Pending issues in draft-ietf-p2psip-base-22

Marc Petit-Huguenin
2012/07/31

Michael Chen 2011/011/07 – Stat Response Definition clarification

I believe the definition of hash_value should explicitly state the hash is computed on the DataValue.value excluding its 32-bit length bytes:

hash_value

A digest using hash_algorithm on the value field of the DataValue excluding its 4 leading length bytes.

The 4 length bytes of DataValue.value is already represented in MetaData.value_length thus should not be part of the hash input.

Michael Chen 2011/11/01 - Question about base draft section [10].7.4.2

Section [10].7.4.2 “Refreshing finger table" of the base draft stated that, "A finger table entry i is valid if it is in the range [n+2^(128-i) , n+2^(128-(i-1))-1]."

This range seems suggest that 'i' is an 1-based integer. However, in the 3rd paragraph, it refers to first entry of the finger table as "search through the finger table entries from i=0 and ..."

The text should declare the range of 'i' in the first paragraph, so its second sentence shall read:

"A finger table entry i is valid if it is in the range [n+2^(127-i) , n+2^(128-i)-1], where i is in the range of [0, 127] inclusive."

Michael Chen 2011/09/21 - Base section [11].4 clarification

A discussion with Marc Petit-Huguenin brings up the issue of "naked Ping" described in section [11].4 of the base draft:

If no cached bootstrap nodes are available and the configuration file has an multicast-bootstrap element, then the node SHOULD send a Ping request over UDP to the address and port found to each multicast-bootstrap element found in the configuration document. This MAY be a multicast, broadcast, or anycast address. The Ping should use the wildcard Node-ID as the destination Node-ID.

It should be clarified that this Ping message, wrapped the Frame Header is sent via UDP without DTLS, thus the term naked Ping. Further implication is that a RELOAD application that supports UDP must multiplex among three protocols: STUN, DTLS and framed_naked_Ping.

Michael Chen 2011/09/03 - Question about base draft [10].7.4.4 Detecting partitioning

Base draft section "[10].7.4.4. Detecting partitioning" says,

"P should then send a Ping for its own Node-ID routed through B."

Say you have a ring looks like this: ...-> X -> B -> Y -> P -> Z ->... where B is P's bootstrap node. If the overlay is healthy, wouldn't a Ping to P's own Node-ID sent to B be routed back to P itself? In that case, P will not be able to discover its possible new successor Z.

Michael Chen 2011/09/01 - Base draft [10].7.4.1 title does not match its content

[...]The title of the base draft section [10].7.4.1. is

"[10].7.4.1. Updating neighbor table"

Its first sentence says,

"A peer MUST periodically send an Update request to every peer in its Connection Table."

Which one is the intended collection of peer for periodic update? The first bullet of [10].7.4 seems to confirm that it should be "neighbor" table.

MPH 2012/07/03 - Signed configuration files in RELOAD

[S]ection 11.1:

" Any configuration file through the overlay (as opposed to directly from the configuration server) MUST be signed by one of the configure-signers from the previous extant configuration. Recipients MUST verify the signature prior to accepting the configuration file."

This text implies that configuration file coming from the configuration server does not need to be signed. But in this case how can a recipient receive a signed configuration file through the overlay?

MPH 2011/10/29 - Reissuing certificate

[S]ection [11].3:

"The enrollment server SHOULD maintain a mapping of users to node-ids and if the same user returns (e.g., to have their certificate re-issued) return the same Node-ID, thus avoiding the need for implementations to re-store all their data when their certificates expire."

[There is] still be two issues:

- How does this work if the user requested multiple certificates from the same login?

- How does this work if the number of Node-Ids requested changes?

[see also draft-ietf-pkix-est-02]

MPH 2011/09/22 - Base section [11].4 clarification

The problem is that it is a bad idea to establish a DTLS connection to an anycast address, as there is no guarantee that the subsequent UDP packets will reach the same host. It is even no guarantee that the ACK for the Ping answer will go to the same host, which is why I also think that Framing should not be used for sending a Ping to an anycast address.

But the problem in the case of anycast is NAT traversal. We cannot use the source IP/port of the Ping answer (or Ping request ACK) as an indication of the unicast address to use for subsequent transactions, because the packet will be dropped by symmetrical NATs. The reasonable thing to do would have been to add an IpAddressPort field in the Ping answer, field that contains the IP address/port of a unicast bootstrap server (as if retrieved in the configuration file), but the authors sent a clear message that breaking compatibility is out of the equation. So what do the authors propose to fix this problem?

Also I think that the spec should clearly state that a unicast bootstrap server MUST support both DTLS-UDP-SR-NO-ICE and TLS-TCP-FH-NO-ICE on its public IP address/port.

MPH 2011/10/31 – p2psip-enroll

The path in the URL used to request the configuration file is “/.well-known/p2psip-enroll”, which does not make much sense as it is not to enroll, and it is no longer specific to p2psip. The path should be something like:

“/.well-known/p2p-config”

MPH 2011/10/31 – Create self signed certificates with multiple Node-IDs

Section [11].3.1 does not define an algorithm to create self-signed certificates that contain multiple Node-IDs.

[The idea would be to] create self-signed certificates by prepending the index (from 1 to the number of Node-IDs needed) as a 4 bytes big endian integer to the public key of the user before applying the digest.