Meeting notes from IPP Security meeting held at Xerox on February 7, 1997

I. Attendees

A. IBM
1. Roger DeBry Architecture & Tech., full time on IPP, Boulder CO
2. Jerry Hadsell, IBM Internet Division, Security Expert,
jhadsell@vnet.ibm.com, New York

B. Xerox: Carl-Uno Manros, Gopal Panchanathan, Steve Okamoto, Xavier Riley, Rick Yardumian, all from Xerox Corporate Research & Technology

II. General Notes

A. What scenarios are most important? Roger said Corporate Intranet first, corporate global Internet next, end user to commercial printer (e.g Kinkos) last.

B. General agreement that IPP should use standard security methods and not invent anything new.

C. Additional security standards not in the Steve Okamoto presentation.
1. SHTTP: Gopal felt SSL is so much better than SHTTP that SHTTP shouldn't be considered.
2. SPK: Light weight certificate mechanism. Might replace X.509 someday.
3. General agreement that LDAP would beat out X.500.

D. Gopal felt payment schemes were very important since he felt IPP would be of most use to the internet, i.e. commercial printers, not corporate intranets. Continuing this discussion, later, Gopal stated that if IPP did not enable new functionality i.e. if IPP does not go beyond LPR, why would users move to it? Gopal feels strongly that IPP should enable electronic commerce.

III. Scenario discussion:

A. Scenarios: (Rick's interpretation of Roger's slides)
1. No security: no user name, server will accept any job that it can handle.
2. Document data is encrypted.
3. Discovery: Example of getting a printer's public key.
4. Authentication: User ID required.
5. Authentication: User ID and password required.
6. Mutual authentication
7. Mutual authentication and exchange of secret keys.
8. Payment

B. Threats listed by connection scenario:
1. Client and IPP printer are both within the same organizational firewall.
   a) Misuse of printer resources by employee, e.g. sending large B/W jobs to expensive color devices.
   b) Confidential data on public printers. Jerry mentioned sub topic of how data is routed after printing.
2. Client and IPP printer are outside firewalls.
   a) Printer perspective:

(1) Misuse of resources by unknown clients, e.g. wasting paper, etc.
(2) Junk mail
(3) Denial of service, "spamming"
(4) Legal liability of printer based on content.
(5) Provability of service.
(6) Defeating payment system.
   b) User perspective:
(1) Incorrect destination
(2) Content integrity:
   (a) Correct rendering/formatting
(i) security marks (watermarks, banners, etc.) illegible
   (b) Correct content, i.e. transmission errors, malicious content change
(3) Confidentiality
   (a) As data flows across network
   (b) As it resides in the printer
   (c) Needed resource corruption
3. The client is inside the firewall, IPP printer is outside a firewall.
   a) Will the firewall allow print data to flow outside?
   b) Legal liability of user’s employer for printed content.
4. The client is outside the firewall, IPP printer is inside a firewall.
   a) Printer
(1) Unauthorized use.
   (a) Do we rely on firewall for authentication of user and capabilities or must the printer participate in authentication?
   b) Client
(1) Incorrect destination.
   c) The client is outside the firewall, IPP printer is inside the firewall, but client is employee. (Variation)
5. The client is inside the firewall, IPP printer is inside a different firewall.
   a) Liability against client Corp. to printer Corp. policies.

C. Real World Scenarios (lead by Jerry Hadsell)
1. Client
   a) Printer Discovery (client talking to directory service)
(1) printer lookup (based on required attributes)
(2) printer certification
(3) location (URL?)
   b) Client to Printer
2. Security Notes
   a) (Microsoft moved to Kerberos for NT 5) (Kerberos is secret key based versus SSL which is public key based and SSL is tied to TCP/IP)
   b) LDAP (aka lightweight X.500)
(1) supports different security schemes such as SSL and Kerberos
   c) SSL basics
(1) Security fixed once session/channel is established. SHTTP differed in that it allowed security levels to be changed on the "field" level.
(2) HTTP that uses SSL is bound to a particular SSL based "port".
(3) HTTP, FTP, etc. sit "on top" of SSL which sits on top of TCP/IP.
(4) Mutual authentication based on "certificates" which contain your public key.
(5) Confidentiality by encrypting the data stream on the network.
(6) Reliable session.
(7) What parameters does IPP need to be aware of to use SSL?

(8) Does IPP require mutual authentication?
(9) Less complex than GSS.
(10) Does not address threats that lie on the client and server since it only addresses the communication link.

IV. Commerce
A. Pay for print
1. Payment models
a) When
(1) Pay before (debit)
(2) Pay during
(3) Pay after
b) Account holder vs. Non-account holder (e.g. walkin)
c) Payment method
(1) Negotiation
(2) Online
(a) credit card
(b) digital check
(c) digital cash
(3) Offline - both electronic and non-electronic
d) Pricing
(1) Negotiation
(2) Estimation
e) Accounting
f) Non-repudiation
(1) audit trail
(2) cryptographic methods

V. Issues:
A. Single/multiple levels of security:
1. Should client and server negotiate what protocols to use?

B. Intranet versus Internet concerns:
1. Strong/weak authentication
2. Access control
3. Payment: Very important to commercial internet but also important to many intranets for cost control.
4. Usage rights

C. Assumptions:
1. Firewalls will be able to identify IPP traffic (even if HTTP is used?).
2. All IPP operations will be initiated from the IPP client. Notifications from the IPP printer to the user is not part of IPP.
3. Status reports are requested by the IPP printer is not part of the IPP.
4. One or more documents can be submitted with a single IPP job submission.
5. Print documents must be contained (by explicit content or URL reference) in the IPP client request.
a) "Pushing" documents asynchronously (e.g. separate ftp from any source) from an IPP client to an IPP server is not part of the IPP.
b) IPP does not specify the method of a server "pulling" a URL referenced document.

D. SSL
1. What parameters would IPP need to be aware of to use SSL?

2. Does IPP require mutual authentication?
3. Carl-Uno wants the client or the printer to have the ability to control the amount of security they need. Jerry said this is worked out during the "negotiation". The resulting URL from the discovery process should indicate if security is required.

VI. Next Phone Conference, Thursday, 13th, 1pm PST. Xerox to set up a phone number.

VII. Action items:

A. Jerry Hadsell to create a diagram showing HTTP/SSL security mechanisms.

B. Steve O. to incorporate his IPP environment diagram into the meeting notes and put into the IPP web site.

Rick Yardumian