Approaches to the Security Analysis of Authentication and Authorization Protocols in Distributed Systems

Igor S. Konstantinov, Sergej A. Lazarev, Vladimir E. Kiselev, Alexander V. Demidov

Abstract— In this article, a review of the most used approaches for the formal analysis of distributed systems cryptographic protocols and software tools implemented on the basis of these approaches has been done. The article examines such approaches as model checking, theorem proving, and believe logic, provides a list of well-known tools for automating the analysis of cryptographic protocols within each approach. On the basis of the conducted research, it was concluded that there is no universal tool for verifying the security of distributed information and computing systems authorization and authentication protocols.

Keywords: formal verification; authorization; authentication; model checking; logical inference.

INTRODUCTION

The annual information security report Cisco for 2017 marked a rapid increase of distributed information and computing systems usage. These systems are using modifications of open authentication and authorization protocols, the most common of which are OAuth 2.0 and OpenID Connect [1]. Given this fact and the steady trend towards the distributed information and computing systems usage [2], the tool for automated protocol security analysis is needed for developers.

Currently, to assess the correctness and security of protocol, there are several basic formal approaches on the basis of which are implemented software tools. However, there remains an open question about the applicability of these solutions for analyzing the security of open authentication and authorization protocols, and especially their modifications used in cloud and distributed information and computing systems [3-4].

This article presents a study of current approaches for the formal analysis of cryptographic protocols, software tools implemented on the basis of these approaches, and analyzes the applicability of these solutions for analyzing the correctness and security of open authentication and authorization protocols.

TASK ASSESMENT

The most used approaches for verification of protocols are: model verification and logical inference, including theorem proving and believe logic. On the basis of these approaches, software tools for automating protocol analysis, as described in [5], have been implemented. These solutions are based on one or several of the listed approaches, as a result, each of these software tools has its own specialized application field. This causes the logical problem of determining the optimal method for the formal analysis of the open authentication and authorization protocols correctness and security.

As part of this work, existing approaches for formal verification of protocols, software tools based on the application of these approaches are investigated, and the applicability of these solutions for assessing the correctness and security of authentication and authorization open protocols of distributed systems are examined.

I. PROTOCOL SECURITY LEVEL DETERMINATION

Protocol - description of a distributed algorithm, in the process of which two participants (or more) consistently perform certain actions and exchange messages. Protocol security is expressed in providing guarantees for the implementation of such properties that characterize security, such as availability, confidentiality, integrity, etc. [5].

The rapid increase of cloud applications integration by employees into distributed networks of organizations [1] negatively affects the vulnerability of distributed systems, and therefore the verification of authentication and authorization protocols for users of distributed systems becomes one of the most important aspects of secure operation.

The security level of a protocol is usually determined by simulating its operation and simulating malicious attacks. In this article, such approaches to protocol verification as «Model checking» and «Logical Inference» will be considered, as well as software tools that allow automating the protocols security verification, based on these approaches. The principal difference of these approaches is that the application of the «model checking» approach gives the greatest effect in a case when the model does not satisfy the set requirements, while the application of the «logical inference» approach is most effective for justifying the model's compliance with the set requirements. And since it is not known in advance whether the protocol meets the set requirements, both approaches should be used

Revised Manuscript Received on April 12, 2019.

Igor S. Konstantinov, Belgorod State University, 85 Pobedy str., Belgorod, Russia

Sergej A. Lazarev, Belgorod State University, 85 Pobedy str., Belgorod, Russia

Vladimir E. Kiselev, Belgorod State University, 85 Pobedy str., Belgorod, Russia

Alexander V. Demidov, Orel State University, 95 Komsomolskaya str., Russia

simultaneously to obtain the most correct assessment.

It should be noted that in addition to checking the correct functioning of distributed systems, protocol verification includes determining the level of information security special properties. The most important of these are:

1. Confidentiality – transmitted information is not available for unauthorized access.
2. Integrity – a guarantee of providing genuine and complete information to an authorized user.
3. Accessibility – ensuring quick access to information and resources for an authorized user.
4. Authentication – user authentication at login.
5. Authorization – verification of user access rights to information and system resources.

Application of modeling approach to the verification of authentication and authorization protocols for distributed systems has several undeniable advantages:

1. The convenience of use – simulation usage for protocols verification allows assessing the security level of a protocol without disrupting the operation of the system.
2. Model variability – the developer determines the model, not including in it the features of the simulated system that are not essential for testing this condition.
3. The possibility of further changes and debugging – depending on the approach used, as a result of the test, the developer receives a report on the model compliance with the requirements set, which helps to detect the inaccuracy of the constructed model or conditions imposed on it.

Also worth noting is the possibility of complicating the system model with the gradual addition of new states and rules to it, which will make the model closer to the original and allows to detect the bottlenecks and the moments of their occurrence [6].

Disadvantages of the simulation approach:

1. The complexity of the process – the model developer must highlight the necessary components of the simulated system to match the real system model.
2. The complexity of the formal presentation – the model developer must formalize its representation in terms of the selected verification tool logic.
3. The complexity of requirements formulation – the model developer must correctly and exhaustively formulate the requirements for the modeled system.

Despite these shortcomings, modeling is a modern and effective method for verifying protocols, and various approaches to models formalization and verification allow obtaining the most correct assessment result [7].

1.1 Protocol security level determination in a distributed system

As an example of a distributed system using modifications of open authentication and authorization protocols, was selected an architecture, which was registered by the authors in the patent for invention RU №266664 [8]. The main idea of this system is to realize the horizontal integration of information and computing resources without changing their structure, as well as increasing the reliability and security of information from unauthorized access. A simplified architecture of distributed system is shown in Fig. 1.

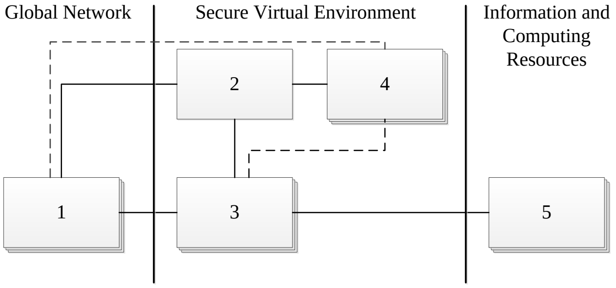
Global Network
Secure Virtual Environment
Information and Computing Resources
1
2
3
4
5

Fig. 1 – A simplified architecture of distributed system

The main components are:

- Multiple client PCs (component 1) located in the global network;
- Secure virtual environment including:
  - Central hub (component 2);
  - Multiple access nodes (component 3);
  - One or more backup central hubs (component 4);
- Distributed information and computing resources (component 5), presented in the form of corporate portals.

Authentication and authorization of users is performed using a modified version of OAuth 2.0 open protocol, so the task of the security and correctness formal verification of this protocol version arises.

To determine the feasibility of practical implementation of the development, it is required to build its formal model, and to analyze its correctness and safety. However, at this stage, the main difficulty is the representation of the system within the formalisms of the chosen logic. Within distributed systems, this process is most difficult due to the complexity of their work.

This article will observe the main approaches to the organization of the formal security analysis process of authentication and authorization protocols.

II. MODEL CHECKING APPROACH

The basic idea of this approach is to build a behavioral model of a system with a finite number of conditions and requirements (properties), subject to verification within the model states.

As a rule, only the main properties of the system are taken in the construction, that affect the test result, thereby achieving a reduction of the model size and an acceleration of the verification process. In this case, the model can be specified both explicitly – by enumerating all the vertices and edges of the model state graph, or implicitly – by boolean functions representing the transition relation and the set of initial states.

Model checking algorithms are based on a full view of the model state space: for each state, it is checked whether it meets the stated requirements. The algorithms are guaranteed to be completed, since the model is finite [9]. The verification method based on model checking uses the system representation as a set of states. In this case, a subset of states with any violated safety criterion is highlighted. For verification in this case, it is necessary to prove that such a set in this model is empty, otherwise the system does not fall into any of the sets.

The main software tools implemented on the «Model checking» approach basis are listed in Table 1.

III. RESULTS & DISCUSSIONS

Table 1 – Software tools implemented on the «Model checking» approach basis

Software tool	Implementation language	Used approaches	Specialized in the cryptographic protocols verification
Scyther	Python/C	Combined approach	Yes
ProVerif	OCaml	Combined approach	Yes
Casper	CSP	Model checking	Yes
SPIN	C/LTL	Model checking	No
FDR2	CSP	Model checking	No
PRISM	Java	Model checking	No
AVISPA	OCaml	Combined approach	Yes (Man-in-the-middle attack type)

The result of applying the «Model checking» approach is a message about successful verification when the model complies with the requirements set, or a sequence of model actions during which non-compliance with the conditions occurs. If a discrepancy is reached as a result of model checking, a verdict of the model incorrectness or the formal requirements incorrectness is made [10].

IV. LOGICAL INFERENCE APPROARCH

In general, the logical inference is a deductive approach to the construction and formal substantiation of assertions (invariants). Requirements for invariants:

1. Each invariant is true at the system start time.
2. After each step of the system, each invariant preserves the truth.
3. System specification is a conjunction of invariants.

Verification method based on logical inference consists of formalizing verifiable protocol, the actions of the attacker and the protocol security criteria as statements in terms of chosen formal logic. Next step is the protocol checking for compliance with the criteria set, possibly using automated tools [11].

When applying the logical inference method for analyzing cryptographic protocols, there are distinguished means based on the approach of theorem proving and believe logic.

3.1 Theorem proving approach

This approach represents a software implementation of a tool for proving statements based on propositional logic and predicate logic. The approach basis is to use the mathematical logic apparatus for the implementation of the final software tool [12].The advantage of this approach is the rigor and commonality of logic, reducible to the solving tasks automation. An obvious disadvantage, logically arising from the rigor of logic, is the need to formalize the statements in the predicates given by the software implementation. The main software tools implemented with the «Theorem proving» approach are given in Table 2.

Table 2 – Main software tools implemented with the «Theorem proving» approach

Software tool	Implementation language	Used approaches	Specialized in the cryptographic protocols verification
Coq	OCaml	Theorem proving	No
Isabelle	Standard ML	Combined approach	Yes
HOL	Light OCaml	Theorem proving	No
Nuprl	CLisp	Theorem proving	No
PVS	CLisp	Theorem proving	No
Tamarin Prover	Haskell	Combined approach	Yes (DH protocol usage)
AVISPA	OCaml	Combined approach	Yes (Man-in-the-middle attack type)

3.2 Believe logic approach

This approach involves the formal rules set usage to determine the veracity (trust) of an assertion. There are such implementations of specialized assertion analysis tools, such as GNY, SvO, etc. based on this approach. One of the most variable tools based on "believe logic" approach, that allows for a formal analysis of authentication and authorization protocols correctness is BAN logic.

The Barrows-Abadi-Needham logic or BAN logic is a formal logic model for analyzing knowledge and trust [13]. This logic is solvable, so there is an algorithm that checks the correctness of the conclusions made from the hypotheses.

This model is a set of structures, or a logical language, and a set of axioms and rules applicable to these structures. The authors of the BAN logic identified the basic constructs for four actions: believing, controlling, seeing and saying messages [14]. These constructs constitute a language for describing the trust between the components of the network during the protocol operation. The rules and axioms of BAN logic allow the derivation of new trusted statements from existing ones [15].

V. CONCLUSION

Currently, there are implemented solutions for the formal analysis of authentication and authorization protocols, each is distinguished by the approach, verification methodology and scope. As a result of the review, it was revealed that the most problematic part of the protocol analysis is the correct and adequate formalization of the modeled system in terms of the chosen logic. This problem is inherent in any approach since the developer is required to build a correct and adequate model of the source system. And in the conditions of rapid count growth of cloud applications with modified open authentication and authorization protocols, to simplify the task of analyzing the security of a distributed system, an urgent task is to apply the automated tools for analyzing protocols.

Also, as a result of the review, it was revealed that each approach to protocol verification has its own characteristics, and there is no universal tool for assessing the security of authentication and authorization protocols. And to obtain the most adequate protocol security assessment usage of a combined approach is required. Combined approach allows compensating the shortcomings of one verification tool at the merits expense of another.

VI. ACKNOWLEDGMENTS

The research is carried out with the financial support of the Ministry of Science and Higher Education of the Russian Federation, project: 2.5681.2017/BP.

REFERENCES

1. Cisco Systems, Inc. Annual Information Security Report. URL: http://nncit.tneu.edu.ua/wp-content/uploads/2017/10/ReportUKR.pdf. Revised Jan. 2018. Accessed 20.03.2019.
2. S. A. Lazarev, A. V. Demidov, V. N. Volkov, A. A.Stychuk, D. A. Polovinkin. Analysis of applicability of open single sign-on protocols in distributed information-computing environment // Application of Information and Communication Technologies (AICT), 2016 IEEE 10th International Conference. – 2016. – INSPEC Accession Number: 17061734. – DOI: 10.1109/ICAICT.2016.7991757. URL: http://ieeexplore.ieee.org/document/7991757/ Accessed 20.03.2019.
3. I.S. Konstantinov, S.A. Lazarev, O.V. Mihalev, V.E. Kiselev, A. V. Demidov. The model of management access to the resources of the closed discretionary information computation environment in the form of corporate portal network // Application of Information and Communication Technologies (AICT), 2016 IEEE 10th International Conference. – 2016. – INSPEC Accession Number: 17061734. – DOI: 10.1109/ICAICT.2016.7991744. URL: http://ieeexplore.ieee.org/document/7991744/?part=1 Accessed 20.03.2019.
4. S.A Lazarev, I.S. Konstantinov, O.V. Mihalev, V.E. Kiselev. Implementation of unified session access model in a closed virtual environment of distributed information-computational resource system as a secured portal network // Research Journal of Applied Science. – 2015. – 10 (10): 629-632.
5. A. Cheryomushkin. Automated protocol analysis tools // PDM, 2009, att. № 1, pp. 34–36.
6. A. Cheryomushkin. Cryptographic Protocols: Key Features and Vulnerabilities // PDM, 2009, att. № 2, pp. 115–150.
7. B. Smyth. Formal verification of cryptographic protocols with automated reasoning // University of Birmingham. – 2011. – 189 с.
8. I. Konstantinov, S. Lazarev, O. Mihalev, V. Kiselev, A. Demidov. The method of providing access to distributed information and computing resources in the form of corporate portals through a secure virtual environment // Invention patent published 31.07.2017. URL: http://www1.fips.ru/wps/portal/IPS_Ru#1540161439213 Accessed 20.03.2019.
9. K. Kogos, S. Zapechnikov. Studying formal security proofs for cryptographic protocols // WISE 2017. IFIP Advances in Information and Communication Technology, vol 503. Springer, Cham, pp 63-73.
10. A. Lependin, A Ubert. Method of models verification in the application to the authentication protocols analysis // News of Altai State University [2012]. URL: https://cyberleninka.ru/article/n/metod-verifikatsii-modeley-v-prilozhenii-k-analizu-protokolov-autentifikatsii Accessed 20.03.2019
11. Analysis of security functions verification approaches // Moscow: Russian Academy of Sciences. Institute of System Programming, 2004. – 101 p.
12. J.Harrison. The LCF Approach to Theorem Proving // Intel Corporation: [2001]. URL: https://www.cl.cam.ac.uk/~jrh13/slides/manchester-12sep01/slides.pdf. Accessed 20.03.2019.
13. Burrows M., Abadi M., Needham R. A Logic of Authentication // Proc. R. Soc. Lond. A 1989 426 233-271; DOI: 10.1098/rspa.1989.0125; pp.3-5.
14. Bleeker A., Meertens L. A semantics for BAN logic // Proceeding of DIMACS Workshop on Design and Formal Verification of Crypto Protocols, 1997.
15. Abadi M., Needham R. Prudent engineering practice for cryptographic protocols // Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy. – 1994. – pp.122-136.