Abstract

Key management is a core mechanism to ensure the security of information in communication channels. Secret key is used for encryption and decryption in cryptographic security modules. Security of communication relies on secure and robust distribution of secret keys. Key need to be renewed periodically to prevent compromise the key. Most of the key distribution protocols consider the pre-distribution of secret key only but did not handles the Key Renovation. The Automatic Key Renovation has several issues when implemented on serial communication link.
When a single channel is used for data communication as well as for key distribution, both communicating systems need to be well synchronized at the time of renewal of key. This paper focuses on such synchronization issues during the key renovation and introduces a solution to resolve it. The proposed solution is independent of the platform and the underlying key distribution protocol. It also ensures zero data loss and minimum delay on data communication.

References

- Predictive YASIR: High Security with lower latency in legacy SCADA. Rouslan V. Solomakhin, Patrick P. Tsang and Sean W. Smith
- Peeyush Jain and Zia Saquib, "Analysis of Different key Distribution Schemes for Distributed Sensor Networks," LNCS-CCIS, 2011
- http://www.slideshare.net/guest61205606/communication-and-synchronization-in-distributed-systems-2323829
- 11711-2010 · IEEE Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links

Index Terms

Computer Science

Databases

Keywords

Key Renovation  Information Security  Serial Communication  Key Distribution  Secret
Key
Bump-in-the-wire
Synchronization