COINS:
Secure Cloud Services and Storage Workshop 2017 Report

B. Hale

The Secure Cloud Services and Storage Workshop 2017 took place in Oslo. The workshop was funded by the Norwegian Research Council (Forskningsradet), as part of the IKTPLUSS project between Norwegian University of Technology (NTNU) in Trondheim, University of Mannheim, and Universitet i Bergen (UiB).

While there were many excellent talks during the workshop, two talks are summarized in the following overview for conciseness. Consequently, this is neither an exhaustive list nor an overview of the most interesting talks. However, it underscores the value of discussion for practical cloud security in the modern and future world.

Project Introduction. Kristian Gjøsteen introduced the cloud project behind the workshop funding. This included an introduction to de-duplication in the cloud environment, where multiple files are uploaded by different users, and the cloud wishes to lower storage demands by storing only one copy. This can create confidentiality issues if users (or the cloud) can link users based on duplicate files.

Key management, including key revocation and deletion, was also touched on in this context. Gjøsteen discussed the idea of cloud-assisted key exchange, where some parties may not be online at the time of the key exchange. While a key exchange protocol was mentioned for handling this, no details were presented.

Talk: Selected Security and Privacy Schemes for Cloud Computing. The first presentation of the program was given by Refik Molva of EURECOM. In his talk, Molva stated that cloud solutions must be asymmetric, as the storage and computation costs are largely on the cloud provider. Moreover, Molva argued that traditional techniques are not sufficient in the cloud environment because they do not scale. Large data contexts demand suitable techniques.

Molva also discussed searchable encryption in the cloud context for a particular use case. Two solutions that explicitly did not scale for the use case are 1) encrypted keyword search algorithms and private information retrieval (PIR). Ultimately, Molva and his team developed PRISM (Privacy Preserving Search in MapReduce) to address this problem, which is claimed to maintain both data and query privacy. The core idea of the PRISM approach is to use PIR on intermediate data maps.

Further in his talk, Molva discussed work he had done on proof of retrievability, which is the case of outsourced data where the customer wishes to check that the data can be retrieved. The client should be able to check that the entire data set is still stored, while not storing any information on the client-side or transferring any data. Molva provided a high overview of a solution to this problem, which will be presented in full at ESORICS '17.

Talk: Gestalt vs. Constructivism: Designing Blind Cloud Storage in the Real. Moti Yung of Snapchat talked about cloud storage in the context of photo applications for the Snapchat company. Specifically, he addressed the cloud context for MEMORIES – a cloud storage for photos uploaded from SPECTACLES (a camera / glasses hybrid).

Yung's use case is summarized as follows: users have authentication mechanisms (e.g. password), and may change devices. Devices may also change owners. Ideally, privacy should be achieved against servers and other users after upload to the cloud. Various solutions that could be considered include password-based key, 128-bit entropy password, and a password-encrypted strong key on device. However, all of these have mobility, weakness, or usability issues.

Ultimately, the solution that was proposed by Yung uses secret sharing, with the overall semblance of password-based secret sharing. Discussing the problem and potential solution, Yung particularly focused on the method of reaching a solution, i.e. Gestalt vs. Constructivism. Referencing the Gestalt view, which consists of looking at the entire problem, Yung noted this method is an approached used in a typical "Crypto"-paper format: Gestalt results in elegant closed systems, where the model makes the results clear. In comparison, Constructivism considers various parts of a system to explain the whole. This is particularly interesting in contexts where system design is not from scratch, such as in the Snapchat context. Important considerations in the case of Snapchat, which can also be consider in other real-world contexts, include:

1. A system exists.
2. Some actions already exist (e.g. black boxes), which can and should be exploited if possible.
3. Adding crypto where crypto exists is performance killing and should be avoided.
4. Systems need flexibility of design to account fo modularity and the development process, and should not disturb the user experience.

Fundamentally, Gestalt provides sophistication while Constructivism provides a little sophistication but is also very usable.

Finally, Yung presented the "Give-and-Take" protocol, a secret-sharing solution in terms of passwords, keeping in consideration the above points while also noting the necessity for future flexibility (i.e. considering and predicting future changes and adaptations to the system). In many aspects, the "Give-and-Take" protocol bears similarities to Kerberos. However, the protocol is intended to achieve *just* the necessary functions for the system – achieving flexibility and minimalism. In a final statement, Yung claimed that servers can be separated, contrary to common arguments, if designed correctly. Such arguments often stem from concerns of server collusion; however, Yung claimed that, given control and design of a system, such concerns can be allayed and use of trust models involving distributed servers can realistically be employed.