draft-ietf-dmm-4283mnids

Charlie Perkins

IETF99 Prague

17th July 2017

Issues raised

- Unclear from draft which MNID types need to be secured (e.g., for privacy)
- Unclear if all MNID types that are included are really needed
- Low volume of discussion in the working group is interpreted as a lack of support.

MNID types in the draft

- IPv6 Address (included for completeness)
- IMSI, P-TMSI, GUTI (for 3GPP adjunct uses)
- EUI-48, EUI-64 address (IEEE types)
  - Would be useful for multi-interface IP addresses
- DUID types
- RFID types
  - Would be useful For Mobile items tracking
  - Would be useful For Mobile banking payment (Wireless NFC Bank cards)
  - Would be useful For new innovative mobile cloud gaming over unique identification of new gaming elements (e. VR, AR, …etc)
- Consider adding new other id types in IoT such as proprietary Sig fox ids, or standard LORA ids, …others

Commentary from mailing list (1)

Vijay:

- Ben Campbell wanted us to explicitly identify which of the IDs have to be encrypted, and not just say that some of them may need to encrypted. … Perhaps we could say it depends on the context? Another option is to say message exchanges that carry a MNID, may need to be encrypted over the air interface, for all MNIDs. That might be the safest.

Charlie:

- I am O.K. with MUST be encrypted.

Commentary from mailing list (2)

Vijay:

- I read Stephen Farrell's DISCUSS a number of times. He seems to be saying any ID that privacy concerns needs to be explicitly justified. I can argue that there are privacy concerns with every single MNID. The user can be tracked using the MNID, irrespective of whether it is an IMSI, or DUID or RFID-GID-96.

Charlie:

- This provides additional justification for MUST encrypt, since we are operating at the network layer and cannot know if the applications need privacy.

Hakima:

- … in the case of RFID I believe, related to privacy, in fact if a device with an RFID tag for instance a bank card has to send in clear its numbers as a MNID in a packet then of course there is an issue, but I believe that matching the MNID with the IP address will be also secured inside the packet is it correct?

Commentary from mailing list (3)

Charlie:

- The downside of including them <i.e., more MNIDs> (assuming proper security measures are taken) is so small.

Suresh:

- This is exactly the crux of the problem (what you have in parentheses). By including the types *this document* is expected to include the proper security measures.

Charlie:

- I am O.K. with MUST be encrypted. I believe this to be a proper measure for each type.

Commentary from mailing list (4)

charlie:

- In fact, uses of such identifiers have been proposed in the past but inhibited by unavailability of the most straightforward identifier formulation. To put an identifier in later is certainly possible, but represents a lot more work in the future -- another multi-month (or year!) review cycle, another learning process to repeat the learning process we have already gone through, and so on.

Suresh:

- The issue is that nobody else is coming forward to say they need most of these types. The lack of enthusiasm in the WG has not reflected well on this draft among the IESG members.

Hakima:

- … remind that Internet to be part of the game of Internet of Things traffic exchange then it has to consider all types of communicating devices, knowing that we are talking in the near future of billions of sensors, actuators, RFID tags talking, then Internet protocols will take care of that and having IDs corresponding to all these types is the way to go to better manage for instance the mobility of those devices as using the device ID as a non changing reference information, and changing the addresses while on move. Other protocols might benefit from this ID information such as service discovery or end to end signaling. I believe the IETF worked years ago on separating the identifier (locator) and the address, this was meant to help mobility management but also securing the sender and receiver mutual authentication with trusted identifiers. Maybe we should think about how to build a secure identifier of each node which will be built upon the original identifier (eg IMSI, RFID, …etc) and another type of secure information. In that case privacy will be saved as the original identifier is not sent in clear? what do you think?

Commentary from mailing list (5)

Hakima, paraphrasing:

- RFIDs are likely to be an important wireless interface technology choice for IoT.
- More specifically unique hardware identification for item tracking
- New applications to be considered with new automatic RFID identification (Mobile banking, mobile gaming with AR, …etc)

Charlie:

- I agree with this.

Some example work in progress

- Mobile RFID tagged items using Mobile IPv6
  - http://www-public.tem-tsp.eu/~chaouchi/TRACKIOTMIP6.pdf

- Heterogeneous IoT Network: TRACK-IoT Platform
  - http://www-public.tem-tsp.eu/~chaouchi/TrackIoT.pdf

Next Steps

- Make sure issue resolutions are satisfactory.
  - Straw proposal: make encryption mandatory
  - Under this circumstance, should be O.K. to keep most existing MNID types.
- Make revisions to draft as determined
- Finish Last Call