Constructing a Highly Efficient Integrated Access Control Scheme for Web Services

黃美治、曹偉駿
E-mail: 9510897@mail.dyu.edu.tw

ABSTRACT
Web services technology is an extreme efficient structure of information system for promoting enterprises to lower operating cost and raise profits. Nevertheless, with the pluralism of trading platforms, the security of transmitting message and how to execute the access control for information systems will become an important issue for securing the web service environment. Using certificate-based public key cryptosystems to solve the problems related to the demand of security under the current environment of web services causes rather complicated identity verifying and management. The methods of access control in operation can be divided into two kinds. One is that each user must register at different web sites, and therefore the system administrator will be busy in establishing the authority connection for these users; the other is at one specific web site, but every single site is connected with the others through the way of “loosely coupled”, but user may face the problem of different level of authority from a variety of web domains. For this reason, in the thesis the mechanism of integrated access control with high efficiency is constructed using the ECC-based self-certified public key cryptosystems and role-based access control scheme. The proposed mechanism can identify the user without employing certificates, and solve the limits of access authority across different web domains without any influence upon current system operations. Furthermore, after the comparisons with the current access control schemes for web services, we can find the proposed one will be superior to the others in terms of security and efficiency. We affirm that the proposed scheme will be able to lower the cost of maintenance and lighten the burden of system administrator, and thus promote the efficiency of access control to web services environments.

Keywords : Web Services ; Role-Based Access Control ; Elliptic Curve Cryptosystems ; Self-certified Public Key Cryptosystems ; Information Security

Table of Contents

第1章 緒論................................. 1
  1.1 研究背景與動機.......................... 1
  1.2 研究目的................................ 2
  1.3 研究流程................................ 3
  1.4 論文架構................................ 5

第2章 文獻探討............................. 6
  2.1 存取控制................................ 6
  2.1.1 存取控制策略.......................... 6
  2.1.2 存取控制方法.......................... 8
  2.1.3 小結.................................. 19
  2.2 網路服務................................ 19
  2.2.1 XML ...................................21
  2.2.2 SOAP.................................. 22
  2.2.3 WSDL.................................. 23
  2.2.4 UDDI.................................. 23
  2.2.5 小結.................................. 23
  2.3 公開金鑰密碼學.......................... 24
  2.3.1 身分為基礎的公開金鑰密碼系統.......... 25
  2.3.2 憑證為基礎的公開金鑰密碼系統.......... 26
  2.3.3 自我驗證公開金鑰密碼系統.............. 26
  2.3.4 橢圓曲線密碼系統...................... 29
  2.4 現行網路服務的存取控制.................. 30

第3章 整合式網路服務存取控制機制........... 37
  3.1 整合式網路服務存取控制運作流程.......... 37
  3.1.1 內部存取.............................. 38
  3.1.2 跨網域存取............................ 39
  3.2 系統設定階段............................ 40
  3.2.1 系統參數.............................. 40
  3.2.2 系統中心存取規則...................... 41
  3.3 註冊階段................................ 42
  3.4 身分驗證階段............................ 44
  3.5 資料加/解密............................. 47
  3.6 交談金鑰................................ 49
  3.7 以角色為基礎的存取控制設計..............50
  3.8 內部存取階段.............................54
  3.9 跨網域存取階段.......................... 57

第4章 安全性及效能分析..................... 61
  4.1 安全性分析.............................. 61
  4.2 效能分析................................ 64
  4.3 與現行網路服務存取控制相比較............ 68

第5章 系統實作與模擬....................... 70
  5.1 系統分析................................ 70
  5.2 系統實作結果............................ 71

第6章 結論................................. 79

參考文獻.................................... 80

REFERENCES

一、中文文獻

二、英文文獻


[34] T. C. Wu, Y. S. Chang and T. Y. Lin, "Improvement of Saeednia's Self-Certified Key Exchange Protocols," IEEE Electronic Letters,


[38] Microsoft, [39] MySQL, [40] Public Key Infrastructure, [41] XML.org,