A Custom-classification of Communication Flow in a Client-server Model

Aleksandar Hudic
SBA Research
Vienna, 1040, Austria
Email: ahudic@sba-research.org

Elise Revell
Kelisec AB
Stockholm, SE 101 23, Sweden
Email: elise.revell@kelisec.com

Dimitris E. Simos*
SBA Research
Vienna, 1040, Austria
Email: dsimos@sba-research.org

*This work was carried out during the tenure of an ERCIM “Alain Bensoussan” Fellowship Programme. This Programme is supported by the Marie Curie Co-funding of Regional, National and International Programmes (COFUND) of the European Commission.

A Custom-classification of Communication Flow in a Client-server Model

In this work we describe a communication method, first proposed in [1] and extended in [2], which gives an approach for establishing secure communication between two entities. In addition, we present a security classification of its communication flow. The original concept given in [1] proposed a key generation method that produces symmetric keys in the nodes themselves without revealing them over an insecure channel. This method assumes a trusted third-party, i.e. a secure server (SeS) and clients (nodes) that want to become members of a secure network.

Based on the communication method given in [2], we propose the following four phases of renewal, authentication, key generation and key scheduling for a client-server model. For the state-of-the-art of client-server models we refer to [3]. A high-level overview of these phases can be seen in Figure 1.

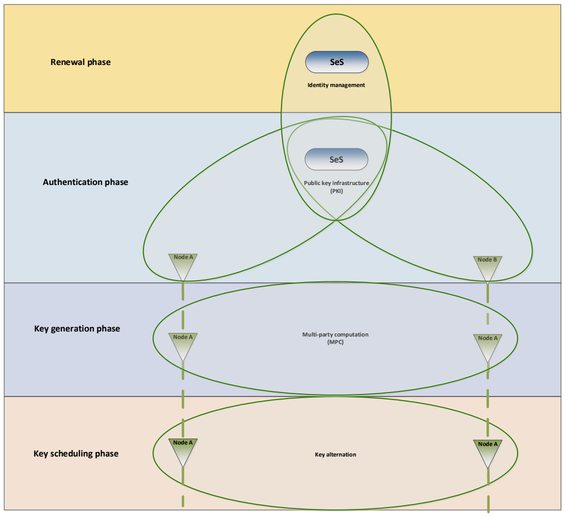

Fig. 1. Proposed communication phases.

a) **Renewal phase:** In this initial phase of the communication method described in Figure 1. In this phase, there are nodes that are already registered in the secure network but not necessarily be authenticated (see also the following phase). Therefore, the authentication tokens of the nodes are renewed in order to avoid replay attacks.

b) **Authentication phase:** Is the second phase of the proposed communication method. We consider, for this phase as an example, the following scenario: *There is a node that wants to become a member of the Secure network. In practical terms, a node could be a bank client operating a transaction through a mobile phone or a tablet. The identity of this node is not known beforehand and therefore we can assume that it can also be a malicious attacker. Therefore, at this phase secure authentication of the node has to be ensured.*

Secure authentication in this phase is ensured through Public Key Infrastructure (PKI), whereby we assume that each entity in the communication process has been uniquely assigned public/private keys. PKI keys are used to perform and ensure secure mutual authentication process between the nodes and SeS server.

c) **Key generation phase:** The key generation phase encompass a key generation method for symmetric encryption without revealing the generated keys over an insecure channel. To avoid any kind of insecure key distribution over the secure network, the key generation process of this phase is conducted in such a manner that the keys are generated within the corresponding nodes.

d) **Key scheduling phase:** The last phase of the proposed communication method provides a key alternation process in order to enhance security. The symmetric key used for session is changing during one communication session, and potentially can increase the security of the communication method.

The baseline of each communication process, between two entities, is to ensure confidentiality, integrity and authenticity of the corresponding entities. Therefore, proper security mechanisms have to be embraced in order to protect the communication channel and the parties that are using it. The concept given in [2], gives an overview of a security architecture in order to provide secure communication between two entities (nodes).

The communication scheme of [1] and [2] can be defined as two independent processes:

- Node to node communication
- Node to server communication

Node to node communication - Two particular nodes are trying to directly establish a shared session and generate a symmetric key.

Node to server communication - Both of the nodes that are participating in the communication, have to be registered and authenticated in the secure network. In order this to be achieved they need to have a direct correspondence with the server.

We now aim to a classification of the communication flow in the client-server model we have used so far. Our goal is to accomplish this classification over the four phases described in Figure 1 by classifying their security levels.

We propose a general security classification, in respect to the communication scheme, by defining the following security classes:

- Low security
- Medium security
- High security

The four phases of the communication method are considered together with the security classes in order to investigate security aspects of the communication flow. We target on communication flow of corresponding parties that are involved in the works mentioned by [1] and [2], i.e. the nodes and the SeS server. The proposed security classes are used to define a rough security classification that represent an initial point of our future security analysis. Through these security classes we would like to investigate and analyze security concerns related with the communication flow, by evaluating the communication correspondence between the server and the nodes. We propose a classification of the communication flow in the previous client-server model in Figure 2. As future work, we plan to extend this communication diagram in a taxonomy classification by uniquely defining its corresponding sub-blocks.

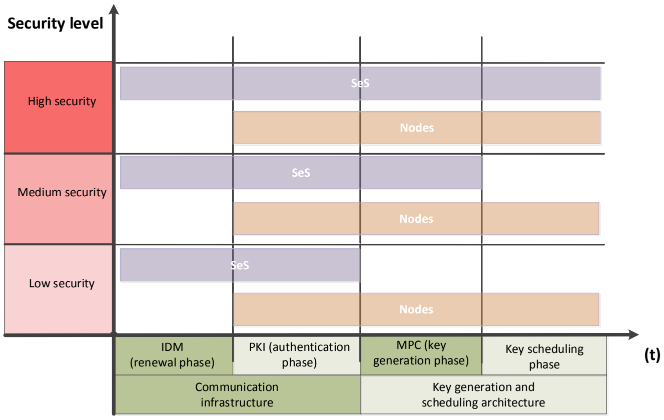
Security level
High security
Medium security
Low security
SeS
Nodes
SeS
Nodes
SeS
Nodes
IDM (renewal phase)
PKI (authentication phase)
MPC (key generation phase)
Key scheduling phase
(t)
Communication infrastructure
Key generation and scheduling architecture

Fig. 2. Proposed classification of the communication flow.

References

[1] E. Revell, "Method for generating an encryption/decryption key," US Patent Application US 2012/0 087 495 A1, 04 12, 2012.

[2] A. Hudic, E. Revell, and D. E. Simos, "A generation method of cryptographic keys for enterprise communication systems," in *8th International Workshop on Frontiers in Availability, Reliability, and Security (FARES2013), to be held in conjuction with the 8th International Conference on Availability, Reliability and Security (ARES2013), to appear*, 2013.

[3] W. Stallings, *Cryptography and network security - principles and practice (3. ed.).* Prentice Hall, 2003.