結合憑證之角色存取控制系統實作

An Implementation of Role-Based Access Control with Certificates

謝濱燦
Bin-Tsan Hsieh
德明財經科技大學資訊管理系
bintsan@mail.takming.edu.tw

林易賢
Yi-Hsien Lin
德明財經科技大學資訊管理系
penguinkern@gmail.com

摘要

「科技始終來自於人性」這句話相信大家都可以朗朗上口，而且時常被引用，在這資訊發達的時代裡，舉凡許多智慧型資訊服務系統，已環繞在我們平常的食、衣、住、行四週，與人類緊密的在一起；但是這些服務系統，時常因人性貪婪慾望無限，於是利用了資訊系統管理上的疏失或程式本身的漏洞，企圖的想使資訊服務系統故障，因此從中獲得利益，近年漸漸出現了民間駭客團體，甚至有國家培養了大批軍隊化駭客組織，伺機駭侵各國民生基礎設施(如伊朗核能設施、日本三菱重工等國防工業承包商、美國國會遭駭侵)，竄改竊取國家機敏資產，輕者僅造成生活不便利，嚴重情形恐將肇生人類滅亡危機；鑒於我國軍資訊系統參數及各項研究資料，攸關了國家重要軍事資訊，一旦遭有心人士滲透修改或國軍重要資訊遭竊，恐使軍隊未戰先亡，國家人民安危實在令人憂心；本文藉由國軍各級人員職務角色設定，給予資訊系統管理的應有權限，期提升國軍資訊系統管理機制，強化國軍整體資訊作業環境安全，杜絕資安管理罅隙。其中將以國軍資安監控軟體系統(例如：移動式媒體管控軟體)等多項系統，提出的資安管控強化機制的架構、操作流程與整體設計上的細節，俾成資訊安全零風險最終目標。

關鍵詞: 職務角色、管理權限、國軍移動儲存媒體監控軟體

ABSTRACT

The catchy slogan that technology comes from human nature has been discussed and cited frequently. In the era of information technology nowadays, the service system of artificial intelligence exists in our daily life and interacts with our lifestyles inseparably. However, due to the human greed and selfish, somebody might intend to obtain illegal benefits from the negligence of system management or software vulnerability. Moreover, crackers and even the official military hackers launch malicious computer hacking to attack infrastructure.(e.g. Iran nuclear facilities, Mitsubishi Heavy Industries, Ltd., and United States Congress were hit by cyber attack.).What the crackers do would destroy facilities and damage our ways of lifestyle; moreover, it might lead to the crisis of human extinction.The military information system, which contains parameters and researches of confidential, conserves important materials. Those people who have evil intentions steal into the military system and then falsify or steal the important data. Therefore, army and even the country will sink into extremely danger. The implementation of role-based access control with certificates confers individual authority on specific managers. The intention is to advance the military management system and strengthen the security of operating environment so that the information security flaw could be eradicated.The usage of military information security system (E.g Mobile media control software) with some specific systems promote the structure of information security system, operating procedures, and details of the whole project. To achieve the zero risk of information security is the supreme destination.

1. 前言

1.1 研究背景

一個先進的國家軍隊擁有許多智慧型資訊服務與監控系統已是不可缺少，然這些資訊系統的管理方式，一定必須在安全無虞的防護架構前提下，防止系統遭受破壞或竄改，才能使服務系統永續運作，近年各國資安業者為提升資訊系統安全強度，在行政院資通安全政策指導推動下，各類的軟硬體防護設備有如雨後春筍般大量出現；而國軍為了使資訊系統作業環境更安全，年年挹注了不少人力與金錢，但是分析了許多國際間駭侵案例及國軍資安違規事件，大部分都是因為資訊管理人員怠惰便宜行事等作業疏忽所肇生無可挽回的資訊災難，即使再多的資安防護設備，也是無法防範,反覜唯有做好各層級人員資訊系統使用、監控、管理的權限分別與限制，回歸到最基本安全防護層面才是最重要的。

1.2 研究動機

現行「國軍資訊安全政策規範」,各軍事單位訂定新進、調、離職、退伍（休）、因公出國之人員資訊安全管制規定與作業程序；然現階段國軍就人員調離差時，僅要求各資訊系統帳號密碼需重新設定變更，若一旦系統管理人員未能完全落實此項作業程序時，將成為有心人員利用此管理漏洞，藉機破壞或竊取國軍重要資訊資料。2016年5月30日新聞報導「美醫療資訊系統有後門漏洞，外人可竄改病歷」,指出MEDHOST公司的手術期間資訊管理系統，因為廠商預留下一組固定帳號密碼,形同後門漏洞,儘管該帳號密碼並未對外公開，但一被有心人士取得，將讓要進行或剛完成手術病人的相關資料，遭受被竄改的威脅。因此若能將權限授予職級、角色，而非直接予個人，再將個人與職級、角色綁定[1],這樣的做法將提供國軍更佳且快速管控各層級人員使用「國軍資安監控軟體系統權限」的資安防護管理機制。

2. 研究目的

本研究的主要目的是設計出一套國軍各層級人員級職藉由憑證卡登載電腦，透過憑證卡自動辨別職務，分出屬資訊職務人員資訊系統使用權限，有鑑於傳統的管理作業耗時繁雜模式，將針對資訊系統管理人、資訊主管及資訊主官，因人員調離職後，所需耗費大量時間及人力，執行各系統帳號密碼異動，本項研究，預期將帶給國軍人員對於角色職務權限支配不一樣的資訊安全管理思維。

3. 研究方法

本系統是使用 VB.NET 語言來撰寫，將導入於「國軍資安監控軟體系統(移動儲存媒體監控軟體)」，未來一旦要在國軍資料輸出入專案電腦前，開通操作設定移動儲存媒體時，均必須使用個人憑證卡登入系統驗證人員職務權限，本存取控制系統，首先欄位須完成人員姓名輸入，第二欄位配合國軍人事資料職稱設定，第三欄位系統權限賦予設計，第四欄位職務結合管制賦予的作業權限，最後欄位人員與職稱結合，俾達成資訊系統管理自動化，且強化了國軍整體資訊作業環境。

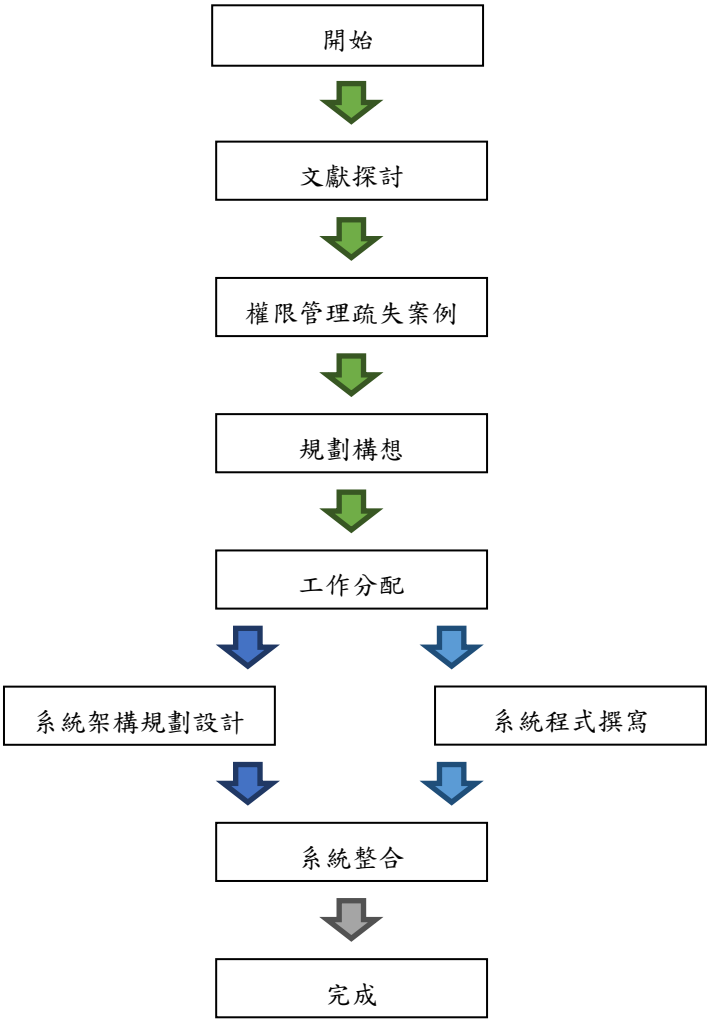

圖 1 研究流程圖

表 1 權限賦予系統功能表

功能	概要說明
一、人員維護	新增人員名稱
二、職稱維護	設定單位處長、副處長、資訊官、資安官、資訊士、資訊兵
三、權限維護	各項資訊系統名稱建置於本權限管控系統
四、職稱權限設定	設定結合職務使用系統權限
五、人員職稱設定	結合建立人員與職稱設定

4. 研究創見

本系統係結合國軍人員憑證卡與結合國軍人事資料庫，可落實國軍人員職務賦予的職掌，避免國軍人員未按編制用人；且本項研究軟體可適用國軍其他各項監控系統或服務系統，另可確遵行政院要求「政府機關(構)資安事件數位證據保全標準作業程序」，建立數位資訊鑑識日誌，落實資安違規肇案設備保全工作，絕不發生刪除檔案、格式化儲存設備，甚至湮滅證據(物)或系統更改簽章認證等情事，有利於系統日後追查更改人員及時間戳記，俾資安事件肇因查察及釐清違失責任。另國軍今年 105 年依「政府機關公開金鑰基礎建設憑證政策」規定，國防部已完成國軍電子憑證第二代金鑰暨簽章演算法升級，各資訊應用系統亦將配合與時俱進要求提升，將全面推行憑證卡使用，可落實職務權限政策。

5. 相關技術

以「國軍移動式媒體管控軟體系統」為例，國軍人員一旦登入個人行政電腦後，即可登載網址點選網頁系統登入中層管理監控系統，如果人員一旦擁有此系統帳號與密碼或因前職務之便紀錄系統帳號密碼，即可登入開通任何內部網路一台行政電腦，讓電腦內所安裝之長駐監控程式(kerberosb 軟體)失效，外來儲存媒體成為可信任設備，使有心人員可以藉由移動式儲存媒體，竊取公文機敏資訊，或放置未知惡意程式與病毒於國軍內部網路，造成國軍資訊作業環境更大傷害，顯見本系統仍有待加強安全防護，如果國軍電腦未來結合憑證之角色存取控制系統，將可強化「國軍移動式媒體管控軟體系統」管理系統資訊安全強度。

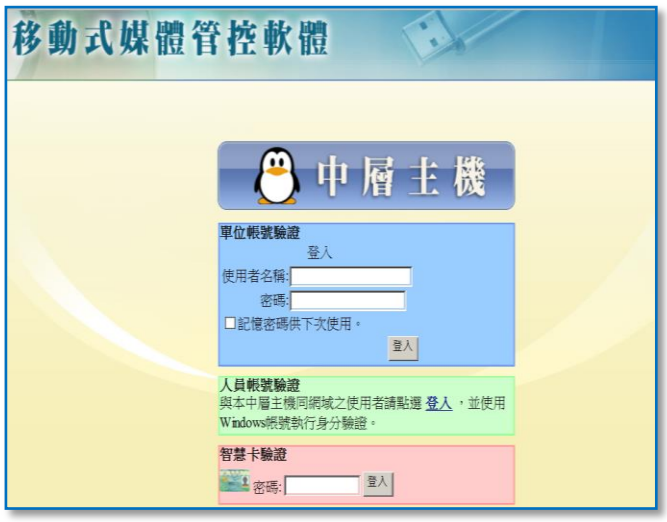

圖 2 國軍移動式媒體管控軟體系統

圖 3 國軍移動式媒體管控軟體系統偵獲違規（未核可裝置）

圖 4 管控軟體系統人員建立

6. 系統實作成果

本系統將以最基礎的程式設計概念，參考「用實例學 Visual Basic 2013 / 2012 程式設計」等書籍[2]，當國軍人員改變職務時，管理者必須對所有的資訊系統修改這個使用者的權限，而且當使用者和系統都越來越多時，要修改的東西也就越來越多，越來越複雜。然而 RBAC 是將傳統授予使用者權利的方式改成了使用者對應到角色、角色再對應到權限；首先我們分別完成人員維護(人員名冊)、職稱維護(角色職稱)、權限維護(國軍各分項系統)、設定職稱權限(角色職稱勾選可以使用之系統)及設定職稱人員(角色職稱勾選人員)等五大類[3]。

圖 5 系統功能分項

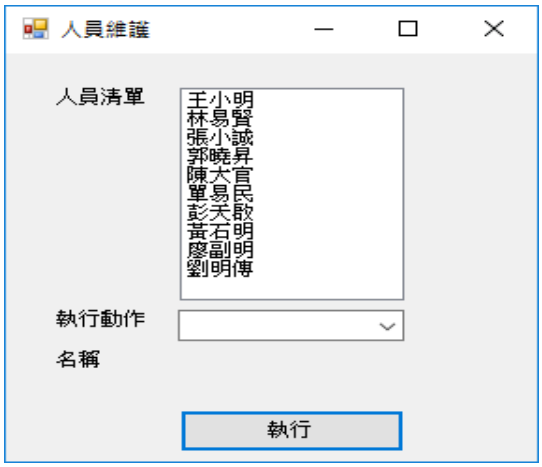

圖 6 人員維護(人員名冊)

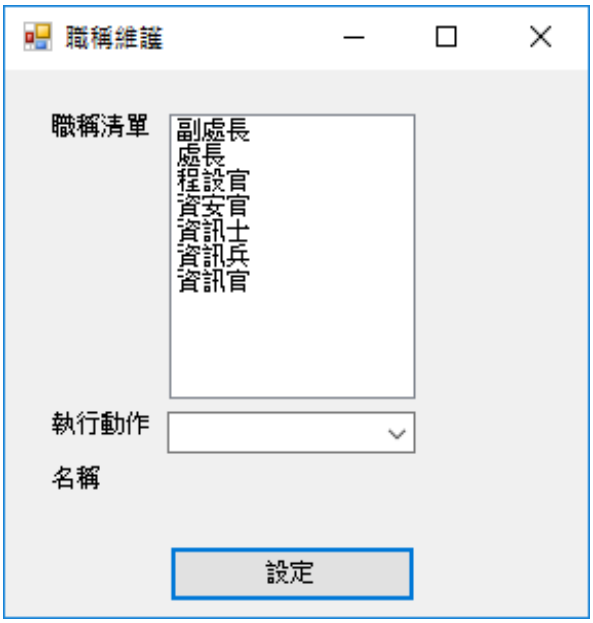

圖 7 職稱維護(角色職稱)

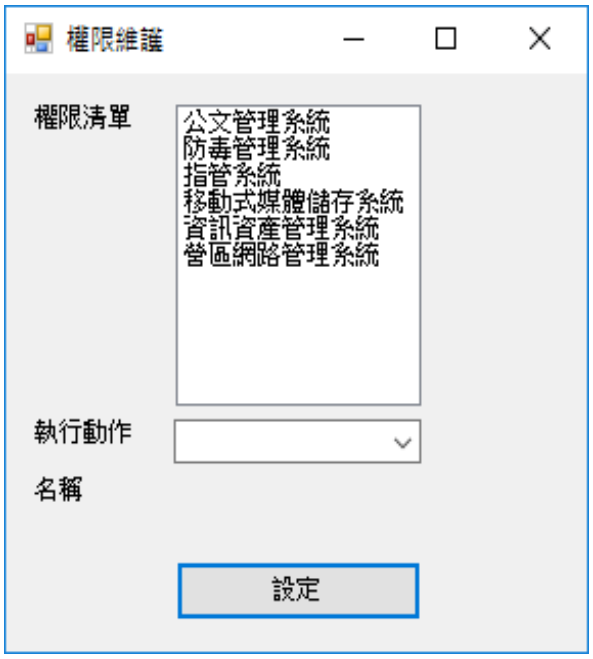

圖 8 權限維護(國軍各分項系統)

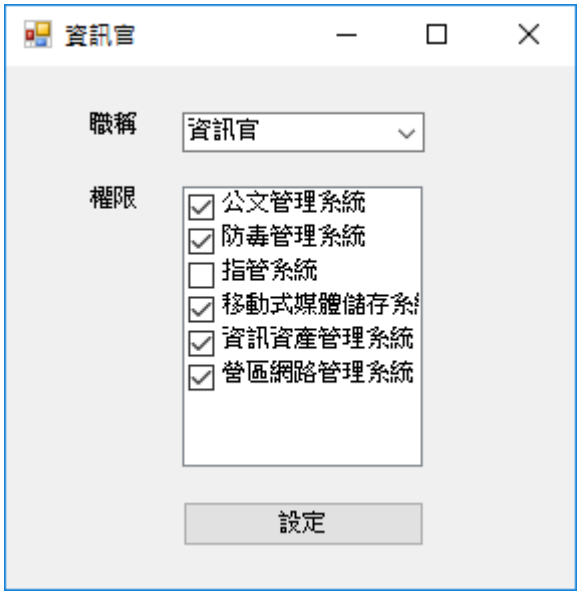

圖 9 設定職稱權限(角色職稱勾選可以使用之系統)

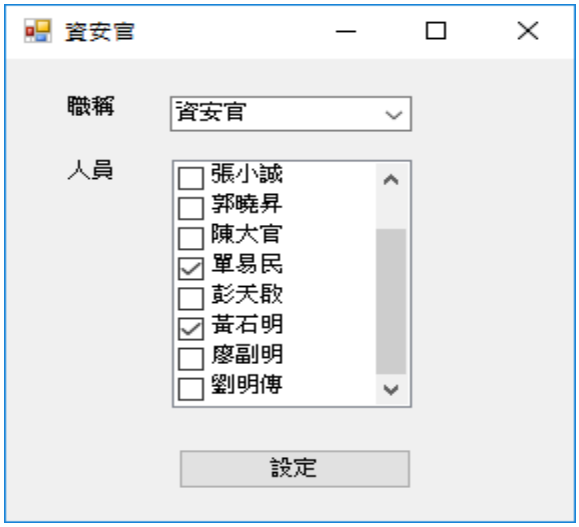

圖 10 設定職稱人員(角色職稱勾選人員)

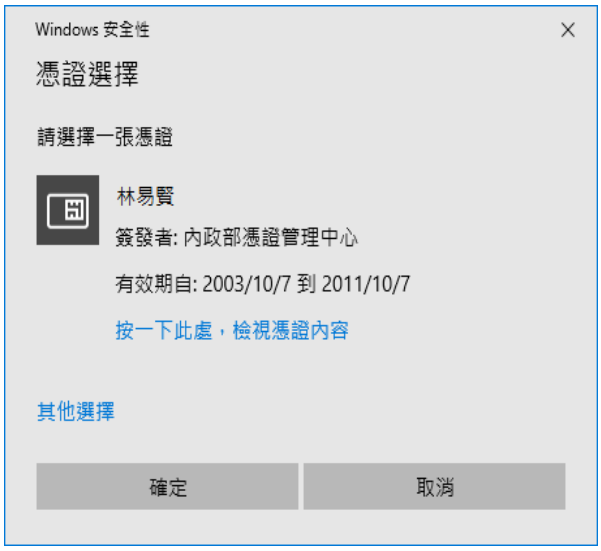

圖 11 憑證圖

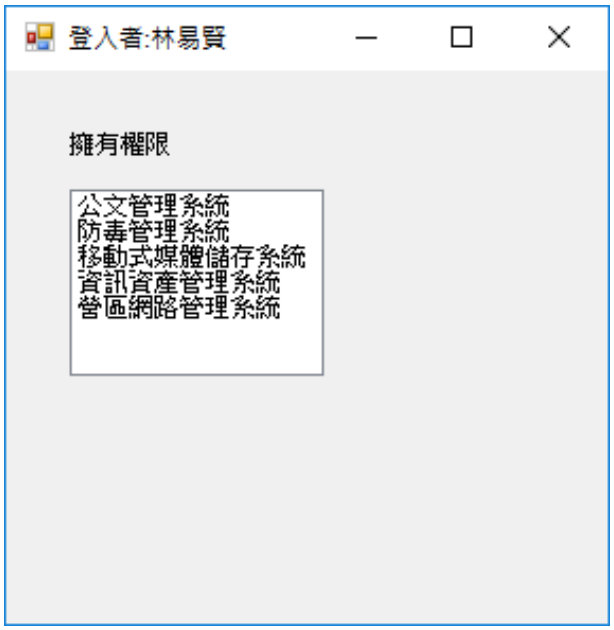

圖 12 人員擁有系統權限

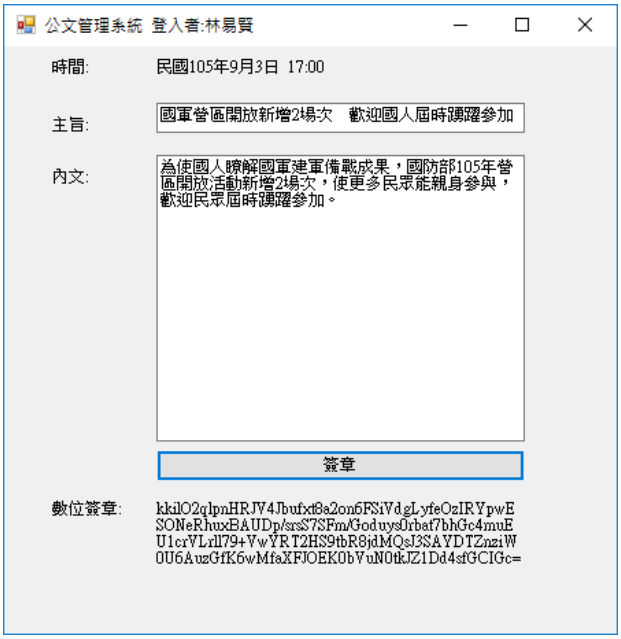

圖 13 驗證成功圖

7. 結論

行政院為提升各部會資訊作業環境安全，已要求各單位必須提升智慧型憑證卡系統，未來如國軍人員全面使用二代智慧型憑證卡加密簽章及人員憑證認證機制(憑證資料庫)，再與本次研究的憑證之角色存取控制系統及國軍人事資料庫相結合，將可以落實國軍組織人事編裝角色任務，賦予職務應有的資訊工作權限，透過這些角色分配，可獲取資訊服務的權限來執行特定的系統功能，日後必定可以提升資訊系統安全強度，不必擔心國軍資訊人員調離職後仍有存取權限，利用

電腦遠端連線進入國軍重要系統。

參考文獻:

[1]張瑞中、陳啟彰,「以角色流程控制為基礎的網格認證機制」資訊科學運用期刊,vol.5,no.2 ,pp.25-44，2009年。

[2]陳會安,2014年,用實例學Visual Basic 2013 / 2012程式設計,碁峰資訊

[3]余美伶,「結合角色和資料夾的存取控制模組設計－以數位學習系統為例」,國立嘉義大學資訊工程學系,中華民國資訊學會通訊,vol.8,no.2 ,2005年。