timestamp between the client and the SP agents to keep the signature of Kerberos in our protocol; however we can replace this technique by a challenge/ response mechanism (nonce). In addition, we could remove the timestamp from any ticket and keep the nonce only.

Password-guessing assault is a common security issue between our protocol and Kerberos. The attacker may try to capture the encrypted messages between the clients and the AS in order to get enough information about each client. Then, these encrypted messages with the password of the client will be run by the attacker through various techniques in order to guess the client password. It is enough for the attacker to guess one password in order to penetrate the security of the protocol. We can reduce the impact of such attack by forcing the client to choose a complex password or by increasing the size of the generated key from the password. Even with this counter measure we cannot prevent all password-guessing attacks or social engineering attacks.

7. Conclusions and Future Work

In this paper, we have formally analyzed the security properties of the DLK protocol that secures the messages exchanged in a distributed agent-based system. The automatic verifier, ProVerif, has been used for this analysis. This study improves the understanding of the protocol by formally verifying the mutual authentication between client and SP agents and proving the secrecy of the information inside the encrypted messages.

We were able to determine some attacks that might occur due to the security protocol design deficiencies. Testing the DLK protocol using ProVerif detected the possibility of a Man-In-The-Middle attack. The mutual authentication problem between the client and SP agents is fixed in this work using nonce-based authentication. The fixed protocol was then verified in ProVerif to prove that it achieved mutual authentication between the client agent and SP agents correctly.

The enhanced DLK protocol is a general security methodology scheme that provides mutual authentication, confidentiality, integrity and authorization, while it is not linked to the multi-agent system. Therefore, we plan to expand our research and find out other application areas that can adopt the DLK protocol without the agent technology. This way, the DLK protocol can be used to provide a secure distribution method for any system. In addition, the ProVerif model we did for the DLK protocol can be used in order to verify any necessary changes in security concepts of the DLK or any other security protocol that we will propose based on the DLK.

8. References

[1] RFC 3394, http://www.ietf.org/rfc/rfc3394.txt, Feb. 2012

[2] H.M.N. Al-Hamadi, C.Y. Yeun, M.J. Zemerly, M. Al-Qutayri; "Distributed lightweight Kerberos protocol for Mobile Agent Systems", IEEE GCC Conference and Exhibition, Dubai, 2011, pp. 233-236.

[3] M. Peters, P. Rogaar; "A review of ProVerif as an automatic security protocol verifier", http://agoraproject.eu/papers/A review of ProVerif as an automatic security protocol verifier.pdf, 13th of Sept. 2011.

[4] R. Kusters, T. Truderung, “Using ProVerif to Analyze Protocols with Diffie-Hellman Exponentiation”, 22nd IEEE Computer Security Foundations Symposium, New York, 2009, pp.157-171.

[5] B. Blanchet, B. Smyth; "ProVerif 1.85: Automatic Cryptographic Protocol Verifier, User Manual and Tutorial", http://www.proverif.ens.fr/manual.pdf, 11th of July 2011.

[6] E. M. Clarke, J. M. Wing; "Formal Methods: State of the Art and Future Directions", ACM Computing Surveys, 1996, Vol.28, pp. 626-643.

[7] B. Blanchet; "CryptoVerif: Cryptographic protocol verifier in the computational model", http://www.cryptoverif.ens.fr, 11th of July 2011.

[8] K. Bhargavan, C. Fournet, A.D. Gordon, S. Tse; "Verified interoperable implementations of security protocols", 19th IEEE Computer Security Foundations Workshop,Venice, 5-7 July 2006, pp. 139 -152.

[9] Q. Li, F. Yang, H. Zhu, L. Zhu; "Formal Modeling and Analyzing Kerberos Protocol", 2009 WRI World Congress on Computer Science and Information Engineering, 2009, Vol.7, pp. 813-819.

[10] M. Butler; "On the Use of Data Refinement in the Development of Secure Communications Systems", Formal Aspects of Computing, 2002, Vol. 14, No.1, pp. 2–34.

[11] Z. Zhang, X. Zhang, R. Sandhu; "ROBAC: Scalable Role and Organization Based Access Control Models", CollaborateCom 2006. International Conference on Collaborative Computing: Networking, Applications and Worksharing, Georgia, 2006, pp. 1-9.

[12] RFC 4120, http://tools.ietf.org/html/rfc4120#ref-NT94, 11th of July 2011.

[13] M.A. Sirbu, J.C.-I. Chuang, "Distributed authentication in Kerberos using public key cryptography", 1997 Symposium on Proceedings Network and Distributed System Security, California, 1997, pp. 134-141.

[14] M. Abadi, C. Fournet; "Mobile Values, New Names, and Secure Communication", Proc. of the 28th ACM Symposium on Principles of Programming Languages (POPL’01), 2001, pp. 104–115.

[15] B. Blanchet, A. Chaudhuri;, "Automated Formal Analysis of a Protocol for Secure File Sharing on Untrusted Storage" , IEEE Symposium on Security and Privacy, California, 2008, pp. 417-431.

[16] M. Bugliesi, R. Focardi, M. Maffei, “Analysis of typed analyses of authentication protocols”, 18th IEEE Workshop in Computer Security Foundations, France, 2005, pp. 112- 125.

