Ciências ULisboa | Informática

Data Privacy and Security

Project

1 First Part

The aim of this project is to give students the opportunity to put the topics they have studied in the lecture and lab classes to practice. In more detail, in this project the students are asked to build a **secure P2P messaging app**, similar to WhatsApp/Signal/Telegram. Next is a list of requirements for the app.

BASIC REQUIREMENTS (10 points):

- The messaging app should be as decentralized as possible
- The app should allow sending messages between any two users with end-to-end encryption guarantees (i.e., only receiver and recipient of a message should be able to learn its contents)
- Communication between users should provide standard reliability guarantees, i.e., message delivery, ordering, etc.
- A client interface should also be implemented for testing and visualization purposes, showing the list of conversations of a user and the contents of a specified conversation

Students can use any programming language, OS, tools, and frameworks they desire to develop their app. Additionally, the security and communication aspects of their apps can be developed using any combination of protocols and algorithms. Projects will be evaluated according to the following criteria:

- Completeness of the solution regarding the basic requirements
- Level of decentralization of the developed solution
- Security guarantees offered (including all aspects of security, such as privacy, integrity, and authenticity)
- Performance of the solution (as a secondary aspect w.r.t. to security, but solutions should still be efficient enough to be usable in practice). Performance includes: the time it takes to send and receive messages (i.e., latency), network load (i.e., communication overhead), and storage requirements (i.e., storage overhead).

Besides developing and submitting the code for their projects, students will also have to submit a written report describing their solution and the developed features. The report should also analyze the security guarantees offered, and why the students consider that they are offered. **Reports should be no longer than 3 pages** and should clearly identify all group members.

Delivery Date: 3/11/2024

2 Second Part

Besides the listed basic requirements, students can choose from a set of extra functionalities to implement in order to improve their score (up to a maximum of 20 points):

GROUP CONVERSATIONS (4 points):

The goal of this extra functionality is to add support for secure end-to-end group conversations between multiple users. Groups are defined by topics of interest. Solutions will be evaluated regarding level of decentralization, security guarantees offered and performance.

LONG-TERM STORAGE OF MESSAGES (6 points):

The goal of this functionality is to add availability guarantees for messages. Persistence is not enough, messages should be replicated to multiple external storage solutions (e.g., cloud providers), as to guarantee that if the user's device and/or a single provider is compromised, messages can still be recovered. Adding this functionality will also open other issues regarding privacy and security of messages, as providers are not expected to be trustable. Solutions will be evaluated regarding the level of decentralization, availability and security offered, as well as performance.

MESSAGE SEARCHING (6 points):

The goal of this feature is to add a privacy-preserving searching functionality to messages of a user, allowing him to search any conversation he has participated by issuing one or more keywords. Solutions will be evaluated according to the expressiveness of queries supported and the level of security guarantees offered, as well as performance.

RECOMMENDATION SYSTEM (8 points):

The goal of this feature is to add a privacy-preserving recommendation system that can analyze messages and send targeted publicity to users, all the while preserving the confidentiality of the users' messages and anonymity regarding which user is targeted by which publicity. This feature will possibly require working with a machine learning framework in order to match users with publicity. Solutions will be evaluated regarding the usability/accuracy of the system and the level of security guarantees offered, as well as performance.

Delivery Date: 13/12/2024

As in the first delivery, students should prepare a **report** of **at most 3 pages**. Additionally, students will have to make a presentation and demonstration of their work for all colleagues (and professor) to attend. This presentation will be scheduled for the end of the semester.

Presentation Date: 16/12/2024