出國報告(出國類別：專題研究)

利用網際網路彙整主計相關資料之應用

服務機關：行政院主計處電子處理資料中心
姓名職稱：蔡東華設計師
派赴國家：美國
出國期間：95 年 6 月 15 日至 12 月 14 日
報告日期：96 年 3 月 9 日

摘　　要

從大型主機的時代後，電腦的架構漸漸走上分散式的系統架構，由一台 Server 管理一群 Client，因此，開發程式的人如何部署程式，便成了一個重要的課題！接著網際網路時代的來臨，資訊的傳遞無遠弗屆，只要地球上任一個使用者端有瀏覽器、PDA 或手機等介面，無須安裝其他應用程式即可透過網際網路存取遠端資料。

本次出國專題研究計畫主要赴美國紐澤西州的紐澤西理工學院進行網際網路資料收集的相關技術研究，本研究工作進行的項目分別為：網際網路環境研究、資料之處理、資訊安全、個案研究、網際網路資料收集語言 XML 等之應用，並參加美國 IASTED 機構舉辦之通訊、網路及資訊安全國際會議 (CNIS 2006 ; Communication, Network, and Information Security Conference)，進行有關電腦通訊、網路及資訊安全相關主題研討。參加美國微軟公司網際網路解決方案與新世代資料整合應用交流研討。本處各項業務如：概預算編製與執行、半年結算、決算、各項統計調查等，均需在有限的作業期間內收集來自全國各地的大量資料作彙整。如何利用網際網路來打破地域限制、減少使用端安裝管理又能安全地將資料收集至本處各業務資料庫作分析與處理，是下一個努力的目標。

目　　次

一、目　　的

(一)主題

隨著 90 年代全球資訊網（World Wide Web）的興起宣告全球數位化時代的來臨。短短十幾年間，電腦與網際網路蓬勃發展已從學術的研究工具變成現代人的生活必需品。本次出國專題研究，係於美國紐澤西州的紐澤西理工學院進行。利用學校的研究環境與學術資料庫在電子與電腦工程系教授指導下進行網際網路資料收集的相關技術研究。

(二)緣起

從大型主機的時代後，電腦的架構漸漸走上分散式的系統架構，由一台 Server 管理一群 Client，因此，開發程式的人如何部署程式，便成了一個重要的課題！如果將程式邏輯寫在 Client 端，每一次版本更新的，系統管理者必須重新至每一台 Client 安裝新版程式；如果將邏輯程式碼集中在一台 Server 中管理，將可以省卻部署的問題。接著網際網路時代的來臨，資訊的傳遞無遠弗屆，只要地球上任一個使用者端有瀏覽器、PDA 或手機等介面，無須安裝其他應用程式即可透過網際網路存取遠端資料。

本處各項業務如：概預算編製與執行、半年結算、決算、統計調查等，均需在有限的作業期間內收集來自全國各地的大量資料作彙整。如何利用網際網路來打破地域限制、減少使用端安裝管理又能安全地將資料收集至本處各業務資料庫作分析與處理，是下一個努力的目標。

二、過　程

本次出國專題研究計畫期間自2006 年 6 月15 日至 12 月 14 日，主要赴美國紐澤西州的紐澤西理工學院進行網際網路資料收集的相關技術研究，期間於10 月3 日至 6 日參加美國微軟公司網際網路解決方案與新世代資料整合應用交流研討。 10 月 9 日至11 日參加美國IASTED機構舉辦之通訊、網路及資訊安全國際會議 (CNIS 2006 ; Communication, Network, and Information Security Conference)，進行有關電腦通訊、網路及資訊安全相關主題研討。10 月 13 日至 16 日參加美國紐約大學網際網路資料收集語言XML等之應用研討。

因為本次研究重點內容為利用既有的網際網路環境蒐集資料，所以資料收集及參訪對象以軟體工程為主。首先了解電子資料蒐集的各個階段及其演進；進而研究各種網際網路蒐集資料的工具及不同的網頁設計語言，其異同，相關性及優缺點。除了網頁存取技術與標準外，本次研究的另一個重點是網路安全，包括資料的完整性，保密及病毒的處理等。

本研究工作進行的項目分別為：網際網路環境研究、資料之處理、資訊安全、個案研究、通訊、網路及資訊安全國際會議、網際網路資料收集語言 XML 等之應用，以下分述之。

(一)電腦化資料蒐集方法的演進

以下的表格概要描述出自從電腦革新了資訊管理後，資料如何收集到中央辦公室(電腦中心)：

	優點	缺點
紙張/信件/傳真 (Paper/mail/fax)	最經濟	收到時沒有確認 (confirmation)； 資料重複輸入； 沒有錯誤檢查機制； 由遞件人員負責安全。
觸鍵式電話(Touch tone phone)	提供輸入 直接收到資料庫 硬體相對便宜 地下電話線提供基本的安全	冗長； 只能輸入數字(Numbers)，不能輸入文字(text)，而且不允許使用者回頭輸入；
磁片/telnet (Disks/ telnet)	依靠程式，提供全螢幕編輯； 允許任何資料型態的輸入，數字(number)，字元(character)，符號(symbol)，等 程式提供錯誤檢查； 使用者輸入的資料可以加密以達好的安全；	很難控制資料輸入軟體的版本； 不能確認資料的接收 (reception)；
網際網路(Internet)	由使用者輸入；避免重複輸入； 使用者介面可提供錯誤檢查：包括邏輯檢查或提供允許的選項； 加密資料傳輸以達最佳安全； 確認資料接收； 單一的軟體版本控制；	設備可能因為需求的複雜而較昂貴。但是這些設備可以與以網頁為基礎(web-based)的環境結合。

在電腦網路化以前，所有的資訊都經由各式表格先郵寄到電腦中心後以人工方式手動輸入資料庫。從資料產生到存放到資料庫的期間，沒有任何機制可以確認原始表格是否正確無誤、郵遞或操作員的資料輸入也沒有很少有線上即時的偵錯設計。資料輸入後電腦可以印出資料庫確認內容但是需大量人工核對原始輸入資料，而且除非核實經也有原始資料產生者的參與，任何人無法保證當初填寫表格時是否有筆誤。資料核實是傳統人工方式手動輸入法的最大挑戰。由於表格可能在郵寄時遺失、沒有全面進行再次確認讀取(secondary proof reading)等原因，錯誤率是所有輸入法中最高的。除了

錯誤率高以外，傳統表格很難加密，也無可靠的方法防止資料遭竄改，所以手動輸入法的安全性也是最低的。

電腦磁片或是磁帶曾是傳遞資料的重要媒介。完整的資料庫通常會產生一個或數個使用者應用程式或使用者介面。在輸入資料前通常使用者必須先在電腦安裝應用程式。應用程式具備一些基本的邏輯及偵錯的功能，譬如日期的格式等。當資料輸入電腦後可直接或經由加密存入磁碟。就像一般表格般，含資料的磁片也經由郵寄到電腦中心。磁片上的資料可直接讀取到主機的資料庫中。因為所有資料僅在最原始產生時被輸入一次所以錯誤率也很明顯地降低。但是郵寄常有遺失或是在郵遞過程中損壞等總是無法避免。磁碟加密磁碟也明顯的保護了資料的完整性。

當數據機(Modem)開始出現並且將電腦變成虛擬網路，大量的資料可經由遠端撥接(dial-in) 輸入到伺服器。這比郵寄資料的方法進步很多。資料產生者可以利用一個配備數據機的電腦， 撥接並登入(dial in and logon)到伺服器。 他可以傳輸先前存成檔案的資料。這個檔案可直接傳入電腦主機並將資訊輸入資料庫。這個方法在 80 到 90 年間非常流行。它解決了所有郵誤的問題。 如果終端程式設計的很好，這樣的介面可以減少因為疏忽導致的錯誤。 一個含有內建強制(sophistic)錯誤檢查的好介面 (sophistic build-in)，可以將錯誤的資料幾乎減至零。但是電話線並不夠安全。有心人(Predicators)可以很容易地竊聽電話偷取敏感資料。另外一個非常重要的課題是終端機應用系統的版本。這個方法依賴遠端資料產生者持續更新遠端電腦的版本。伺服器有時候很難追蹤資料產生者是否用最新版本的軟體。

使用觸鍵電話(touch phone)輸入資訊已經有很長一段時間到現在還使用中。因為所有的問題是由伺服器產生並由資料產生者輸入回應(the response)直接進到資料庫，所以這也是最直接的資料輸入方法。但是這個方法只能運用在簡單的資料輸入或選項。當操作時間超過一分鐘以上，會使使用者變得不耐煩。如果在操作過程中產生錯誤而需回頭修改時，這個方法會很困難。

當網際網路在 90 年代逐漸流行，資料蒐集的方法開始合併到以網頁為基礎的應用系統。尤其最近幾年當新技術的發展使這個方法滿足安全，精確，及效率問題。

(二)以網頁為基礎(web-based)資料收集方法的發展

遠端輸入最顯著的進展是可在網頁上利用表格(form)輸入資料。這個方法目前已經變成一個最流行的收集資料的方法，因為網際網路發展非常快速，可以將資料由遠端直接輸入到中央資料庫，而且這個方法不需特別的設備(specific types of equipment)即可輸入資料。網頁為主(web-based) 的方法可以在輸入資料時作及時檢誤與編輯，如果需要的話網路程式(web programming 也提供許多傳統的技術作輸入介面(inputting responses) 例如：文字方塊(textboxes)、 下拉式選單(dropdowns)、核取方塊 (checkboxes)或其他形式(styles)等，只要有網頁瀏覽器不需在用戶端(client)安裝額外的軟體。

早期網頁開發者必須使用 Hyper Text Markup Language (HTML) 來開發網頁表格，透過用戶端的瀏覽器顯示這些表格並允許資料輸入，再將資料傳送(submitted) 到伺服器。JavaScript 程式語言則是在資料被傳送到伺服器之前用來驗證(validated)資料。動態式(Dynamic) HTML (DHTML)加強 HTML 功能與使用 Cascading Style Sheets (CSS) 讓開發者更容易控制對網頁、表格及圖形影像(graphical images) 的外觀(appearance)。伺服端程式語言 (例如 Java, Active Server Pages (ASP),及 Personal Home Page (PHP)) 用來撰寫伺服端系統並在連結至網路站 (website) 時執行，這些系統將伺服器上資料庫、檔案或其他資料來源(sources)的內容用問卷 (questionnaires) 的方式表現。這些伺服端程式語言同時用來撰寫伺服端檢誤系統可以大量地檢驗由遠端電腦送來的資料。最近，可擴展標示語言 the eXtensible Markup Language (XML) 已經被許多開發者採用來有系統地傳遞資料。藉由結合 eXtensible Stylesheet Language (XSL) 可發展更豐富而有用的系統使用內建驗證(built in validation)技術及利用控制(controls)和圖像(images)來收集和顯示資料。網際網路標準 W3C 委員會在二零零三十月提出新的建議： Xform standard –用 XML 為基礎開發下一代網頁資料收集工具。隨著 ASP.Net 程式語言及功能更強的 JAVA, PHP 及其他程式語言的出現，程式開發者現在有非常多的開發工具可用來發展系統。

1.現有網頁技術與標準

本文標示語言： HTML* 、 XHTML* 、 XML* 、 XForms*

樣式格式描述語言： CSS* 、 XSL*

動態網頁技術： CGI 、 ASP 、 ASP.NET 、 ColdFusion 、 JSP 、 PHP

客戶端交互技術： ActiveX 、 Java Applet 、 Flash 、 AJAX 、 XMLHTTP*

客戶端腳本語言： JavaScript 、 JScript 、 VBScript 、 ECMAScript

標識定位語言： URL 、 URI 、 XPath 、

文檔綱要語言： DTD* 、 XML Schema*

* 表示由 W3C 制定和維護的標準與規範

2. HTML

HTML 是網路世界最通行的程式語言。它用來撰寫超文件(Hypertext)到全球網際網路。是由標準通用置標語言(Standard Generalized Markup Language SGML)發展出來，任何文字處理器均可撰寫與編輯 HTML 文件。

HTML 使用標籤(tags)例如 <h1> 和 </h1> 將本文區分成標題(headings)、段落(paragraphs)、清單(lists)、超文件連結(hyperlink)等。HTML 文件也是 "網頁(Web pages)" 的代名詞。瀏覽器經由網際網路可以檢索(retrieves)存放在全世界任何伺服器上的網頁。

以 HTML 為基礎的網頁很適合簡單的瀏覽，它也具備基本的伺服器與使用者之間資料交換的功能。但是 HTML 最大的限制是它無法處理較複雜的表格，也不具有邏輯編譯的功能。

3. XHTML

XHTML 是當前 HTML 版的延伸，因為 HTML 語法比較鬆散，網頁編寫者可以很容易的編寫網頁，但對於瀏覽器來說，語言的語法越鬆散，處理起來就越困難。傳統的電

腦瀏覽器還有能力相容鬆散語法；但對於許多其他較新，非傳統的設備，比如手機等，就比較困難。因此產生了由文件型態定義 (Documents Type Definition,DTD)定義規則，語法要求更加嚴格的 XHTML(The Extensible HyperText Markup Language)。XHTML 文件型態也是根據 XML 設計的，所以可以與 XML 開發環境相容。

XHTML 1.0 是 HTML 自從 HTML 4.0 在 1997 年發佈後第一個主要的變化。它是 W3C 發展 的標準，採用嚴謹的語法產生 XML 網頁，可以用在多種新的瀏覽器平台包括手機、電視、汽車、皮夾大小的無線通訊器(wireless communicators), 公用電話亭(kiosks)及桌上型電腦。XHTML 1.0 從新編譯 HTML 成為 XML 規格，使得它容易處理與維護 。XHTML 1.0 借用 W3C's 用在 HTML 4 的元件和屬性，因此現存的瀏覽器可以依循一些簡單的規則來編譯 XHTML 網頁。

3.1 XHTML 1.0 的三個型態：

XHTML 1.0 有三個不同的型態，文件開始第一行的指令來指明文件的型態。每一種型態有它自己的 DTD - 文件型態定義 (Documents Type Definition) – 定義出非常嚴謹，該文件特有的規則。

XHTML 1.0 Strict – 當只需要一個嚴謹而平整的文件，但不需要任何特殊的版面安排時(markup associated with layout)可採用這個型態。可與 W3C's Cascading Style Sheet language (CSS) 結合取得字型(font)、顏色(color)和其他你要的效果(effects)。

XHTML 1.0 Transitional –

這種型態是許多撰寫網頁者常用的。網頁本身包含許多新一代的屬性如背景圖案、特殊字型或連結等。利用 XHTML 一些新的功能並只對標誌(markup)作一些小幅度調整，即可在舊版，不了解格式頁(style sheets)的瀏覽器瀏覽。

XHTML 1.0 Frameset –

當需要將瀏覽器畫面分割成多個框架(frames)時，使用這個變化。

XHTML Basic

XHTML Basic 是 XHTML 家族中第二種被推出的。

XHTML Basic 文件形式只包含了 XHTML Host Language 文件型式最基本的模組並加上對圖像(images) ，表格(forms) ，基本表單(basic tables)及物件(object) 的支援。它是為了一些無法支援 XHTML 屬性的網路使用端設計的，例如：行動電話(mobile phones), 個人數位助理(Personal Digital Assistant,PDA), 呼叫器(pagers), and 機上盒(settop boxes)。這種文件型式本身就足以展現豐富的內容。

XHTML Basic 設計成可以容易擴充的語言，舉例來說：它可以依實際狀況外加一個事件模組(event module)或直接藉由 XHTML Modularization 例如 the Scripting Module 來擴展功能。XHTML Basic 的目的是一個通用語言(common language)來支援不同型態的使用端(User agents) 。

3.2 XHTML-Print

XHTML-Print 是 XHTML 程式語言家族的一員，也是由 XHTML 模組化(Modularization of XHTML)下發展出來的.。它是為了提供一些行動裝置可以從基本功能的印表機列印。這些印表機可能沒有整頁的記憶(full-page buffer) 或只能從上至下，由左到又列印；而且也不能旋轉。XHTML-Print 也是為了一些不能安裝特定印表機驅動程式且對格式列印要求不高的環境設計。

4. XHTML 2.0

XHTML 2.0 是一個標誌語言(markup language) 用來支援多功能的可攜式網頁為基礎(portable web-based)的系統。它是由 HTML 4, XHTML 1.0, 及 XHTML 1.1 演進而來但卻與它的前身不相容。

XHTML 2 也是 XHTML 標誌程式語言家族的 一員，它是伺服器端語言的一種同樣的也是由 XHTML 模組化(Modularization of XHTML)發展出來的。XHTML 2.0 不但更新

了許多前一個版本模組化的定義，它還包含了許多新的模組及其語法。XHTML 2.0 也可以使用其他語言如 Ruby, XML Events, 及 XForms 的模組.

4.1 XHTML + MathML + SVG 組件

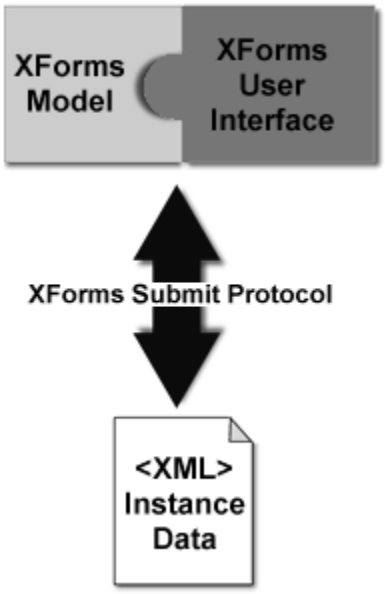
一個 XHTML+MathML+SVG 組件(Profile)是由 XHTML 1.1, MathML 2.0 和 SVG 1.1 組合而成。利用 XML "namespaces"指令，這個組件可以將 XHTML, MathML 以及 SVG 混合在同一份文件。

5. XForms

XForms 是由 HTML 表格(HTML form) 演變而來的。它是也依循 W3C 的標準，採用 XML 的格式，易於使用。傳統的 HTML Web forms 並不區分表格的設計(presentation)與功用(purpose)，相反的 XForms 用不同的段落來描述表格的功用及表格的設計。這樣表格的運用可以比較靈活，也可以把傳統的 XHTML 表格加到 XML 表格定義中。

右面的圖示簡單的表示一個與設備無關(device-independent)的 XML 表格定義 (XForms Model) 可以與多種標準或使用者相容。

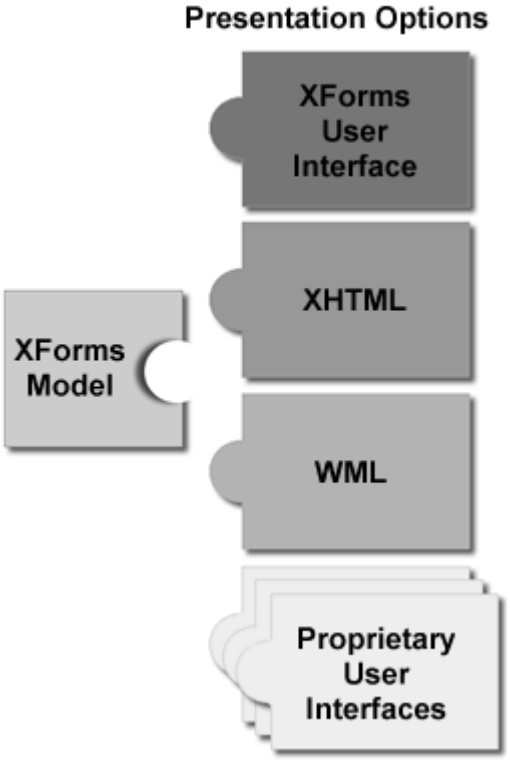
XForms 的使用者介面(User Interface) 提供一個標準的視覺控制(visual controls)組來取代 XHTML 表格控制。這些表格控制可直接用在 XHTML 及其他 XML 文件。



XForms 一個重要的概念是表格收集的資料用 XML 模式資料(XML instance data)形式表示。 XForms 模組(Model) 用來描述模式資料 (instance data)的結構。就像 XML 一樣，表格表達結構化的資料交換。工作流程(Workflow)，自動填寫(auto-fill) 和預先填寫(pre-fill)表格的系統也支援使用模式資料。

最後，需要一個管道來處理模式資料與 XForms 處理器(Processor)的資料交換。為此，XForms Submit Protocol 定義了 XForms 如何傳送與接收資料，也包括暫停(suspend)及重新啟動(resume) 完成一個表格。

右面的圖示彙總 Xforms 的主要觀點：



Xforms 的主要目的

- 支援掌上形處理器(handheld)，電視，桌上型電腦瀏覽器，加上印表機及掃描器
- 更豐富的使用者介面滿足企業、消費者及設備控制系統(device control applications)
- 分開處理資料、邏輯(logic) 及顯示畫面(presentation)
- 國際化
- 支援結構化表格資料
- 加強表格邏輯(logic)
- 一頁多表格、一表格多頁
- 支援暫停(suspend)及重新啟動(resume)
- 與其他 XML tag sets 密切地整合

6. XFrames

XFrames 是一種 XML 應用軟體用來把文件組合在一起，取代 HTML Frames。

XFrames 嚴格來說並不是 XHTML 的 一部分，它提供類似 HTML Frames 的功能，藉由讓框架(frameset)的本文(content)在它的 URI 檢視，因此使用上的問題比較少。

7. Extensible Markup Language (XML)

可伸展的標置語言(Extensible Markup Language XML)是起源於 SGML (ISO 8879)的一個簡單，十分靈活的本文格式。原來是為了迎接大量電子出版而設計的，XML 也在網路上各種各樣日益增長的資料交換上的扮越來越吃重的角色。

XML 是構造彈性資料的一種標置語言；它將會用來取代 HTML。HTML 也是源於 SGML，但因為 HTML 固定的元件組和屬性缺乏彈性，所以 SGML 直接的應用到網際網路上就顯得複雜。一般而言。XML 被定義為 SGML 的一個功能的子集("profile")。XML 用 DTD 定義資料型態(經常被稱為“綱要”或者“文件類別”)，這起源於 SGML 以文件為重心的觀點。XML 在企業對企業(Business to Business, B2B) 環境中十分成功，並且在日益增長地資料交換(相對於”文件交換”)領域中佔有重要地位。因為資料的屬性與文件的屬性的描述方式不同，例如：內建資料型態和型態起源(type derivation)等。XML 綱要已經被定義成 DTD 的一種取代品，這使得 XML 在企業對企業的環境中非常適用。

XSL 是 eXtensible Stylesheet Language 的縮寫，它是一種為 XML 提供表達形式而設計的語言。由於 XML 的擴展性所以不包含顯示格式的標識。XSL 可以選擇和過濾 XML 中的數據，並將其轉換為 HTML 或者 PDF 等其他格式文件。

XSL 可以分為三部分:XSLT（XSL Transformations），XSL-FO（XSL Formatting Objects）以及 XPath(XML Path Language)。

XSL 是一種格式頁語言 (Style Sheet Language)，它可以用來定義 XML 文件的顯示的方式。使用 XSL 處理文件需經過兩個步驟：第一個步驟使用 XSLT1.0 傳遞 XML 文件，第二個步驟是使用 XSL FO 提供傳遞的結果。XSL 比 CSS 較強大得多，因為傳遞步驟(使用 XSLT 1.0)能執行 XML 文件的多變複雜的傳遞，而 CSS 不能夠對 XML 文件作任何結構的變化。

格式頁語言(Style Sheet Language)是描述為了文件的格式頁(style sheets)定義的基本規則。一個格式頁(style sheet)是用來控制文件的表達(presentation)。一個格式頁語言(Style Sheet Language)被認為是 “半資料(Meta Data)”因為它規定一種資訊來源的表達方式； 因此，它就資料的內涵來規範資料。

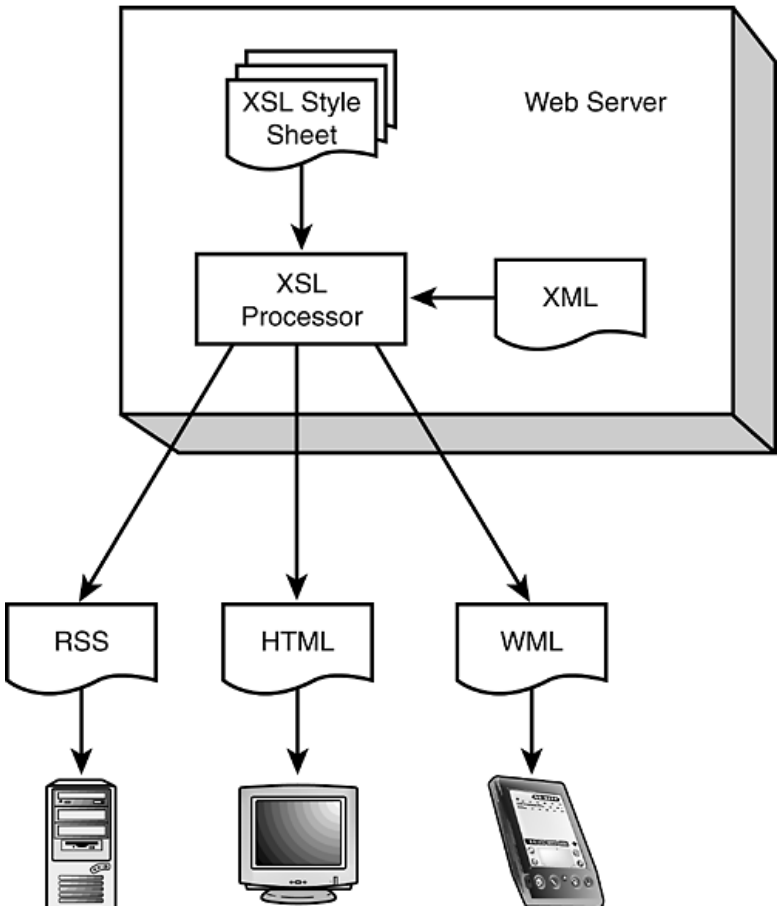
網路環境仍然是不成熟且易變的。當 Microsoft 和 Netscape 競爭正激烈時，即所謂的" 瀏覽器 戰爭" Web 環境每六個月就一次大變動。現在雖然比較穩定了，但是瀏覽器戰爭卻延伸到完全不同的戰場。這將會對來不及準備者造成很大的傷害。

根據 W3C 的資料，非桌面瀏覽器到 2008 年可以佔所有網路瀏覽器中的 80%。非桌面瀏覽器包括行動電話，PDA (例如 PalmPilot)，和 WebTV。

大多數這些裝置將不會只使用 HTML。在瀏覽器戰爭期間，設計者至少能依賴一些兩主要的瀏覽器之間的通用水準。情況將不再相同，闢如說行動電話使用是 Wireless Markup Language (WML)，這是 HTML 不相容的一種特殊的語言。

這問題該如何解決？應該限制文件供應者(content providers) (出版商，作者，和公司) 只使用 HTML 或 WAP 嗎？他們應該支援兩種格式嗎？他們應該準備更多格式嗎？

發展原始文件(文章，書，報告，如此等等)是昂貴的。為了降低成本，文件供應者想要儘可能廣泛地分發他們的內容。理想上，它不應該和讀者是否使用一台個人電腦，一台行動電話，或者一種其他裝置有關。



7.1 XML 的結構

網頁管理者通常使用一般的 HTML 編譯器編輯他們的網頁。這種方法的將會"凍結" 網站。事實上，要改變網頁必須手動重編每一個頁面。做得到但是這要花很多工夫。

XML 解決方法是把產生網頁的過程(authoring)與出版(publishing)分開。頁面的作者將文件寫在 XML 中。當這樣做時，作者可以先專注於網頁的內容，利用 XML 詞彙著重於文件安排的特質：如段落，標題，摘要等。當網頁完成後再考慮出版的細節。出版文件後可簡單地要求把文件改變成為 HTML，WML，或者其他流行的格式。幸運地，因為原來的 XML 文件包含了所有的結構，因此文件的轉換可以自動進行。對於中大型的網站，自動化的轉換比較經濟。更動數個頁面或可用手動；然而手動更動上百的頁面就太昂貴了。

右圖指出 XML 的原則：

Figure: XML separates authoring and publishing.

7.2 XML Stylesheet Language

XSL 是為了出版 XML 文件而設計的，XML 格式頁語言(Stylesheet Language)。更精確的說，我們將使用 XSLT，轉化格式頁語言(XSL Transformation)。不同於早期的格式頁語言，如 CSS(Cascading Style Sheet)，或者文字處理器格式頁語言，XSLT 是一種腳本語言可以將 XML 文件之間的轉換最佳化。

CSS 描述每一元素在螢幕應該如何被顯示：如字形，顏色，大小等。XSLT 把 XML 文件轉變成為其他 XML 文件。除了簡單的表達指令外，事實上，XSLT 能完全重新的安排文件；譬如說增加一個目錄或者刪除一個段落。為甚麼要這麼做呢？XSLT 將結構完整的 XML 文件轉換成為包含顯示指令的一種網頁格式，例如 HTML 或者 WML。瀏覽器 (或者一個其他設備 viewers)能將轉換後的文件顯示在螢幕或者在紙上。什麼顯示格式比較適合呢？下列一些比較一般的選擇:

HTML—嚴格地說，HTML 不是一種 XML 詞彙。這不是一 XML 對 XML 的傳遞。然而，HTML 是那樣流行的，和如此接近 XML，以至於 W3C 決定支援它。

XHTML—HTML 的 XML 版本。

WML—WAP 裝置的 markup 語言。

開啟的 eBook—eBooks 的格式，基於 HTML。

XSLFO—為了被列印的文件被最佳化的一種新的顯示語言。當撰寫時，兩個 XSLFO viewers 存在： 一瀏覽器(www.indelv.com)和一個 PDF 轉換板(xml.apache.org)。

8. Microsoft's Active Server Pages (ASP)

在過去當 web 開發者希望開發的網頁可以更生動地展現資料時，必須借用 CGI (Common Gateway Interface) 和 Perl 的功能。雖然這個方法可用 (事實上目前許多網站仍在使用)，但是 CGI 並不是一個很有效率的開發動態連續網頁的工具。有一段過度時期大家使用 ISAPI，但因為它需要比較複雜的程序撰寫動態過濾器(dynamic filter)網頁，超過一般程式開發者的能力所以現已不在使用。最後出現 web scripting 程式語言及 Microsoft's Active Server Pages: 一個伺服端 scripting technology 用來建立動態及互動網頁。

ASP (Active Server Pages)，是一套由微軟公司開發的伺服器端運行的腳本平臺，ASP 也是 Internet Information Services (IIS)中的一部分。

ASP 是經過伺服器執行原始碼之後再將資料送回瀏覽器，所以有了 ASP 就不必擔心客戶的瀏覽器是否能運行你所編寫的代碼。因為包括所有嵌在普通 HTML 中的腳本程序都在網頁伺服器端執行，當程序執行完畢後，伺服器僅將執行的結果返回給客戶瀏覽器，這樣也就減輕了客戶端瀏覽器的負擔，大大提高了互動的速度。但在伺服器端因為普通的 HTML 頁面只需要瀏覽器就能夠解析，而 ASP 則必須是伺服器將整頁的代碼都執行一遍之後再發送數據，所以執行 ASP 頁面的伺服器較普通的 HTML 頁面要慢一點。因為任何包含 ASP 的網頁必須透過要求支援 ASP 的一個網路伺服器開啟而無法直接在瀏覽器中開啟，這是 ASP 代表 Active Server Pages 的原因，沒有伺服器就沒有互動的網頁。

由於代碼是需要經過伺服器執行之後才向瀏覽器發送的，所以在客戶端看到的只能是經過解析之後的數據，而無法獲得原始碼，故編寫者不用擔心自己的原始碼會被別人剽竊。但不排除駭客利用系統漏洞竊取伺服器端的 ASP 原始碼。

ASP 內置許多由經驗豐富的程式設計師根據動態網頁最常用的功能而開發的組件。利用這些組件可以很有效率的開發動態網頁。當我們呼叫到一個或者一些 ASP 的內在的物件在 active server page 建立動態的元素，這些物件立即可以移入 ASP 開發者和完全涵蓋所有建立動態和交談方式的頁面的主要觀點。在 ASP3.0 中，共有 5 個這樣的組件：

- 應用(Application)
- 要求(Request)
- 回應(Response)
- 供應者(Server)
- 段落(Session)

每一物件有他們的集合(collections)，方法(methods)， 性質(properties) 以及事件(events)提供所有的功能。例如常見的 Cookies 就是利用 Session 組件設計的。同時還可以利用外加的組件來擴充 ASP 的功能，如利用 MailSender 組件發送電子郵件等。

- ASP 的句法和文法容易理解，功能足夠強大到可以：
- 支援頁使用者和伺服端之間互動(interaction)
- 允許網頁存取資料庫和目錄服務(directory services)
- 相互作用結合並且利用高效率的 COM 元件

ASP 使用伺服端腳本動態地生產不受網站存取者使用的瀏覽器的型態影響的網頁。用於寫 ASP 的預設腳本語言是 VBScript，但我們能使用其他腳本程式語言像是 JScript (微軟版本的 JavaScript)。通過 ASP 我們可以結合 HTML 網頁、ASP 指令和 ActiveX 元件建立動態、互動且高效率的網頁伺服器應用程序。ASP 提供與資料庫的互動，如 Microsoft SQL Server、Microsoft Access、MySQL 和 Oracle，比較流行的是 ASP 和 Microsoft SQL Server 的組合。ASP 程序（包括與資料庫連接的部分）都是嵌入在普通 HTML 和其他客戶端語言中的。ASP 已經是.NET 的成員之一，即 ASP.NET。當 ASP 首先被微軟發表到它的網路伺服器-- Internet Information Services (IIS)上的時候，搭配 Windows 2000/XP Pro/NT 執行效率最好。

因為 ASP 是以伺服端為基礎且與無關瀏覽器無關，實用上只有跨瀏覽器顧客端腳本和格式頁(stylesheet)。我們可使用 HTML 和本文建立一個靜態的頁面，或是用標準的

HTML 表格詢問用戶端；同時，使用 ASP 建立一頁面把他們的回答結合到本文中。這是使用 ASP 在顧客伺服(client-server)環境下互動最簡單的形式。

9. 網際網路資料收集的缺點

網際網路資料收集依然有其缺點，有些用來傳遞和驗證資料的收集方法，例如 XML 或 JavaScript 通常都太冗長而增加用戶端和伺服端之間的資料流量。有時網頁靜態 static (或事前定義好的 pre-defined)表格很長需要使用者經常上下捲動畫面，而打斷使用者的思緒 。靜態網頁表格很難修改或變動因為通常需要程式開發者(或網頁設計者)與原始表格設計人員的配合，尤其當彙總表(summary report)包含多個問題單(questionnaires)時， 追蹤網頁表格變動是一件很困難的事情。而且設計一個以網頁為主的表格需要許多技術與設備的配合。此外雖然表格本身並不會受到病毒的侵害，但是遠端的電腦有可能因病毒而減慢或無法與伺服器連線來存取表格。最後這種資料收集方式還需要遠端電腦能有夠穩定的連線到網際網路甚至需要高速或寬頻網路處理較大量資料或較複雜的表格，但網際網路無法避免斷線。而且高速或寬頻網路並非垂手可得。

雖然最近幾年已有大量的工具和方法革新和改進，但是處理收集精確的資料仍然很困難。 學術研究盡力發展新方法來幫不同網站更精確地收集資料，尤其是幫同一個預算下分散各地的單位或是那些網際網路連線不穩定的遠端(offsites)單位。通常這需要多步驟(multi-step) 處理 ，包括產生紙上表格、填寫回答、交換到可連線的地方輸入電子表格到資料庫，最後根據資料性質產生不同的標籤(variable labels)和本文(text) 給不同單位作進一步的資料分析。這個新方法需要很多步驟，每一個步驟都可能產生錯誤而造成不正確的結果。市面上有很多新的商業套裝軟體可以處理這些問題，但需要考慮其成本及使用的難易度。

(三)網路安全

相對於傳統方式而言，網路服務具有許多優點譬如較易取得資料，動態的系統間連線，並且高度的自動化(無須操作員) 等所以非常具有吸引力。但是網路安全卻是一件非常重要的課題。一切令網路具有吸引力因素都違反傳統的電腦安全模式和控制。較具挑戰的議題和尚未解決的問題如下：

- 透過網路服務通訊協定在伺服器間傳輸資料的機密和完整性
- 提供完整的網路服務除了要事先整合相互網點間的互信外，並且要建立單筆交易間的互信。
- 面對阻絕服務 (DOS) 攻擊時暴露出網路服務特有的弱點，尤其攻擊時針對核心服務，諸如受其它服務依賴的發現服務的攻擊。以週邊為基礎的網路安全技術（ 例如：防火牆，入侵偵測） 因為下列的原因無法充分保護服務式網路架構 (SOA, Service Oriented Architecture):
    - 服務式網路架構是動態的，並且很少只在單一的網路上運作
    - 簡單物件存取協定 (Simple Object Access Protocol, SOAP) 在 HTTP 上傳輸，而 HTTP 允許資料無限制地穿過大多數防火牆。此外，(Transport Layer Security, TLS)，這被用來鑑別及對網路資料加密的工具，因為它只在送與收的兩端點（endpoints）上作業，對保護 SOAP 之類可能經由多個網點的傳輸方式並不合適。
    - TLS 不能保護像網路服務般同步多網點傳輸的網路標準。當 SOAP 訊息和 XML 檔案在沿著長和複雜的消費者，供應者，和中間伺服的連鎖鏈傳遞時，SOA 處理模型需要有能力確保 SOAP 訊息和 XML 檔案的安全。網路服務處理的性質使得那些服務容易受特有的攻擊，以及熟悉的以網路伺服器為主的攻擊的變體。

確保網路服務的安全牽涉到實施使用鑑別（authentication），授權（authorization），機密（confidentiality），和完整性機制（integrity mechanisms）的新的安全框架。在

本次研習及參訪過程中有機會了解到美國聯邦政府由其標準局（National Institute of Standards and Technology，NIST）下轄的資訊實驗室（Information Technology Laboratory，ITL）主導對網路安全『建議』了一系列的規範。其中最主要的一個規範是編號 800-95，Guide to Secure Web Services。其內容相當繁複，僅將其目錄列於附錄三以供參考。

下列是網路服務的安全技術的摘要：

- 保持加密 XML 網路服務的機密：這是一種 W3C 提出的規格將 XML 檔案譯成密碼。
- 使用 XML 簽名的網路服務的完整性：這是被 W3C 和 IETF 共同生產的一種規格。XML 簽名的功用是有選擇地簽署 XML 資料。
- 網路服務 使用 OASIS 標準組所建議的 SAML 和 XACML 的認證和授權。
- 使用 XKMS 的網路服務的 PKI。
- 網路服務的安全規格：這規格為了端對端（end-to-end）SOAP 訊息安全定義一套 SOAP 標題延伸（header extensions）。它允許通訊夥伴們透過在網路服務環境中交換簽署的加密資訊以支援資訊完整性和機密。
- UDDI 的安全通訊協定：UDDI（Universal Description, Discovery and Integration）通訊協定使網路服務容易地被定位並且後續接觸。UDDI 的安全協定不但認證資訊提供者，查詢者和使用者的身分，並要求他們登錄自己的資料。

1. 安全威脅

對公司的網際網路與網路安全的最巨大威脅是什麼？根據"針對超過 600 個美國企業 2004-2008 世界性的資訊技術安全軟體，硬體，和服務的種調查預測"（Worldwide It Security Software, Hardware, And Services 2004-2008 Forecast），31%從特洛伊 Trojans，病毒和惡意的程式碼（malicious codes）；13% 從僱員無意的錯誤，10%來自網際網路惡性程式碼 worms； 其後是 7% 間諜軟體；6%駭客；5%破壞；5%因為諸如 Windows 安全洞的應用弱點； 4%從垃圾信和 2.5%從網路恐怖破壞（cyberterrorism）。

安全破壞的一些例子如下:

BAD BUG BYTES 2000 —Western Union—駭客攻擊

駭客侵入網站並複製 15,700 張客戶信用卡與金融卡號碼。客戶被告訴得到新的信用卡和帳號。

BAD BUG BYTES 2003—Siebel—駭客攻擊

駭客侵入網站並且得到客戶滿意調查。他們洩漏所有消極的評論給分析人員並且施壓。

BAD BUG BYTES 2003-SiebelData Processing Internal—processing AE, MS, Visa, Discover Cards—駭客攻擊

- 影響萬事達（Mastercard） 兩百二十萬張信用卡號碼
- 影響威士卡（Visa）三百四十萬張信用卡號碼
- 美國運通（American Express） 及發現 （Discover） 卡也受波及

內部攻擊 HIT BY INSIDER June 2004 –AOL

全美連線（American Online）一個離職的僱員被控偷竊網際網路供應者的整個的使用者清單（--超過 3 千萬個消費者，和他們 9 千萬個螢幕名稱）並把它賣給垃圾信件寄發者。

Lost in Transit: Bank of America

美國 BOA 銀行當把備份磁帶裝運到其他地點儲存時，遺失存放包括 60 位美國參議員及 1 百 20 萬個聯邦僱員信用卡帳戶記錄的磁帶。

反觀國內，由於垃圾信及惡意郵件氾濫，行政院科技顧問組提報「95 年度政府機關資安攻防演練報告」中提出「電子郵件社交工程 Social Engineering 攻擊演練」的結果，部份部會資安意識表現較差，需加強訓練。本處電子中心資料組為此建置郵件過濾器

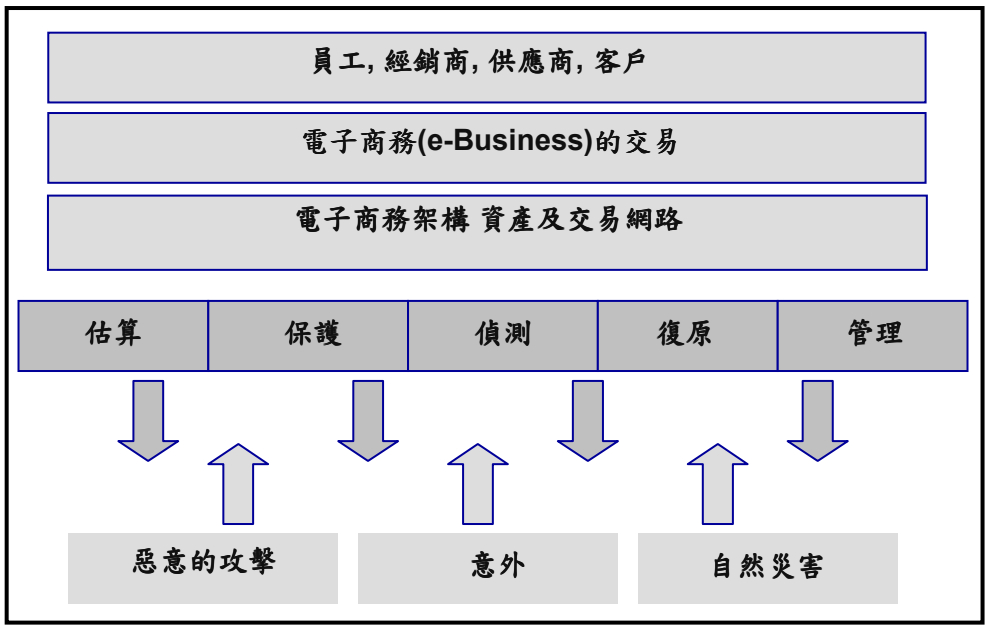
加強攔截惡意郵件，並要求提高同仁資安意識，遵照電子郵件使用規定，將郵件軟體設定為純文字模式閱讀，並對來路不明及主旨內容與業務無關郵件，立即刪除。

另外此次資安攻防演練其他攻擊方面，例如，第三局之勞動力調查結果網頁，受到資料隱碼(SQL injection)攻擊，部分網頁內容被置換，這也是軟體程式漏洞的實例。

2. 安全考量：

下圖簡略的指出所在一般電子資料交換中所有數據的轉換處理過程：

上圖描述電子商務包含的多層介面及他們之間的關係。第一層是人員介面，列出與電子商務相關人員。第二層是電子商務本身。第三層是電子架構層，包括硬體、軟體、網路及儲存的資料。第四層是保護層，包括軟硬體安全設施和災難回復。最後一層是



可能影響電子商務的一切因素。

3. 安全部署:

安全是關於管理風險的，而不是除去它—因為除去風險是幾乎不可能的。把風險減少到一個可接受的水準才是可能的。安全是一個程序，不僅是一種產品。軟體無法解決有關人的問題。

網際網路安全事件報告年鑑（Annual Internet Security incident report）：在 2000 年從少於 300 件穩定地增加到在 2003 年的 13,000 件到 2006 年超過 30,000 到。文件證明

Win32 病毒也已增加從在 2001 年上半年少於 300 件到 2004 年上半年超過 4000 件。從 2002 年以來軟體和網路漏洞的數字每年大約固定 2,500 個事件

攻擊或者誤用的型態如下（CSI/FBI 2003 電腦犯罪和安全調查 Computer Crime And Security Survey）:

- 病毒 Virus, 82%;
- 對網路接近的內部人員濫用, 80%
- 筆記型電腦 Laptop, 59%;
- 內部人員未經許可的使用: 45%;
- 伺服的拒絕: 42%;
- 系統突破 System Penetration, 36%;
- 破壞 Sabotage: 21%;
- 專利資訊的偷竊行為: 21%;
- 金融的詐騙 Financial fraud: 15%;
- 電信詐騙 Telecom fraud: 10%;
- 電信竊聽 Telecom eavesdropping, 6%
- 竊聽器 Active wiretap: 1%.

病毒的可能來源（美國“電腦安全協會的電腦病毒流行調查” “Computer Security Association’s Computer Virus Prevalence Survey”）:

- 電子郵件的附件： 56%;
- 從外部來的磁片： 38%;
- 從外部來源的下載： 11%
- 網路瀏覽: 3%
- 被傳染內部: 2%.

因此從 CIO 觀點， 一般公司曾經歷安全的最嚴重的影響是什麼？

- 不方便並且失去生產率： 73%;
- 公開尷尬： 17%;
- 客戶與賣主無法恢復資訊： 8%;
- 損失切實的價值，諸如資料，收益： 2%

發生過最嚴重的安全事件（FORTUNE, October 18, 2004.）

Name, Year	Worldwide Impact
1. Love Bug, 2000	$8.75 billion
Hopelessly lonely recipients think they are getting a real love letter in their e-mail.	
2. MyDoom, 2004	$4.75 billion
At its peak, infects one in 12 e-mails on the 網際網路	
3. Sasser, 2004	$3.5 billion
German cybercops nab its teenage author, Sven Jaschan. An IT Security firm then offers him a job.	
4. NetSky, 2004	$2.75 billion
One of its variants disguises itself as a Harry Potter computer game.	
5. SoBig, 2003	$2.75 billion
Hits a week after Blaster （No. 8, below）, helping cause a summer of pain for computer users and Microsoft.	
6. Code Red, 2001	$2 billion
Give the phrase "denial of service" new meaning.	
7. Slammer, 2003	$1.5 billion
Targets small 商業 es running Microsoft programs most didn't even know they had	
8. Blaster, 2003	$1.5 billion
Shuts down Maryland DMV for a day. Famous for twitting Billing Gates: "Stop making money and fix your software."	
9. Klez, 2002	$1.5 billion
Randomly spews files of its victims everywhere as e-mail attachments.	
10. Nimda, 2001	$1.5 billion
Striking the week after 9/11, this combination virus and worm triggers three FBI investigations.	

我們如何武裝來對付日益增多的資訊風險（information risk）？較理想的資訊安全層次（Information Security Hierarchy）如下：

層次 1: 資訊安全政策和標準（Policy & 標準）
層次 2: 資訊安全架構和程序（Architecture & Processes）
層次 3: 資訊安全警覺和訓練（Awareness and Training）
層次 4: 資訊安全技術和產品（Technologies & Products）
層次 5: 審查（Auditing）, 監控（Monitoring），調查（Investigating）
層次 6: 驗證（Validation）

4. 來自網路世界（Cyber space）的安全威脅

通常我們想到『來自網路世界的安全威脅』時，我們通常會想到：

- 駭客
- 恐怖分子
- 外國政府

- 組織性犯罪
- 自然因素

但是我們常常忘了：

- 競爭者
- 不道德的內部員工
- 人為錯誤

到底是誰在侵入我們的系統？根據統計數字顯示 82%從不滿的現職和離職的僱員或承包單位； 6%從有組織的罪行（敲詐，洗錢，內線交易）； 5%從網路犯罪（Cybercriminals，欺騙和資訊轉賣），小於 2%從純粹好玩的人。

根據 Forrester 研究（Forrester Research, Cambridge, Massachusetts, forrester.com），幾年以前大多數公司花費 IT 大部份的資源在把防火牆升級或者新增到他們的網路。最近幾年愈來愈多公司已經把他們的安全資源變換成為譯成密碼，數位憑證和遠端存取解決方案（Encryption, Digital Certificates and Remote Access solutions）。雖然防火牆是避免系統被侵入的最重要的技術但是其它新出現的技術更可補助對防火牆。

5. 網路服務安全的挑戰

雖然許多現有的標準已足夠用來規範網路伺服，但是有些部分—尤其是網路伺服發現和可靠性的部分—有些標準制定組織正在訂立新的規範。Web Services Interoperability（WS-I）組織認為下列領域尚須深入探討：

- 拒絕處理 (Repudiation of transactions);
- 個別資料的安全確認(Secure issuance of credential)s;
- 隱藏的通道的使用(Exploitation of covert channels);
- 被破壞的服務(Compromised services);
- 透過 SOAP 資訊傳播病毒和特洛伊木馬程式;
- 阻絕服務的攻擊;
- 不正確的服務執行計畫;
- 不良的服務設計.

6. 查詢服務(Discovery)

在網路服務查詢時，提供服務者根據 UDDI 規則先用網路伺服描述語言（Web Services Description Language, WSDL ）描述服務內容。因為在登錄裡的網路服務的種類很多，找到使用者所需的服務的時間因個案不同。當網路服務的項目越來越增加，

就需要更高階的工具來幫忙辨識使用者的需求及其對安全的考量 。不論網路服務的供給者或使用者都必需非常明確的描述他們需要的服務範圍。UDDI 經由 tModel 資料結構提供一些類似的基本服務。但是利用 Semantic Web 的技術可以更進一步提高網路服務查詢的品質。舉例來說，Ontology Web Language for Services（OWL-S） 就具有這個能力，但是需要更多的努力才能把網路技術與網路查詢登錄結合在一起。在 OWL-S 裡，服務申請者可用 semantic model 的名詞描述服務需求。用特殊的技術可以自動地配合服務的項目以及查詢者的申請。UDDI 和 OWL-S 可以用來說明網路服務和它的安全屬性，但這並不屬於查詢服務的一部分。真正的網路自動化還必須查詢者網路服務定義安全需求 。

7. 點對點的服務品質和保護品質

大部分的網路服務部署並沒有提供服務品質（Quality of Service, QoS）或保護品質（Quality of Protection, oP）的保證。QoS 在定義一個特定的網路伺服的性能所能期待的水準時很重要。透過網路流量管制可改進系統的全面的性能。網路服務訊息可靠性（WSReliability，WS-ReliableMessaging）標準提供某些程度的 QoS。這兩個標準都提供保證訊息的發送。但這些標準在考慮其他 QoS 因素時（例如錯誤率和平均延遲）常因為只處理低階通訊協定而超過它的能力之外。網路服務真的要支援 QoS, 現有的 QoS 支援一定要能同時傳送網路服務訊息及其相對的封包。不像 QoS, 網路服務雖有 QoP 標準但是並沒有標準機制定義 QoP 的提供者。目前網路服務查詢完全只針對他的功能而不考慮其他方面類似 QoP 的服務 。對某些複合服務來講，單一服務的 QoS，點對點的 QoS 和 QoP 非常重要。有很多合作夥伴的大企業必須很有效地安排他們的資源，才能再很短的時間處理商業。由於網路服務是動態及複雜的關係，QoS 是網路服務最主要的挑戰。

8. OASIS 和 W3C 之間的標準重覆

由多個標準制定組織發展類似的和重覆的網路服務安全標準造成系統開發者的混淆。甚至，這些標準持續不斷地更新導致互通性的問題。所以我們需要更多正式的規格和標準的測試。

9. 網路服務安全的方法

當今主要強調網路伺服安全在基本的基礎設施（例如：通訊協定和語言）上。當技術成熟時，並且網路服務變得廣泛地被採用，將需要安全方法幫助開發者辨識哪些智慧資產需被保護，分析可能的攻擊並且決定保護水準和折衷方案。

10. 生命週期管理

網路服務在變動的環境中作業，而商業合作者可能改變他們的政策或者通訊協定。管理在 SOA 方面的變更是既困難且昂貴的因為服務可能橫跨多個應用系統。

11. 可用性(Availability)和保護以免受到阻斷服務（Denial of Service）攻擊

可用性能夠讓某個網路服務程式（a Web Services Application） 偵測到阻斷服務（ DOS ）的攻擊，可以勉強作業；然後在 DOS 進攻之後能從容的恢復正常作業。同時需要複製資料和伺服的技術已備當錯誤發生後以確保不中斷的服務。系統為達到一定的服務水準，必需有管理和監控方面的軟體來了解服務效率及可用性。

12. 安全系統的架構和設計

安全的再造工程

在設計一個軟體時除了功能之外，還要考慮它的效率和穩定度。當軟體完成後不論任何原因修改都是一個很複雜的工作。可惜網路軟體在發展過程中總是必須不斷地加強安全設計。所以軟體必須不斷的配合安全的改善而升級。再加上有些新一代的安全系統並不與現有的軟體相容，這對軟體設計是一個很大的挑戰。在統一安全標準下整合不同系統更是一件幾乎不可能的任務；例如 Unix 系統使用使用較嚴謹的密碼及存取控制；CORBA 用較有彈性的 Kerberos-based 認證，所以整合這兩個系統非常不容易。此外由於各式網路服務越來越普及，常有使用者要求單一登入到不同的網路服務。由於不同網路服務的認證、授權及安全標準不同使得單一登入也暫時屬於不可能的任務之一。

系統的驗證

挑戰：以應用為主 Implementation-based 驗證方法

一個以應用為主的系統須有自動工具來正確地找到安全漏洞。有一個方法用模式檢驗的方式去從程式碼裡找出潛在的安全漏洞。

另外一個方法是利用 Verisoft 的方法去建立常用 APIs 的惡意程式碼 ，經由呼叫這些 APIs 去模擬 攻擊程式找出潛在的漏洞。一個應用程式可以重新連結去抵抗這些惡意程式碼。

安全的計算，而非安全的電腦（Secure Computations, Not Secure Computers）

所有軟體系統都容易有潛在地錯誤，因而產生不正確的結果。如果以安全的考量，使用者可能會擔心系統是否會受到攻擊而執行不正常。通常需要花很多的精力去找出計算的結果是否正確。

早先在這領域的研究包括執行檢查經由未授信的線路向安全電路傳輸編碼的操作過程。其他的方法是用 quorum schemes 去在伺服器之間用編碼 threshold cryptography 去傳播信任。但是使用 quorum schemes 影響執行效率。

在低階的改進法是用安全的資料結構。在這方面，一個處理器將儲存的資料傳送至未受權的輔助處理器，需要確認從輔助處理器傳回的資料是否正確；例如類似記憶體間資料的傳輸、安全堆疊及佇列 (stacks and queues) 和其他被連結的資料結構。一個高階的做法是用類似 "系統伺服器"提供有用的服務來產生附加證明的正確回應。

網路安全建議：

1. 複製數據和伺服以改進可利用性：既然網路服務容易受到阻絕服務 Denial of Service（DOS） 攻擊，複製資料和應用系統是一種必要的方法。複製和冗餘能在一個嚴重錯誤情況下保證還能存取關鍵的資料。它也能讓系統協同作出反應處理。

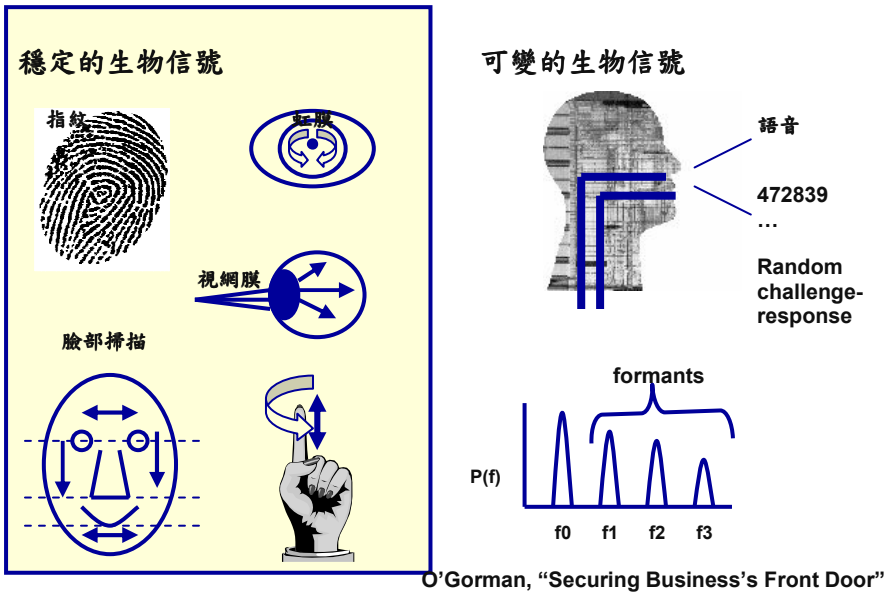
2. 使用交易記錄以更盡責：整個 SOA 交易需要登入機制來加強責任制。已有少數的登入標準被應用，例如幾種 UDDI 登錄用來跨越整個 SOA。

3. 使用安全的軟體設計的方式來防止弱點：在處理階層用最少的授權原則可以減少弱點。安全的軟體設計的目標是確定網路服務軟體在設計與實施階段不含會被破壞的缺點。用軟體檢查技術來作威脅模式和風險分析。軟體 安全測試應該包括安全為主程式碼檢查及滲透測試。

4. 應用效率分析(Performance Analysis)和模擬技術(Simulation Techniques)在點對點的 Quality of Service 和 Quality of Protection：Queuing 網路和模擬技術長期以來被應用在設計、開發與管理複雜的資訊系統時扮演重要角色。模擬技術用來確保品質與網路服務。相對於單一服務 QoS 而言，點對點 QoS 對大部分複合的服務更重要。

5. UDDI 內用電子簽名(Digitally sign) 來驗證每一單項的作者. UDDI 登錄公開的提供網路服務的目的還有如何存取的細節。就像 WSDL 的描述一般，每一 UDDI 單項提供太多網路服務的資訊，同樣的這些資訊也提供給網路攻擊者。除此之外，網路服務使用 UDDI 登錄在執行時查詢並動態連結網路服務，因此使用電子簽名去驗證 UDDI 內每一單項的來源常重要。

6. 實體的存取控制(Physical Access control)



O'Gorman, "Securing Business's Front Door"

現有的驗證技術和分類: 生物科技(Biometrics)

利用生物科技（Biometric）的安全管理分析：

身體部位	型態	如何運作	優點	缺點
臉	臉部辨識	臉部辨識從影帶或者靜態影像捕捉臉部的特徵並且把他們轉成數位型式	適合於辨識應用； 比較謹慎	容易傾向于由環境的影響（如光，太陽鏡，的面部的頭髮等等） 造成的誤差; 昂貴
眼睛	視網膜掃描	捕捉血管的獨一的圖樣。這方法極端安全和精確。	安全而精確	昂貴； 要求完美的調整： 使用者通常必須看向單眼或者雙眼的儀器
	虹膜掃描	捕捉虹膜的獨一的圖樣	安全；不需要實體的接觸和非侵入性	昂貴；對環境的條件敏感
語音	語音辨識	捕捉語音的獨一的特點	容易使用和理解, 不貴	對諸如噪音的背景條件敏感
手	手 幾何學	捕捉多達 90 個獨一的手特徵	容易使用, 不貴	儀器較笨重 對環境敏感
	指紋	辨識是迴圈，弧形，和渦紋的獨一的圖樣。	容易使用，不貴；指紋資料庫已很完整	不如視網膜或虹膜掃描可靠

13. 結論

以網路服務為基礎的計算目前是軟體工業一種很重要的原動力。以服務為主的計算主要目標是經由標準化通訊協定收集軟體服務，這些通訊協定的功能應該可以自動地查詢並整合到應用系統。當許多個標準制定單位（例如：W3C 和 OASIS）正在鋪設網路服務的基礎，, 許多研究的問題要先解決來確定網路服務的可行。一些自動和復合網路服務的服務性質（Service description），自動化服務查詢（ automatic service discovery）還有服務品質 QoS、可靠度和（reliability）保護（protection ）方面的考量是重要且須解決的課題。

即使有許多安全的挑戰， 網路服務已逐漸變成一般企業資訊系統的一部分；因此開發及部署安全網路服務對大多數機構的資訊系統基礎建設是不可或缺的。然而網路服務安全標準並沒有提供所有必須的屬性來開發耐用、安全及可靠的網路服務。為了充分

地支援以網路服務為基礎的應用系統的需求，必須要有效風險管理及部署適當的替代方案是。安全工程所提供的深層保護，安全軟體發展及風險管理可提供這些應用系統所需的耐用性及可靠性。

14. 遠端存取資料的安全參考文件

NCSA News, The Journal of the National Computer Security Association, NCSA （10 South Courthouse Ave., Carlisle PA 17013）.（717） 258-1816

INFO Security News, MIS Training Institute Press 498 Concord St., Framingham MA 01701-2357.（508） 879-9792

CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, Pittsburgh PA 15213-3890. E-mail: cert@cert.org.（412） 268-7090 24-hour hotline

National Infrastructure Protection Center, www.nipc.gov

The Firewalls mailing list Send e-mail to majordomo@greatcircle.com with the following as the first and only line of text in the body: subscribe firewalls （your address）

Various online World-Wide Web resources include: catless.ncl.ac.uk/risks

http://www.tansu.com.au/info/Security/html

http://www.tis.com

http://www.alw.nih.gov/WWW/Security.html

The COM-SEC BBS,（415） 495-4642 modem,（415） 495-1811 ext. 10 voice

Computer Security Institute, 600 Harrison St., San Francisco CA 94107（415） 905-2626 voice

15. IT 安全資源

15.1 Cert Coordination Center: www.cert.org

軟體工程學會（Software Engineering Institute）的網際網路安全專門技術中心，一個由卡耐基梅隆大學運作聯邦投資的研究與發展中心。關於保護你的系統的資訊和訓練，對目前草寫的問題作出反應和預言未來的問題。

15.2 SANS Institute: www.sans.org

關於 IT 安全發佈的研究，教育和訓練

15.3 Center for Internet Security: www.ciSecurity.org

方法和工具改進，測量，監控並且比較網際網路連線的系統和應用的安全狀態.

15.4 Internet Security Alliance: www.isalliance.org

分享關於安全發佈的資訊的一個論壇

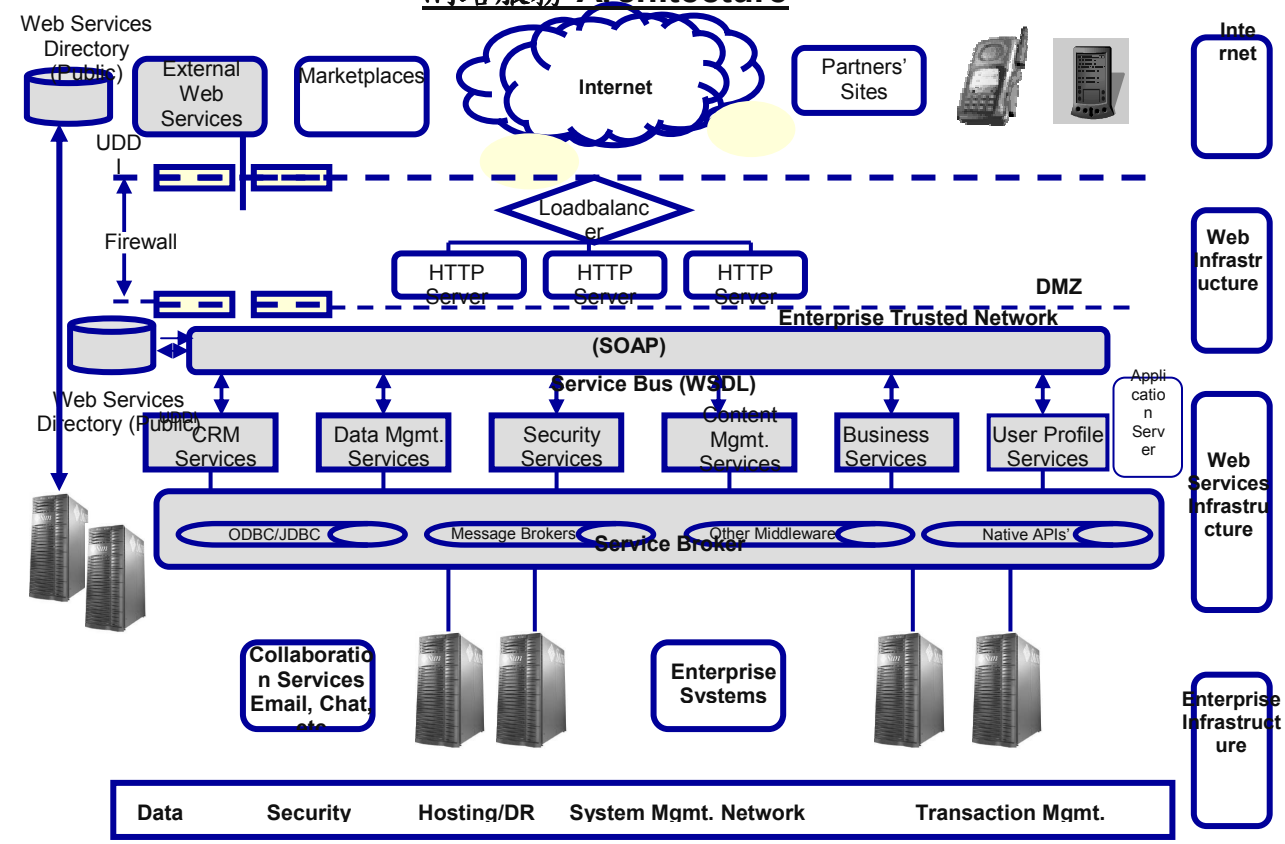
15.5 Information Security Forum: www.Securityforum.org

一個國際性會員資格組織共享關於安全發佈的資訊。.

15.6 提供加強網路的安全模組與套件的主要的供應商：

供應商	解決方案	作業平台
IBM Tivoli Ibm.com	Access Manager, Directory Integrator, Directory Server, Identity Manager, Privacy Manager for e-Business, Risk Manager, Security Compliance Manager	AIX, HP-UX, Linux, Solaris, Windows
Microsoft Microsoft.com	Identity Integration Server 2003	Windows
Netegrity netegrity.com	eProvision, IdentityMinder, SiteMinder, TransactionMinder	HP-UX, Linux, Solaris, Windows
Novell novell.com	iChain, Nsure	AIX, Linux, NetWare, Solaris, Windows
Oblix Oblix.com	CorelD, ShareID, CoreSV	AIX, HP-UX, Linux, Solaris, Windows
openNetwork opennetwork.com	Universal IdP	AIX, Solaris, Windows
RSA Security RsaSecurity.com	I&AM （Identity and Access Management）	AIX, Solaris, Windows

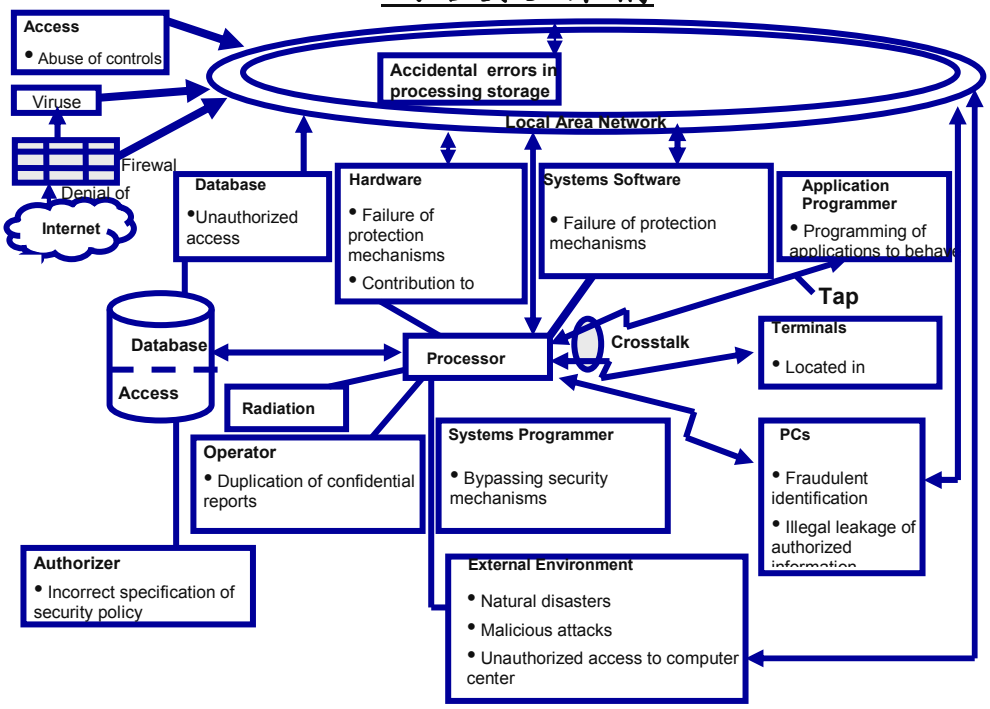
網路服務 Architecture



Based on Web services standards
Ref: RCG Information Technology; 'White Paper on Web Services Architecture' By Rasesh Trivedi, Senior Manager - RCG IT

www.rcgit.com/company/whitepapers/WebServicesArchitectureModelsWPv1.pdf

網路安全架構



(四)實例參考

實例 1: 比利時健康部（Belgium Ministry of Health）：入口網站加速資料的收集

範圍

比利時健康部低效率的醫療資料收集系統導致錯誤和延遲，而限制了該政府健康政策規畫的品質。

計畫概要

應比利時健康部的要求，使用一個特別設計的應用系統 Portahealth，來改善處理程序以提升健康照護的品質。比利時的健康食品安全與環境公共服務部門（ Federal Public Service for Health, Food Chain Safety and Environment (FPS) ）負責根據由比利時境內大約 200 家醫院收集的資料來規劃健康計畫、設備、政策及預算。自從 1990 年代醫院即開始系統化地收集及記錄這些資訊，並用不同的方式如郵件、傳真和光碟片等每六個月轉移到 FPS。FPS 必須將資料輸入後先檢誤後再將這些資料送回醫院校正及傳回檔案。

FPS 要求實施一個新的與醫院之間的標準資料交換格式但要保持原有的資料庫, 分析和檢核工具。唯一改變的是資料交換通道。經過小規模適用後，Portahealth 軟體在 20 家醫院試用 8 個月後再推廣到全國所有醫院。FPS 協同一家私人公司專案管理小組動員 30 個人，如期完成這包含軟體、硬體及人員費用總預算達一百萬歐元的計畫。

Portahealth 軟體集合 3 種主要功能—資訊傳遞、後續處理和使用者管理—來確保資料收集處理程序的每一步驟正確。醫院的資訊系統由自己管理因此 FPS 就不需要去協助醫院的資訊部門。對醫院來講整個處理程序變的比較簡明。醫院用自己的管理者權限授權管理輸入(input)、讀取(read)和傳輸(transfer) 資訊等操作權限。在 FPS 的監管下每一個使用者都有身分證明，以確認使用者的身分和資料的來源。最後 FPS 的資料分析結果可以直接經由這個入口作後續處理。

新流程收益:

資料交換由原先 3 星期變成只須 3 小時。健康部和醫院的使用者不必重複地不斷的來來回回檢核並重登資料，這些使用者現在可以把時間，精力用於資訊分析等更有用的工作。

除了為政府追蹤醫院的資料，Portahealth 的功能可展開至含蓋發遍及比利時的健康照護領域。醫院將可以輸出資料到他們自己的資訊系統並且有工具分析使用資料和檢核 FPS 進行的工作。 Portahealth 架構也將複製到其他公共健康領域，包括藥品認證、精神病治療、護理和急診服務等。

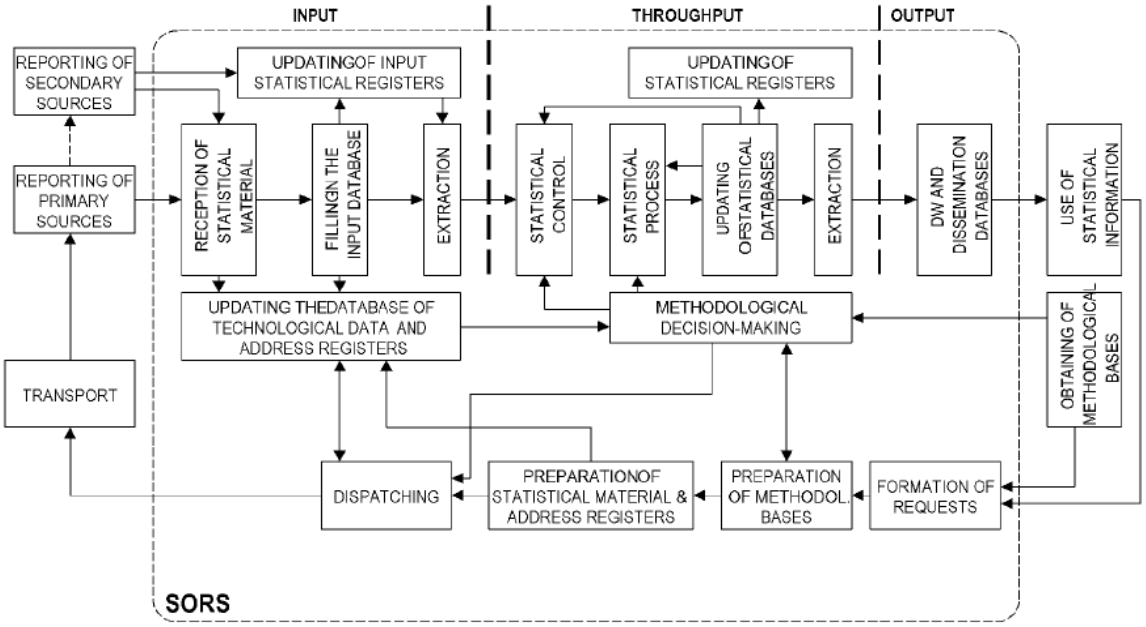
實例 2—斯洛文尼亞共和國(Republic of Slovenia)統計局與數據報告電子化相關的管理，組織和政策問題

範圍

建立以網路為中心搜集關於統計數據。第一個計畫(EDI-FIN)與電子數據收集方面有關，利用從 Eurostat TELER 的計畫下累積的經驗和工具直接地從企業財政紀錄內擷取數據。 QUESTOR 是第二個計畫與統計局輸入部門維護數據管理有關。 第三個計畫有關於與教育、科學和體育部和統計局在中等教育方面綜合的方式。

計畫概要

自 1971 年統計局開始自大企業從磁碟、紙帶和卡片搜集數據以來， 1997 斯洛文尼亞加入 TELER 計畫與其他歐洲國家參加測試和評估一個由荷蘭統計局開發的稱 EDISENT 的軟體和資料蒐集過程。並在「夥伴企業化」的計畫中測試電子數據收集和所需的軟體。整個計畫資料結構和電子傳輸使用了 EDIFACT (RDRMES)標準。各企業間對電子數據收集的熱烈反應和自願的積極合作是進一步推動企業界和統計局間電子數據交換計畫的原動力。電子資料交換將成為政府機關和一般企業之間較理想的通信方式。我們將力爭電子彙集成為其中一個搜集數據最重要的方法。它不但節省時間和金錢，且通過電子查詢表收集的數據較可靠，因為當回答紙上表格和將紙上數據輸入電腦時難免有錯誤。無紙的過程、整體化、標準化、品質和安全是統計局推動電子數據收集的主要理由。



上圖是統計局的整個資料流程。統計局內部的基本功能分成三個步驟。輸入的重點集中於統計局以外的世界。數據收集後同時彙報，連接和存放。 數據保密和歸檔也是關鍵和焦點之一。統計局的資料處理的核心從資料輸入，數據以可變方式(metadata)輸出，分類和處理下一個步驟的數據，及總資料處理量等。數據通過統計編輯，計算和其他統計步驟(算法處理、SAS 工具等等。) 計算結果先一般化(de-individualized)後被轉移到資料輸出。各種資料傳播包括紙，網路應用程序等均是客戶指定的並且安全無虞的方法。

上述過程由統計局內部區域網路、計算機系統和通信系統所支援。統計局內部區域網路是政府網絡(HKOM)的一部分。它是一個非常安全的網絡，由資訊中心(政府機構之一)管理。HKOM 租用或使用專線、路由器和防火牆聯線到網際網路。HKOM 用戶看不到統計局的伺服器。在統計局內部區域網路內的數據、系統和應用程式是安全的。網際網路伺服器位於政府網路的共同，保護區域。第二個防火牆保護 HKOM 內的統計局的伺服器。這種設計可保護數據本身或誤用數據。

結論

EDR 不能解決從統計過程中有關內容和組織的問題！在辦公室內必需保留適當的專門技術人員。需要國際合作來制定電子數據彙集的國際標準。國際標準組織 (NSIs) 可分享開發費用以減少本身的負擔。已開發成本與相對收益而言數據蒐集網路化是不可逆的趨勢。數據格式的標準化則是整個計畫成功的關鍵。

實例 3— 2005 年人口普查—以網路為主的調查及登錄

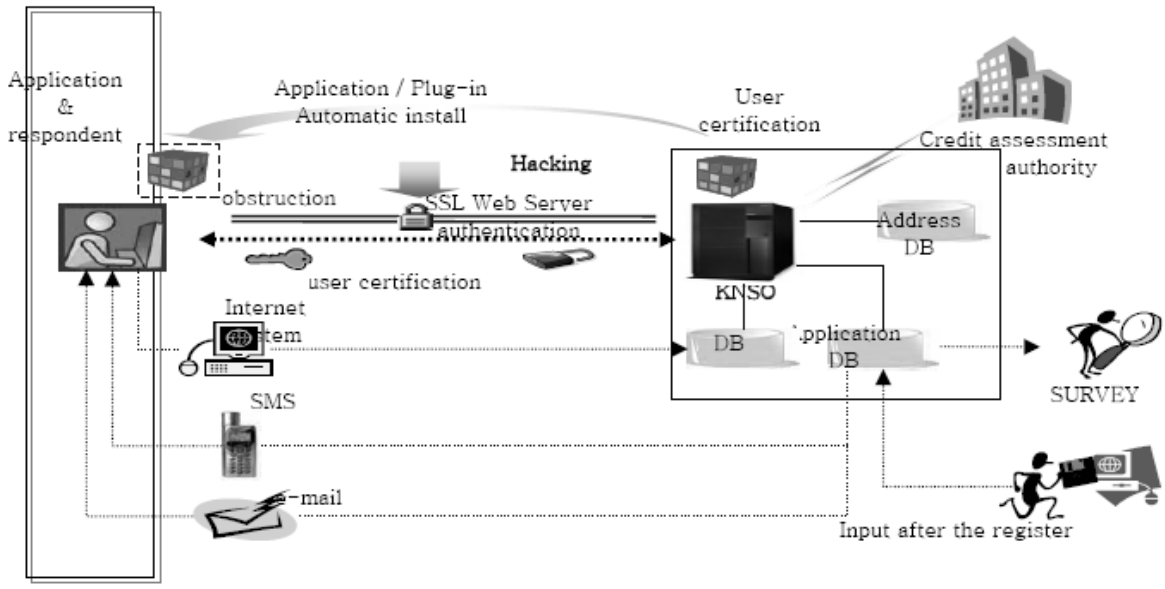
範圍

建立網路人口普查的系統以便民眾經登錄及認證後可自行輸入必要 的資料。

計畫概要

傳統上韓國的人口普查資料是由紙上問卷及人口普查員蒐集的。這個方式效果還不錯但是越來越多的家庭希望由他們自己來完成問卷；也有少數人表明希望經由網路來輸入資料。除此之外有許多家庭不易聯絡上。日益增加的單人或二人家庭及其非常忙碌的生活方式也使得與他們聯絡不易。

為了克服以上不易統計的情況，不斷增加的普查成本，以及減少被普查民眾的負擔，有約百分之二的普查資料是經由網路普查而來。



Schematic of the process:

1. the internet respondents must apply and approved through the KNSO home page;
2. 根據申請者所提供的資料決定核准其申請與否；
3. 在申請者申請成立一個新的帳戶後完成整個申請流程；
4. 普查局確認申請者的地點；
5. 申請者登錄至新申請成立的帳戶內並完成人口普查問卷。

挑戰:

1. 矯正錯誤例如在一個家庭之內重複和遺漏某一成員
2. 數據保密：每個家庭專用的 ID 和密碼及 128 位加密
3. 計算伺服器和網絡容量和系統正式連線
4. 為各種各樣障礙所擬的應變計劃：如何繼續一個被中斷的普查
5. 確認在網路完成人口普查問卷申請人的住所

結果

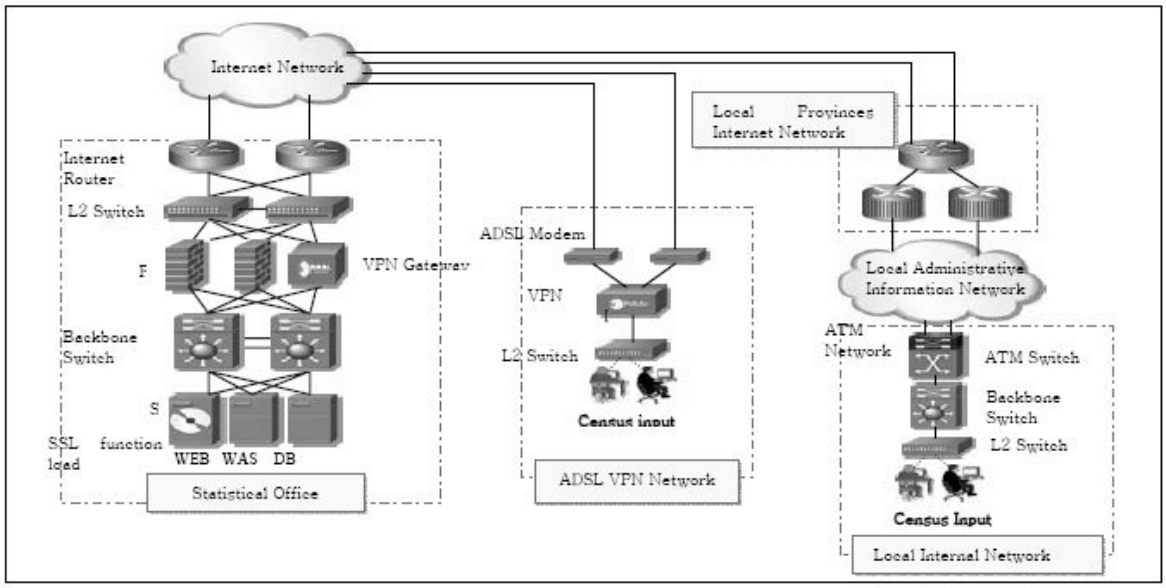
數據處理時間從 12-18 個月減少了 3-6 個月；統計員數字也顯著的削減了。

系統架構

1. 網絡伺服器：共 8 臺伺服器每一臺有四個中央處理器、十六 GB 記憶體和 292GB 硬碟。
2. WAS 伺服器：共 2 臺伺服器每一臺有八個中央處理器、卅二 GB 記憶體和 584GB 硬碟
3. 資料庫伺服器：共 2 臺伺服器每一臺有十六個中央處理器、64GB 記憶體和 584GB 硬碟
4. 1 臺 DW 伺服器及 1 臺 SMS 伺服器各含四個中央處理器，1 臺備用伺服器含 2 個 CPU，2 存貯的每一個含 10 TB 和 2 SAN 開關每一個有 16 個連接阜。
5. 2 DBMS，1 ETL，1 OLAP 工具和幾種系統軟件

網絡架構

1. 網絡設備：2 個路由器，2 個 L3 中堅開關(Back-bone Switch 和 2 W/G 開關。
2. 安全設備：2 防火牆和 2 個 VPN (虛擬專用網絡)門戶



(五)參訪摘要

1. IASTED 舉辦之 CNIS 會議簡介

國際通訊，網路及資訊安全會議 (CNIS; Communication, Network, and Information Security Conference) 於 2006 年 10 月 9 日到 11 日在位於美國劍橋的麻省理工學院舉行。這個會議討論電腦安全議題，整個網路環境的新技術，包括通訊安全、資訊安全、網路安全及通訊資訊網路安全(分成四組，每一組發表 9 篇論文)。會議議題包含下列及其他相關主題：

通訊安全組：

存取控制(Access Control)

使用者認證(Authentication)

Cryptographic Protocols and Applications

數位簽名(Digital Signatures)

Disaster Protocols

Hash Functions

預警系統(Warning Systems)

資訊安全組：

生物測量(Biometrics)
數位所有權(Digital Rights Management)
Digitally Embedded Signatures
DNA, Fingerprint, Iris, and Retina Scanning
Identify Theft
Information Hiding
Legal and Regulatory Issues in Communication
Operating System Security
Plagiarism
Privacy and Confidentiality
Software Security
Spyware
Standards
Watermarking

網路安全組：

Computer/Network Disaster Recovery

Global Security Architectures and Infrastructures
Hacking and Intrusion Detection
Secure Deletion
Secure Email
Spam
Viruses and Worms
Web Security
WiFi Spying/Sniffing
Wireless Privacy
Wireless Security

虛擬專用網路 Virtual Private Networks

專題報告

“Magic Boxes, Boots, and Cores: 以硬體為基礎的網路安全” 發表者： Prof. Sean W. Smith(USA)

在目前的資訊基礎架構上想要保證絕對安全的運算環境就有如緣木求魚一般。然而，因 為計算的過程一定要在某種形式的硬體上運行。因而使這個困難的問題較容易解決。傳統的方法是先製造一個可信任的計算裝置，然後將這個裝置嵌入在較大的計算系統中。近來出現一種非傳統的新方法：對電腦架構本身作基本的變更使得安全問題的處理變的較簡單。這次演講回顧在這個令人興奮新領域上的工具和技術並且討論在工業界和學術界中新出現的一些技術。

網路應用 Social Process
網際網路 Internet
應用程式 High-level Program
作業系統 OS
C 語言、組合語言 C & Assembly
硬體 Hardware

上圖指出一般電腦軟硬體環境，硬體位在最底層且是處理計算的地方，所以直接由硬體進行安全保護效果更佳。

(一)MagicBoxes：通常是一種專門用途的硬體裝置，例如：IBM 4758[1997]是世界第一個支援 FIPS 140-1 level 4 的硬體，提供實體安全偵測和反應。但是 4758 體積太大、太昂貴、速度也太慢。

SFE 理論[Yao 1986]：採用 Secure Function Definition Language(SFDL)、由編譯器產生電路、執行時的引擎

SFE 是具有較小體積的硬體 Trusted Third Party(TTPs)。

(二)報告中還介紹一些現有的 Magic Boots：例如

Embedded Security Sub System ESS
Trusted Platform Module TPM
TCPA
DRM

Trusted computing Group TCG
TSS
PCRS

平台和應用系統等資料，可參考：http://enforcer.sourceforge.net/

(三)Magic Cores：例如：

AEGIS(MIT)
XOM
SG

(四)用虛擬化技術可改進跨主機的相容性。其他例如：VM Ware, Terra, .XEN, SHype, VT, LT, Presidio, Pacifica, separate CPMS, CELL, Multicore.

“覆疊網路(Overlay Networks)概述” Presenters: Dr. J.-H. Cui, Dr. Z.J. Shi, and Dr.B. Wang (USA)

這個專題介紹包含對覆疊網路基本的概念和應用，特別著重于覆疊網路的安裝，管理和安全的研究挑戰。先介紹覆疊網路的定義及 end-host based overlays 及 infrastructure based overlays 兩種基本型態的特徵；接著將這兩種型態的覆疊網路與其他虛擬的架構例如 peer-to-peer networks 及虛擬專用網路 (Virtual Private Networks, VPNs)作比較。然後說明應用覆疊網路的運作較不受網路錯誤的影響，性能較佳，和支援較廣泛的網路功能諸如多重廣播 multicast 和 QoS 等。另一個主要的講題著重在覆疊網路各種研究議題，包括覆疊設計，管理，覆疊和底層(underlay)網路相互作用；以及往路安全等。最後簡要描述有利於覆疊網路研究的基礎設施和工具。

論文發表

在資訊安全小組會議中，討論話題環繞在如何保持資料的完整性，並且如何防止資料落入不相關人的手上。 Yan Zhang[1] 等討論如何為企業建立保護資料的機制。統計顯示 84%的洩密案例是由"局內人"造成的，而 95%的資料損失是因疏忽而起。限制存取控制或者監控網路流量對對洩密或者誤用應用系統的功效有限。該論文提出一種 “Trust Computing” 方法給近端所有者及遠端使用者。 Kastanis[2] 等 和 Ali[3] 提出一種較有效率的認證模式給可用作存取控制的智慧卡(smartcard)使用。 Soon[4] 等已則提出兩

種方法計算隱藏通道的時機。在這個小組的其他論文[5-8]偏重在以各種的浮水印或者數位簽名技術來保護著作權或者是資料的完整性。

在通訊安全小組會議中，主要的課題是無線網路安全、 認證、 加密、防火牆等。Sobolewski[9], 等使用射頻率指紋鑑別確認意指貨櫃的內裝並未在運送過程中遭到更動。Ayachit[10] 等討論傳統的防火牆和 XML 防火牆的差異。他們建議一種新的正式 SML 防火牆安全規則，含以角色為基礎的存取控制及使用者認證和使用者授權。 其他的論文則著重在不同的加密技術[11-12] 及安全金鑰管理。加密的技術在無綫(ad-hoc)網路[13-15]尤其重要。

在網路安全小組會議中，主題涵蓋整個網路安全相關議題，包括存取控制、監控、虛擬專用網路(virtual private network VPN)、預防侵入、 反制垃圾信的技術等。 Keller[16] 為了學生設計一種電腦安全實驗室的藍圖。他使用虛擬機器的方法模擬各種各樣的安全突破而能迅速地重設試驗環境。Eggendorfer[17] 等試著運用較主動的預測方式以改善反制垃圾信的被動式過濾器。他們提出一個結合 HTTP 與 SMTP 的電子陷阱(tar pit)來防止濫發信件者蒐集電子郵件信箱。 Qi[18,19] 等提出一個更有效率分類封包的演算法叫做延伸多維截斷(Extended Multidimensional Cuttings, ExCuts)；及一個更有效的侵入偵測系統 sBits。 Mattes[20] 等及 Fujinoki[21] 等研習不同伺服端的存取控制技術。Fujinoki 等發現 SYN-cookie 在不同情況下的聯綫比率完美。未修正的 TCP 在低請求率(每秒 50 次以上)失掉至 5%的聯綫。Kumar[22] et, al. 的研究重點是各種伺服器端的存取控制技術。利用全球定位系統(GPS) 和以角色為基礎的存取控制 role-based access control (RBAC) ，他們發展出一套定位及定時的存取控制的存取控制系統。 Prandini[23]討論安全又不會被使用者誤用，價位合理的以 Linux 伺服器為基礎的分享網路。

還討論到其它十分重要的主題，如資料庫的整體的效率，安全和隱私。Bhakthavathsalm[24] 提出一個新的演算法當網路嘗試解決累積的封裝程序時，減少上行鏈路存取延遲可產生較高的流量。Wang[25]等 描繪出能保證安全地執行即使可能是惡意的不受信任的程式的必要的安全屬性所具有的特徵。Alhazmi[26] 等檢視主要的作業系

統及網路伺服器軟體的弱點資料集。他們嘗試著辨識每一類別的屬性以更加提高安全性。

---

1. Zhang, et. al, "*Proactive, Content-Aware, Sensitive Data Protection Framework for Enterprises*", Paper #547-028.
2. Kastanis, et. al, "*An Efficient Authentication Scheme for Contactless Smartcards using Elliptic Curve Cryptography*", paper 547-023
3. Ali, "*Designing SSL/TLS Protocol for Resource Constrained Devices*", paper 547-043
4. Son, et. al. "*Covert Timing Channel Capacity of Rate Monotonic Real-Time Scheduling Algorithm in MLS Systems*", paper 547-091.
5. Okada, et. al. "*A Robust Image Watermarking Method to Geometric Attacks*", paper 574-078
6. Yu, et. al. "*Slantlet Transform-based Image Fingerprints*", paper 547-063
7. Salami, et. al. "*A Multi-Bit Watermark Generation Algorithm with Properties of Error Correction*", paper 547-071
8. Obimbo, et. al. "*A Grey-Level Image Watermarking Method based on Block DCT and Statistic Correlation Adjustment*", paper 547-015
9. Sobolweski, et. al, "*Object Authentication in Closed Containers by Ultra-Wideband Multipath Profile Examination: An Application to National Security*", paper 547-067
10. Ayachit, et. al., "*A Petri Net based XML Firewall Security Model for Web Services Invocation*", paper 547-034
11. Eskeland, "*Access Control by Secure Multi-Party EPR Decryption in the Medical Scenario*", paper 547-092
12. Tipper, et. al, "*A Method for Deriving Paths Across a Distributed Web of Trust*", paper 547-042
13. Askoxylakis, et. al., "*Elliptic Curve and Password based Dynamic Key Agreement in Wireless Ad-Hoc Networks*", paper 547-022
14. Owen, et. al. "*Self-Organising Quorum Systems for Ad Hoc Networks*", paper 547-089
15. Trostle, "*The Lightweight Key Management Protocol (LKMP)*", paper 547-096
16. Keller, et. al, "*Design of a Virtual Computer Security Lab*", paper 547-045
17. Eggendorfer, et. al., "*Dynamically Blocking Access to Web Pages for Spammers' Harvesters*", paper 547-033
18. Qi, et. al, "*Towards Effective Packet Classification*", paper 547-058
19. Qi, et. al, "*An Efficient Hybrid Algorithm for Multidimensional Packet Classification*", paper 547-027
20. Mattes, et. al "*Access Control Platform for Submitted Jobs in Computational Grid Environment*", paper 547-059
21. Fujinoki, et. al., "*Performance Studies of the Server-Side Access Control for SYN-Flooding Distributed Denial of Service Attacks using Real Systems*", paper 547-020
22. Kumar, et. al., "STRBAC - An Approach Towards Spatio-Temporal Role-based Access Control", paper 547-803
23. Prandini, "*Securing a Linux-based Multi-User Web Server*", paper 547-805
24. Bhakthavathsalm, "Reinforcement of Privacy in 802.16 MAC Common Part Sublayer using the Principle of Circularity", paper 547-085
25. Wang, et. al. "An MSLS-EMM for Enforcing Confidentiality in Malicious Environments", paper 547-094

26. Alhazmi, et. al. “Security Vulnerability Categories in Major Software Systems”, paper 547-097

會議時程

~ CNIS 2006 ~
MIT Faculty Club,
Cambridge, Massachusetts, USA
October 9–11, 2006
PRELIMINARY CONFERENCE PROGRAM LOCATION
MIT Faculty Club,
50 Memorial Drive, E52, 6 Fl.
Cambridge, Massachusetts, USA

COMMUNICATION, NETWORK, AND INFORMATION SECURITY

PROGRAM OVERVIEW

Monday, October 9, 2006
07:00 – Registration
08:30 (Foyer)
08:30 - Welcome Address
09:00 (Main Dining Room East)
09:00 - (Lawtech) Keynote Address –
10:00 "Owning Avatars: Legal Control of Human and Nonhuman Data Representations"
(Main Dining Room West)
10:00 – Coffee Break
10:30 (Foyer)
10:30 Session 1 – Information Security I
(Main Dining Room East)
13:30 Session 2 – Communication Security
(Main Dining Room East)
15:00 – Coffee Break
15:30 (Foyer)
15:30 Session 2 Continued

Tuesday, October 10, 2006
08:30 – 09:30 Keynote Address – “Magic Boxes, Boots, and Cores:
Hardware-Based Cybersecurity”
(Main Dining Room East)
09:30 – Coffee Break
10:00 (Foyer)
10:00 Session 3 – Information
Security II
(Main Dining Room East)
13:30 Session 4 – Communication, Network and Information
Security
(Main Dining Room East)
15:00 – Coffee Break
15:30 (Foyer)

15:30 Session 4 Continued
19:00 - Cocktail Reception
(Dining Room 5)
19:30 – Dinner Banquet

(Dining Room 5)

Wednesday, October 11, 2006
08:30 Tutorial Presentation - "An Overview of Overlay Networks"
(Main Dining Room East)
10:00 – Coffee Break
10:30 (Foyer)
10:30 Tutorial Presentation Continued
13:30 Session 5 – Network Security
(Main Dining Room East)
15:00 – Coffee Break
15:30 (Foyer)
15:30 Session 6 Continued

MONDAY,
OCTOBER 9, 2006
07:00– 08:30 REGISTRATION
IASTED Staff: TBA (Canada)
Room: Foyer
08:30 – 09:00 WELCOME ADDRESS
Room: Main Dining Room East
09:00 – LAWTECH KEYNOTE
ADDRESS – “OWNING AVATARS: LEGAL CONTROL OF HUMAN AND NONHUMAN DATA REPRESENTATIONS”
Presenter: Prof. Dan L. Burk (USA)
Location: Main Dining Room West
10:00 – 10:30 COFFEE BREAK
Location: Foyer
10:30 – SESSION 1 -
INFORMATION SECURITY I
Chair: TBA
Room: Main Dining Room East
547-072
Pro-Temp-Z: An XML based Authorization System with Provisional Authorization and Temporal Certification Support
V.V. Singh (USA)
547-078
A Robust Image Watermarking Method to Geometric Attacks
K. Okada and S. Wada (Japan)
547-091
Covert Timing Channel Capacity of Rate Monotonic Real-Time Scheduling Algorithm in MLS System
J. Son and J. Alves-Foss (USA)
547-093
Security Analysis of a Large-scale Voting Scheme

S. Eskeland (Norway)
13:30 – SESSION 2 -
COMMUNICATION SECURITY
Chairs: TBA
Room: Main Dining Room East
547-022
Elliptic Curve and Password based Dynamic Key Agreement in Wireless Ad-hoc Networks
I.G. Askoxylakis, D.D. Kastanis, and A.P. Traganitis (Greece)
547-034
A Petri Net based XML Firewall Security Model for Web Services Invocation
M.M. Ayachit and H. Xu (USA)
547-042
A Method for Deriving Paths Across a Distributed Web of Trust
P. Tipper and C. Edwards (UK)
547-043
Designing SSL/TLS Protocol for Resource Constrained Devices
A.M. Ali (USA)
547-053
Security Framework for Supervisory Control and Data Acquisition, Automation Systems, and Networks
C. Obombo, F. Haji, L. Lindsay, and D. Patel (Canada)
547-067
Object Authentification in Closed Containers by Ultra-Wideband Multipath Profile Examinatiojn: An Application to National Security
S. Sobolewski and M. Buehrer (USA)
547-089
Self-Organising Quorum Systems for ad hoc Networks
G. Owen and M. Adda (UK)
547-092
Access Control by Secure Multi-Party EPR Decryption in the
Medical Scenario
S. Eskeland (Norway)
547-096
The Lightweight Key Management Protocol (LKMP)
J. Trostle (USA)
15:00 - 15:30 COFFEE BREAK
Room: Foyer
15:30 – SESSION 2 CONTINUED

TUESDAY,
OCTOBER 10, 2006
08:30 – 9:30 – KEYNOTE ADDRESS – “MAGIC BOXES, BOOTS, AND CORES: HARDWARE-BASED CYBERSECURITY” Presenter: Sean W. Smith (USA)
Room: Main Dining Room East
09:30 – 10:00 COFFEE BREAK
Room: Foyer
10:00 – SESSION 3 –
INFORMATION SECURITY II

Chairs: TBA
Room: Main Dining Room East
547-015
A Grey-Level Image Watermarking Method Based on Block DCT and Statistic Correlation Adjustment
C. Obimbo and J. Ni (Canada)
547-023
An Efficient Authentication Scheme for Contactless Smartcards using Elliptic Curve Cryptography
D.D. Kastanis, I.G. Askoxylakis, and A.P. Traganitis (Greece)
547-028
Proactive, Content-aware, Sensitive Data Protection Framework for Enterprises
Y. Zhang, R.J. Enbody, and J.R. Floyd (USA)
547-063
Slantlet Transform-based Image Fingerprints
L. Yu and S. Sun (PRChina)
547-071
A Multi-bit Watermark Generation Algorithm with Properties of Error Correction
B. Salami and C. Obimbo (Canada)

13:30 – SESSION 4 –
COMMUNICATION, NETWORK, AND INFORMATION SECURITY
Chairs: TBA
Room: Main Dining Room East
547-048
Artificial Immune using Multilevel Negative Selection Approach to Anomaly Detection
A.A.A. Youssif, A.Z. Ghalwash, and S.A. Mohamed (Egypt)
547-085
Reinforcement of Privacy in 802.16 MAC Common Part Sublayer Using the Principle of Circularity
R. Bhakthavathsalam (India)
547-094
An MSLS-EMM for Enforcing Confidentiality in Malicious Environments
B. Wang and J. Alves-Foss (USA)
547-095
A Classification of Security for the Transactions Between a Requester, an Intermediary, and a Web-Service
J. Muñoz Arteaga, R. Mendoza González, F.J. Álvarez (Mexico), and M. Vargas Martín (Canada)
547-097
Security Vulnerability Categories in Major Software Systems
O.H. Alhazmi, S.-W. Woo, and Y.K. Malaiya (USA)
547-802
ARP and ICMP Weaknesses: Impact and Network Performance Analysis of a Novel Attack Strategy
A. Anand, R. Rishi, and M. Kumar (India)
547-803
STRBAC - An Approach Towards Spatio-Temporal Role-based Access Control
M. Kumar and R.E. Newman (USA)
547-804

Experimental Efvaluation of Network Security Through a Hierarchical Quantitative Metrics Model
F. El-Hassan, A. Matrawy, N. Seddigh, and B. Nandy (Canada)
547-805
Securing a Linux-based Multiuser Web Server M. Prandini (Italy)
15:00 – 15:30 COFFEE BREAK
Location: Foyer
15:30 – SESSION 4 CONTINUED
19:00 – COCKTAIL RECEPTION
Room: Dining Room 5
19:30 – DINNER BANQUET
Room: Dining Room 5

WEDNESDAY,

OCTOBER 11, 2006
08:30 – TUTORIAL PRESENTATION – "AN OVERVIEW OF OVERLAY NETWORKS"
Presenters: J.-H. Cui, Z.J. Shi, and B. Wang (USA)
Room: Main Dining Room East

10:00 – 10:30 COFFEE BREAK
Location: Foyer
10:30 – TUTORIAL
PRESENTATION CONTINUED
13:30 – SESSION 5 – NETWORK SECURITY
Chairs: TBA
Room: Main Dining Room East
547-020
Performance Studies of the Server-Side Access Control for SYN-Flooding Distributed Denial of Service Attacks using Real Systems
H. Fujinoki and R.K. Boyapati (USA)
547-021
A Scalable Approach to IP
Anycast
A. Pathak and D. Sanghi (India)
547-027
An Efficient Hybrid Algorithm for Multidimensional Packet Classification
Y. Qi and J. Li (PRChina)
547-030
Introducing Trusted EAP Module for Security Enhancement in
WLANs and VPNs P. Urien (France), M. Dandjinou (Burkina Faso), and M. Badra (France)
547-031
Optimizing Multi-Thread String
Matching for Network Processor based Intrusion Management System
J. Yu, Q. Huang, and Y. Xue (PRChina)
547-033
Dynamically Blocking Access to Web Pages for Spammers'
Harvesters T. Eggendorfer and J. Keller (Germany)
547-045
Design of a Virtual Computer Security Lab

J. Keller and R. Naues (Germany)
547-058
Towards Effective Packet Classification
Y. Qi and J. Li (PRChina)
547-059
Access Control Platform for Submitted Jobs in Computational Grid Environment
L. Mattes and J.A. Zuffo (Brazil)
15:00 – 15:30 COFFEE BREAK
Location: Foyer
15:30 – SESSION 5 CONTINUED

2. 美國微軟公司網際網路解決方案與新世代資料整合應用交流研討

本處主計資訊系統 DGA 現有的系統開發環境平台與使用開發工具分別為微軟 Windows 98、SQL 6.5、VB 6.0、ASP 等，因此安排參訪美國微軟總部，了解其公司最新發展策略，資訊安全技術，新版本資料庫以及 Vista 作業系統等。

SQL Server 2005

Samir Shah 先生介紹 SQL Server 2005 年版著重在企業數據管理和分析並詳細討論微軟的關係數據庫(Relational Database)平臺和它的核心能力包括安全、擴充性、可及性和以軟體設計開發為重點。由提供完整的端到端數據管理和分析平臺，及透過與 Visual Studio and Office 的緊密結合， SQL Server 可幫助改進整個組織的生產力。

SS - SQL Server 的功能更完整，例如以報告服務撰寫報告，分析服務並且可綜合其他的應用軟體使用。它的特點是能處理所有數據和特有的服務。軟體設計開發者可使用 Visual Studio 開發應用軟體，之後撰寫報告並將報告綜合在實用軟體之中。整個開發過程的經驗也可用於開發更高階智慧型的商業軟體。企業用戶能通過辦公室軟體或以其他軟體為橋樑以 access 數據。

同時 SQL Server 亦較安全。甲骨文(Oracle)有 17 項安全認證，大多數 9i、8x 和 7x 等版本； 10g 只有 1 份證明。SQL Server 2000 則達到 C2 安全標準并且提供類似單一登錄， PKI， Kerberos，網絡封包加密等特點。特殊的 SQL Server 特點包括： 加密，高級核驗，認證，授權， EAL4+認證等。

安全創新研究在 2006 年五月中暴露了 Oracle 10g/RHEL 3 有 210 個弱點，但 SQL Server/WS2003 只有 63 個弱點。 2005 年從四月到十月 Oracle 供發布了 33 個安全方面的補強程式。因此 SQL Server 是一個更加安全的系統。

Trustworthy Computing

在高可信度(Trustworthy Computing)的資訊處理方面的介紹，David Aucsmith 報導現今各種安全的威脅和他們代表的趨向。他也報導微軟高可信度計算的策略，也是微軟的長期策略以創造安全，隱私有和更可靠的計算的經驗。

微軟的高可信度方式是：

由設計起：認識威脅，檢查原始碼和滲透測試。

預置設定：關閉所有未使用的功能，減少攻擊表面和降低特權。

部署管理：嚴格的訓練、安全工具和企業管理

微軟視窗包括幫助保護視窗用戶免受間諜軟體(spyware)和其他不需要的軟體的反間軟體(AntiSpyware)。

OCA 檢查並且警告造成視窗當機的 malware，惡意軟體移除工具並可幫助保護無防毒軟體的用戶。

微軟新視窗版本 Vista 與新的 Server 版本 Longhorn 是同時設計所以它們之間的功能也有互補作用；Vista 同時提高安全的設定和用戶的功能。

三、心得與建議

(一) 以網頁為基礎(web-based)資料收集方法，開發語言包括 HTML、JavaScript、DHTML、CSS 等；伺服端程式語言 Java、ASP、PHP 等。近來 XML 已經被許多開發者採用來有系統地傳遞資料，藉由結合 XSL 可發展更豐富而有用的系統使用內建驗證(built in validation)技術及利用控制(controls)和圖像(images)來收集和顯示資料。網際網路標準 W3C 委員會在二零零三十月提出新的建議： Xform standard 下一代網頁資料收集工具。隨著 ASP.Net 程式語言及功能更強的 JAVA, PHP 及其他程式語言的出現，程式開發者現在有非常多的開發工具可用來發展系統。

(二) 網路服務具有許多優點譬如較易取得資料，動態的系統間連線，並且高度的自動化(無須操作員) 等所以非常具有吸引力。但是網路安全卻是一件非常重要的課題。一切令網路具有吸引力因素都違反傳統的電腦安全模式和控制。

(三) 網路服務的安全技術的包括：保持加密 XML 網路服務的機密、使用 XML 簽名的網路服務的完整性、網路服務使用 OASIS 標準組所建議的 SAML 和 XACML 的認證和授權、使用 XKMS 的網路服務的 PKI、網路服務的安全規格：SOAP 標題延伸（header extensions）、UDDI 的安全通訊協定。

(四) 由多個標準制定組織發展類似的和重覆的網路服務安全標準造成系統開發者的混淆。例 OASIS 和 W3C 之間的標準重覆，所以我們需要更多正式的規格和標準的測試。

(五) 國際通訊，網路及資訊安全會議 (CNIS; Communication, Network, and Information Security Conference) 討論電腦安全議題，整個網路環境的新技術，包括通訊安全、資訊安全、網路安全及通訊資訊網路安全等。與會者提出利用硬體、軟體方法、網路加密、浮水印簽章等方法來改進網路各方面的安全防護。

(六) 微軟電腦公司新版本的視窗作業系統為 Vista，資料庫為 SQL 2005，並推出許多網路服務與系統安全認證機制。本中心已於去年下半年對於現有各應用系統與 Vista 的相容性進行測試，作為將來平台版本提升的考量依據。

(七) 主計資訊系統 DGA 現有系統開發環境平台與使用開發工具為微軟 Windows98、SQL6.5、VB6.0、ASP 等，版本十分老舊，維護不易，系統每年因應預決算編製要點又須不斷增修，而會計制度的變更將會對本系統造成巨大衝擊，建議主計資訊系統藉此機會與政府歲計會計系統 GBA 重新規劃整合。

(八) 本處業務電腦化起步很早，由早期 IBM 大型主機（現在普查調查系統仍繼續使用中）、個人電腦 PC DOS、區域網路、Client-Server 架構、Windows 平台，到最近因應網際網路時代的趨勢，陸續開發各項 Web 版應用系統，為了因應環境變遷與技術的提升，除應加強 Web 開發工具的技術訓練外，更應持續加強不斷面臨挑戰的 Web 服務安全監控管理。

(九) 資訊工程是一項新生的科技，電腦軟硬體產品仍在不斷發展更新，本中心員工教育訓練應配合不斷學習新的技術以面臨新的挑戰。

四、名詞對照

英文縮寫	英文全稱	中譯	解釋
ASP	Active Server Pages		
CSS	Cascading Style Sheets	層疊樣式表	一種 HTML 規範。該規範容許 HTML 文檔的作者和用戶為其添加樣式表。樣式表中包含版式資訊，規定字體等頁面外觀。該規範還規定了 HTML 文檔樣式表和用戶樣式的混合方式。亦稱為層疊樣式表機製（Cascading Style Sheet mechanism）。
DHTML	Dynamic HTML	動態超文本標記語言	
DOS	Denial of Service	阻斷服務	指使系統長時間無法提供正常的服務的一種狀態
HTML	Hyper Text Markup Language	超文本標記語言	
IETF	Internet Engineering Task Force	網際網路工程工作小組	
NIST	National Institute of Standards and Technology.		
OASIS	Organization for the Advancement of Structured Information Standards	結構化資訊標準組織	
PHP	Personal Home Page	個人主頁	
PKI	public key infrastructure	公共密鑰匙基礎結構	
QoP	Quality of Protection	保護品質	
QoS	Quality of Service	服務品質	
RBAC	role-based access control		
SFDL	Secure Function Definition Language		SFE 使用
SOA	Service Oriented Architecture		
SOAP	Simple Object Acess Protocol		
TTP	Trusted Third Party		
UDDI	Universal Description, Discovery and Integration protocol		
URI	Uniform Resource Identifier	通用資源標誌符	
VPN	virtual private network	虛擬專用網路	
VPN	virtual private network	虛擬專用網路	
W3C	World Wide Web Consortium	全球資訊網聯盟	
WML	The markup language for WAP devices		
WS	Web Services	網路服務	
WSDL	Web Services Description Language		
WS-I	The Web Services Interoperability organization		

英文縮寫	英文全稱	中譯	解釋
WSReliability	Web Services Reliability	網路服務	WS-Reliability 的目的在提供網路服務應用程式一個可靠的訊息需求，並保證網路上的訊息傳輸的可靠性和安全性。WS-Reliability 標準定義了符合目前網路服務標準的訊息可靠性，且可與現有的通訊協定結合使用。最適合與 WS-Reliability 一同使用的通訊協定是 W3C SOAP 1.1 和 1.2 版，WS-Reliability 可以在 SOAP Header 的區塊中描述其可靠訊息的相關敘述。
WS-ReliableMessaging	Web Services ReliableMessaging	網路服務	
XHTML	The Extensible HyperText Markup Language		
XML	the eXtensible Markup Language	可擴展標記語言	
XPath	XML Path Language		
XSL	eXtensible Stylesheet Language	可擴展樣式語言	
XSL-FO	XSL Formatting Objects		
XSLT	XSL Transformations		文件產生工具，XSLT 強大的轉換功能 Transformations，可以用來產生 HTML XML PDF 和 SVG 等類型檔案
	web-based	以網頁為基礎	
	Script language	腳本語言	
SSL	Style sheet language		
	Overlay Network	重疊網路	Overlay Network 是架構在實體網路之上的另一層網路
	underlay Network	底層網路	
	Watermarking	浮水印	
	Discovery service	查詢服務	
	Re-Engineering	再造工程	
	digital certificate	數位憑證	

五、附　件

(一) CNIS 2006 通訊、網路及資訊安全研討會會議資料

(二) 微軟電腦公司網際網路解決方案與新世代資料整合應用

(三) NIST：Guide to Secure Web Services

參考資料一

The Third IASTED International Conference on "Communication, Network, and Information Security"

會議內容摘要

INFORMATION SECURITY

Protemp-Z: An Xml Based Authorization System with Provisional Authorization and Temporal Certification Support

Vishav Vir Singh
Computer Engineering Department
San Jose State University
One Washington Square, San Jose CA 95192-0180
USA
Vishav.Singh@yahoo.com

ABSTRACT

The eXtensible Markup Language (XML) is a flourishing standard for information interchange and representation. Endeavors at various levels are underway to make this format effectual and project it as a unified and homogeneous data model absolutely imperative to establish security frameworks that protect data from Many different threats. We propose a model ProTemp-Z that synthesizes the notions of provisional authorization and temporal certifications, resulting in a system that is powerful enough to enforce security based on a well-defined set of provisions and also based on the temporal coordinates of data. The temporal orientation of this model also accounts for the safeguard of security of dynamically changing data, which is of great value. We present an implementation of the authorization logic.

A Robust Image Watermarking Method To Geometric Attacks

Kosuke Okada and Shigeo Wada
Graduate School of Engineering, Tokyo Denki University
2-2 Kanda-Nishiki-cho, Chiyoda-ku, Tokyo 101-8457, Japan
05gme06@ed.cck.dendai.ac.jp and wada@cck.dendai.ac.jp

ABSTRACT

The embedding digital signature in image invisibly to protect from geometric and data compression modifications are an important issue. In this paper, a robust image watermarking method to geometric attacks is proposed. The proposed method has the robustness to geometric distortions such as rotation, scaling and translation. In the embedding process, a valuable wavelet transform is used to become an invisible watermark system. The log-polar transform and autocorrelation are used to estimate the geometric distortions, and the watermark is detected in the wavelet transform domain in the extraction process. In the simulations, the effectiveness of our method is demonstrated. The robustness to the geometric attacks and JPEG compression is examined. The performance with respect to bit error rate characteristics and degradation of image quality is also evaluated.

Covert Timing Channel Capacity of Rate Monotonic Real-Time Scheduling Algorithm in MLS Systems

Joon Son and Jim Alves-Foss
Center for Secure and Dependable Systems
University of Idaho
POBOX 441008 Moscow, ID 83844-1008
email: [son2320,jimaf]@uidaho.edu

ABSTRACT

Real-time systems must satisfy timing constraints. In our previous work, we showed that a covert timing channel cannot be completely closed in some system configurations due to the timing constraints imposed by the Rate-Monotonic (RM) real-time scheduling algorithm. In this paper, we construct a probabilistic model to

measure two quantities of a covert timing channel in RM based systems: channel capacity and quantity of specific information. We show how these two metrics can be calculated from our probabilistic model and why they are useful metrics in evaluation of a covert (timing) channel.

Security Analysis of A Large-Scale Voting Scheme

Sigurd Eskeland
Agder University College
Grooseveien 36,
4876 Grimstad, Norway
email: sigurd.eskeland@hia.no

ABSTRACT

Yun and Lee proposed recently a voting scheme for large scale elections that are based on pseudonymity and blind signatures. In this paper, we show that their voting scheme is insecure because it is possible to compute an arbitrary number of forged signed ballots without being detected. We also propose a small modifcation that thwarts the attack

A Grey-Level Image Watermarking Method Based on Block Dct And Statistic Correlation Adjustment

Computing & Information Science
University of Guelph
Guelph, ON N1G 2W1
Canada
cobimbo@uoguelph.ca jni@uoguelph.ca

ABSTRACT

The watermarking technology provides an ideal tool of copy and copyright protection. It relies on embedding a secret imperceptible signal, a watermark, into the host data in a way that it always remains presence. In this paper, we presented a new method of watermarking, which embeds a binary sequence into the DCT domain of a grey-level host image. The embedding procedure is carried out by slightly modifying the correlation coefficients of those middle frequency bands in the DCT blocks. Experiment results show that our algorithm is robust to certain types of attacks, such as the JPEG compression.

An Efficient Authentication Scheme for Contactless Martcards Using Elliptic Curve Cryptography

Diomedes D. Kastanis, Ioannis G. Askoxylakis, and Apostolos P. Traganitis
Foundation for Research & Technology – Hellas, Institute of Computer Science (FORTH-ICS)
P.O.Box 1385, Heraklion, Crete, GR-711-10
GREECE
{asko, tragani}@ ics.forth.gr, diomedes.kastanis@orange-ft.com

ABSTRACT

Nowadays the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional, is a very important issue that concerns the information society. The scope of this paper is to develop a Contactless Smartcard protocol, which will be able operate securely and effectively, under a variety of attack methods. The system implements a novel mutual authentication procedure between a Contactless Reader and a Smartcard, calculates securely the corresponding parameters, and protects the system against malicious attacks. The system can be used in a wide spectrum of applications that require simplicity, ease of use, long life, low cost and portability. Suitable applications could be, Electronic Payments, Public Transport Electronic Fare, Highway toll payments, Medical Applications, and Access Control.

Proactive, Content-Aware, Sensitive Data Protection Framework for Enterprises

Yuan Zhang and Richard J. Enbody
Department of Computer Science and Engineering
Michigan State University
East Lansing, Michigan, USA
zhangyu6, enbody@cse.msu.edu
John R. Lloyd
Department of Mechanical Engineering
Michigan State University
East Lansing, Michigan, USA

lloyd@egr.msu.edu

ABSTRACT

Sensitive data about customers, finances or intellectual property are often the most important assets of enterprises. The majority of information leakage (84%) is caused by insiders, and 95 percent of data loss is caused by unintentional application misuse. Restricted file access control and strong user account management do not provide enough fine-grained authorization to protect against insiders misusing legitimate applications. Monitoring network traffic can catch misuses, but it suffers from false positives and the inability to detect new patterns of sensitive data use. Trusted Computing is a new technology which creates a trustworthy system for local owners (using TPM and secure booting) and for remote users (using Remote Attestation). However, it also has drawbacks, such as software upgrading, and locking a user to certain operating systems and applications. Our framework builds on top of the current infrastructure, and takes advantage of the reality that all systems in an enterprise can be highly controlled by the IT administrators. The framework employs strong user profiling and isolation to protect against malware and uses sensitive-dataconfigurable applications to proactively protect against unintentional misuses.

Slantlet Transform-Based Image Fingerprints

Longjiang Yu and Shenghe Sun
Dept. Automatic Test and Control, Harbin Institute of Technology
Building A2, Science Park, Harbin Institute of Technology, No.2 Yikuang Street, Nangang District, Harbin 150080
Heilongjiang, P.R.China
longjiang_yu@yahoo.com.cn

ABSTRACT

Image fingerprints are related to cryptographic hash functions. In contrast to cryptographic hash functions this robust digest is sensitive only to perceptual change. Minor changes, which are not affecting the perception, do not result in a different fingerprint. In addition applied in authentication and tamper detection as traditional digital signatures, image fingerprinting technique is used in content-based retrieval, content-based monitoring, and content-based filtering. In this paper we present a slantlet transform based method for image fingerprints. The slantlet transform is a kind of orthogonal wavelet and performs better in data compression than discrete cosine transform and the other wavelets. Phase information is extracted from slantlet domain for image fingerprints. Better performance is verified in experiments evaluating robustness (e.g. against operations like lossy compression, scaling and cropping) and discriminability in comparison to an existing method.

A Multi-Bitwatermark Generation Algorithm with Properties of Error Correction

B. Salami
Department of Computing and Information Science
University of Guelph
Guelph, Ontario, Canada
email: bendigi@gmail.com
C. Obimbo
Department of Computing and Information Science
University of Guelph
Guelph, Ontario, Canada
email: cobimbo@uoguelph.ca

ABSTRACT

Digital watermarking is a technique developed for the protection and identification of digital media by embedding digital data directly onto multimedia objects such that it can be detected or extracted later. Watermarks often carry no extra information and are not very useful. On the other hand, multi-bit watermarks typically include a second signal used in error correction and thus decrease the amount of useful information or payload that can be embedded. In this paper, we present a multi-bit watermark generation scheme that enables the decoder to automatically correct the extracted information without the need of a second reference signal. Our method converts the provided ownership information into a bar-code like image and embeds the encrypted version into any color image. Under this scheme, the extracted watermark can be corrected.

COMMUNICATION SECURITY

Elliptic Curve and Password Based Dynamic Key Agreement in Wireless Ad-Hoc Networks

Ioannis G. Askoxylakis, Diomedes D. Kastanis, Apostolos P. Traganitis
Foundation for Research & Technology – Hellas, Institute of Computer Science (FORTH-ICS)
P.O.Box 1385, Heraklion, Crete, GR-711-10
GREECE
{asko, tragani}@ ics.forth.gr, diomedes.kastanis@orange-ft.com

ABSTRACT

Ad-hoc networking is a relatively new operating mode for rapid mobile host interconnection. However, it suffers from the lack of a fixed infrastructure that forces each ad-hoc host to rely on each other, in order to maintain the network stability and functionality. This singularity of ad-hoc networks introduces several issues, most of which concern the system's security. This paper focuses on investigating the security threats of ad-hoc networks together with their unique ability to meet specific emergency requirements, such as the rapid deployment of emergency networks which can enhance and optimize the disaster relief efforts after a natural disaster or a terrorist attack. Moreover this particular type of networks can be found very efficient in military environments where the cellular/PCS services may not be available.

Considering the difficulty of establishing a secure network where the impacted group members share no prior electronic information, and moreover considering how this can be achieved through the most reliable, secure and efficient way, we propose a new protocol for dynamic multiparty password key agreement, based on Elliptic Curve Cryptography.

A Petri Net Based Xml Firewall Security Model FOR Web Services Invocation

Mihir M. Ayachit and Haiping Xu
Computer and Information Science Department
University of Massachusetts Dartmouth
North Dartmouth, MA 02747
Email: {g_mayachit, hxu}@umassd.edu

ABSTRACT

An XML firewall differs from a conventional firewall because its major task is to control access to web services rather than to filter untrusted addresses. An XML firewall can effectively protect web services from being attacked by inspecting a complete XML message including its head and data segments, and rejecting unauthorized web services invocation. In this paper, we propose a formal XML firewall security model using role-based access control (RBAC). Our proposed model supports user authentication and user authorization according to information stored in a user database and a policy database associated with an XML firewall. The formal model is designed compositionally using Petri nets, which can serve as a high-level design for XML firewall implementation. The key components of our compositional security model are the application model and the XML firewall model. To illustrate the advantages of our formal approach, we use an existing Petri net tool to verify some key properties of our model, such as boundedness and liveness.

A Method for Deriving Paths Across A Distributedweb of Trust

Paul Tipper
Computing Department, InfoLab 21
Lancaster University
email: p.tipper@lancaster.ac.uk (PGP Key: 5FAF443D)
Christopher Edwards
Computing Department, Infolab 21
Lancaster University
Email: ce@comp.lancs.ac.uk

ABSTRACT

This paper gives an overview of ongoing research into building a distributed web of trust usable for deriving paths of trust between keys and performing secure key exchange. It gives example algorithms for creating, maintaining and searching such a web, set against the background of current research. The paper also examines

attacks against the proposed system as well as methods by which it prevents or reduces the threat of them. The paper concludes by giving an overview of the direction of future research.

Designing SSL/TLS Protocol for Resource Constrained Devices

Asad M. Ali {asad.ali@gemalto.com}
Gemalto, Smart Card Research
8311 North FM 620 Road, Austin TX, 78726, USA

ABSTRACT

Secure Sockets Layer (SSL) and its successor Transport Layer Security (TLS) are the de facto standards for securing communication between web servers and web browsers. Although once considered the realm of high-end enterprise systems, these protocols can now be implemented on increasingly smaller devices. Smart cards are one example of such devices. They have extremely limited resources; both in terms of memory and processing power. Because of these limitations, designing and implementing a TLS stack on a smart card has its unique challenges. The TLS protocol stack and the required cryptographic computations have heavy memory requirements, and making them run in resource constrained devices calls for an optimized software design. This paper describes various design optimizations for enabling TLS support on embedded smart card architectures with only a few kilobytes of RAM. This combination of smart card hardware security, and the TLS network protocol security can prove to be an extremely powerful amalgam for securing Internet transactions.

Security Framework for Supervisory Control and Data Acquisition, Automation Systems, and Networks

Charlie Obombo, Fardeen Haji, Larry Lindsay, and Darshana Patel
Dept. of Computing and Information Science
University of Guelph
Guelph, Ontario, Canada N1G 2W1

ABSTRACT

Supervisory Control and Data Acquisition Systems (SCADA) are used in industrial applications to monitor and control plant equipment and processes. Originally, SCADA systems were designed around reliability and safety, not security. Since these systems have become increasingly interconnected through the usage of "open" standards, vulnerabilities that traditionally affected the corporate network are now causing havoc on SCADA systems and networks. The focus of this paper is to study and evaluate the security risks as well as discuss countermeasures to minimize threats of these systems and the supported communication infrastructure.

Object Authentication in Closed Containers By Ultra-Wideband Multipath Profile Examination: An Application to National Security

Sylwester Sobolewski and Michael Buehrer
Mobile and Portable Radio Research Group Laboratory
Department of Electrical and Computer Engineering
Virginia Tech, Blacksburg, VA 24061
{sobolews, buehrer}@vt.edu

ABSTRACT

Maintaining national security in this era of growing terrorist threats and worldwide unrest is of utmost importance. This article suggests one solution to the particular problem of authenticating content of large metal transport containers to make sure they contain the same objects at the points of origin and destination. The case of shifted objects is also considered.

The proposed authentication method uses the concept of Radio Frequency Fingerprinting and has two components. First, probability distribution functions of correlations of UWB multipath profiles at the origin and destination are compared. Second, the eigen-values of the same UWB profiles are compared. The experimental results show that it is possible to determine whether the same objects are present in the container and whether they have been shifted.

Self-Organising Quorum Systems for Ad Hoc Networks

Gareth Owen and Mo Adda
School of Computing, University of Portsmouth
Buckingham Building, Lion Terrace, Portsmouth
England, PO1 3HE

{gareth.owen, mo.adda}@port.ac.uk

ABSTRACT

There are many essential applications for quorum systems in ad-hoc networks, such as that of location servers in large-scale networks. Existing research proposes many approaches to the problems, many of which are incomplete, cumbersome, or incur significant cost. We describe and analyse a self-organising quorum system that creates an emergent intelligence to minimise overhead and maximise survivability. We then examine the quorum's performance as a location server and suggest improvements to the query mechanism and routing algorithm using the information.

Access Control by Secure Multi-Party EPR Decryption in The Medical Scenario

Sigurd Eskeland
Agder University College
Grooseveien 36,
4876 Grimstad, Norway
email: sigurd.eskeland@hia.no

ABSTRACT

Due to that medical patient data may be highly confidential, it is essential that electronic patient records (EPR) are properly protected. Accordingly, only legitimate medical personnel should be allowed access to relevant patient data. In this regard, it is reasonable that patients should be able to exert control over their own medical data. In this paper, we propose a security scheme that allows electronic patient records or specific EPR modules to be stored encrypted at the EPR server where each EPR is encrypted with a unique and secret key. In order to obtain access to the protected medical data, medical teams collaborate with the concerning patient in order to blindly reconstruct EPR cryptokeys for decryption at the EPR server. The scheme prohibits the secret EPR cryptokeys from being disclosed to any party, and it is privacy-preserving in the sense that the collaborating parties are able to perform the computations without revealing their private inputs to each other.

The Lightweight Key Management Protocol (LKMP)

Jonathan Trostle
ASK Consulting and Research, Inc., USA

ABSTRACT

We present requirements for authentication and key distribution in typical wireless scenarios, including fast handoffs and small user devices (e.g. cell phones). We show that Kerberos V5 is inadequate for some wireless scenarios. A new solution, the LKMP protocol, is then presented. We also present a new crossrealm authentication protocol, the LKMP passthrough exchange, and its advantages over existing Needham-Schroeder derived crossrealm protocols. We give a performance analysis of the LKMP protocol, based on our prototype. We include a performance and security comparison to Kerberos V5 including an analysis of some of the performance bottlenecks in Kerberos and the MIT Kerberos implementation in particular. Our results show that Kerberos is significantly under-optimized, and we describe some security improvements.

COMMUNICATION, NETWORK, AND INFORMATION SECURITY

Artificial Immune Using Multi-Level Negative Selection Approach to Anomaly Detection

Aliaa A. A. Youssif, Atef Z. Ghalwash, & Samir A. Mohamed
Faculty of Computers & Information, Helwan Univ.,
Cairo, Egypt
draliaa@gmail.com, ghalwash@idsc.net.eg, samir.a.mohamed@gmail.com

ABSTRACT

Natural immune system (NIS) provides a rich source of inspiration for computer security in the age of the Internet. The Artificial Immune System (AIS) is one of the promising techniques that seek to capture some aspects of the natural immune system. One of the major algorithms to implement the AIS is the Negative Selection (NS) algorithm. The paper proposes an immunological algorithm based on the Negative Selection Algorithm and the Clonal Selection technique, called the Multi-Level Negative Selection (MLNS).

The proposed algorithm is compared with the previous work of the AIS. Data from the international DARPA data set is used to train and test the feasibility of the new algorithm. The recorded experimental results show that the proposed algorithm outperforms the previous work and a higher detection rate is achieved (96%:94.5%). Meanwhile, a comparable false alarm rate is attained (1%:0.9%). A remarkable advantage, of the proposed algorithm, is the noticeable reduction in the number of detectors needed to achieve the stated results since it comes down to nearly a quarter (22.3%) of those generated with the previously used single scale detector.

Reinforcement of Privacy in 802.16 Mac Common Part Sublayer Using the Principle of Circularity

R Bhakthavathsalam
Supercomputer Education and Research Center, Indian Institute of Science
Bangalore 560012
INDIA
bhaktha@serc.iisc.ernet.in

ABSTRACT

Owing to the addition of various security overheads at different layers, the cumulative encapsulation causes more access delay in the uplink data transmission in WiMax resulting in low throughput. The upstream channel is a stream of minislots with a dynamic mix of contention and reservation based opportunities affording privacy between transmitter and receiver. The contention resolution algorithm used in WiMax is based on a truncated binary exponential backoff, maintaining privacy between Base Station and Subscriber Stations, with initial backoff window and maximum backoff window controlled by the Base Station. The performance of the system is affected by the collisions of bandwidth request messages in uplink transmission. In this paper, we introduce a new paradigm of circularity by selectively dropping appropriate control messages in order to obviate the overall bandwidth request collisions with some modifications of the same backoff overheads for supporting privacy. This new mechanism reduces the uplink access delay and thereby yields higher uplink throughput resulting in better utilization of available bandwidth.

An MSLS-EMM for Enforcing Confidentiality in Malicious Environments

Bei Wang and Jim Alves-Foss
Center for Secure and Dependable Systems
University of Idaho
POBOX 441008
Moscow ID 83844, USA
email: [wang4056, jimaf]@uidaho.edu

ABSTRACT

The use of security policy enforcement mechanisms has been a topic in recent literature. Particular focus has been on the class of policies that can be enforced by these mechanisms but not on the security policy guiding the execution of the monitoring mechanisms. It has been a challenge to enforce information confidentiality in a multi-level secure system since malicious users can exploit covert channels within the enforcement mechanisms to propagate confidential information. In this paper, we characterize necessary security properties for an enforcement mechanism that can ensure secure execution of the untrusted programs even though they may be malicious.

A Classification of Security Patterns for the Transactions Between A Requester, An Intermediary, and A Web-Service

Jaime Muñoz Arteaga , Ricardo Mendoza González , Francisco J. ÁlvarezCentro de Ciencias Básicas.
Universidad Autónoma de Aguascalientes.
Av. Universidad N° 940, Ciudad Universitaria, C.P. 20100. Aguascalientes, Ags. México.
mendozagric@yahoo.com.mx; {jmunozar, fjalvar}@correo.uaa.mx
Miguel Vargas Martín University of Ontario, Institute of Technology.
Oshawa, Canada
miguel.vargasmartin@uoit.ca

ABSTRACT

It is very important to have a security model to try to avoid the security risks related with the transactions between a Requester and a Web-service. Nevertheless, the design of this model can be difficult because many security techniques exist. The use of patterns can ease the design of the security model and the selection of the involved elements. However, as far as we know, there are not specific classifications of security patterns available as the one we propose in this paper. We propose a classification of security patterns for the transactions between a Requester, an intermediary, and a Web-service.

Security Vulnerability Categories in Major Software Systems

Omar H. Alhazmi, Sung-Whan Woo, Yashwant K. Malaiya
Colorado State University
omar| woo|malaiya@cs.colostate.edu

ABSTRACT

The security vulnerabilities in software systems can be categorized by either the cause or severity. Several software vulnerabilities datasets for major operating systems and web servers are examined. The goal is to identify the attributes of each category that can potentially be exploited for enhancing security. Linking a vulnerability type to a severity level can help us prioritize testing to develop more effective testing plans. Instead of using an ad hoc security testing approach, testing can be directed to vulnerabilities with higher risk. Modeling vulnerabilities by category can be used to improve the post-release maintenance and patching processes by providing estimation for the number of vulnerabilities of individual types and their severity levels. We also show that it is possible to apply vulnerability discovery models to individual categories which can project the types of vulnerabilities to be expected in near future.

ARP and ICMP Weaknesses: Impact and Network Performance Analysis of A Novel Attack Strategy

Ashish Anand, Rahul Rishi, Mukesh Kumar
Dept. of Computer Science
Technological Institute of Textile & Sciences, Bhiwani
Maharishi Dayanand University
Haryana, India
ashish.anand@titsbhiwani.org, rahulrishi@titsbhiwani.org, mukesh.kumar@titsbhiwani.org

ABSTRACT

After the ARP and IP were drafted, a subtle weakness in the Address Resolution Protocol was discovered. Unlike TCP, ARP relies on raw sockets and like UDP; ARP provides no means to establish the authenticity of the source of incoming packets. Although this problem can be resolved in case of UDP packets by considering alternate approaches such as DNS replies being sent over TCP rather than UDP using the DNSSEC architecture so that false DNS replies may not be accepted by a host; ARP is still prone to similar attacks. This paper identifies known weaknesses of the ARP and analyses the impact of a network flooding utility developed by us, the underlying ideology of which is this very weakness of the ARP. The purpose of our implementation is to extend what conventional tools can do, by incorporating a network flooding module in it, and to simulate a flooded network where hosts are forced to broadcast outgoing packets to the entire network. In some network conditions, the gateway may also be brought into broadcast mode, leading to undesired results. Various attack strategies are considered and the network performance during these attacks is measured. We also reveal a strategy by which ICMP replies are received by a host trying to PING a destination, but the host fails to recognize these replies. Such a weakness in the ICMP can lead to erroneous network management.

Strbac - An Approach Towards Spatio-Temporal Role-Based Access Control

Mahendra Kumar
CISE Department
University of Florida
Gainesville, FL 32608
email: makumar@cise.ufl.edu
Richard E. Newman
CISE Department
University of Florida
Gainesville, FL 32608
email: nemo@cise.ufl.edu

ABSTRACT

The rapid emergence of GPS enabled devices, sensors and mobile equipment in commercial as well as government organizations has led to considerable research in time- and location-based access control schemes. Location-based access policies enhance the security of an application by restricting access to an object only from specified locations. On the other hand, temporal constraints provide granularity in security features and also limit damage to an application to a specific time interval (e.g. when staff are present to respond if necessary). This paper introduces a novel approach to location- and time-based access control mechanism using Role-Based Access Control (RBAC).We believe that it is well-suited for organizations that require time- and location-based access control over static or mobile objects.

Experimental Evaluation of Network Security Through A Hierarchical Quantitative Metrics Model

F. El-Hassan and A. Matrawy
Dept. of Systems and Computer Engineering
Carleton University
Ottawa, ON, Canada
Emails:ffadi,amatrawyg@sce.carleton.ca
N. Seddigh and B. Nandy
Solana Networks
Ottawa, ON, Canada
Emails:fnseddigh,bnandyg@solananetworks.com

ABSTRACT

In this paper, we present an approach towards the evaluation of network security. This approach is based on a Hierarchical Quantitative Metrics (HQM) model that enables the representation of important aspects of network security using quantitative metrics. The proposed model, combined with a general evaluation framework, would enable the generation of a grand metric that gauges the overall security status of a network. The main contributions of this work are (1) Proposal and use of the HQM for network security evaluation (2) Demonstration of the HQM model's applicability through an example set of Intrusion Detection System (IDS) metrics and the implementation of a prototype tool that automates the use of this model (3) Presentation of results for experiments conducted using traces of real network traffic which is, to the best of our knowledge, the only results reported in this area using real network traffic. Our results are followed by a discussion on the impact of different factors affecting the evaluation process.

Securing A Linux-Based Multi-User Web Server

Marco Prandini
DEIS - Università di Bologna
Viale Risorgimento, 2
40136 Bologna, Italy
mprandini@deis.unibo.it

ABSTRACT

A commonplace solution for putting a web site on-line at a reasonable cost is *hosting*, that is placing it on a shared server, together with other sites. Hosting providers face significant security problems, both in terms of avoiding misuse of their servers by "guests", and in terms of providing effective isolation between them; the Discretionary Access Control model implemented by traditional operating systems can fail to provide adequate solutions to these problems. This work describes a system based on the integration of the widely adopted Apache/PHP platform with the powerful Mandatory Access Control features offered by the Security-Enhanced Linux project. The resulting solution combines a sound approach to the most common security problems with a very tolerable impact on system administration complexity.

NETWORK SECURITY

Performance Studies of The Server-Side Access Control for Syn-Flooding Distributed Denial of Service Attacks Using Real Systems

Hiroshi Fujinoki
Department of Computer Science
Southern Illinois University Edwardsville
Edwardsville, Illinois 62026-1656, USA
E-mail: hfujino@siue.edu
Ravi Kumar Boyapati
Department of Electrical Engineering
Southern Illinois University Edwardsville
Edwardsville, Illinois 62026-1656, USA
E-mail: rboyapa @siue.edu

ABSTRACT

This paper presents our on-going project on performance evaluation of the major existing solutions based on server-side access control for SYN-flooding distributed denial-of-service attacks using a real network system. Although many solutions have been proposed and implemented, there is no formal performance study that measures and compares the solutions based on server-side access control. The successful connection rate of the existing solutions was measured, compared and analyzed using an experiment test bed developed by LINUX-based PCs. We have tested SYN-cookie, Random Drop and the unmodified TCP in various conditions. We also simulated different types of legitimate clients in the end-to-end signal propagation delay to evaluate the fairness in connections. The results of our experiments showed that SYN-cookie resulted in the perfect (i.e., 100%) connection rate in all the experiments and configurations. Regardless of the length of the end-to-end delay, the connection rate of the unmodified TCP dropped to below 5% for a low request rate of 50 requests per second or more. Random Drop was more effective in improving connection rate than the unmodified TCP if the end-to-end delay was short or when the TCP backlog queue size was increased to more then 300 slots.

A Scalable Approach Toip Anycast Security

Abhinav Pathak
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur, India
abhinav.pathak@gmail.com
Dr. Dheeraj Sanghi
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur, India
dheeraj@cse.iitk.ac.in

ABSTRACT

Anycast is vulnerable to security attacks such as denial of service, theft of service etc. The client which requests for service through anycast, can not verify the authenticity of the responding server. Also, any node can advertise itself to be a member of the anycast group. The router does not have a mechanism to verify the authenticity of the node which claims to be member of the anycast group. We propose a scalable and secure model for anycast communication. Our model is based on a single entity in the network that controls the group management of the anycast group and also helps clients to verify membership of a particular node. We show that our model achieves the security standards required by IP anycasting while being scalable. We define additional secure anycast protocol features and show that our model achieves these set of additional features.

An Efficient Hybrid Algorithm for Multidimensional Packet Classification

Yaxuan Qi1 and Jun Li1,2
1 Research Institute of Information Technology (RIIT), Tsinghua University, Beijing, China, 100084
2 Tsinghua National Lab for Information Science and Technology (TNLIST), Beijing, China, 100084
{yaxuan, junl}@tsinghua.edu.cn

ABSTRACT

Multidimensional Packet Classification is one of the most critical functions for network security devices such as firewalls and intrusion detection systems. Due to the worst case bounds found in computational geometry,

most of the existing algorithms for multidimensional packet classification trade memory usage for search speed in order to achieve better overall performance. Although some of these algorithms are proved to be efficient on small number of classification rules, they scale poorly in either search time or memory usage when the number of rules grows. In this paper, we propose an efficient hybrid algorithm named sBits, which combines the advantages of two best existing algorithms, RFC and HiCuts. Compared to RFC and HiCuts, sBits uses 10 to 400 times less memory storage and 30% to 50% less time in worst case search. sBits also reduces the heavy computational burden in pre-processing. Its full update time is 10 to 100 times less than RFC and HiCuts.

Introducing Trusted EAP Module for Security Enhancement in WLANS and VPNS

Pascal Urien, Mesmin Dandjinou, Mohamad Badra
Ecole Nationale Superieure des Telecommunications (ENST)
37/39 rue Dareau 75014 Paris
France
Pascal.Urien@enst.fr, Mohamad.Badra@enst.fr
Universite Polytechnique de Bobo-Dioulasso
Burkina Faso
Msmin.Dandjinou@voila.fr

ABSTRACT

The Extensible Authentication Protocol (EAP) is a kind of *Esperanto* used for access control in various network technologies such as WLAN or VPN. We introduce the *trusted EAP module*, a tamper resistant chip that computes the EAP protocol. Its functional interface is compatible with IETF emerging specifications. We present an open smartcard platform which enables the design of cheap components, both on client and server side; furthermore we describe a management model that remotely modifies embedded credentials and applications. An implementation of a RADIUS server working with EAP server modules is detailed and analyzed. Finally experimental performances are commented and we underline that today EAP modules compute complex protocol like EAP-TLS in less than 5s, and therefore may be deployed in existing networks.

Optimizing Multi-Thread String Matching for Network Processor Based Intrusion Management System

Jianming Yu,1, 2 Quan Huang1, 2 and Yibo Xue2, 3
1 Department of Automation, Tsinghua University, Beijing, China
2 Research Institute of Information Technology, Tsinghua University, Beijing, China
3 Tsinghua National Lab for Information Science and Technology, Beijing, China
yujm03@mails.tsinghua.edu.cn

ABSTRACT

String matching is the core algorithm and the most time consuming operation of almost every modern Network Intrusion Management System (NIMS). In this paper we aim at integrating string matching with multi-thread parallelism to dramatically improve the performance of NIMS. The string matching procedure under multi-thread parallelism situation is modeled and researched. The results are utilized to instruct the design of an improved Aho-Corasick (AC) algorithm, named as AC_MT, for network processor (NP) based NIMS. A simplified NIMS prototype and both the AC and AC_MT algorithms are implemented on Intel's NP platform IXDP2850. The evaluation results tested with SmartBits 600 reveals that the performance of the NIMS prototype is improved by 44.7%~148.8% depending on the different lengths of the input packets and different number of threads, under both algorithms using the same number of threads situation.

Dynamically Blocking Access to Web Pages for Spammers' Harvesters

Tobias Eggendorfer
ITIS e. V. Institut für Technik Intelligenter Systeme
An-Insitut der Universität der Bundeswehr Neubiberg
Werner-Heisenberg-Weg 39
85579 Neubiberg, Germany
tobias.eggendorfer@unibw.de
Jörg Keller
FernUniversität in Hagen
Lehrgebiet Parallelität & VLSI
58084 Hagen, Germany
joerg.keller@fernuni-hagen.de

ABSTRACT

Almost all current anti spam measures are reactive, filtering being the most common. But to react means always to be one step behind. Reaction requires to predict the next action of the attacker. So the focus on fighting spam should rather be on prevention. Current proposals focus on fixing SMTP's lack of authentication, but introduce two new major problems: First, all current attempts break existing SMTP functionality and, second, it seems to be hardly possible to enforce a change of SMTP world wide. Therefore other preventive measures should be implemented. The most promising approach is to prevent spammers from collecting email addresses. Several proposals show ways to obfuscate addresses on web pages and to create HTTP tar pits in order to catch spammers' harvesters. In our previous work, we combined a HTTP tar pit with a SMTP tar pit and found it to be very effective in trapping harvesters. Here, we extend the use of the combined tar pit to identify harvesters and to dynamically block access to web pages for harvesters, because of the combined tar pit's high efficiency. We present a test setup to validate the effectiveness of our tool. As the experiment is still running, we can only report on preliminary findings so far.

Design of A Virtual Computer Security Lab

J¨org Keller and Ralf Naues
LG Parallelit¨at und VLSI
FernUniversit¨at in Hagen
58084 Hagen, Germany
{joerg.keller,ralf.naues}@fernuni-hagen.de

ABSTRACT

We present the design and a prototype of a lab course on computer security, the necessity of which arises from the students' need to complement course work by hands-on experience. In order to guarantee maintainability of a number of Linux systems on which students change configurations, we decided to employ a virtual machine approach. This allows to reset configurations quickly without another costly operating system installation. We sketch the types of tasks the students are to perform, and our approach to check immediately whether students have completed a task. As students operate in larger groups, and the server hosting the virtual machines can only run a finite number of them simultaneously, a reservation scheme is employed to guarantee fair access for all participants.

Towards Effective Packet Classification

Yaxuan Qi1 and Jun Li1, 2
1 Research Institute of Information Technology (RIIT), Tsinghua University, Beijing, China, 100084
2 Tsinghua National Lab for Information Science and Technology (TNLIST), Beijing, China, 100084
{yaxuan, junl}@tsinghua.edu.cn

ABSTRACT

A variety of network security services, such as access control in firewalls and protocol analysis in intrusion detection systems, require the discrimination of packets based on the multiple fields of packet header, which is called Multidimensional Packet Classification. In this paper, we propose a very effective packet classification algorithm called Extended Multidimensional Cuttings, ExCuts in short. As an extension of HyperCuts, which is the best-known existing decision tree algorithm, ExCuts refines the node merging mechanism using a two-step discontiguous space aggregation scheme, which minimizes the number of child nodes. To further reduce the memory usage of the decision tree structure, ExCuts adopts a bit string mapping scheme to compress the large pointer arrays in internal nodes. Due to the significant memory reduction, ExCuts is able to pick a fixed number of cuttings and thus provides explicit worst-case search time. Experimental results show that ExCuts outperforms the best result of existing algorithms on both real-life rulesets and synthetic classifiers.

Access Control Platform for Submitted Jobs in Computational Grid Environment

Leonardo Mattes, João Antonio Zuffo
Laboratório de sistemas integráveis – Universidade de São Paulo (USP)
Caixa Postal 15.064 – 91.501-970 – São Paulo – SP – Brazil
{leo,jazuffo}@lsi.usp.br

ABSTRACT

Computational grid aiming to get a better improvement of the resources by the use of distributed and flexible systems. However, the utilization of this system brings new challenges in relation to security. One of the foreseen grid functionalities creates dynamic jobs and services, as well as operation, bringing flexibility to the

system that should be exploited for installations of “malicious” application. This work present a platform of role base fine access control to Java application in computational grids in order to improve the control of jobs and services created in a dynamic way. A study of case shows in a practical way a use of the present platform.

參考資料二

Microsoft SQL Server 2005 Enterprise Data Management and Analysis

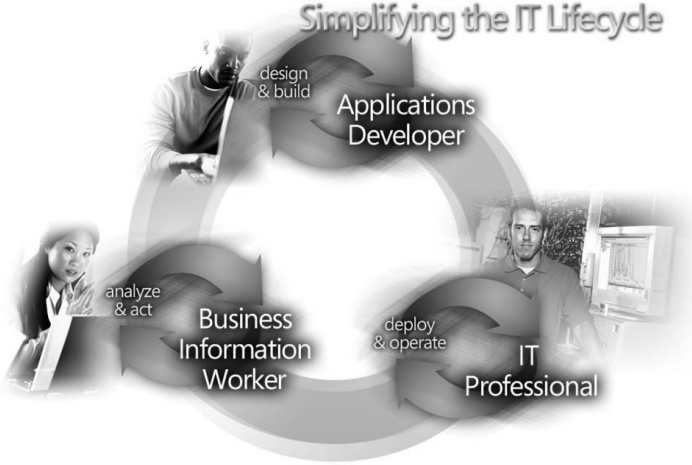
SQL Server 2005 Enterprise Data Management and Analysis

Samir Shah
Enterprise Technology Strategist
Microsoft Customer Advocacy and Technical Marketing

Agenda

- Microsoft's Relational Database Platform
  - Database Progress with SQL Server 2005
  - Core Abilities – Security, Scalability, Availability, Developer Focus
- Microsoft Business Intelligence
  - ETL – SQL Integration Services
  - Reporting – SQL Server Reporting Services
  - Analytics – SQL Server Analysis Services
  - Microsoft Office Business Scorecard Manager 2005
- Open Discussion

Our Vision



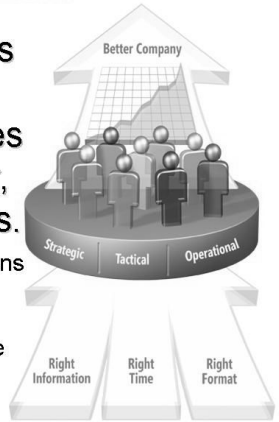
SQL Server

The comprehensive, integrated data platform

Microsoft's BI Vision

Improving organizations by providing business insights to all employees leading to better, faster, more relevant decisions.

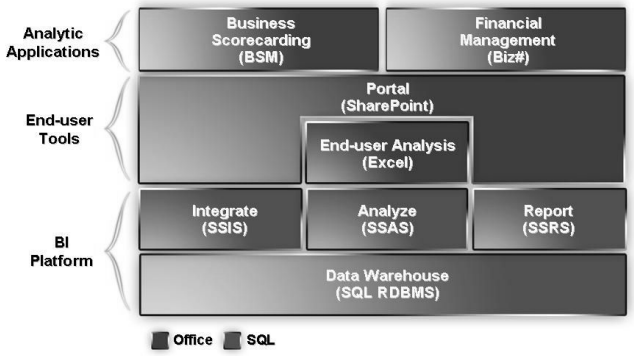
- Integrated platform and applications
- Secure and personalized
- Collaborative
- Cost effective and comprehensive



SQL Server Business Intelligence

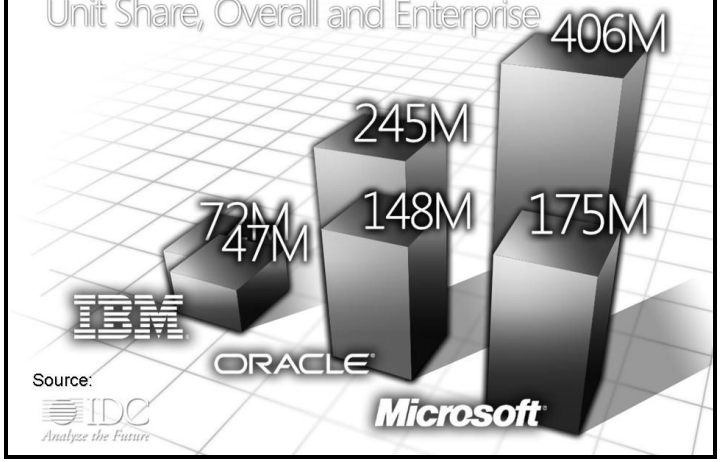
Microsoft Business Intelligence

Complete, Accessible, designed for broad usage



The Database Market

Unit Share, Overall and Enterprise



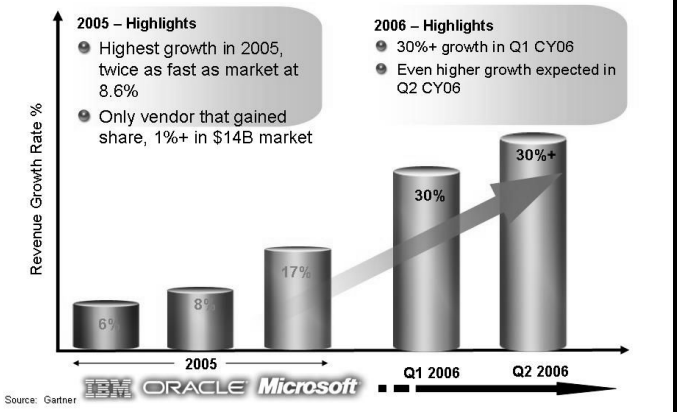
SQL Server Generations

History of Innovation

1st Generation	2nd Generation		3rd Generation
SQL Server 6.0/6.5	SQL Server 7.0	SQL Server 2000	SQL Server 2005
• Differentiation from Sybase SQL Server • Windows integration • First to include Replication	• Re-architecture of relational server • Extensive auto resource management • First to include OLAP & ETL	• Performance, scalability focus • XML support • First to include Notification • First to include Data Mining & Reporting	• High availability • Security • Developer productivity • Native XML • First to include Enterprise ETL & Deep Data Mining

Cross-release objectives • *Reliability & Security* • *Integrated Business Intelligence* • *Lowest TCO* • *Automatic Tuning*

SQL Server Momentum



Customer Concerns

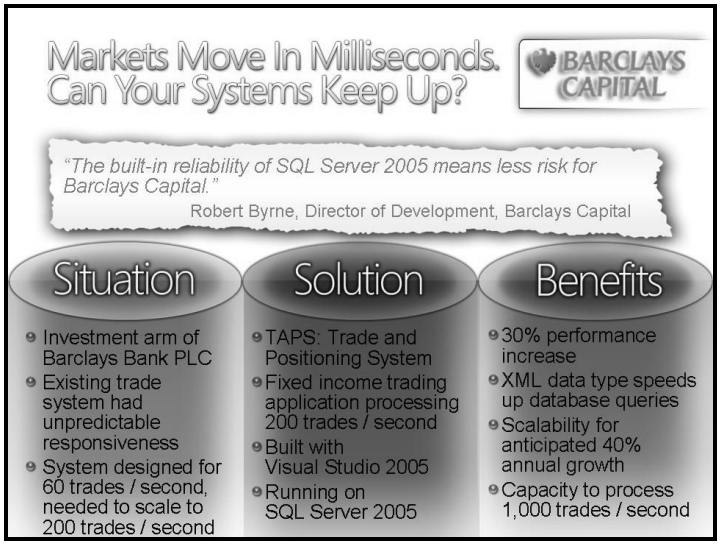
- Scalability
- High Availability
- Manageability
- Security
- Price/TCO
- Analytical Capabilities – Business Intelligence

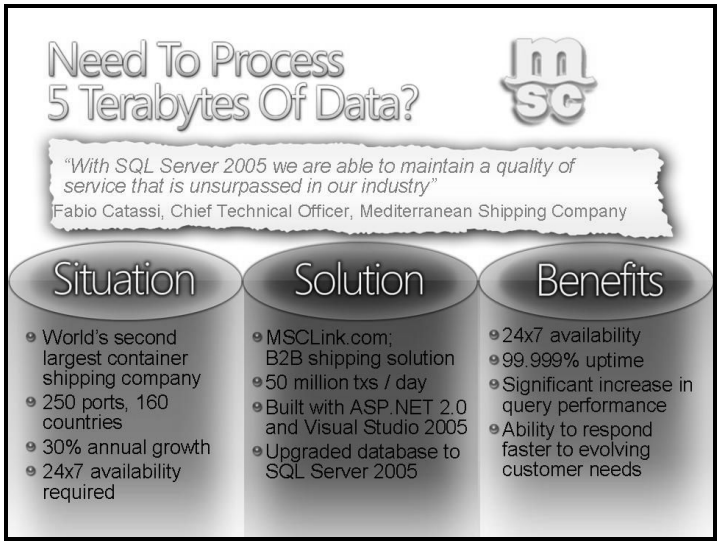
Can You Get Mainframe-like Availability And Low TCO?

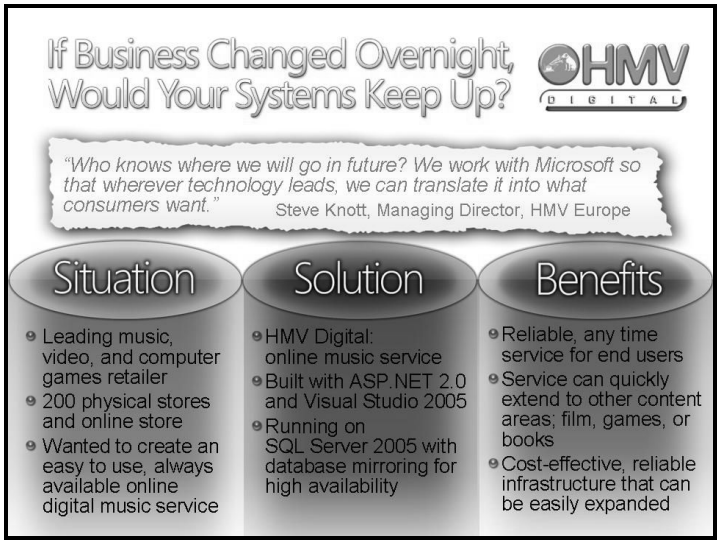
NASDAQ

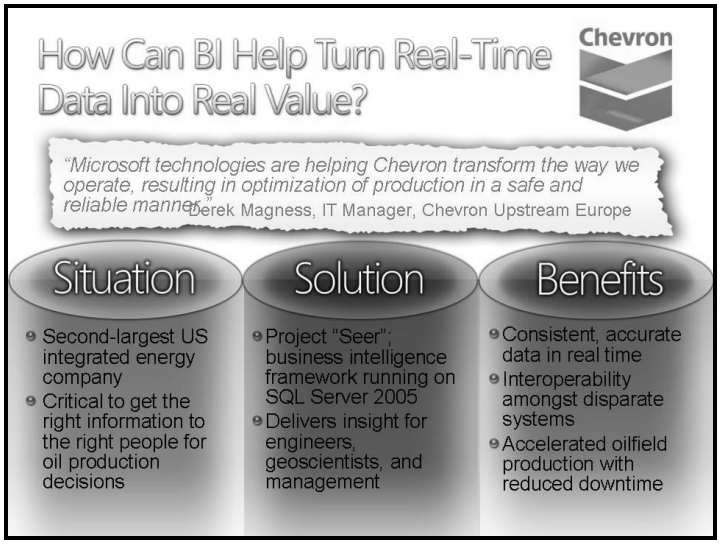
"The fact that we can move mission critical applications from Tandem to SQL Server 2005 proves that it is enterprise-grade."
Ken Richmond, Vice President for Software Engineering, NASDAQ

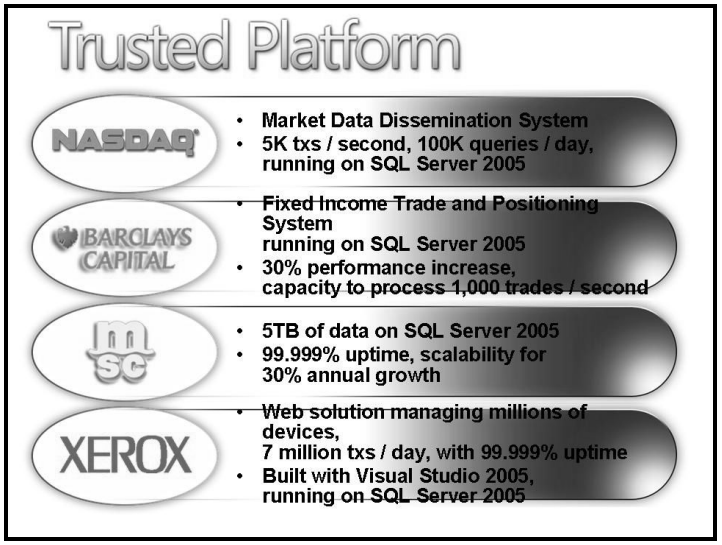
Situation	Solution	Benefits
• Largest US electronic stock market • Replacing aging Tandem systems • Wanted to update system for real-time trade summary, risk management, and broker clearing	• MDDS: Market Data Dissemination System • 5K txs / second, 100K queries / day • Running on SQL Server 2005 with database mirroring for high availability	• Enterprise availability • Scalability to handle 8 million new rows of data per day • Lower total cost of ownership • Real-time reporting • Developer agility

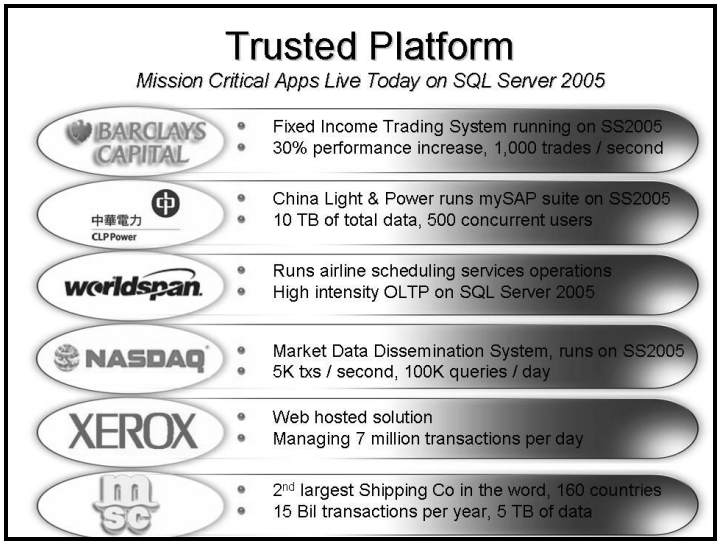

Markets Move In Milliseconds. Can Your Systems Keep Up?
BARCLAYS CAPITAL
"The built-in reliability of SQL Server 2005 means less risk for Barclays Capital."
Robert Byrne, Director of Development, Barclays Capital
Situation
Solution
Benefits
Investment arm of Barclays Bank PLC
Existing trade system had unpredictable responsiveness
System designed for 60 trades / second, needed to scale to 200 trades / second
TAPS: Trade and Positioning System
Fixed income trading application processing 200 trades / second
Built with Visual Studio 2005
Running on SQL Server 2005
30% performance increase
XML data type speeds up database queries
Scalability for anticipated 40% annual growth
Capacity to process 1,000 trades / second


Need To Process 5 Terabytes Of Data?
"With SQL Server 2005 we are able to maintain a quality of service that is unsurpassed in our industry"
Fabio Catassi, Chief Technical Officer, Mediterranean Shipping Company
Situation
Solution
Benefits
World's second largest container shipping company
250 ports, 160 countries
30% annual growth
24x7 availability required
MSCLink.com; B2B shipping solution
50 million txs / day
Built with ASP.NET 2.0 and Visual Studio 2005
Upgraded database to SQL Server 2005
24x7 availability
99.999% uptime
Significant increase in query performance
Ability to respond faster to evolving customer needs


If Business Changed Overnight, Would Your Systems Keep Up?
HMV DIGITAL
"Who knows where we will go in future? We work with Microsoft so that wherever technology leads, we can translate it into what consumers want."
Steve Knott, Managing Director, HMV Europe
Situation
Solution
Benefits
Leading music, video, and computer games retailer
200 physical stores and online store
Wanted to create an easy to use, always available online digital music service
HMV Digital: online music service
Built with ASP.NET 2.0 and Visual Studio 2005
Running on SQL Server 2005 with database mirroring for high availability
Reliable, any time service for end users
Service can quickly extend to other content areas; film, games, or books
Cost-effective, reliable infrastructure that can be easily expanded

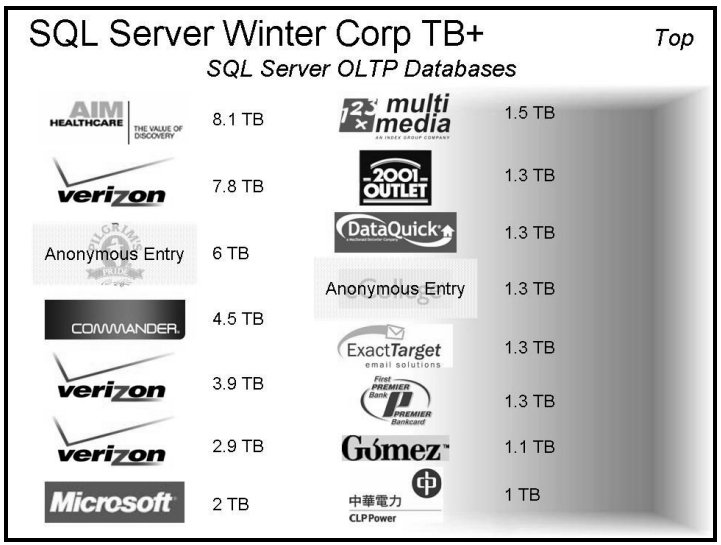

How Can BI Help Turn Real-Time Data Into Real Value?
Chevron
"Microsoft technologies are helping Chevron transform the way we operate, resulting in optimization of production in a safe and reliable manner."
Derek Magness, IT Manager, Chevron Upstream Europe
Situation
Solution
Benefits
Second-largest US integrated energy company
Critical to get the right information to the right people for oil production decisions
Project "Seer"; business intelligence framework running on SQL Server 2005
Delivers insight for engineers, geoscientists, and management
Consistent, accurate data in real time
Interoperability amongst disparate systems
Accelerated oilfield production with reduced downtime





Comparing with 2003 Survey Winter Corp TopTen 2005

	TopTen 2005	TopTen 2003
#Terabyte+ Entries (> 1 TB)	43	15
#Terabyte-Size Entries (> 0.5 TB)	50	19
#DW Entries	22	4
#OLTP Entries	21	13
#OLTP Entries in Top Ten categories for All Platforms	4	1
#DW Entries in Top Ten categories for All Platforms	2	0
#DW Entries in DB Size TopTen for Windows	7	1
Top DW Entry for Windows	Yes	No



SQL Server Winter Corp TB+ Top

SQL Server Data Warehousing Databases

UNISYS Imagine it. Done.	19.5 TB	Microsoft	2.8 TB
USDA	12.7 TB	PREMERA BLUE CROSS	2.2 TB
Edcon	6.2 TB	BARNES & NOBLE BOOKSELLERS	2 TB
hp invent	6.1 TB	Scottish and Southern Energy plc	1.9 TB
Sage TELECOM	5.8 TB	RAYMOND JAMES You first.	1.6 TB
dpf	4.8 TB	MarketerNET	1.4 TB
First PREMIER Bank PREMIER Bankcard	4.2 TB	STRATAPULT See how far it takes you	1.1 TB
SHOPRITE	3.9 TB	CLALIT HEALTH SERVICES	1.1 TB

2005 New Features

Database Engine
- Service Broker
- HTTP Access
- Database Tuning Advisor
- Enhanced Read ahead & scan
- Indexes with Included Columns
- Multiple Active Result Sets
- Persisted Computed Columns
- Try/Catch in T-SQL statements
- Common Table Expressions
- Server Events
- Snapshot Isolation Level
- Partitioning
- Synonyms
- Dynamic Management Views

.NET Framework
- Common Language Runtime Integration
- CLR-based Types, Functions, & Triggers
- SQL Server .NET Data Provider

Data Types
- CLR-based Data Types
- VARCHAR(MAX), VARBINARY(MAX)
- XML Datatype

Database Failure and Redundancy
- Fail-over Clustering (up to 8 node)
- Database Mirroring
- Database Snapshots
- Enhanced Multi-instance Support

XML
- New XML data type
- XML Indexes
- XQUERY Support
- XML Schema (XSD) support
- FOR XML PATH
- XML Data Manipulation Language
- SQLXML 4.0

Database Maintenance
- Backup and Restore Enhancements
- Checksum Integrity Checks
- Dedicated Administrator Connection
- Dynamic Configuration AWE
- Highly-available Upgrade
- Online Index Operations
- Online Restore

Management Tools
- MDX & XML/A Query Editor
- Maintenance Plan Designer
- Source Control Support
- Profiler access to non-sa
- SQLCMD Command Line Tool
- Database Mail

Performance Tuning
- Profiling Analysis Services
- Exportable Showplan & Deadlocks
- Profiler Enhancements
- New Trace Events

Full-text Search
- Backup/Restore includes FT catalogs
- Multi-instance service

SQL Client .NET Data Provider
- Server Cursor Support
- Multiple Active Result Sets

Security
- Catalog and meta-data security
- Password policy enforcement
- Fine Grain Administration Rights
- Separation of Users and Schema
- Surface Area Configuration

Notification Services
- Embed NS in existing application
- User-defined match logic
- Analysis Services Event Provider

Replication
- Seamless DDL replication
- Merge Web Sync
- Oracle Publication
- Peer to Peer Transactional replication
- Merge replication perf and scalability
- New monitor and improved UI

Analysis Services and Data Mining
- Analysis Management Objects
- Windows Integrated Backup and Restore
- Web Service/XML for Analysis
- Integration Services and DM Integration
- Eight new Data Mining algorithms
- Auto Packaging and Deployment
- Migration Wizard

Integration Services
- New high performance architecture
- Visual design and debugging environment
- Extensible with custom code and scripts
- XML task and data source
- SAP connectivity
- Integrated data cleansing & text mining
- Slowly changing dimension wizard
- Improved flow control
- Integration with other BI products

Reporting Services
- Report Builder
- Analysis Services Query Designer
- Enhanced Expression Editor
- Multi-valued Parameters
- Date Picker
- Sharepoint Web Parts
- Floating Headers
- Custom Report Items
- XML Data Provider

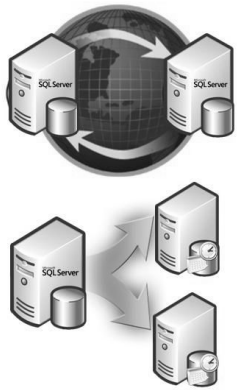
Highly Available Databases

SQL Server 2005 Technology

- Database Server Failure or Disaster
  - Failover Clustering
  - Database Mirroring
  - Peer-to-Peer Replication
- User or Application Error
  - Log Shipping
  - Database Snapshot
- Data Access Concurrency Limitations
  - Snapshot Isolation
  - Online Index Operations
  - Replication
- Upgrade
  - Software and Hardware
- Database Maintenance and Operations
  - Fast Recovery
  - Partial Availability
  - Online Restore
  - Media Reliability
  - Dedicated Administration Connection
  - Dynamic Configuration
- Availability at Scale
  - Data Partitioning
  - Replication
- Tuning
  - Database Tuning Advisor

Mission Ready Ultra-High Availability

Microsoft SQL Server 2005



Fast & Predictable Failover

- Database Mirroring
- Failover Clustering

Always Online

- Online index operations
- Fast recovery
- Fine-grained online repairs
- Database snapshots

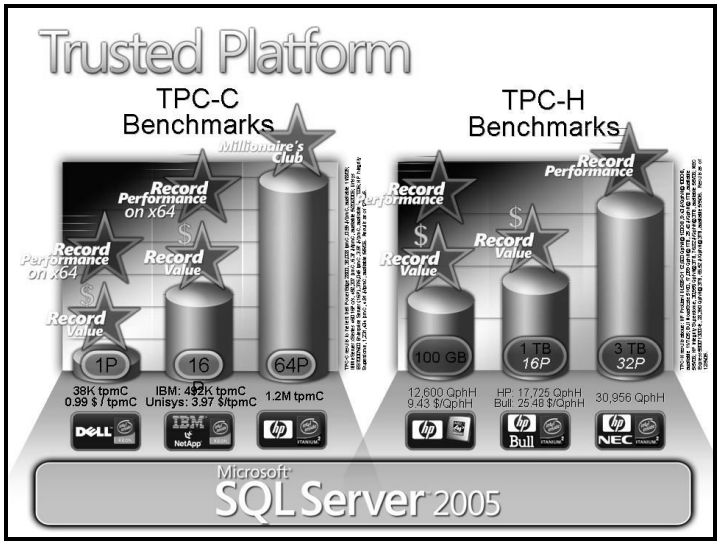
High Throughput Data Access & Large Data Management

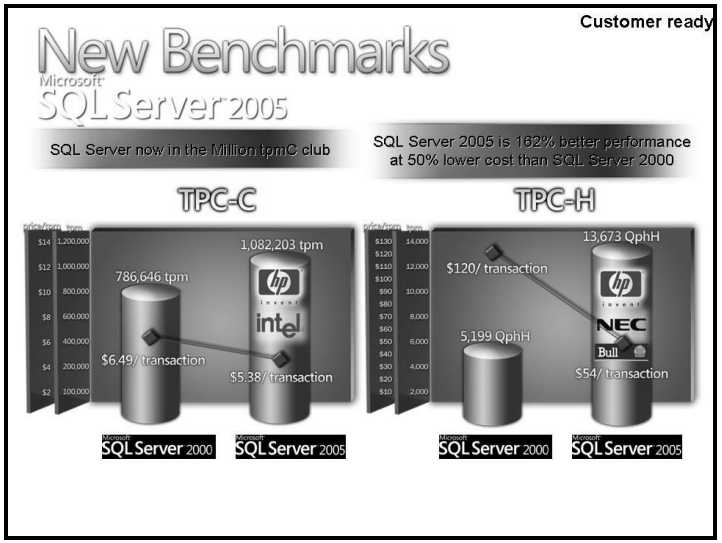
- Snapshot isolation
- Table Partitioning

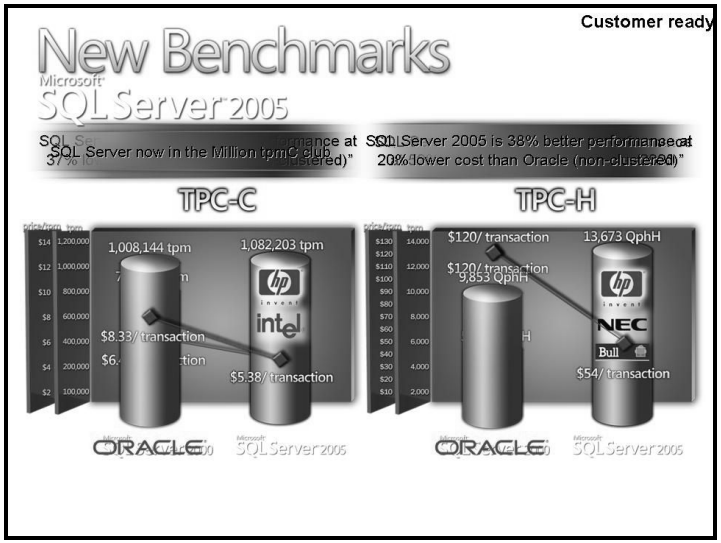
Scalability & Performance

SQL Server 2005 Technology

- Benchmarks
- 64-bit
- NUMA aware SQL 2005
- Concurrency Model
- Query Plans and statistics
- Plan Guides
- Threads and scheduling
- Scale-out solutions



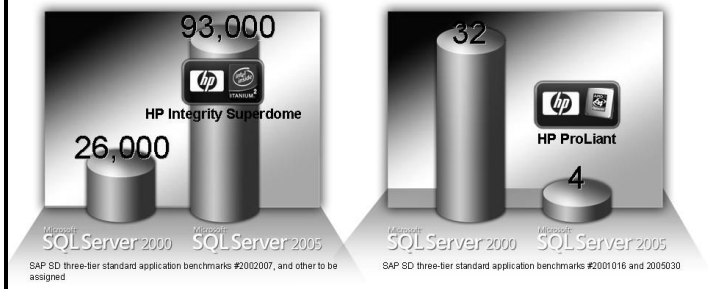




SQL 2005 provides great scalability and outstanding price/performance: 93,000 concurrent users on a 64-proc server (10x the largest SAP customers in the planet), and 18,000 concurrent users on a standard server (only 4 processors!)

3.5X Scalability!
Max number of concurrent users

8X Improvement!
No. of proc for 18,000 concurrent users



SAP SD three-tier standard application benchmarks #2002007, and other to be assigned

SAP SD three-tier standard application benchmarks #2001016 and 2005030

Microsoft SQL Server 2005 – 64 bit

Scalability

- Optimized for Windows Server 2003 including Itanium and X64 (AMD and Intel support)
- Great performance
  - Large memory addressability (up to 16 TB)
  - Nearly unlimited virtual memory (up to 8 TB)
  - I/O savings due to larger memory buffer pools

Manageability

- T-SQL code-compatibility with SQL Server 2000
- 8 node clustering support
- Same on-disk format as 32-bit for easy migration
- One setup for database & OLAP based on Windows Installer technology

Cost Savings

- Compelling alternative to expensive Unix solutions

The highly scalable database platform for memory intensive, performance-critical business applications

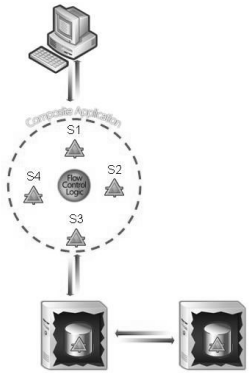
Windows Server 2003

SQL Server 2005 Scale-Out Architectures For High-End Systems

Data Dependent Routing	For distributed, independent databases
P2P Replication	For read-mostly scale-out
Shared Scalable Database	For read-only scale-out
Service Oriented Database Architectures (SODA)	For new SOA based applications

Developer Productivity

Database Development



Integrated with Visual Studio and .NET
- Integrated development & debugging experience
- Execution location & programming language choice

SQL Server Service Broker
- Asynchronous queuing for highly available applications
- Reliable messaging for scale out

CacheSync
- High performance ASP.NET 2.0 apps

XML Data Type
- Native XML support in the DB

SQL Server 2005

Mission Ready Stronger Security

Microsoft SQL Server 2005

Reduced Surface Area
- More installation options
- Explicit feature configuration

Enhanced Data Security
- Native data encryption
- Certificate mgmt infrastructure
- Auditing & authorization
- Password policy enforcement

Configuration Guidance
- Best Practices Analyzer

Secure by
- Design, Default and Deployment

Secure: SQL Server is more secure than Oracle

http://www.secunia.com (Includes both SQL Server and MDAC)

Gartner Research

Publication Date: 23 January 2006 **ID Number: G00137477**

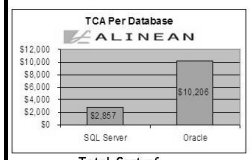
Flaws Show Need to Update Oracle Product Management Practices

Rich Mogull

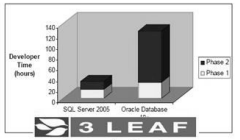
A new set of critical vulnerabilities shows that Oracle can no longer be considered a bastion of security. Database and application managers must begin protecting and maintaining Oracle systems more aggressively.

http://www.gartner.com/resources/137400/137477/flaws_show_need_to_update_or_137477.pdf

SQL Server: Lower Overall TCO than Oracle

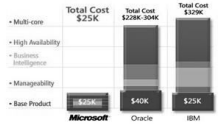


Total Cost of Administration Report



Lower Application Development Cost

Microsoft SQL Server 2005

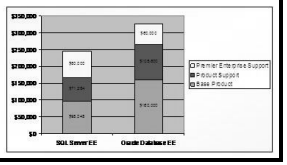


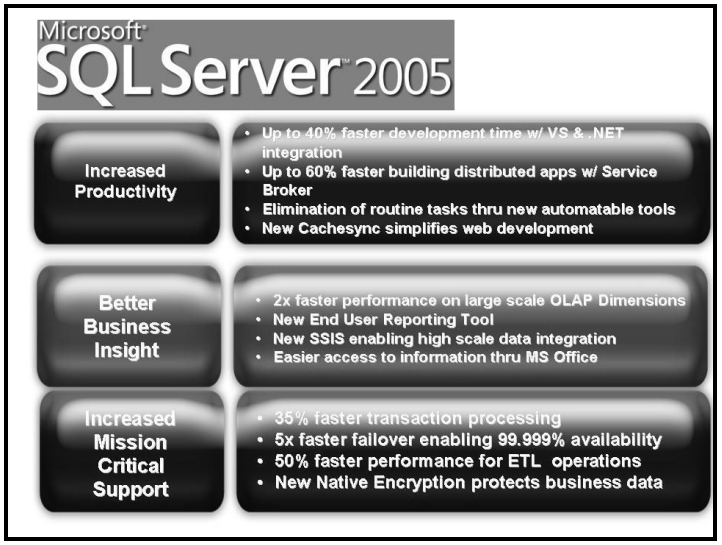
Lower Software License Cost

Lower Hardware Cost

Server Class	Number of CPUs	SQL Server's Best	Oracle's Best	Advantage
Small Servers	1	$0.99	No Result	SQL Server
	2	$1.80	$1.81	SQL Server
	4	$2.04	$3.94	SQL Server
Medium Servers	8	$3.96	$5.26	SQL Server
	16	$3.97	$4.40	SQL Server
High-End Servers	64	$5.52	$8.33	SQL Server

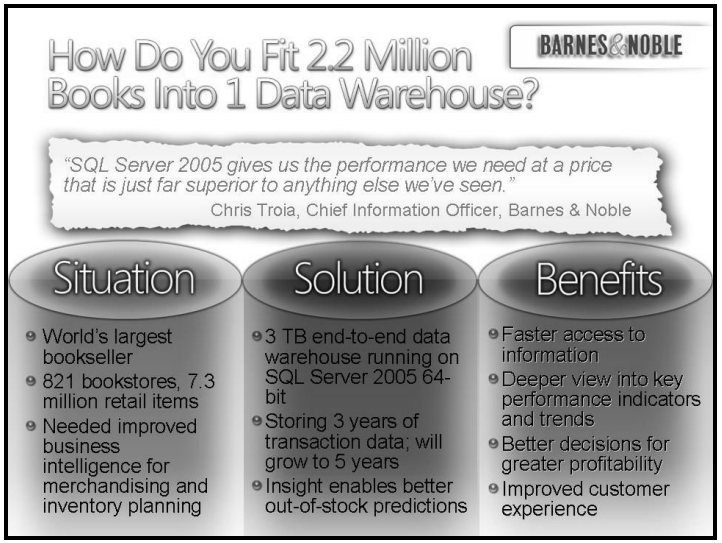
Lower Support Cost

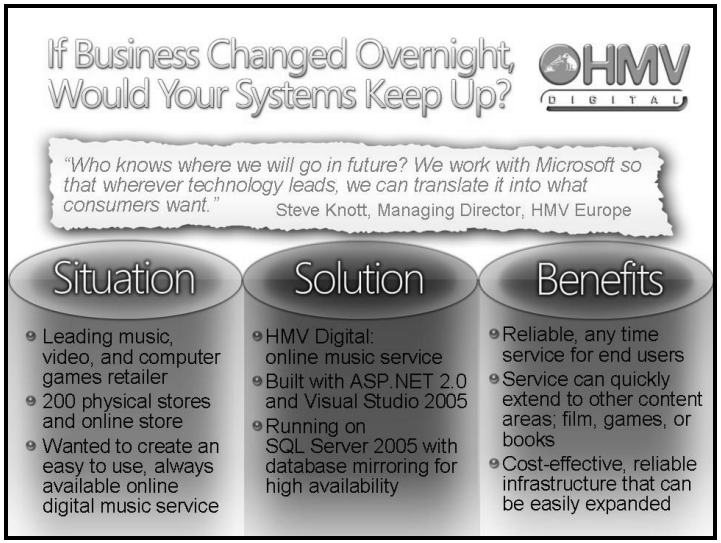


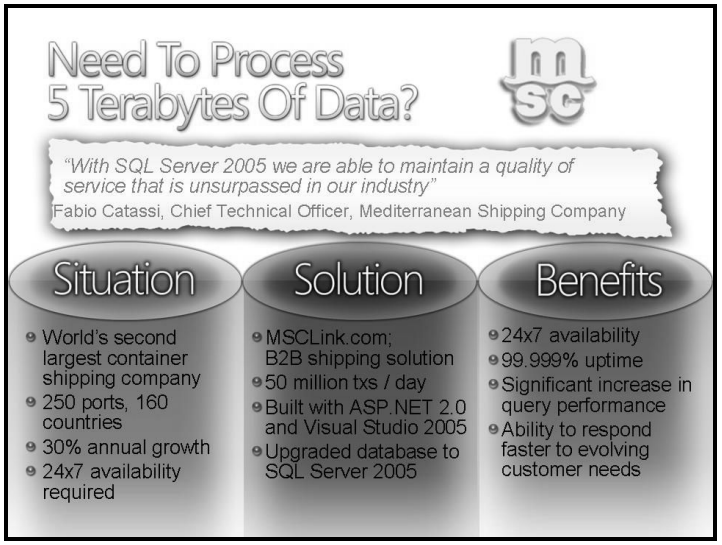


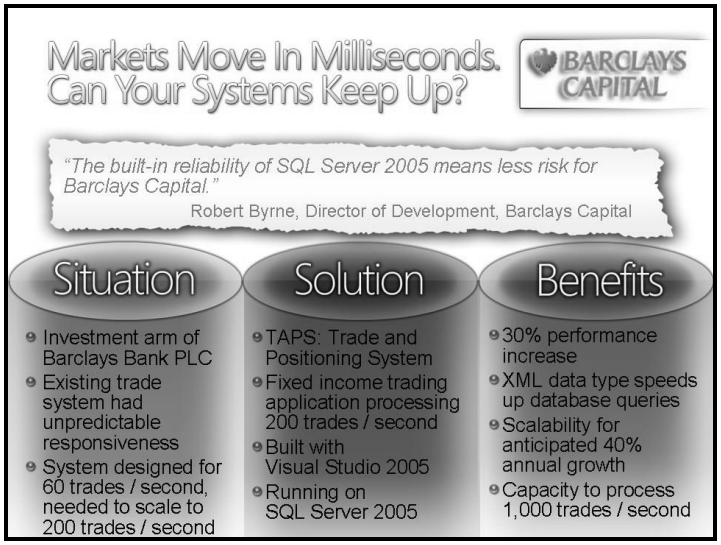
Agenda

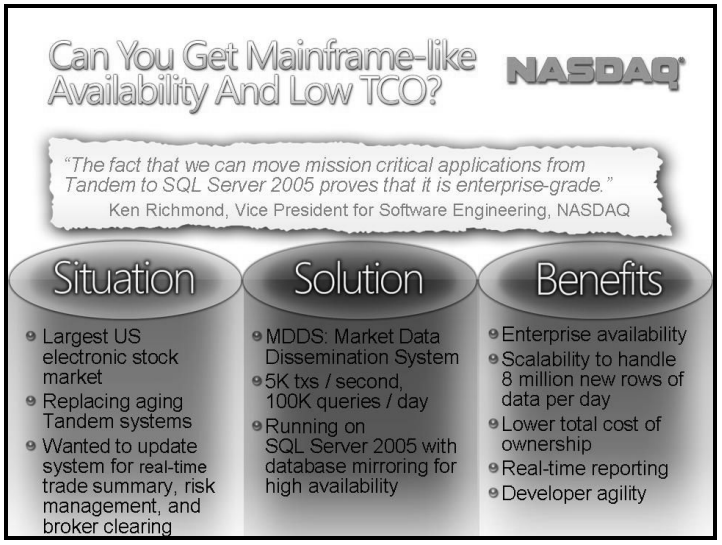
- Microsoft's Relational Database Platform
  - Database Progress with SQL Server 2005
  - Core Abilities – Security, Scalability, Developer Focus
- Microsoft Business Intelligence
  - ETL – SQL Integration Services
  - Reporting – SQL Server Reporting Services
  - Analytics – SQL Server Analysis Services
  - Microsoft Office Business Scorecard Manager 2005
- Open Discussion

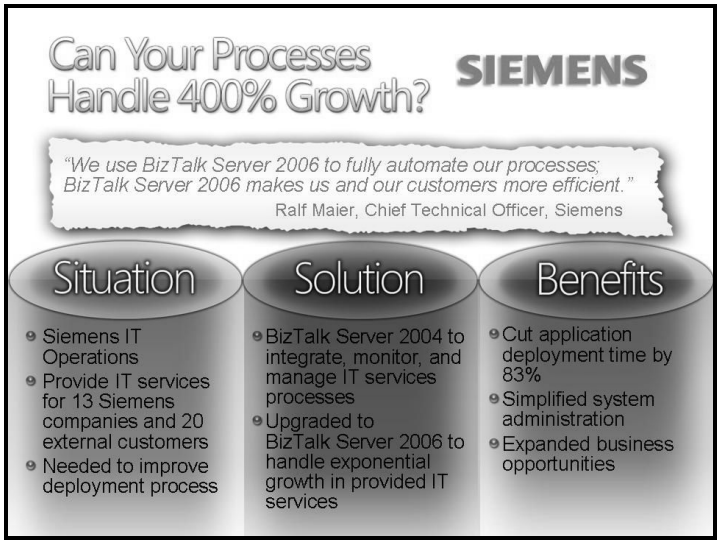


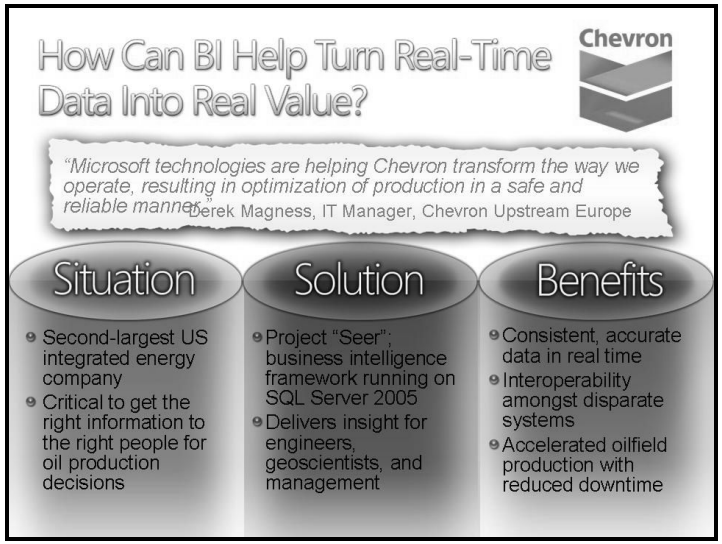



Need To Process 5 Terabytes Of Data?
"With SQL Server 2005 we are able to maintain a quality of service that is unsurpassed in our industry"
Fabio Catassi, Chief Technical Officer, Mediterranean Shipping Company
Situation
World's second largest container shipping company
250 ports, 160 countries
30% annual growth
24x7 availability required
Solution
MSCLink.com; B2B shipping solution
50 million txs / day
Built with ASP.NET 2.0 and Visual Studio 2005
Upgraded database to SQL Server 2005
Benefits
24x7 availability
99.999% uptime
Significant increase in query performance
Ability to respond faster to evolving customer needs


Markets Move In Milliseconds. Can Your Systems Keep Up?
BARCLAYS CAPITAL
"The built-in reliability of SQL Server 2005 means less risk for Barclays Capital."
Robert Byrne, Director of Development, Barclays Capital
Situation
Investment arm of Barclays Bank PLC
Existing trade system had unpredictable responsiveness
System designed for 60 trades / second, needed to scale to 200 trades / second
Solution
TAPS: Trade and Positioning System
Fixed income trading application processing 200 trades / second
Built with Visual Studio 2005
Running on SQL Server 2005
Benefits
30% performance increase
XML data type speeds up database queries
Scalability for anticipated 40% annual growth
Capacity to process 1,000 trades / second


Can You Get Mainframe-like Availability And Low TCO?
NASDAQ
"The fact that we can move mission critical applications from Tandem to SQL Server 2005 proves that it is enterprise-grade."
Ken Richmond, Vice President for Software Engineering, NASDAQ
Situation
Largest US electronic stock market
Replacing aging Tandem systems
Wanted to update system for real-time trade summary, risk management, and broker clearing
Solution
MDDS: Market Data Dissemination System
5K txs / second, 100K queries / day
Running on SQL Server 2005 with database mirroring for high availability
Benefits
Enterprise availability
Scalability to handle 8 million new rows of data per day
Lower total cost of ownership
Real-time reporting
Developer agility


Can Your Processes Handle 400% Growth?
SIEMENS
"We use BizTalk Server 2006 to fully automate our processes; BizTalk Server 2006 makes us and our customers more efficient."
Ralf Maier, Chief Technical Officer, Siemens
Situation
Siemens IT Operations
Provide IT services for 13 Siemens companies and 20 external customers
Needed to improve deployment process
Solution
BizTalk Server 2004 to integrate, monitor, and manage IT services processes
Upgraded to BizTalk Server 2006 to handle exponential growth in provided IT services
Benefits
Cut application deployment time by 83%
Simplified system administration
Expanded business opportunities


How Can BI Help Turn Real-Time Data Into Real Value?
Chevron
"Microsoft technologies are helping Chevron transform the way we operate, resulting in optimization of production in a safe and reliable manner."
Derek Magness, IT Manager, Chevron Upstream Europe
Situation
Second-largest US integrated energy company
Critical to get the right information to the right people for oil production decisions
Solution
Project "Seer"; business intelligence framework running on SQL Server 2005
Delivers insight for engineers, geoscientists, and management
Benefits
Consistent, accurate data in real time
Interoperability amongst disparate systems
Accelerated oilfield production with reduced downtime

Trustworthy Computing

Trustworthy Computing

David Aucsmith
Senior Director
Institute for Advanced Technology in Governments
Microsoft Corporation

Microsoft Institute for Advanced Technology in Governments

Advanced scientific and engineering work for government

Leveraging commercial products, research, and development

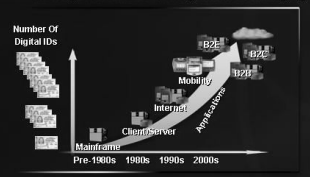
For high impact, rapid implementation

Skunkworks!

2

Threat Trends

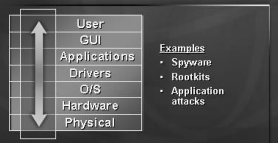
Exponential Growth of IDs
Identity and access management challenging



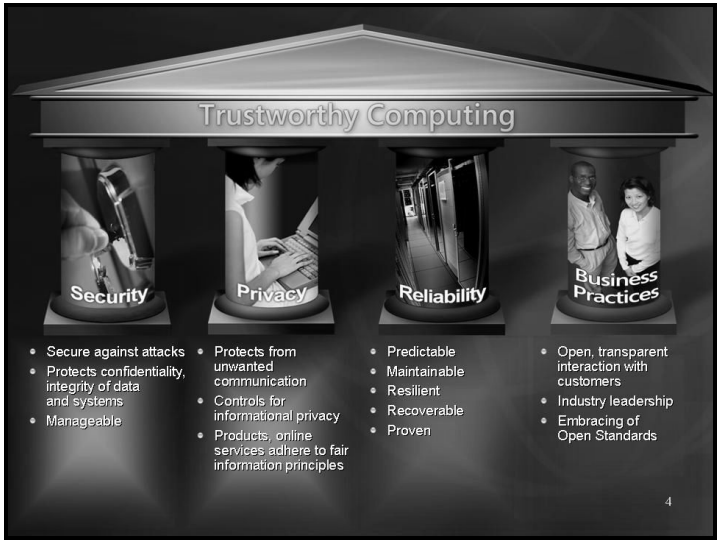
Days From Update To Exploit Decreasing
Updating alone is not sufficient

Organized Crime On The Rise
IP protection is critical

Attacks Getting More Sophisticated
Traditional defenses are inadequate



3



4

Security Focus

Working with government and industry to build a trusted computing platform

Technology Investments

- Excellence in fundamentals
- Security innovations

Prescriptive Guidance

- Scenario-based content and tools
- Authoritative incident response

Industry Partnership

- Awareness and education
- Collaboration and partnership

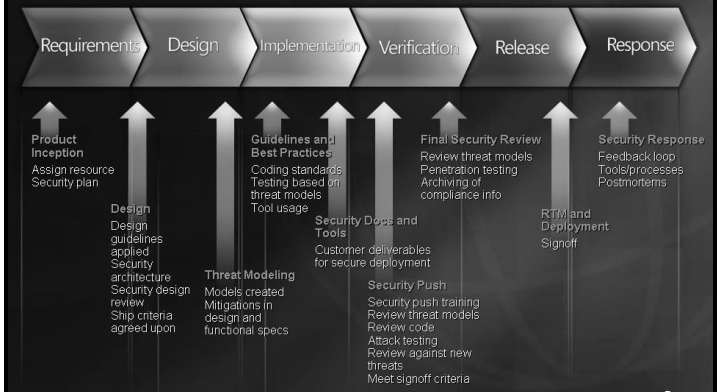
5

Engineering For Security

Secure by Design	• Threat modeling • Code inspection • Penetration testing
Secure by Default	• Unused features off by default • Reduce attack surface area • Least privilege
Secure by Deployment	• Prescriptive guidance • Security tools • Enterprise management
Culture of Security	• Security is a priority • Part of everyone's job • Continuous learning

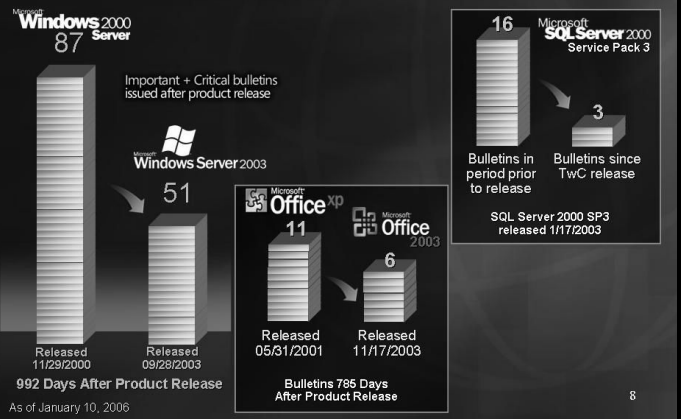
6

Security Development Lifecycle



7

Focus Yielding Results

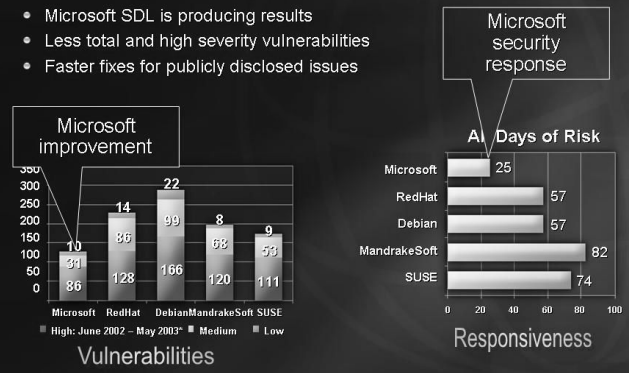


As of January 10, 2006

8

Industry View Of Improvement

- Microsoft SDL is producing results
- Less total and high severity vulnerabilities
- Faster fixes for publicly disclosed issues



Source: "Is Windows More Secure than Linux?", Forrester, March 2004
NIST: US National Institutes of Standards and Technology

Security Progress

Windows XP Service Pack 2
- More than 260 million copies distributed
- 15 times less likely to be infected by malware
- Significantly fewer important and critical vulnerabilities

Windows Server 2003 Service Pack 1
- Security configuration wizard
- More secure by design; more secure by default
- More than 4.5 million downloads

Microsoft Windows Antispyware Beta
- Most popular download in Microsoft history
- Helps protect more than 25 million customers
- Great feedback from SpyNet participants

Microsoft Windows Malicious Software Removal Tool
- 2B total executions; 200M per month
- Focus on most prevalent malware
- Dramatically reduced the # of Bot infections

As of January 10, 2006

Windows Defender

Microsoft Windows AntiSpyware

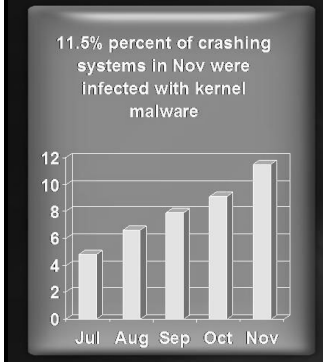
Helps protect Windows users from spyware and other potentially unwanted software

Detect and remove spyware
- 17 million downloads, 23 million spyware packages cleaned
- Scheduled scans help maintain PC security and privacy

Improve Internet browsing safety
- Continuous protection guards 50+ ways spyware gets on a PC
- Intelligent alerts handle spyware based on your preferences

Stop the latest threats
- Global SpyNet™ community helps identify new spyware
- Automatic signature downloads keep you up-to-date

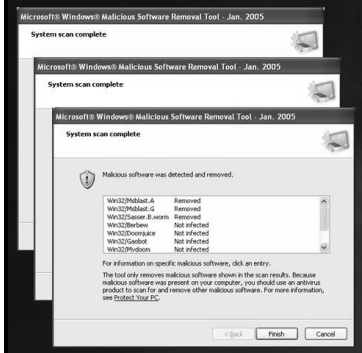
Kernel Malware Growing



- OCA warns customers about 15 malware families (sets of drivers with related technology)
- Over 50 suspicious drivers are under investigation
- Drivers are added to the suspicious list via several heuristics
  - Driver has modified the kernel and is not mapped to any known commercial organization
    - Hooked system service table
    - Hooked interrupt dispatch table
    - Modified kernel to call driver
  - Driver has common linker timestamp and size but more than 100 different file names

Malicious Software Removal

Complements traditional Antivirus technologies by providing one tool that removes prevalent viruses and worms from a PC

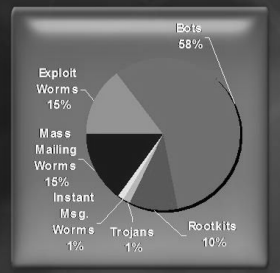


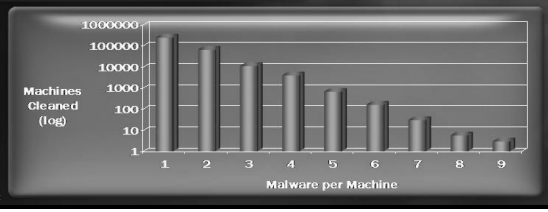
- Updated monthly to remove prevalent malware
- Targeted at consumers without antivirus
- Enterprise deployable as part of a defense-in-depth strategy
- Available through:
  - Windows Update
  - Auto Update
  - Online interface
  - MS Download Center

13

Cleaner Statistics

Release	Days Live	Executions	Disinfections	
			Value	%
January	28	124,613,632	239,197	0.1920%
February	28	118,209,670	351,135	0.2970%
March	35	145,502,003	443,661	0.3049%
April	28	125,150,400	590,714	0.4720%
May	35	164,283,730	1,154,345	0.7027%
June	28	162,763,946	642,955	0.3950%
...	...	...	...	...
Total	362	1,804,565,652	8,679,656	0.481%





Source: Microsoft

14

15

Windows Vista

Delivering Business Value

Infrastructure Optimization

Stream[illegible] desktop deployment and management[illegible] cost and complexity

Empowered Professional

Enable faster, more informed business decisions with smart tools to find and organize data

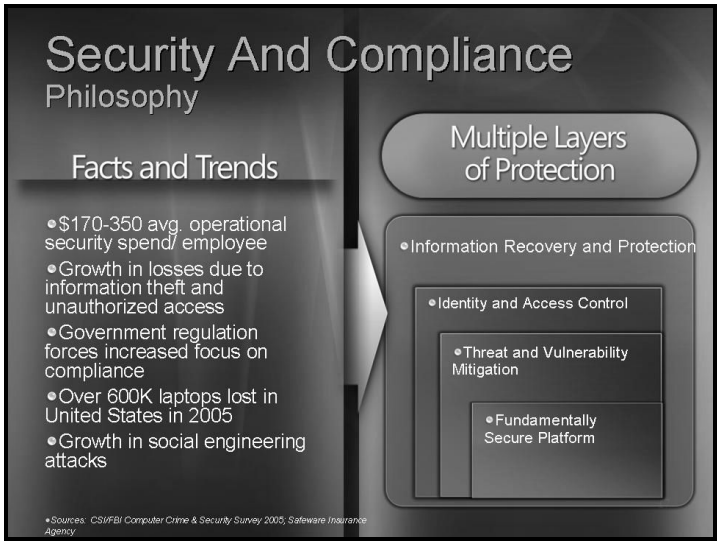
Security and Compliance

Reduce security risks, protect confidential data and simplify[illegible] compliance

Enabling Virtual Workforce

Ensure easy, secure connectivity to information, network[illegible] for your mobile users

16


Security And Compliance
Philosophy
Facts and Trends
•$170-350 avg. operational security spend/ employee
•Growth in losses due to information theft and unauthorized access
•Government regulation forces increased focus on compliance
•Over 600K laptops lost in United States in 2005
•Growth in social engineering attacks
•Sources: CSI/FBI Computer Crime & Security Survey 2005, Safeware Insurance Agency
Multiple Layers of Protection
•Information Recovery and Protection
•Identity and Access Control
•Threat and Vulnerability Mitigation
•Fundamentally Secure Platform


Fundamentals
•Security development lifecycle
•Threat modeling and code reviews
•Government and standard bodies certification
Threat and Vulnerability Mitigation
•Internet Explorer Protected Mode; Anti-phishing
•Windows Defender
•Windows Service Hardening
Security and Compliance
Identity and Access Control
•User Account Control
•Strong User Authentication
•Granular Auditing for Security Events
Information Protection
•BitLocker™ Drive Encryption
•EFS Smartcards; RMS Client
•Control over Removable Devices
18


Fundamentals
• Improved Security Development Lifecycle (SDL) process for Windows Vista
• Periodic mandatory security training
• Assignment of security advisors for all components
• Threat modeling as part of design phase
• Security reviews and testing built into the schedule
• Security metrics for product teams
• Common Criteria (CC) Certification
19


Threat And Vulnerability Mitigation
Protect against malware and intrusions

Windows Service Hardening
Defense in depth

- Services run with reduced privilege compared to Windows XP
- Windows services are profiled for allowed actions to the network, file system, and registry
- Designed to block attempts by malicious software to make a Windows service write to an area of the network, file system, or registry that isn't part of that service's profile

21

Windows XP SP2 to Windows Vista Service Changes

Windows XP SP2		
LocalSystem	Wireless Configuration System Event Notification Network Connections (netman) COM+ Event System NLA Rasauto Shell Hardware Detection Themes Telephony Windows Audio Error Reporting Workstation ICS	RemoteAccess DHCP Client W32time Rasman browser 6to4 Help and support Task scheduler TrkWks Cryptographic Services Removable Storage WMI Perf Adapter Automatic updates WMI App Management Secondary Logon BITS
Network Service	DNS Client	
Local Service	SSDP WebClient TCP/IP NetBIOS helper Remote registry	

Windows Vista		
LocalSystem *Firewall Restricted*	WMI Perf Adapter Automatic updates Secondary Logon	App Management Wireless Configuration
LocalSystem	BITS Themes Rasman TrkWks Error Reporting	6to4 Task scheduler RemoteAccess Rasauto WMI
Network Service *Fully Restricted*	DNS Client ICS DHCP Client	browser Server W32time
Network Service *Network Restricted*	Cryptographic Services Telephony	PolicyAgent Nlasvc
Local Service *No Network Access*	System Event Notification Network Connections Shell Hardware Detection	COM+ Event System
Local Service *Fully Restricted*	Windows Audio TCP/IP NetBIOS helper WebClient SSDP	Event Log Workstation Remote registry

22

Internet Explorer 7

Social Engineering Protections

- Phishing Filter and Colored Address Bar
- Dangerous Settings Notification
- Secure defaults for IDN

Protection from Exploits

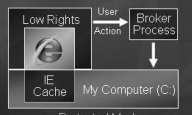
- Unified URL Parsing
- Code quality improvements (SDLC)
- ActiveX Opt-in
- Protected Mode to prevent malicious software

23

ActiveX Opt-in And Protected Mode
Defending systems from malicious attack

- ActiveX Opt-in puts users in control
- Reduces attack surface
- Previously unused controls disabled
- Retain ActiveX benefits, increase user security
- Protected Mode reduces severity of threats
- Eliminates silent malware install
- IE process 'sandboxed' to protect OS
- Designed for security and compatibility

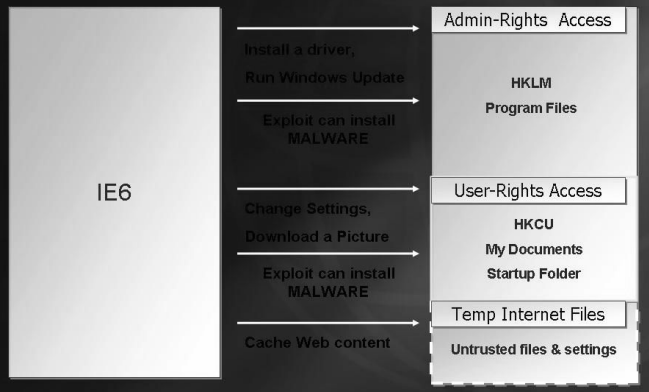
ActiveX Opt-in



Protected Mode

24

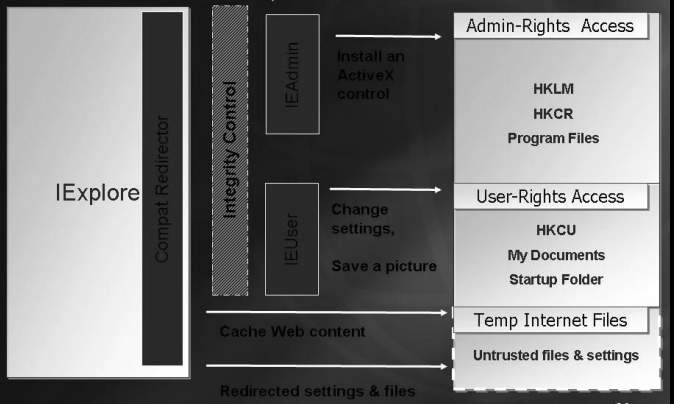
IE6 running with Admin Rights



25

Advanced Malware Protection

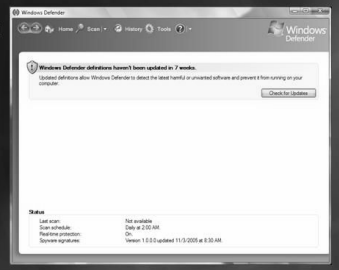
Protected Mode IE, UAC contain threats



26

Windows Defender

- Improved Detection and Removal
- Redesigned and Simplified User Interface
- Protection for all users



27

Windows Vista Firewall

- Combined firewall and IPsec management
  - New management tools – Windows Firewall with Advanced Security MMC snap-in
  - Reduces conflicts and coordination overhead between technologies
- Firewall rules become more intelligent
  - Specify security requirements such as authentication and encryption
  - Specify Active Directory computer or user groups
- Outbound filtering
  - Enterprise management feature – not for consumers
- Simplified protection policy reduces management overhead

28

Identity And Access Control

Enable Secure Access to Information

Challenges

- Users running as admin = unmanaged desktops
  - Viruses and Spyware can damage the system when run with elevated privileges
  - Enterprise users running elevated privileges can compromise the corporation
  - Users can make changes that require re-imaging the machine to undo
- Line of Business (LoB) applications require elevated privileges to run
  - System security must be relaxed to run the LoB application
  - IT Administrators must reevaluate the LoB applications for each Operating System release due to inconsistent configuration settings
- Common Operating System Configuration tasks require elevated privilege
  - Corporations can't easily deploy applications unless they compromise Operating System Security
  - Simple scenarios like changing the time zone don't work
  - Users are not able to manage non-sensitive account information

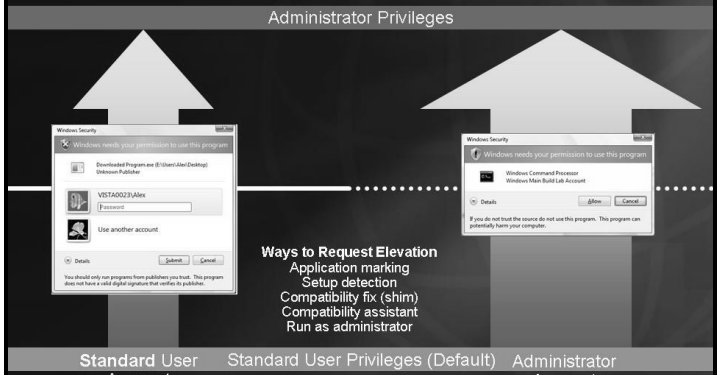
30

User Account Control

- Goal: Allow businesses to move to a better-managed desktop and consumers to use parental controls
  - Make the system work well for standard users
    - Allow standard users to change time zone and power management settings, add printers, and connect to secure wireless networks
    - High application compatibility
    - Make it clear when elevation to admin is required and allow that to happen in-place without logging off
    - High application compatibility with file/registry virtualization
  - Administrators use full privilege only for administrative tasks or applications
  - User provides explicit consent before using elevated privilege

31

User Account Control Elevation



32

Authentication Improvements

- Plug and Play Smart Cards
  - Drivers and Certificate Service Provider (CSP) included in Windows Vista
  - Login and credential prompts for User Account Control all support Smart Cards
- New logon architecture
  - GINA (the old Windows logon model) is gone.
  - Third parties can add biometrics, one-time password tokens, and other authentication methods to Windows with much less coding

33

Improved Auditing

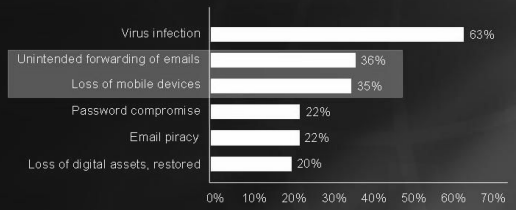
- More Granularity
  - Support for many auditing subcategories: Logon, logoff, file system access, registry access, use of administrative privilege
  - Previous versions of Windows only support high-level categories such as System, Logon/Logoff, and Object Access, with little granularity
- New Logging Infrastructure
  - Easier to filter out "noise" in logs and find the event you're looking for
  - Tasks tied to events: When an event occurs, such as administrative privilege use, tasks such as sending an Email to an auditor can run automatically

34

Information Protection

Protect Corporate Intellectual Property and Customer Data

Information Leakage Is Top-of-mind With Business Decision Makers



"After virus infections, businesses report unintended forwarding of e-mails and loss of mobile devices more frequently than they do any other security breach"

Jupiter Research Report, 2004

36

Windows Vista Information Protection

Who are you protecting against?

- Other users or administrators on the machine? EFS
- Unauthorized users with physical access? BitLocker™

Scenarios	BitLocker	EFS	RMS
Laptops	●		
Branch office server	●		
Local *single-user* file & folder protection	●		
Local *multi-user* file & folder protection		●	
Remote file & folder protection		●	
Untrusted network admin		●	
Remote document policy enforcement			●

Some cases can result in overlap. (e.g. Multi-user roaming laptops with untrusted network admins)

37

Group Policy For Device Installation

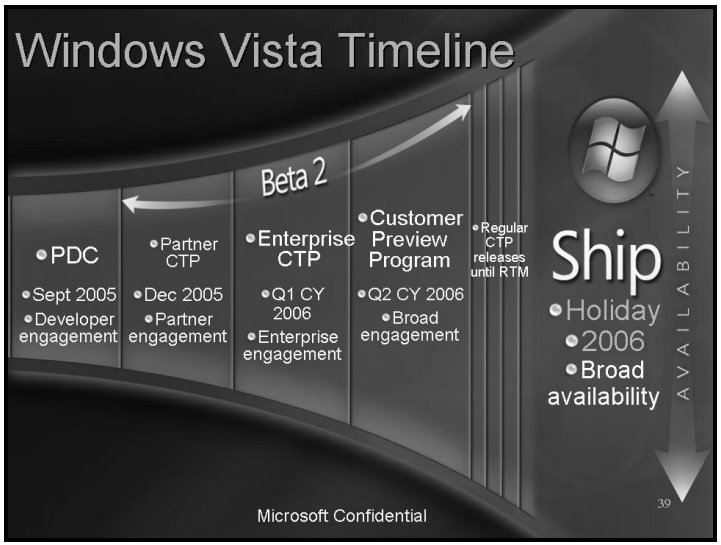
Addressing Compliance Concerns Over USB Flash Devices

Options

- Block installation of removable storage devices
- Block all device installations by end user
- Block all except specified device classes
- Block all except specified device IDs
- Block all except signed drivers
- Allow all except specific device classes
- Allow all except specific device IDs

38

Windows Vista Timeline



Microsoft Confidential

39

Windows Vista Security Summary

40

參考資料三

NIST 800-95，Guide to Secure Web Services, Draft

NIST is pleased to announce the public comment release of draft Special Publication (SP) 800-95, *Guide to Secure Web Services*. SP 800-95 provides detailed information on standards for Web services security. This document explains the security features of Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), the Universal Description, Discovery and Integration (UDDI) protocol, and related open standards in the area of Web services. It also provides specific recommendations to ensure the security of Web services-based applications.

Table of Contents

List of Figures

List of Tables