URN etd-0407109-183715-1164
Author Li-Sheng Su
Author's Email Address No Public.
Statistics This thesis had been viewed 42 times. Download 0 times.
Department
Year 2004
Semester 2
Degree Master
Type of Document Master's Thesis
Language zh-TW.Big5 Chinese
Title The design of key agreement protocols resistant to denial-of-service attacks
Date of Defense 0000-00-00
Page Count 64

Keyword Denial-of-service
Key agreement protocol
Resource-exhaustion

Abstract
Recently, with the growth of network and various network applications, security of the network communications have been attached importance. Denial-of-service（DoS）attacks become an important issue of network security. It is different from now and before. Denial-of-service is , in order to exhaust server’s resource, including storage-resource and CPU-resource, trying to paralyze server’s services.
Key agreement protocol provides privacy, integration and identification, including the communications and data, for open network systems. However, the traditional key agreement protocols are vulnerable to the DoS attacks. A malicious attacker can achieve his/her resource-exhaustion attack easily. To remedy this shortcoming, several researches have been proposed one after another.
According to authentication protocols, we can be divided them into two categories：public-key based key agreement protocol and identity-based key agreement protocols. Most authenticated key agreement protocols resistant to denial-of-service attacks are focus on the former.
In this thesis, we will survey the related works for some countermeasures used to defeat DoS attacks. And then, we will discuss the cryptanalysis of those DoS-resistant protocols, based on public-key and identity-based key agreement protocols. We point out those protocols are insecure against the DoS attacks. Finally, we propose a public-key based key agreement protocol and follow some security requirements to prove our protocol can resist DoS attacks.
Advisory Committee Her-Tyan Yeh - advisor

Files No Any Full Text File.
Date of Submission 2005-07-19