLS) or network layer security (IPSec)[4].

In the case of object security, each object is encrypted and sent over either a secure or an insecure channel. The recipient has the corresponding key to decrypt the object and get the contents. The most widely used object security mechanisms are S/MIME [5], S-HTTP [6] and PGP/MIME [7].

3.4.3 Client Authentication and Authorization

This scenario requires client authentication which may also be used for authorization. A user ID and password may be used for authorization purposes, and may be encrypted by the lower security layer. S/MIME and TLS are good examples of this. TLS supports both one sided and mutual authentication.

3.4.4 Mutual Authentication, Authorization and Message Protection

This scenario requires mutual authentication and message protection. TLS and Secure Sockets Layer version 3 (SSL3) are good channel level security providers in this category.

4.0 Security Services

Now that we have described the security threats that exist in the various environments in which IPP may operate, we will discuss the security services that are generally available to counter these threats. Security in general encompasses the software and hardware functionality to deliver the following services:

Authorization: Only authorized users should be able to gain access to systems, applications, data or services. Authorization may be based on authenticated identity, location, time of day, role, possession of a physical device or token, or other criterion.

Authentication: Authentication is the process of proving who a user or system is, and may apply to individual identities, roles, or groups. Authentication may be done with traditional methods such as passwords or challenge-response mechanisms, or with publicly recognized methods such as certificates.

Message Protection: Access control protects data when it is within a secure system environment. However, when data must travel outside of a secure system, such as across a public network, it needs to be protected. Message protection includes the following:

Data origin authentication guarantees that the data originates from an identified source.

Privacy protection guarantees that the data cannot be observed except by authorized parties.

Integrity protection guarantees that the data cannot be undetectably modified except by authorized parties.

Non-repudiation protection guarantees that actions taken on data cannot be denied by the subjects performing those actions.

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. Provability of service requires non-repudiation.

Payment and Accounting System: The Printer should insure that the wrong person is not charged when someone issues a print request.

5.0 Applying Security to IPP Operations

An IPP client uses the IPP protocol to invoke operations on remote Printer and Job objects. We now need to understand which security services are required for the various IPP operations. The IPP Operations are:

Create-Job - Create an instance of a Job object
Send-Document - Append enclosed data to a Job object
Print-Job - Print the enclosed job, with attributes
Cancel-Job - Cancel a previously submitted print job
Validate-Job - Validate attributes for a specific object
Get-Jobs - Return job queue information for a Printer object
Get-Attributes - Return attribute information for a Printer or Job object
Print-URI - Print a document by reference
Send-URI - Append enclosed document reference to a Job object
Get-Operations - Return IPP operations supported by the server

Every time a new connection with a Printer Object or with a Job Object is opened a new security context must established. An administrator may set up different security requirements for different operations, i.e. a user may be able to query a printer, but not submit a job. Once a Job is created, the same (or greater) level of security will be required to perform additional operations on that job.

5.1 Create-Job

When creating a print job, authentication of the client and the Printer are primary security considerations. Client authentication, along with authorization, protects against unauthorized use of print resources. Printer authentication guarantees the identity of the remote Printer.

5.2 Send-Document

When sending document content to the Printer, message protection is the primary security service required.

5.3 Print-Job

Print-Job combines the functions of Create-Job and Send-Document, therefore authentication, authorization, and message protection are all required.

5.4 Cancel-Job

Cancel-Job is only used to cancel a job. An end user may only be allowed to cancel his or her own print jobs. Therefore authentication is required to protection against unauthorized cancellation of a job.

5.5 Validate-Job

Validate is used to validate the attributes of a remote object. Administrators may choose to restrict the ability for certain end users to see the attributes of a Printer, so authentication and authorization are required services.

5.6 Get-Jobs

The level of security associated with the Get-Jobs operation depends on the policy set by an administrator. One common policy is for the complete job queue to be returned to anyone who asks. This policy requires no security. For more secure Printers, a common policy is to list details only on the print jobs owned by the end user, while giving little or no details about other jobs. This policy requires client authentication and authorization to match the client to the print jobs.

5.7 Get-Attributes

An administrator should be able to establish the level of security associated with getting the attributes of a printer. How security affects which attributes are returned is a policy decision and outside the scope of IPP.

5.8 Print-URI

Print-URI is like Print-Job except that only a reference to the document to be printed is sent in the request. Thus the Printer must fetch the document from the given URI in order to print the job. In IPP version 1.0 we only allow unprotected (see section 3.3.1) documents to be printed by reference. Additional, as yet undefined security mechanisms are required to print a protected document by reference.

5.9 Send-URI

Send-URI is like send-Document except that only a reference to the document to be printed is sent in the request. This operation has the same security concerns as Print-URI.

5.10 Get-Operations

An administrator should be able to establish the level of security required for someone to see the operations supported on a Printer.

5.11 Asynchronous Notification

When submitting a print job, a user may include an attribute which describes the address and method to be used for notifying the user of Printer events such as job completion. Notification is outside the scope of IPP and includes such methods as email and ftp. When security mechanisms are employed in delivering asynchronous notifications, security levels should be consistent with those used in submitting the original print job.

6.0 Comments on existing security technologies

TLS - Transport Layer Security: Seems OK, is near completion in the IETF and existing SSL product are probably compliant, or can be made compliant without much effort. TLS Provides channel level security.

SSL 2 and SSL 3 - Secure Socket Layer: Proprietary solution initially by Netscape, but TLS is very close. Provides channel level security.

PGP/MIME - Pretty Good Privacy MIME variant: The original PGP is widely deployed (but not much liked by the US government). The PGP/MIME version is now being worked on but is still not out, not yet stable, and not yet implemented and deployed. PGP/MIME provides object level security.

S/MIME - Secure MIME: Currently a private implementation from RSA. Although coming out as product from a number of vendors, unlikely to make it on the IETF standards track unless RSA decides to release their proprietary products as open standards. S/MIME provides object level security.

SASL - Simple Authentication and Session Layer [7]: This security feature negotiation protocol and does not provide any security services in itself. Hence quite limited usefulness for IPP.

HTTP 1.1 Digest Access Authentication: This provides some limited security services, mainly only client side authentication. It transmits a cryptographic digest derived from the user name, password, and a server generated challenge.

SHTTP - Secure HTTP: Although on the IETF standards track, this seems to lack some important features and does not seem to go anywhere in the market place.

IPSec - IP Security is an IETF standards track protocol for security on the IP layer. It consists of two separate mechanisms. The IP Authentication Header (AH) and the IP Encapsulating Security Payload (ESP). They can be used together or separately. The IP Authentication header provides integrity and authentication of IP datagrams. The IP Encapsulating Security Payload provides integrity, authentication and privacy. IPSec allows for either host keys or user keys to be used in security. IPSec can satisfy the IPP requirements for integrity and privacy. IPP Authentication, however, would require both IPSec use user keys and that the IPP application request use their own IPSec security association. Both requirements are recommended by IPSec but are not required.

6.1 Recommended Security Mechanisms

IPP implementations should provide a range of security options to meet the needs of different installations and user populations. The specific security services employed will be established by a site administrator. The mechanisms used to establish these services and to define user IDs and passwords to the system are implementation defined and outside the scope of IPP.

The security protocol used by a particular IPP operation will depend upon the security services implemented on the Printer, the security policy established by a site administrator, and the selection made by the client. This requires that the right handshake messages be passed to invoke the selected security service. These are described in the references for each security mechanism and are normally invoked by the client. Two printer attributes, message-protection-supported and authentication-authorization-supported are provided to help the end user know what to expect in terms of security. These attributes should also appear in the directory entry for each Printer.

When utilizing HTTP 1.1 as a transport for IPP, the security considerations outlined in HTTP 1.1 apply. When set by an administrator, IPP servers MUST generate a 401 (Unauthorized) response code to request client authentication and IPP clients should correctly respond with the proper Authorization header. Both basic authentication and digest authentication flavors of authentication should be supported. The administrator chooses which type(s) of authentication to accept. Digest authentication is a more secure method and is always preferred to basic authentication.

For secure communication (privacy in particular), IPP should be run using a secure communications channel. Both TLS and IPSec provide secure communications channels and provide for mutual authentication. The secure communications channel must be initiated prior to running the IPP protocol. There is no mechanism for bootstrapping a secure communication channel from within the IPP protocol itself.

It is possible to combine a secure communication channel with either Basic or Digest Authentication.

6.2 Firewall Considerations

Firewalls mostly play a role of enforcing corporate security policies, beyond that established for individual servers within the firewall. For example, an IPP Printer may be set up to report back features to anyone. This is allowable as long as the user is behind the firewall, but may be prohibited if the user is outside of the firewall.

Thus, the firewall acts as a proxy for all IPP Printers behind the firewall and intercepts all incoming HTTP POSTs from the outside. Firewall software may then respond appropriately, based on the established security policy: It could pass the message along to the Printer, close the connection, or respond with some error response. This could be done on an operation by operation basis. Likewise, the IPP Printer responses would be filtered by the firewall software before passing them back to the external client.

Firewall software could additionally filter requests based on job attributes, so, for example, only jobs specifying a single copy or only duplex jobs could be printed. However, it is very unlikely that firewall software would check for features specified in the actual document content, i.e. in the page description language.

7.0 References:

[1] T. Dierks, C. Allen, "The TLS Protocol", <draft-ietf-tls-protocol-03.txt>, March 24, 1997.

[2] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, **T. Berners-Lee, "Hypertext Transfer Protocol - HTTP/1.1",** RFC 2068, January 1997

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

[4] R. Atkinson, "Security Architecture for the Internet Protocol, RFC 1825", August 1995

[5] S. Dusse, "S/MIME Message Specification", <draft-dusse-mime-msg-spec-00.txt, Sep. 1996.

[6] E. Rescorla, A. Schiffman, "The Secure Hypertext Transfer Protocol" <draft-ietf-wts-04.txt>, March 1997

[7] M. Elkins, "MIME Security with Pretty Good Privacy (PGP)" RFC 2015, October 1996

[8] J. Myers, "Simple Authentication and Security Layer (SASL)", <draft-myers-auth-sasl-11.txt>, April 1997.

8.0 Authors' Addresses

Roger deBry
HUC/003G
IBM Corporation
P.O. Box 1900
Boulder, CO 80301-9191
rdebry@us.ibm.com

Jerry Hadsell
1130
IBM Corporation
Rt. 100
Somers, N.Y. 10589
hadsell@us.ibm.com

Daniel Manchala
Xerox Corporation
701 Aviation Blvd.
El Segundo, CA 90245
manchala@cp10.es.xerox.com

Xavier Riley
Xerox Corporation
701 Aviation Blvd.
El Segundo, CA 90245
xriley@cp10.es.xerox.com

John Wenn
Xerox Corporation
701 Aviation Blvd.
El Segundo, CA 90245
jwenn@cp10.es.xerox.com

Other Contributors

Scott Isaacson, Novell
Carl-Uno Manros, Xerox