**Integrated MSc Course on Informatics Engineering, DI/FCT/UNL**

**Computer Networks and Systems Security / Semester 1, 2019-2020**

**WORK-ASSIGNMENT #2 REPORT for Evaluation**

A Secure Socket-Based Messaging Repository System with Mutual TLS Client/Server Authentication and Access Control

REPORT

**Authors:**

**Francisco Cardoso (**[**fj.cardoso@campus.fct.unl.pt**](mailto:fj.cardoso@campus.fct.unl.pt)**)**

***Summary***

A Secure Socket based Messaging Repository Service, providing mutual TLS authentication and access-control for authorized clients. The system enables users to exchange messages asynchronously. Messages are sent and received through a non-trustworthy central repository, which keeps messages for users until they fetch them. In the system model there are the following components: a Rendezvous Point or Server, and several clients exchanging messages.

To achieve confidentiality of the messages exchanged, messages are encrypted with a session key (256bits AES key), that key is encrypted with the private RSA key (2048bits) of the sender followed by the encryption with the public RSA key of the receiver. Then the encrypted message and encrypted key are concatenated and sent to the server to store the message in the receiver mailbox. Using these multiple encryptions, confidentiality and authentication of the sender and receiver is achieved.

To achieve integrity an HMAC of the message in plaintext is created using the same session key and stored in the receipts of the sender. When an user reads a message, again an HMAC of the received message in plaintext is generated and sent to be stored next to HMAC generated when sending the message. These 2 hashes are compared and if the generated hash from both users match, the message was successfully delivered and its integrity is achieved.

**1. Introduction**

From what you said in the Abstract, try to elaborate more on the motivation, introduction or background in approaching the work objectives, the implemented and validated objectives and the main aspects related to your implementation. If and when you consider relevant use bibliographic references to related work, related technology or any other bibliographic sources that can help to clarify the framework of your proposed and implemented solution. Try to have a good introduction in a half page as reference.

**2. System model and architecture**

**2.1 System model**

The system model for the project is composed by the following and related entities: (i) the multiple clients, through which users interact, and (ii) a server (used as rendezvous endpoint) for all clients to connect. All interactions between server and clients are made through sockets, with the possibility to user server-only unilateral TLS authentication or mutual client-server TLS authentication.

**2.2 Architecture**

In this section you can now discuss in more detail the software components and services, and how they are supported in your software architecture. In this you can include the description of the runtime and distributed system model and related technology used, as well as interfaces and operations supported in detail. Discuss the advantages and drawbacks of your implementation, as approached. Try to describe this in õne half page (except possible additional pictures, tables, temporal-diagrams or sequence diagrams that could illustrate the operations between entities and components.

**2.3 Threat model**

Discuss here the threat model beyond your designed and implemented system, explaining the considered attack-surfaces, security properties, security services and used mechanisms in your implementation used as countermeasures against the considered possible threats. Consider ~1 half page as average reference for the description of the threat model.

**3 Implementation details**

Use this section to describe your implementation details. the way you addressed the support for your system and their architectural components, involved software/development technology, as well as, system runtime support components and required installations to deploy and to run your solution. It would be interesting to have a complete vision on your implementation. For example you can add a table with all relevant technology you used, as well as, versions/releases and references that you can include in your final references.

With the description of this sections it must be clear for the reader to understand the main and more relevant aspects of your implementation, mapped on the system model and architecture initially explained.

You are free to consider a good and complete discussion but your exercise must be to address a reasonable and clear description of the most relevant and highlighted implementation details that you want to argue for your work done. 1 half page to 1 page must be a good reference in size, but you must see this related to the greater or lesser complexity of your implementation, as well as the related features, including configuration for flexibility and generality of the implemented solution. Try not to go over a page but if you consider additional details as relevant, consider using complementary annexes.

**4. Work Evaluation and Validation**

Use this section to discuss the validation and correctness of your designed system and related implementation (prototype). Explain the experimental evaluation done, the considered, focused and observed evaluation criteria. Discuss how you evaluated or measured your system for those criteria (referring experiments, practical observations/deployment and possible qualitative, as well as, quantitative metrics you’re your performed observations). If you want to structure more clearly the section, can use an initial paragraph describing the evaluation and validation objectives as addressed, dedicating a sub-section to specific observations done and argumentation about the system validity from your observations.

**5. Conclusion**

Use this section to summarize your main conclusions (aligned with the initially referred objectives addressed). Highlight in conclusion what you consider more relevant in your implementation and what you learned and what you consider more relevant form your experience in developing the work. You can finalize addressing how to overcome the limitations or drawbacks, or what you would propose as interesting to address, why and how in a perspective of future work hypotheses.

**References**

Put your cited references here, ex:

[1] Course on Computer Networks and Systems Security, MSc Program in Informatics Engineering, DI/FCT/UNL 2019/2020, Work-Assignment #2 Statement and Initial Specifications, November/2019.

[2] M. Schliep, N. Hopper, End-to-End Secure Mobile Group Messaging with Conversation Integrity and Deniability, in Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society, London UK, November 2019

[3] Katriel Cohn-Gordon, C. Crammers, L. Garrat, J. Milican, K. Milner, On Ends-to-Ends Encryption: Asynchronous Group Messaging with Strong Security Guarantees, in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, New York USA, October 2018

[4] Spring Framework, <https://spring.io> (available and retrieved in November/2019).

[5] Paul Sklenar, Securing REST APIs With Client Certificates, DZone Tutorial and implementation, <https://dzone.com/articles/securing-rest-apis-with-client-certificates> (available and retrieved in October/2019).

[6] Simplest method to Implement 2 Way Authentication using SSL, OpenCodez Tutorials, <https://www.opencodez.com/java/implement-2-way-authentication-using-ssl.htm> (Available and retrieved in October/2019).

[7] Jie Ma, Bn Qi, Kewey Lv, Fully private auctions for the highest bid, in Proceedings of the ACM Turing Celebration Conference, Chengdu - China, May 2019

# etc