**MINUTES OF MEETING**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name of the Meeting** | **GSSM#16 IoT WG** | | |
| **Date** | 11/03/2013 | | |
| **Time** | 10:00 AM to 11:30 PM (IST) | | |
| **Meeting Type** | Audio Call | Video Call | Face to Face |
| - | - | HMR Institute, Delhi |
| **Participants List** | Prof. Prasad (GISFI), Anand (NEC), Arvind (CISCO), Sivabalan(NEC), Ritesh(NEC), Niranth (Huawei), P Garg (GISFI), T R Dua (GISFI), Ashok Chandra (GISFI), Jijo(NEC), Bhagyashree (CDAC), Arjit (TCS), HMR Faculties and Students | | |

**Agenda**

|  |  |
| --- | --- |
| Sl. No | Details |
| 1 | Recap of Work items |
| 2 | New Contributions   1. GISFI\_IoT\_201403xxx: “Communication & Security In Internet of Things” CDAC : Bhagyashree Katole, Senior Technical Officer, NISG, CDAC, Pune 2. GISFI\_IoT\_201403yyy: Input to Technical Specifications on Low Overhead Security Scheme for Lightweight Application Protocol for IoT, Arjit, TCS, Kolkatta 3. GISFI\_IoT\_201403445: Study report on mapping the interface requirement of GISFI Lightweight IoT architecture with OneM2M architecture |
| 3 | Any other points |

**Action Item**

|  |  |  |  |
| --- | --- | --- | --- |
| Sl. No | Details | By | Deadline |
| 1. | Technical document need to be provided based on the architecture and security aspects discussed in this meeting | Bhagyashree , CDAC | Before next GSSM |
| 2. | Modified TR with all the details on the proposal including assumption and algorithms | Arjit,  TCS | Before next GSSM |

**Main Conclusion**

|  |  |
| --- | --- |
| Sl. No | Details |
| 1 | First draft on the technical specification need to be released during next GSSM |

**Discussion**

|  |
| --- |
| General Discussion |
| Ramjee prasad introduces GISFI activities to HMR students and faculty  Chaired by Sivabalan  Introduces IOT to audience  Agenda:  1. Reference Architecture  2. CDAC : Bhagyashree Katole, Senior Technical Officer, NISG, CDAC, Pune  Presentation on communication and security in IOT  Introduction  Device mobility in IOT  Device communication  Standards for Things to communicate:  - PASIS initiative to standardize IBM MQTT protocol  - OMG data distribution service (DDS) standard  MQTT based bridge interfaces  -optimized for centralized data collection and analysis  - HIVE MQ frontend  - Data distribution service (DDS): when all data need not be monitored in centralized way ?  - provides details of the software prototype implementation at CDAC pune  Security in IOT  Existing packages  - Key management for TinyOS  - Elliptic Curve Cryptography (ECC) packages for TinyOS  Conclusions:  1. intelligence reuired at device level for implementing sensor level security  2. Authentication and other features need support from base station  Questions:  1. What is TIny OS  Ans: it is OS for sensor networks.  2. What is MQTT ?  Ans: Publish subscribe system in sensor networks.  Discussion on the tradeoffs in prcessing and memory for MQTT  3. What si the role of data freshness in security for IOT  Ans: time stamped data needs to be tracked for considering recent data.  4. How privacy is maintained in IOT?  Ans: Chair inteerupts and suggests questions to be taken offline  ACTION:  There would a be document provided as input to the architecture and security technical specification  II. Arijit from TCS  Overview of specification document on IOT from TCS  SEcurity aspects on IOT  -General security requirements  -Proposed lightweight security for IOT  - Security requirements are listed  IOT-Sec-LTE : proposed solution  - using NONCE - number used once  - prevention of replay attack  - AES-128 CBC mode. - confidentiality for private key encryption  Results from UBICOM 2013 conference paper from TCS presented.  Questions:  1. how to differentiate between oriiginal and replay key  Ans: replay attack -> attacker captures encrypted userid and pswd and dlater stage authenticate using these.  NONCE used to protect from previously used authentication keys  2. is it similar to Google alternate authentication  Ans: no, user not in picture here.  3. Anand: clarifies on wider forms of replay attacks  More details on the NONCE proposal?  Ans: Details not shared here.There is a paper.  Anand: how do you propose to proceed?  Ans: we will give a modified document with all the details on the proposal.  Anand: Security rquirements depend on applications. we should have a statement on applicability of the proposed mechanism based on the application targeted.  Ans: one solutions doesnot fit all. for lightweight stuff, this may be sufficient.  Anand: request section on assumptions and equirements to be addressed  Siva: is this solution for I1 or I2 interface ?  Ans: for application, using COAP part. can be used for any interface.  III. NEC contribution: mapping interface requirement of GISFI lightweight IOT architecture with OneM2M  Sivabalan Arumugam  Existing functional entitites  Comparison with existing architecture and mapping of GISFI IOT interfaces  Mainly for healthcare usecases.  Qn: what is the use of mapping these interfaces  ans: there are many SDOs worldwide doing similar work. In an integrated environment, standardized solution is required.  Minutes of the session will be circulated within a week. |