Journal of Engineering and Applied Sciences 11 (Special Issue 2): 3294-3297, 2016
ISSN: 1816-949X

Session Control Model on the Basis of the Session Public Key Certificate Releases

Igor S. Konstantinov, Sergej A. Lazarev and Oleg V. Mihalev
Belgorod State University, Pobeda St., 85, 308015 Belgorod, Russia

Abstract: In this study, the diagram description of creating the session control model on the basis of the session public key certificate releases is provided in the closed distributed information environment in the form of enterprise portals network in case of algorithm implementation of the simplified user authentication.

Key words: The user session, session public key, the distributed information resources, portals network, the closed virtual environment, user authentication

INTRODUCTION

The task of creating infrastructure of the Distributed Information Environment (DIE) safety in the form of enterprise portals network assumes implementation of an access control uniform policy to resources on the basis of forming the uniform hierarchy of user groups.

Portals network as the mechanism having uniform entry point and providing a uniform policy of access demarcation for users and administrators is described in operations (Lazarev and Demidov, 2010, 2012; Ivashchuk *et al*., 2014; Lazarev *et al*., 2015a, b) and represents set of the nodes monitoring the access integrated in a single network with the Portals Control Center (PCC). Within PCC the uniform policy of information exchange control including the possibility of the authorized access to the protected information resources of all network, the uniform mechanism of the user session control providing the necessary security level is implemented.

To control the user operation in multi-user program systems we use mechanisms of session access (the user session), including the user identification and confirmation of his possibilities within the active session (Konstantinov *et al*., 2014a-c, 2015; Lazarev *et al*., 2015a, b). For the purposes of increasing safety of information exchange within a distributed portals network, at the same time saving simplicity of authentication process for the user, use of the mechanism of asymmetric encoding in case of data transfer about the user session by means of forming the keys couple (opened, closed) and providing certificates of the user session on the basis of public key is expedient (Tagger *et al*., 2013).

MATERIALS AND METHODS

Problem definition: The most important components of the primary user authentication in a services development section of the simplified authentication and the algorithms providing these are components of user session control. The development diagram of primary user authentication services is provided in Fig. 1 to language notations of ArchiMate architectural simulation.

Participating in authentication process are the user and the system (the application client, the application server). The user possesses the authentication data necessary for his identification and the proof of authenticity. The application client realizing a possibility of dialog with the user is responsible for functions of information input-output, as well as organizes generation and transmission of managing directors and session data to the checking side under which the application server functions. At the same time the server provides information storage about sessions of all users who underwent the authentication procedure. Results of the primary authentication developed algorithm execution are:

- Application client having a couple opened/closed keys of a session and the session public key certificate
- Application server having association of session public key with the specific user of system

It is supposed that components of primary authentication settle down on a hardware platform of the control center whereas components of the simplified authentication are integrated with components of authorization and function on hardware platforms of the network nodes.

In the elementary case for passing the procedure of the simplified authentication it is enough for client application to show the network node processing a request, existence of the session public key certificate signed with the control center as authenticity confirmation as well as the fact of having a private key. At

Corresponding Author: Igor S. Konstantinov, Belgorod State University, Pobeda St., 85, 308015 Belgorod, Russia

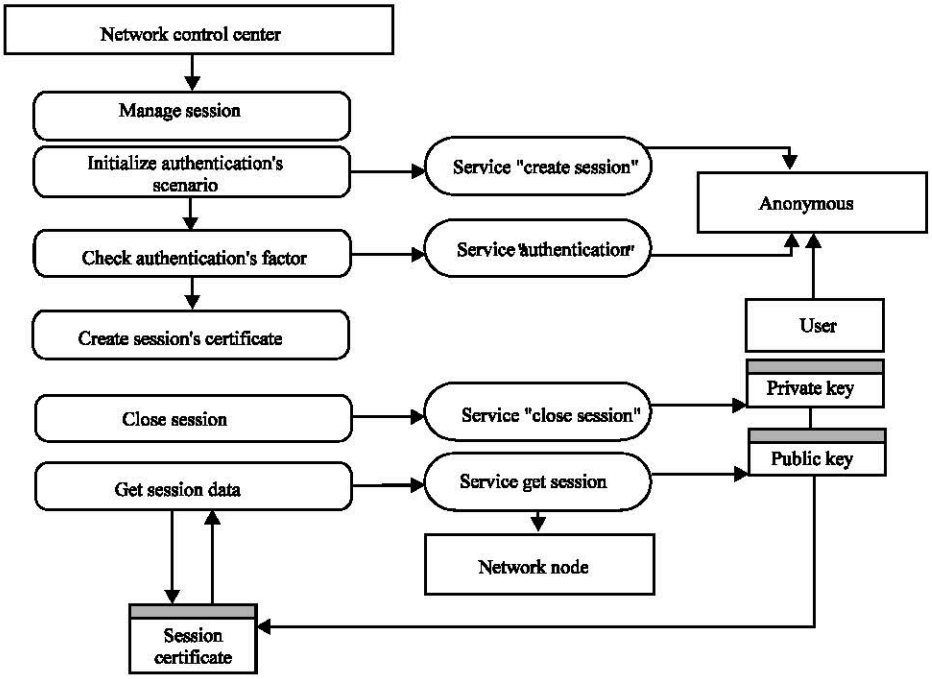

Fig. 1: Diagram of authentication services of the distributed information environment

the same time it is expedient to use possibilities of mutual authentication of the information exchange sides according to the TLS protocol (both participants of interaction possess the digital certificates allowing to carry out an inspection of authenticity according to protocols of asymmetric cryptography).

The similar protocol of interaction has possibilities of deactivating user session; the session will inevitably come to end after period of its public key certificate validity ends, as well as in case of the certificate withdrawal on the command proceeding from the user. It becomes possible as for support of the necessary security level, the network node is obliged to carry out an inspection of the certificate validity received from the user by addressing the archive of the control center user sessions.

RESULTS AND DISCUSSION

The generalized event model is provided to ArchiMate architectural simulation language notations in Fig. 2. The user initializes a session, at the same time the application client creates couple of opened and closed session keys. During passing of the primary authentication procedure the user enters the authentication data which are transferred to the control center according to cryptography protocols together with session public key. The private key is not disclosed to any other party of interaction.

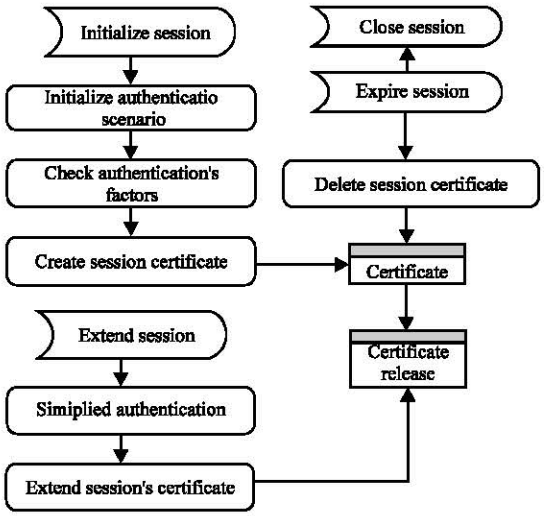

Fig. 2: Event model of the user session public key certificate control

In a case of authenticity confirmation the control center creates the session public key providing certificate with limited duration. In case of user addressing the network nodes, the client application and server components of a network node carry out mutual authentication according to the cryptography protocol of asymmetric encoding with use of the public key certificate providing the user session (Fig. 3). At the same time, the

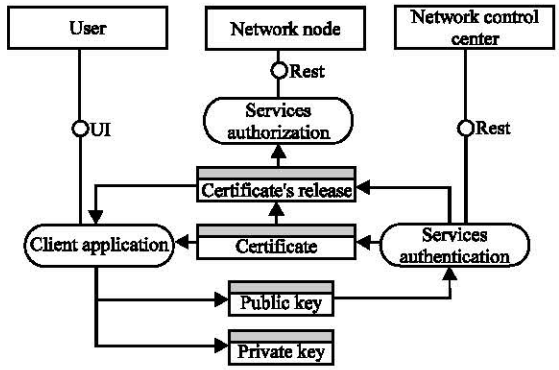

Fig. 3: Model of authentication service entities control

network node creates addressing to archive of the user sessions to be convinced that the certificate is valid and is not withdrawn.

After validity of providing the certificate ends,should the user continue to interact actively with information resources of a network, the client application is obliged to undergo the procedure of the simplified authentication on server components of the control center according to the cryptography protocol of asymmetric encoding with use of the last valid public key certificate providing user session for validity period extension. At the same time the new the certificate based on the same session public key and connected to the same user is provided but is limited by new periods.

The user session provided by the session public key certificate reflects passing the scenario of authentication in the server of the control center and provides confirmation of the user authenticity in case of addressing the network nodes. The reality of a session at the time of addressing the archive of the user sessions is reflected not by a session, but by the connected entity "The public key certificate".

The providing the certificate represents a status of the public key certificate of user session in a certain and finite period from the moment of creating release before the termination of its validity period. It is possible to describe life cycle of user session and the public key certificate a set of statuses (Fig. 4). In Fig. 4 life cycle of user session is described in the form of the finite-state machine (in the notation of a UML modeling language), transitions are enumerated respectively:

- 1-Initialization of user session and certificate of its public key
- 2-Passing an authentication factor with the positive result

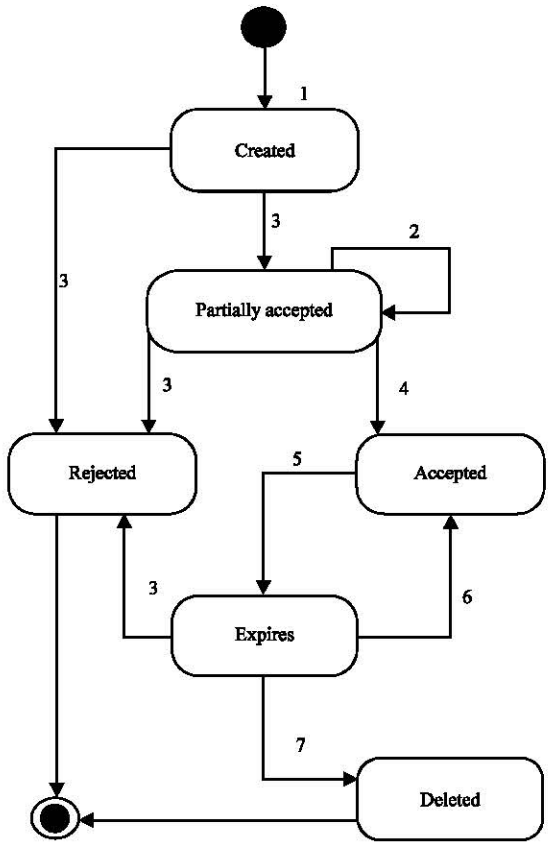

Fig. 4: Life cycle of an "User session" entity

- 3-Passing the scenario of authentication with the negative result
- 4-Passing the scenario of authentication with the positive result
- 5-Expiration of the session public key certificate
- 6-Initialization of new providing the session public key certificate
- 7-Relocation of the session public key certificate in archive

Summary: In this study need of using certificates for the user session on the basis of public key for the purposes of increasing information exchange safety on the distributed portals network is justified. The diagram of component interaction of authentication service is considered. The event model of the public key certificate control for the user session and model of authentication service entities control is offered, life cycle of a "User session" authentication service entity in the form of the finite-state machine model is described.

CONCLUSION

The approach considered in article formed a basis for algorithm implementation of the user authenticationfor the

closed distributed information environment in the form of portals network. As the fundamental mechanism of this algorithm implementation the model of user session control on the basis of providing certificates of public key is used. Finally, the user session provided by the session public key certificate provides confirmation of the user authenticity in case of addressing the network nodes.

ACKNOWLEDEMENTS

The research concerning this issue was sponsored by the RF Ministry of Education and Science. The project ID is RFMEFI57514X0099.

REFERENCES

Ivashchuk, O.A., S.A. Lazarev, I.S. Konstantinov and K.A. Rubcov, 2014. Mechanism of information exchange management within portal network of environmental monitoring subjects. Intl. J. Appl. Eng. Res., 9: 16789-16794.

Konstantinov, I.S., S.A. Lazarev and O.V. Mihalev, 2014a. [Realization of a single model session access in the distributed network portals]. Herald Comput. Inform. Technol., 6: 44-49, (In Russian).

Konstantinov, I.S., J.G. Chashin and S.A. Lazarev, 2014b. Simulation of the Software-Defined network for a high-performance computing cluster. Res. J. Appl. Sci., 9: 704-706.

Konstantinov, I.S., S.A. Lazarev, O.V. Mihalev and V.L. Kurbatov, 2014c. Analysis of the single session access model in the distributed portal network of the interacting parties of the informational space. Res. J. Appl. Sci., 9: 771-773.

Konstantinov, I.S., S.A. Lazarev and P.P. Silaev, 2015. Safety mechanism for multi-factor authentication with digital access key use in closed virtual environment of distributed information resources. Intl. J. Appl. Eng. Res., 10: 44927-44932.

Lazarev, S.A. and A.V. Demidov, 2010. [The concept of construction of a control system of an information exchange in the network of corporative portals]. Inform. Syst. Technol., 4: 123-129, (In Russian).

Lazarev, S.A. and A.V. Demidov, 2012. Features of a subsystem development for the system access management in respect of information exchange of corporate portal network. Inf. Syst. Technol., 4: 103-110.

Lazarev, S.A., I.S. Konstantinov, O.V. Mihalev and V.E. Kiselev, 2015a. Implementation of unified session access model in a closed virtual environment of distributed information and computing resource system as a secured portal network. Res. J. Applied Sci., 10: 629-632.

Lazarev, S.A., I.S. Konstantinov, O.V. Mihalev, A.V. Demidov and R.V. Shateev, 2015b. The development of infrastructure security for distributed information computer environment based on secured portal network. Int. J. Applied Eng. Res., 10: 38116-38120.

Tagger, B., D. Trossen, A. Kostopoulos, S. Porter and G. Parisis, 2013. Realising an application environment for information-centric networking. Comput. Networks, 57: 3249-3266.