

Internet Printing Protocol Working Group  
at the 38th IETF

These minutes were recorded by Don Wright.

The meeting was called to order by Carl-Uno Manros at 9:03 AM CST on April 8th at the Peabody Hotel in Memphis Tennessee.

Planned agenda:

- 1) Introduction of WG Charter and Internet-drafts
- 2) Protocol
- 3) Security
- 4) Requirements
- 5) Model and Semantics

CHARTER:

Carl-Uno reviewed the WG charter including the lists of:

- Advisor, Chairs, Editors
- Current Drafts

The goals and background information of the charter were then reviewed. (Carl-Uno's charts will be available as a part of the proceedings) A question was asked as to what directory methods would be used. The current plan is to define the directory schema so as to be directory neutral and to be optional. Since the original IPP BOF at the last IETF meeting, significant security requirements have been added to the charter. A question was raised as to how the directory information would keep up to date when used in a cached environment. Since IPP is not defining the directory access method only the schema, IPP will not be addressing the area of caching of directory information. Many people felt that the directory work should be a milestone after the protocol is done; however there were others concerned that while the actual document could be done later, it needed to be considered while working on the model. The WG will produce recommendations for inter-operation between IPP clients/servers and LPD clients/servers.

Charter Milestones:

March 97: Internet Drafts: requirements, model, protocol,  
and directory schema

May 97: Several implemented prototypes

August: Requirements I-D to IESG as informational RFC  
Mapping IPP/LPR mapping as informational RFC

Other documents submitted as RFCs

Contact Information:

Discussion list is [ipp@pwg.org](mailto:ipp@pwg.org).  
To subscribe: [ipp-request@pwg.org](mailto:ipp-request@pwg.org)  
Archive is <ftp://ftp.pwg.org/pub/pwg/ipp>  
Web Server is <http://www.pwg.org/ipp/>

A long discussion on what should be covered within the directory schema. One of the major potential problems identified was how to include access control as a part of the information available through the directory. The scope of IPP at this time does not cover administrative functions like job accounting.

PROTOCOL:

Steve Zilles presented an outline of the general direction the group is going in the area of "protocol." (Steve's charts will be a part of the proceedings.) A concern was raised that if multiple, alternative ways are defined to do something, we will fail. This comment was directed at the current direction to perhaps support Application/IPP and Multipart/Form-data as well as support both HTTP/1.1 and some new IPP TBD. The current protocol issues Steve identified are:

- 1) Status inquiries during data transmission
  - posting all the data at once
  - versus---
  - create job, send data
- 2) What must the server implement?
  - full HTTP/1.1
  - IPP subset of HTTP/1.1 (non-caching, origin server)
  - TBD protocol

Questions:

- Can we really subset HTTP/1.1?
- Work level difference between creating a new protocol versus subsetting?
- Harald Alvestrand. presented a concept of layering and a HTTP/HTML presentation of data to be send via or received from an IPP protocol.

Interoperability issues with potentially two protocols and syntaxes are:

- 1) One protocol, two syntaxes
  - server must implement both

- 2) Two separate protocol
  - formdata over HTTP
  - application/ipp over tbd
  - server may implement either
- 3) Does the request format determine the response format?
- 4) How are the operations coded?
  - in the formatted data
  - in the protocol header
  - in the URL that is the target.

#### SECURITY:

Carl-Uno presented the work being done on security for IPP. (These charts will be available in the proceedings.) The type of attacks that could be deployed against IPP were described including masquerading, eavesdropping, tampering, replaying, denial of service, document malicious content code (embedded programs in the print job), liability and provability of service. All these were mapped against security services like client authentication, server authentication, data confidentiality, data integrity, non-repudiation and timestamping/nonces. There were some areas of the chart that need to be updated with additional "yes"es. "Signing" was identified as something that has been very useful as a combination of authentication and integrity.

The group has looked at a number of security services being investigated including HTTP/1.1 (Digest Authentication -- RFC 2069), SSL(V2), SSL(V3) and LDAP. Additional security service suggested to be examined include sHTTP, SMIME and PGP.

Simple security service (like LPD user name) would probably not be appropriate for a standards track document (Keith Moore.) Adequate security must be defined but the security level may be negotiated between the client and the server.

Harald A: Decisions on security should be made by the working group not by the Area Directors but having no security will probably be a problem.

#### MODEL DOCUMENT:

Harald A. expressed his opinion that while the model document is very large, it seems incomplete. He had a several comments and will document them in detail to the distribution list.

Due to a lack of time, the Requirements document was not discussed.

The meeting was adjourned at 11:35AM CST.