**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 Contributions1. 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 facultyChaired by SivabalanIntroduces IOT to audienceAgenda:1. Reference Architecture2. CDAC : Bhagyashree Katole, Senior Technical Officer, NISG, CDAC, PunePresentation on communication and security in IOTIntroductionDevice mobility in IOTDevice communicationStandards for Things to communicate:- PASIS initiative to standardize IBM MQTT protocol- OMG data distribution service (DDS) standardMQTT 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 puneSecurity in IOTExisting packages- Key management for TinyOS- Elliptic Curve Cryptography (ECC) packages for TinyOSConclusions:1. intelligence reuired at device level for implementing sensor level security2. Authentication and other features need support from base stationQuestions:1. What is TIny OSAns: 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 MQTT3. What si the role of data freshness in security for IOTAns: 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 offlineACTION:There would a be document provided as input to the architecture and security technical specificationII. Arijit from TCSOverview of specification document on IOT from TCSSEcurity aspects on IOT-General security requirements-Proposed lightweight security for IOT- Security requirements are listedIOT-Sec-LTE : proposed solution- using NONCE - number used once- prevention of replay attack- AES-128 CBC mode. - confidentiality for private key encryptionResults from UBICOM 2013 conference paper from TCS presented.Questions:1. how to differentiate between oriiginal and replay keyAns: replay attack -> attacker captures encrypted userid and pswd and dlater stage authenticate using these.NONCE used to protect from previously used authentication keys2. is it similar to Google alternate authenticationAns: no, user not in picture here.3. Anand: clarifies on wider forms of replay attacksMore 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 addressedSiva: 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 OneM2MSivabalan ArumugamExisting functional entititesComparison with existing architecture and mapping of GISFI IOT interfacesMainly for healthcare usecases.Qn: what is the use of mapping these interfacesans: 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. |