IEEE P802.21 Media Independent Handover Services

Teleconference Minutes of the IEEE P802.21a Security Task Group

Chair: Yoshihiro Ohba

Editor: Lily Chen

Minutes taken by Lily Chen

Date: September 28, 2010, 9:00 am -12:00 noon, US EDST

Chair called the teleconference to order, reminded the IEEE-SA patent policy and introduced the participants:

List of Participants:

Lily Chen (NIST)

Yoshihiro Ohba (Toshiba Corporation)

Rafael Marin-Lopez (University of Murcia).

Fernando Bernal-Hidalgo (University of Murcia)

Ajay Rajkumar (Alcatel-Lucent)

Karen Randall (NSA, IAD)

Subir Das (Telcordia)

**Chair** called the teleconference to order and introduced the participants. Also reminded the IEEE SA patent and policy procedures.

DCN# 21-10-0203 was resented by Lily Chen. This describes key derivation in 802.21a.

**Q**: Do we want to use all 512 bits for MSK and do we need to support only HMAC or CMAC?

Comment: For example, we do not know why 802.11 only uses 256 bits for HMAC while deriving the second half of the MSK.

Lily plans to check with 802.11 folks and understand why they have chosen that route.

Comment: Hashing one is better than hashing twice. So we do not need to derive the keys separately.

A: The thinking process was to use two key derivation functions and call them separately when each them were needed. For example, if length was different but there was no particular reason why one function cannot be used.

Discussion focused on key derivation algorithm choice and at the end it was decided that a single key derivation will be used for both integrity and encryption keys

Q: Do both MIH peers know after pre-authentication, the key needs to be derived either for MIH service specific keys only or both MIH service specific keys and media specific root key and their distribution? In other words, is there any way both peers will know if there is a bundle or non-bundle case?

A: Yes, TLVs should be defined to have the indication and this will be exchanged during initial negation phase.

DCN #21-10-0204 was presented by Rafa and Fernando.

Discussion happened around MIHS header and security indication.

Q: Can you, Subir and Dapeng coordinate the security header?

A: MIH header is to indicate that MIH security is available or not. Our case and Dapeng’s case MIH will include the EAP which is not the case for Subir. There is no overlap with Subir’s proposal at this point.

Q: Dapeng’s primitives and your primitives are different names and seemed to be different.

A: Yes, we need to co-ordinate with Dapeng.

Rafa will work with Dapeng to harmonize this.

Q: Can we move P and F- bits by defining a generic security TLV?

A: It may be possible to move F-bit but not P-bit since P-bit is necessary even in case when security is not enabled.

Rafa will try to define a generic security TLV.

Comment: This will be included in the issue list.

Discussion also took place around the following questions that were listed in DN#21-10-0204.

-- Does MIH Finalization phase should be removed?

-- Capability Discovery 🡪 should parameters be removed?

 --Network selection could be affected

-- Should Session ID TLV be removed?

-- Do we really need the MIHS?

 -- Do we need protect the MIH Header?

A lot of discussions happened whether we need to include cipher-suite parameters in capability discovery or authentication message negotiation or both. We also need to define IEs to include

the cipher suite algorithms.

Teleconference ended at 12 noon.