Abstract

A novel protocol to achieve privacy-preserving universal authentication protocol for wireless communications called Priauth. Verifier-Local Revocation Group Signature with Backward Unlinkability (VLR-GS-BU), it can satisfy all requirements. Priauth belongs to the class of Universal Authentication Protocols in which same protocol and signaling flows are used regardless of the domain (home or foreign) a roaming user is visiting. Allowing people to get connected seamlessly using their devices without being limited by the geographical coverage of their own home networks roaming service should be deployed. The key is used to encrypt data transmitted to the servers or users. The efficient distribution of the new key for multiple membership changes is a critical problem in secure group communication. The goal of the
enhancement is to evaluate trade-off between storage and revocation cost. Storage is computed in terms of keys that each user (respectively, VA) maintains and revocation cost is computed in terms of the encryptions performed, and the number of messages transmitted by the VA.

References

- G. Yang, D. Wong, and X. Deng, "Deposit-case attack against secure roaming," in Proc. ACISP, 2005.

Index Terms

Computer Science
Keywords
Priauth  Hierarchical Key Management  Rekeying  Storage Trade-offs