COE817: The PROJECT

analysis/design/implementation

Deadline: April 09, 2021.

Requirements

1. You must do this project in a group of 3 - 4 students. Please submit your group members name and ID to TA.
2. A written report has to be generated per group. The report must be at least 10 pages long but no more than 20 pages (excluding the source code pages for the appendix). Use Times New Roman font size 12. Your report **must** include the following 4 parts:

Introduction:

Introduce the purpose and goals of the project. Provide any background material necessary. Discuss the scope, limitations and your brief contribution of your project.

Design and Implementation:

Briefly describe how the project is implemented.

Architecture Diagram: modules description and their functionalities.

Detailed description of security protocols used in your project. Include any techniques/principles that you have used in your design.

Results:

Screenshots of user interfaces, results and discussions.

Conclusion:

What have you learnt from the project? Describe leadership experience received for each member from the project. Describe contributions of each member in your group.

3. You may choose any suggested project or define your own comparable project. Your proposed project must be a programming work on security protocol or solution that may from but not limited to the following fields.

- AI in security
- IoT security
- Secure payment
- Attack and Defense
- Cloud security
- SDN Security

Please search some online papers to help you to determine the topic of your project. All your chosen project must be approved by the instructor.

4. You **must** provide the names and student IDs of group members in your report. All team members of a group will receive the same marks for their project. Marks will also depend on the contribution you described in conclusion section for each group member.
5. The report will be assessed not only on their technical or academic merit, but also on the communication skills of the author as exhibited through the report.
6. You must demonstrate your project before the deadline.

Cheating

- **No copying is permitted.** Cheating involves copying code or project from the web, other student's work, or projects of previous students, etc. The punishment for cheating is a zero in the project and will be subject to the university's academic dishonesty policy.

Suggested Topics

1. Implement SSL protocol with Java security framework.

Familiar yourself with the following 4 parts of Java security framework described in https://docs.oracle.com/javase/tutorial/security/.

API and Tools Use for Secure Code and File Exchanges
Signing Code and Granting It Permissions
Exchanging Files
Generating and Verifying Signatures

Design and implement SSL handshake and record layer protocol at the application layer (your implementation on record layer protocol may not include the compress and decompress steps). Use as many ciphers, protocols, algorithms/functions from the framework.

2. Digital Certified Mail

This project implements the digital certified mail scheme. A more theoretical discussion is found in "A Randomizing Protocol for Signing Contracts," by Even et. al., *Communications of the ACM*, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.98.7448&rep=rep1&type=pdf. The objectives of digital certified mail are (1) to require that a recipient sign for a message prior to receiving it, and (2) to prevent a sender from forging a receipt.
The solution involves several exchanges of keys to ensure that when the sender has a valid receipt, the recipient will also have a decrypted version of the text. Both sides must generate random DES keys, and encrypt receipts and one bogus message (to be sent by the Sender). Both sides will transfer the keys to each other using the oblivious transfer protocol.

3. *Secure Purchase Order*

Implement a secure purchase order system that allows the user to enter a purchase request and routes it (by secure email) to a supervisor for signature and then to the purchasing department.
• All connections between parties will be preceded by public-key mutual authentication.
• The signatures of both the purchaser and the supervisor will be public key based, and will be performed on a hash of the purchase order. The signature of the purchaser will be sent to both

the supervisor and the orders department along with a timestamp. If an order is approved by the supervisor, the orders department can cross-check the digest signed by the supervisor with the digest signed by the purchaser. The signature and time-stamping is obviously important in preventing repudiation. I am purposely ignoring the possibility that a user will "publish" their key to back up a repudiation. Ideally, the user's key will not be easily accessible and, since the whole process takes place in one organization, the possible means of revealing a key are very limited. The biggest threat is a user using another user's machine the forge an order.

- All messages will be encrypted using RSA public-key cryptography. Depending on performance (and time) this might be optimized by using RSA to only send a one-time secret key.

4. ***Flow Table Security in Software Defined Networks (SDN)***

Software Defined Networking (SDN) is an emerging networking paradigm in which the control plane and the data plane of the network are separated. In SDN, a controller monitors the whole network and makes decisions on packet forwarding (data plane) for the switches inside the network. In existing SDN frameworks, the main interface to the network switches is OpenFlow. An SDN controller inserts and updates flow entries, forwarding rules for the current traffic flows into one or more flow tables inside each switch. The resulting decoupling of the control and data plane simplifies network monitoring, fault tolerance and at the same time it introduces new security issues. In this project you need to investigate the security challenges and proposed solutions discussed in different scholarly articles.

Submitting your project

(1) Submit your project report and source code to D2L before the due.
(2) Demonstrate the project in the lab.