Dynamic Password Authentication Scheme for Multi-server Environments

王興翰、曹偉駿
E-mail: 9806264@mail.dyu.edu.tw

ABSTRACT

Recently, as the technology of Internet spread fast, all users have emphasized on information security issues. Thus, more and more security schemes have been developed and applied in various environments, in order to effectively ensure that the information can be securely transmitted via the network environments. Moreover, most of these schemes must satisfy at least two security requirements, including user authentication and data confidentiality. To do so, we use password-based mechanisms because they are popular with users, cost-efficient, easy to use. However, if current schemes are used in multi-server environments, then authentication messages must be stored in the server side, which are easily vulnerable to a variety of attacks. Most of approaches employ the public key cryptography or one-way hash function with smart card to solve this problem. Unfortunately, these approaches don't mention how to effectively add a new server to the system to provide service. Therefore, we propose a smart card based dynamic multi-server password authentication scheme using Bilinear Pairing and Newton interpolating polynomial, which has characteristics of high efficiency and security. Specially, we affirm that our proposed scheme will be able to save lots of costs when a new server is added and deleted.

Keywords: multi-server, bilinear pairing, password authentication, smart card

Table of Contents

中文摘要 ..................... iii
英文摘要 ..................... iv
誌謝詞 ...................... v
內容目錄 ..................... vi
表目錄  ..................... vii
圖目錄  ..................... viii

第一章  緒論 ................... 1
  第一節  研究背景 ............... 1
  第二節  研究動機與目的 ........... 2
  第三節 研究限制 ............... 2
  第四節 研究流程 ............... 3
  第五節 論文架構 ............... 5

第二章  文獻探討 ................. 6
  第一節  雙線性配對 .............. 6
  第二節  牛頓內插法 .............. 9
  第三節 適用多伺服器密碼認證方法 ....... 10

第四章 安全性與效能分析 ............. 28
  第一節 安全性分析 .............. 28
  第二節 效能分析 ............... ...

第五章 結論與未來展望 .............. 32

參考文獻 ..................... 40

REFERENCES
