以SAML為基礎之安全採購系統研究

盧振華、曹偉駿

E-mail: 9314337@mail.dyu.edu.tw

摘 要

隨著網際網路的全球普及，企業間的電子交易日益頻繁，大 量取代以往用電話及傳真的交易模式，因此企業間的交易模式逐 漸從利用專線的EDI 轉變成為利用Internet 的XML 交易模式，費 用得以大幅降低。 然而，XML 本身並無法提供完整的網路交易安全的特性，例 如：(1)身分驗證-Authentication (2)授權-Authorization (3)不可否認 性-Non Repudiation，所以必須藉由SAML 安全機制來保護交易資 料的安全。 為了提供安全的Web Service，除了目前常用的SSL 安全機制 外，尚有Microsoft Passport 及SAML 兩種。由於SSL 安全性已被 RSA 公司證明安全性不足[23]，並不適合作為B2B 的安全機制。此外，Microsoft Passport 必須使用Microsoft 作業平台才能提供服 務，對其他系統目前則無法支援，如UNIX，LINUX，PDA 或其 他非Microsoft 的交易平台等，因此為了適合不同裝置及作業平台 的通用性，本研究捨棄Microsoft Passport，採用SAML 標準作為 研究基礎。SAML 為OASIS 提出之新一代電子商務交易安全標準 ，此標準具有：(1) Authentication Assertion (2) Attribute Assertion (3)Authorization Decision Assertion 的特性，這些方法可達到提高 XML 架構的安全性。 除此之外，本研究亦模擬一個採購系統，在Web-based 部分 結合SAML 安全機制，來滿足B2B 網路交易安全的特性。

關鍵詞 : SAML，XKMS，B2B，XML，Ws-Security

目錄

參考文獻

[1] 張思源, 「Web服務安全標準及實務應用」, 民國92年 [2] 林以章, 「發展一企業間的電子商務系統模式－以物料需求計 劃為例」, 大葉大學資訊管理系碩士論文, 民國89 年（指導教 授:梁文耀 博士） [3] 李長庚, 「一個開放的WEB-based single sign-on 服務架構」, 國 立交通大學資訊管理系碩士論文, 民國92 年(指導教授:羅濟群 博士) [4] 潘士豪, 「關鍵鍊專案管理與全球資訊運籌系統」, 國立台灣大 學機械工程系碩士論文, 民國92 年(指導教授:陸一平 博士, 陽毅平博士) [5] Fabio Arciniegas 著, 張嘉麟 譯, 「XML 程式開發指南」, 民國91 年, 麥格羅．希爾 [6] 陳燦煌 編著, 「Delphi 電子商務 網站建構實務」, 民國90 年, 博碩文化 [7] David Carlson 著, 小宇 譯, 「XML 與UML 整合開發實務」, 90 年12 月, 台灣培生教育出版股份有限公司 [8] 林錦雀, 江高舉 著, 「XML 基礎領航」, 民國92 年4 月, 金 禾資訊股份有限公司 [9] 林胤良, 「企業間電子商務認證交換平台發展程序」, 南華大 學資訊管理系碩士論文, 民國92 年 (指導教授:吳光閔 博士) [10] 陳志昌編譯, 「UML 技術手冊」, 民國90 年, 美商歐萊禮股 份有限公司台灣分公司。譯自UML in a Nutshell, 原著 Alhir,S. S.

[11] OASIA, http://www.oasis-open.org,[SAML Version 2.0 Scope and -Work Items], 7 November 2003。

[12] XML台灣資訊網, http://www.xml.org.tw (2004.6.30) [13] Tae-Sun Chung , Hyoung-Joo Kim ,[Techniques for the evaluation -of XML queries: a survey], Data & Knowledge Engineering 46(2003) 225 – 246 [14] Thomas Gros IBM Zurich Research Laboratory Security Analysis -of

the SAML Single Sign-on Browser /Artifact Profile, IEEE2003 [15] OASIS SAML Interoperability Event Demonstrates Single Sign- -On at RSA Conference http://xml.coverpages.org/ni2004-02-19-a.html (2004.6.30) [16] TestMaker http://www.pushtotest.com/ptt/books/thebook.html(2004 .6.30) [17] Web Services Security (WS-Security) http://msdn.microsoft.com/ -webservices/default.aspx?pull=/library/en-us/dnglobspec/html/wssecurity. -asp#ws-security__toc6120228 (2004.6.30) [18] Imamura, Takeshi, et al.,“ XML Encryption Syntax andProcessing ,” W3C, 2002/3 [19] Moses, Tim and Prateek Mishra, et al.,“ Security and Privacy -Considerations for the OASIS Security Assertion Markup -Language (SAML),” Organization for the Advancement of -Structured Information Standards(OASIS), 2002/4 [20] 瞭解 ws - security http://www.microsoft.com/taiwan/msdn -/library/2002/Nov-2002/understw.htm (2004.6.30) [21] 網際網路交易安全 http://www.taica.com.tw/education/ca-1-1.htm (2004.6.30) [22] 網際網路加強安全把關 WS-Policy http://taiwan.cnet.com/ -news/story/0,2000022589,20061608,00.htm (2004.6.30) [23] SSL 不足以提供電子商務安全 http://taiwan.cnet.com/news/ -software/0,2000064574,20083409,00.htm (2004.6.30) [24] XML 加密標準（W3C XML Encryption，簡稱XMLEnc） - http://www.w3.org/TR/xml-encryption-req (2004.6.30) [25] 身分驗證及權限控制的SAML 標準（ OASIS Security -Assertions Markup Language，簡稱SAML），http://www.oasisopen. -org/ committees/security/#documents (2004.6.30) [26] 管理存取權限的XACML 標準（OASIS Extensible Access -Control Markup Language ）， http://www.oasisopen. -org/committees/xacml (2004.6.30) [27] 取代PKI 來管理公開金鑰的XKMS 標準，XML 金鑰管理規 範（XML Key Management Specification，簡稱XKMS），http://www.oasis-open.org/cover/xkms.html (2004.6.30) [28] XML 加密語法處理規範 http://www.w3.org/TR/2002/RECxmlenc- -core-20021210/， XML Encryption Syntax andProcessing (2004.6.30) -Schema: http://www.w3.org/TR/2002/REC-xmlenc-core- -20021210/xenc-schema.xsd (2004.6.30) -Example: http://www.w3.org/TR/2002/REC-xmlenc-core- -20021210/enc-example.xml (2004.6.30) [29] XML 簽章解密轉換標準 http://www.w3.org/TR/2002/RECxmle -nc-decrypt-20021210 (2004.6.30) [30] OASIS 的Web 服務安全技術委員會 http://www.oasisopen.org/committees/tc_home.php?wg_abbrev=wss (2004.6.30) [31] OASIS WEB SERVICE SECURITY:SAML Token Profile -Working Draft 09,27 January 2004 [32] Computerworld SAML Secures Web Services : - http://www.computerworld.com/developmenttopics/development/ -webdev/story/0,10801,73712,00.html (2004.6.30) [33] Computerworld SAML's Cousin: WS-Security - http://www.computerworld.com/developmenttopics/development/ -webdev/story/0,10801,73662,00.html (2004.6.30) [34] 數位認證:該用Liberty 或Passport？ John Pescatore and -Avivah Litan/Gartner ‧ 陳奭璁譯 2003/11/19 - http://taiwan.cnet.com/enterprise/technology/0,2000062852,20085635,00.htm (2004.6.30) [35] 黃崇德，「XML 導入與產業電子化XML Key Management -Specification (XKMS 2.0)」，中原資管所，民國93 年 [36] Article Single Sign-on Simplicity with SAML May 9, 2002 http://java.sun.com/features/2002/05/single-signon.html(2004.6.30) [37] XML Key Management (XKMS 2.0) Requirements http://www.w3.org/TR/xkms2-req (2004.6.30) [38] 澄清 SAML 的不實說法和誤解 http://www-900.ibm.com/ -developerWorks/cn/xml/x-samlmyth/index.shtml#11 (2004.6.30) [39] XML 測試網站 http://www.w3schools.com/xml/xml_ http.asp(2004.6.30) [40] Taiwan.cnet.com 科技資訊網 微軟連夜彌補Passport 安全漏洞 http://taiwan.cnet.com/news/software/0,2000064574,20073844,00.htm (2004.6.30)