WP4 Interim Report - Jan. 2018

Topic 1 – Secure Intermediary

(UH)

Targeted Scenarios

WP2 intends to develop technologies for cloud-assisted trust relation databases (**WP2-02: Private Graph Search**) for evaluating trust relationships among communicating entities in untrusted environments. All the communicating nodes are modeled as vertices in a connected graph where each vertex has a unique fingerprint. Any two vertices (i.e. nodes) can only communicate if they have a directed (trusted and verified) path between them. The presence (or absence) of such a path is dictated by the security policies of the destination and an administrator.

Achieved Results

We have been developing methods for making anonymous queries to the cloud to find out if there is a path from one node to another. This work **has been accepted to NTMS '18** [1].

This protocol does not necessarily require usage of a secure intermediary. However, such an entity could help participants in the protocol, thus making the solution more feasible.

One scenario that utilizes secure intermediaries is as follows. The party that owns the trust relation database calculates the transitive closure matrix of the graph corresponding to the database. He sends to every party that is allowed to make queries the mapping he used between users-hosts pairs in the database and the columns and rows of the matrix. He also sends the matrix to a secure intermediary 1 that encrypts it and releases the result to the cloud.

The party that makes queries to the database sends his query to another secure intermediary 2 who encrypts the query and sends it to the cloud. The cloud calculates the encrypted answer to the query and sends it to the querier through the secure intermediary 2. With the help of the secure intermediary 1 the querier decrypts the result.

The cloud learns nothing, the first secure intermediary only knows the trust relation database without labels and the second intermediary knows nothing.

We have implemented the most important parts of the protocol, the encryption of the graph, the encryption of the query, the calculations for the result and the decryption of the result. We have been able to show that the protocol works in reasonable time. We have also an implementation of the secure intermediary functionality. The next step is to implement the whole system.

Other scenarios that include secure intermediaries are also possible. We are carrying out studies in order to identify the most promising ones and later plan to extend the system implementation to cover also these other scenarios.

We have also implemented a similar structure for using secure intermediary in **private membership testing of WP1-01** [2].

1. S. Ramezanian, T. Meskanen, V. Niemi. Privacy Preserving Queries on Directed Graph. Accepted to NTMS'2018 - Security Track
2. S. Ramezanian, T. Meskanen, M. Naderpour, V. Niemi. Private Membership Test Protocol with Low Communication Complexity. International Conference on Network and System Security, 31-45, 2017.

Topic 2 – Trusted Hardware in the Cloud

(Aalto)

Targeted Scenarios

TEE-based solution for **private membership test (WP2-01)** assumes that trusted computing technologies can be used in the cloud settings. WP4 focused on studying the feasibility of these technologies when utilized in the cloud. Another possible scenario that could benefit from trusted computing in the cloud is **IoT cloud assisted management (WP1-02).** WP4 identified the main challenges of using trusted computing technologies in the cloud settings and proposes solutions to them.

Achieved Results

As identified in the WP4 requirements one the main challenges if supporting live migration of VMs that contain Intel SGX enclaves. WP4 developed and implemented a solution that takes into account architectural limitations when dealing with migrating SGX enclaves. The work is **submitted to DSN 2018.** The achieved results show that it is possible to support the VM migration with enclaves with small overhead. The protocol is based on including a library into a migratable enclave that provides migratable alternatives to native SGX functions. Additionally, each cloud provide physical host should contain a management VM with a migration enclave that performs mutual attestation between the source and the destination and handles the migration in a secure fashion.

Supporting scalability is another important aspect of cloud environments. Related project work identified the need for enclaves that maintain a rate-limiting cap. The adversary should not be able to overcome the limitation by launching multiple instance of the enclave. On the other hand, it should be possible to revoke enclaves from the system and the rate limit should not decrease due to this operation. This requires a consensus protocol between enclaves. The design of such protocol is presented in the paper [2].

1. F. Alder, A. Kurnikov, A. Paverd, N. Asokan. Migrating SGX Enclaves with Persistent State. Submitted to DSN 2018.
2. K. Krawiecka, A. Kurnikov, A. Paverd, M. Mannan, N. Asokan. Protecting Web Passwords from Rogue Servers using Trusted Execution Environments. Accepted to WWW 2018.