International Institute of Information Technology Hyderabad

System and Network Security (CS5470)

Lab Assignment 2: Formal Security Verification of Security Protocols using the AVISPA backends: OFMC and CL-AtSe

Hard Deadline: **March 1, 2020 (23:55 P.M.)**

Total Marks: 100 [Implementation (Coding + correct results): 75, Vice-voce: 25]

Note:- *It is strongly recommended that no student is allowed to copy programs from others. Hence, if there is any duplicate in the assignment, simply both the parties will be given zero marks without any compromise. Rest of assignments will not be evaluated further and assignment marks will not be considered towards final grading in the course. No assignment will be taken after deadline. Please upload in the HLPSL code along with a README file in the course moodle portal through a ZIP file (Lab2-RollNumber.zip).*

Implement the protocol using HLPSL language of AVISPA specifying clearly the basic roles for the parties involved in the network, and mandatory roles for session, goal and environment. Your code must be well-commented and easy-to understand. You must also specify the secrecy and authentication goals in the implementation. Simulate the protocol using the OFMC and CL-AtSe backends.

1 Description of the Protocol with ODD Roll Number Students

Consider the protocol:
Muhamed Turkanovic, Bostjan Brumen, and Marko Holbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," in Ad Hoc Networks (Elsevier), Volume 20, 2014, Pages 96–112, https://doi.org/10.1016/j.adhoc.2014.03.009.
(http://www.sciencedirect.com/science/article/pii/S157087051400064X)

Implement this scheme of Turkanovic *et al.* provided in Section 4 (pages 99-104) for the pre-deployment phase (Section 4.1), registration phase (Section 4.2), login phase (Section 4.3), and authentication phase (Section 4.4). The paper is also with name (Turkanovic-Paper1-OddRollNos.pdf) at the Resources directory in the moodle. Note that pre-deployment phase and registration phase need to be executed via secure channel, and hence, you assume that the pre-shared secret keys between a user (U_i) and the gateway node (GWN), and between the GWN and a sensor node (S_j). However, login phase (Section 4.3) and authentication phase (Section 4.4) are executed via open channel as per the protocol.

2 Description of the Protocol with EVEN Roll Number Students

Consider the protocol:
Kaiping Xue, Changsha Ma, Peilin Hong, Rong Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," in Journal of Network and Computer Applications (Elsevier), Volume 36, Issue 1, 2013, Pages 316-323, https://doi.org/10.1016/j.jnca.2012.05.010.
(http://www.sciencedirect.com/science/article/pii/S1084804512001403)

Implement this scheme of Xue *et al.* provided in Section 2 (pages 318-321) for the (1) Registration phase; (2) Login phase; (3) Authentication and key agreement phase. The paper is also with name (Xue-Paper2-EvenRollNos.pdf) at the Resources directory in the moodle. Note that the registration phase needs to be executed via secure channel, and hence, you assume that the pre-shared secret keys between a user (U_i) and the gateway node (GWN), and between the GWN and a sensor node (S_j). However, login phase, and authentication and key agreement phase are executed via open channel as per the protocol.

Remark

In HLPSL, bitwise XOR operation $A \oplus B$ is represented as xor(A, B). All other descriptions regarding HLPSL implementation are available at http://www.avispa-project.org/.

All the best!