URN etd-0407109-183703-180
Author Chun-Chang Pan
Author's Email Address No Public.
Statistics This thesis had been viewed 67 times. Download 0 times.
Department
Year 2006
Semester 1
Degree Master
Type of Document Master's Thesis
Language zh-TW.Big5 Chinese
Title Group Tags Authentication Protocols For RFID
Date of Defense 0000-00-00
Page Count 70

Keyword
RFID
User privacy
Mutual Authentication
Integrity
Replay attack

Abstract RFID has been considered as the one of the most important technologies. It makes products be accurately tracked by factory owner and accelerates the process efficiency by radio frequency. For example, RFID can be applied to stock management and import/export products in the factory. Because tags can be tracked and no mutual authentication mechanism between tags and readers, an adversary thus can use an illegal reader to access the information stored in the tags. It is harmful to user privacy. Therefore, how to design a valid mutual authentication protocol between the reader and the tag has become an important issue.
In 2005, Chang proposed a security mechanism to enhance the security of RFID. However, we find out that Chang authentication protocol can be easily broken by eavesdropping on the communication between the reader and the tag. For this reason, we further propose an improved mutual authentication protocol which can resist attack and protect user privacy. Meanwhile, we enhance the improved protocol to get better performance and provide the property of forward security.
Besides, we research on different scenarios which need to check double tag or group tags simultaneously. In 2004, Juels proposed a protocol using a couple of tags to verify the integrity of couple of objects. However, in 2005, Saito and Sakurai pointed out that Juels' protocol encountered the replay attack. Thus, Saito and Sakurai utilized timestamp to improve security and defeat the replay attack, but we find out that their protocol had a security flaw. Since the output of the reader can be predicted, the adversary can try to transmit the predicted time to the tag and acquire a legal value to pass the authentication. For example, the manufacture needs to scan products periodically. Consequently, an adversary can take the advantage of the predicted time to obtain a legal value and pass the authentication. Therefore, we propose an improved protocol to defeat the predicted time attack. In addition, we find out that this kind of protocols does not have definite executed sequence of tag. Finally, we propose a group tags authentication protocol can authentication the tags in order.
Advisory Committee Narn-Yih Lee - advisor

Files No Any Full Text File.
Date of Submission 2007-08-19