適用於企業電子化應用的認證及加密方法

學生: 高銘智　　指導教授: 陳登吉博士

國立交通大學資訊工程學系

摘要

公司行號為了降低成本及營運效能而進行企業電子化。電子化企業營運環境跟原本的營運環境的不同點有:沒有已經建立好信任關係的面對面運作,所有的交易均電子化並經由網路傳送完成,交易的參與者分佈於網際網路及內外部網路及可以處理以儲存的資料會經常有小變動情形的加密的儲存系統。由於這些不同的特性,電子化企業的相關應用需要下列三種基本元件以建立參與者間的信任關係:

1. 加密元件:提供電子文件在不同生命週期的機密性保護。
2. 摘要函式:保證特定資料片段的正確性。摘要函式常與其他密碼演算法結合,用於保證資料不被竄改。
3. 數位簽章:避免非授權的修改及否認。在電子化應用中,數位簽章也用於判斷是否為合法的資料存取。

然而,目前的解決方案無法適用於企業電子化環境的所有狀況。因此,本論文發展一些解決方案改進這些障礙。這些方案包含如下的計畫:

- 關於區塊密碼,本論文針對加密模式及填充模式,發展了兩個解決方案。在加密模式方面,首先分析了由 Katz 等人所提的不可偽造的加密演算法並提出新的演算法改進。所發展的演算法比原先的演算法更適合儲存的資料會經常有小變動的情況。在填充模式方面,本論文發展出新的填充模式。此填充模式具有低資訊洩漏的特性,同時也可抵擋"padding oracle"攻擊。此種攻擊可用於攻擊 SSL/TLS (安全傳輸層/傳輸層安全)協定,這兩個協定用於保護網頁伺服器及瀏覽器之間的傳輸安全(也就是 hypertext transfer protocol secure, https)以及一些無線網路認證協定,如 EAP-TLS。

- 關於認證程序，現有的解決方案，如 SET(Secure Electronic Transaction)，使用 dual signature 以滿足完整性、認證、不可否認性、機密性及關連性等需求。然而，基於 dual signature 的認證程序的參與者侷限於兩個。針對這限制，本論文提出可供更多參與者的 orthogonal signature。同時，基於 orthogonal signature 發展出參與者個數較具彈性的認證程序。

Authentication and Encryption for Electronic Business Applications

Student: Min-Chih Kao Advisor: Dr. Deng-Jyi Chen

Abstract

A firm keeps e-Business applications, such as e-Commerce, Supply Chains, and e-Services, running for cost down and efficiency. An e-Business environment has some different characteristics from the original business environment such as no face to face operations without established interpersonal trust among participants, all e-Business transactions that are performed electronically with the use of communication networks, the participants involved in through Intranet, Extranet, and Internet, and an encryption storage system in which the underlying data is constantly changing yet encrypted versions must be stored. Due to the different characteristics, three basic components of security mechanisms are needed to create trust relationship among the participants:

1. Encryption: provides confidentiality for each document life cycle in the electronic document management system.
2. Hash Functions: ensure the correctness of content of a piece of information. Hash Functions usually integrate with other cryptographies to ensure that no data should be corrupted in an electronic business application.
3. Digital Signatures: prevent unauthorized modification and repudiation. Digital signatures are also related to legitimate pattern of operations in data access in a business process.

However, current solutions can not fit in with all conditions of the e-Business environment. So, the dissertation develops some schemes to improve the barriers. The developed schemes include as follows:

- For block cipher, three are two schemes proposed for encryption modes and padding (the last block) respectively. For the encryption mode scheme, Katz et al's unforgeable

encryption scheme is analyzed and improved. The improved unforgeable encryption is more fit in with the condition when the inputted document changes frequently and small than original one. For the padding scheme, a new padding with low information leakage is developed. The new padding scheme can prevent padding oracle attacks. Such attacks are useful for the SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocol, which is not only used for building secure channel such as hypertext transfer protocol secure (https) https but also used for some authentication protocols such as EAP-TLS

- For authentication procedure, the current solutions, such as SET, HK, used dual signature to satisfy the requirements such as integrity, authentication, non-repudiation, confidentiality, and relationship. However, the number of the participants of authentication procedures based on dual signature restrict to two. For this restriction, this dissertation proposed an orthogonal signature scheme that can work within multiple parties more than two parties and a flexible authentication procedure based on orthogonal signature.

誌 謝

本篇論文的完成，要感謝的人很多；首先感謝指導教授 陳登吉教授及葉義雄教授，在求學過程中提供費心的指導，以及在不順利的時候的鼓勵，我才能夠順利畢業，希望這篇論文可以讓已經在天上的葉老師放心一些。

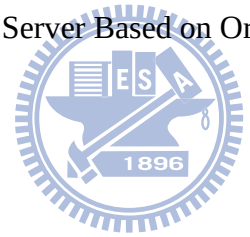
此外，也要感謝曾建超教授、蔡錫鈞教授及黃世昆教授在論文寫作後期給予的建議與指正，使得論文更加完整。

再來要感謝我的家人，尤其是太太及其二姐，幫我照顧小女兒，讓我可以專心讀書，取得博士學位。

最後要衷心祝福陳登吉老師恢復往日的活力。

Contents

List of Figures



List of Tables