Public key Tracing Framework using Blockchain

Supervisors: Prof. Dr. Alexander Pretschner, Mohsen Ahmadvand
Email: ahmadvan@in.tum.de
Phone: +49 89 289 – 17, 314
Starting date: immediately

Context
In recent years, instant messaging has become a popular means of communication among users. This has led to an increased amount of data exchange over the network. The exchanged data is usually privacy-sensitive, which makes data protection crucial in such systems.

The market leaders (such as Whatsapp and Telegram) aim at mitigating the risk by utilizing end-to-end asymmetric encryption, where all the exchanged data is encrypted with the corresponding public key of users. Despite the utilization of advanced encryption, clients could still be tricked to encrypt data with public keys of attackers instead of their recipients’ keys [5,6]. These attacks, known as Man-in-the-Middle (MitM) [4], could lead to the violation of privacy. The weakness lies in the fact that users are incapable of authenticating, or at the very least tracking, their recipients’ public keys over time. Users’ possession of multiple devices (and thus multiple keys) and the possibility of legitimately obtaining new keys (e.g. in case of a device loss) worsen the situation.

Goal
The goal of this thesis is to enable users to track and authenticate any changes in the public keys of their recipients to mitigate, or at least detect, MitM attacks. To achieve this goal, we aim to bring transparency to the system by resorting to unforgeable transactional systems. In this model, all users (without any involvement of the main server) report their key changes to a distributed ledger. These unforgeable transactions later help establish a chain of the key changes upon which malicious records can be detected.

In this thesis, the student will review existing adaptations of transactional systems to cope with MitM attacks, e.g. Blockchain based DNS chain [2] and secure logging based certificate transparency [1], and subsequently compare their applicability, advantages and disadvantages for the given use case. Based on the outcome of the review, they will adopt the technique that best suits the use case. Using the selected technique, the student will then implement an authentication mechanism and integrate it with a real-world messaging application. Lastly, the security as well as the performance of the implemented mechanism will be thoroughly evaluated.
Workplan

1. Write a state-of-the-art survey on MitM mitigation techniques using transactional systems
2. Compare cons and pros of different schemes w.r.t. the use case
3. Adopt the scheme that best suits the context
4. Implement an authentication mechanism based on the selected technique
5. Conduct a case study with a real-world messaging software
   a. Integrate of the mechanism into the existing system
   b. Evaluate the security using attack defense trees
   c. Evaluate the performance of the mechanism including memory and runtime overhead analysis
6. Write the final thesis document
   a. Description of the problem and motivation
   b. Description of the theoretical background
   c. Implementation description
   d. Performance evaluation of the implementation
   e. Security evaluation
   f. Conclusions and future work

Deliverables

- Docker container able to run a demo of the implementation, including instructions on how to run the demo
- The container should also include the source code of the implementation
- Technical report with comprehensive documentation of the implementation, i.e. design decision, architecture description, API description and usage instructions
- Final thesis report written in conformance with TUM guidelines

References