A Study on Weak Key Protectable Authenticated Key Exchange Protocols

劉孟宗、顏嵩銘

E-mail: 8515743@mail.dyu.edu.tw

ABSTRACT

The birth of Internet makes the physical frontier disappear and we can communicate with each other elsewhere in the world just sit in front of the computer terminals. The development of technology brings a great of convenien-ce to us and accompanies with a lot of problems at the same time. Computer networks shorten the distance between you and me but it''s not the same as conventional face to face communication. How to identify the other people becomes extremely important and necessary. And the privacy protection is also very important when our information is transmitted over the open network structure. We have to notice that maybe someone is eavesdropping our communic-ation over the open network. To guarantee the network security, both identity authentication and data protection must be provided. About the data protection, it''s not a question if we choose the session key properly. For the identity authentication, it''s a common way to use user''s password. Unfortunately, almost all human- chosen passwords are weak keys and suffer from the dictionaryattacks. In this thesis, a series of discussions about the problems of weak key protection are given. In spite of the introduction about possible weak keyattacks, we provide some suggestions and notices for designing authenticationprotocols. Finally, an easy to implement weak key protection structure is proposed which can overcome the drawbacks in previous authentication protocols.

Keywords : Weak Kay Protect ; Cryptography ; Information security

Table of Contents

REFERENCES

0