URN etd-0407109-183725-2077
Author Yu-Hsien Li
Author's Email Address No Public.
Statistics This thesis had been viewed 51 times. Download 0 times.
Department
Year 2007
Semester 2
Degree Master
Type of Document Master's Thesis
Language zh-TW.Big5 Chinese
Title The Study of Off-Line Authentication Protocol for RFID tags
Date of Defense 0000-00-00
Page Count 48

Keyword
Radio frequency identification system
Off-Line
Privacy
Delegation
Security

Abstract
Recently, RFID researches have been considered as the main development by the government. Basically, RFID sends messages through radio wave. Therefore, how to recognize the tag information correctly and protect users' privacy have become important issues. For solving these security issues, many scholars proposed some RFID protocols. However, most protocols are relying on one on-line backend server and cannot work on an off-line environment. In 2007, Fouladgar and Afifi first proposed the off-line SiDES protocol. Later, Lin proposed a TCD-RP protocol. They allow that the backend server could delegate the reader to identify the tag information. But the Fouladgar and Afifi's SiDES protocol will suffer from the replay attack, forgery attack, Denial-of-Service attack and fail to achieve the forward security. Although Lin's protocol uses timestamp to control the delegation, it does not keep forward security property under the same time frame. Therefore, this thesis designs a more secure RFID protocol to fix these security flaws. In 2007, Fouladgar and Afifi also proposed EDTOP protocol which is based on AES and keeps higher performance on the operations of tag ownership transform. However, it also fails to achieve the forward security. Therefore, this thesis further proposes an improved protocol which can achieve the forward security.
Advisory Committee Narn-Yih Lee - advisor

Files No Any Full Text File.
Date of Submission 2008-07-23