Changes to DPWS Section (Security)

Dan Driscoll
Microsoft Corporation
dandris@microsoft.com

Security Issue 1

Describe use of x.509v3 certificates and TLS/SSL as the mechanism for identity/authentication and connection integrity

Current the Security section describes protocol negotiation instead of mandating a single mechanism. The negotiation is removed in later issues.

Security Issue 2

Remove reference to WS-Security

wsu: http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd [WS-Security-2004]

Reference is currently unused

Security Issue 3

Remove HTTP authentication

R4069: CLIENTs and DEVICEs MUST support HTTP Basic Authentication.

This requirement is not widely implemented and does not have the advantages of cryptographically security identity (x.509v3 certificates)

Security Issue 4

Clean up Network Model (7.1.5)

Remove:

- *It is assumed that MESSAGEs received from/via other administrative domains cannot be trusted.*

Security Issue 5

Remove section 7.1.6 (Security Association)

This section is too abstract to be practically useful.

Example:

R4013: Following discovery, the CLIENT MUST invoke the association process by authenticating the DEVICE using a protocol for security and parameters supported by both CLIENT and DEVICE as negotiated via Policy for the EPR.

Security Issue 6

Remove 7.1.8 (Security Protocols and Credentials) and clean up restrictions that depend on 7.1.8 (R4032 and R4036)

This section relies on mechanisms not defined in the rest of DPWS.

Ex: metadata in EPRs at Discovery:

*R4026: A DEVICE SHALL select from the list of Security Protocols and Credentials indicated by the CLIENT which Security Protocol the DEVICE wishes to use and return that selection in /soap:Envelope/ soap:Body/ */ wsa:EndpointReference/ wsx:Metadata of the corresponding Probe Match (or Resolve Match) SOAP ENVELOPE.*

Security Issue 7

Remove R4031

R4031: In the absence of any policy assertion for security, no security SHALL be required.

DPWS defines a fixed binding for dpws:Device, so no policy assertion is necessary. Adding a policy assertion would also require a WSDL for dpws:Device, which is currently unnecessary.

Security Issue 8

Replace sections on multiple identity with explicit non-statements

Example: *R4035: If a DEVICE has multiple credentials, it SHOULD send separate Hello SOAP ENVELOPEs using different credentials to sign each.*

Fix: *This section does not define any rules or requirements associated with a device that has multiple credentials or cryptographic identities.*

Security Issue 9

Fix R4038 to apply only to TLS.

R4039: If TLS is ~~negotiated as the Security Protocol~~ used, the CLIENT MUST initiate authentication with the DEVICE by setting up a TLS session.

Security Issue 10

Add xAddrs to R4070

R4070: A DEVICE MUST indicate the use of TLS for a MESSAGE exchange using the "https" scheme URI contained in the DEVICE description, discovery xAddrs, and WSDL.

Security Issue 11

Remove content negotiation from R4057

R4057: All secure communication for Description, Control, and Eventing between the CLIENT and DEVICE MUST use the Secure Channel. ~~*The protocols for encryption as well as the keys used for encryption are negotiated during the authentication phase.*~~

Security Issue 12

Remove R4009

R4009: Security MUST be applied for all MESSAGEs received from, sent to, or traversed through other administrative domains.

Should remove this to make a non-statement about composability of security profiles.

Editorial changes

- Fix R4005 to apply to “SENDER”/”RECEIVER” instead of “DEVICE”/”CLIENT”
- Fix R4008 to cover “RECEIVER” instead of “SERVICE”