Abstract

TCG group introduced the Remote Attestation Protocol, which has a weak point that makes it vulnerable to a masquerade attack. In this paper, a new method is introduced for improving the security of this protocol against masquerading attacks. The security of the improved protocol is analyzed using AVISPA tools. Advantages of the improved protocol include a reduced number of messages and lower cost, which prevents useless communication. Furthermore, an improved mechanism for measuring and reporting the changes is recommended. Combining the above mentioned, improved protocol with the improved integrity measurement and reporting mechanism can solve the existing problem in certain critical applications.

References

Dynamic Change Reporting of Platform Configuration

- David Safford, Mimi Zohar, A Trusted Linux Client (TLC), T. J. Watson Research Center IBM, Final report.
- Frederic Stumpf, Omid Tafreschi, Patrick R’oder, Claudia Eckert, December 2006, A Robust Integrity Reporting Protocol for Remote Attestation, Second Workshop on Advances in Trusted Computing (WATC &apos;06 Fall), Tokyo, Japan.
- Jan Camenisch, Better Privacy for Trusted Computing Platforms, Final report, IBM Research. Zurich Research Laboratory, CH-8803 R’uschlikon, Switzerland.
- Song Cheng, Liu Bing, Xin Yang, Yang Yixian, Li Zhongxian, Yin Han, 2009, A Security-Enhanced Remote Platform Integrity Attestation Scheme, IEEE.
- Trent Jaeger, Reiner Sailer, Umesh Shankar, 2006, PRIMA: PolicyReduced Integrity Measurement Architecture, SACMAT&apos;06, ACM, Lake Tahoe, California, USA.

Index Terms

Computer Science  Networks

Keywords

remote attestation  Trusted Platform Module  integrity measurement
masquerading attack
formal analysis