政府組織的軟體安全建置

應用軟體被攻擊的比例與日俱增，美國政府現在對於軟體開發方面，不僅需要「從開始發展軟體就注意安全」的文化，還需關注更多元的層面.....

介紹

美國政府選出第一個國家首席技術官(CTO)，在此刻這是個正確的抉擇。美國政府開始意識到需採取系統化與全面的方法來確保軟體安全。不僅可以藉由僱用合適的人、發展統一的軟體安全標準，並通過實施軟體安全保證（SSA）等前導計劃，引導商業機構以及美國空軍可以一起實行，但直至今日，美國政府似乎還未就緒。

承諾實施 SSA 的全球私人組織可以藉由提升開發、採購以及訓練水準的方式來實證。這像是什麼呢？Fortify 與 Cigital 組織一起推動由全球頂尖的資安公司正在實施的 110 種最佳實務之「建立安全成熟度模型(BSIMM)」等相關活動。

美國政府是軟體產業最大的生產者和最大的消費者，而且很少有私人機構有能力對付恐怖組織/國家層級的駭客襲擊。聯邦與州政府獲取軟體的方式很多元 - 自行開發、簽約開發以及採買現成的商用軟體（COTS），甚至是上述方法的所衍生的其他方式。他們通常遵循著鬆散的原則、或任意的標準、或甚至根本並未遵循。而 IT 人員僅以傳統的方式在網路邊界進行防禦，有時候還忽略了來自網際網路之應用軟體層的威脅。不過，這是一種基本的心態的問題：消極反應與積極行動的對比。假使在軟體或系統未被入侵時，或許這都不會有什麼問題，但這種思維不僅是有問題的，而且非常危險。

軟體在美國政府基礎設施的各方面元件都是非常重要的。聯邦政府組織管理不同的關鍵系統，像聯邦稅務系統、航空交通管制、社會保障援助金...以及其它更多的重要系統。因此，聯邦政府必須簽約客製或採購開發各種特殊的軟體，某些軟體已是用很久前的語言，像 COBOL 語言開發的，而且有些開發方式還是很困難或根本很難去測試它的安全威脅問題。若想移植這些系統到新的安全軟體平台，將花費極高的成本代價，因此這些舊型的應用軟體通常比預期用得還要久。

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461 台北市中山區德惠街 9 號 5 樓　TEL：(02)2586-7890　FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 315 號 13 樓之 3　TEL：(07)586-6195
海外據點：上海、北京、東京　www.gss.com.tw

很不幸地，愈來愈多的國家與犯罪駭客組織已利用網路來攻擊他國，一個最重要的原因是該系統與金錢、個人資料或有價值的智慧財產權有關。2002 年，一系列被稱為" Titan Rain"的攻擊被導向美國國防部。2006 年，又出現一個針對美國羅德島紐玻特城的海軍作戰學院的攻擊。2007 年也出現一系列針對五角大廈類似的攻擊，還一度造成網路中斷。近年來針對應用程式層的攻擊急劇增加，美國空軍在近兩年不到的時間被從軟體層攻擊的百分比從原本的百分之 2 升高至 33 了。

政府及私人機構的案例

如果軟體從一開始就安全，軟體的保安措施就會更容易。這聽起來也許像天方夜譚，但卻是可以做得到的。例如：銀行在商用作業系統上，透過各家銀行不同的系統執行著上兆美元的交易。負責管理銀行網路安全的美國聯邦金融機構檢查委員會(FFIEC)，列出了一些強化系統的必要步驟，例如：關閉一些不需要的特定功能。此外，美國財政部貨幣監理辦公室也指出金融機構必須執行的軟體風險評估措施，國家信用管理局也建議其成員可以採取七類從軟體到實體安全的一些指引措施。

由超過500家金融服務相關、安全與個別銀行所組成的信用卡產業(PCI)，要求其成員遵循12個步驟 - 包含了原始碼審查(Code Review)、滲透測試以及限制員工存取持卡人的資料，而其下游的零售業者若要符合PCI規範也要依照此規則進行。

北美電力可靠度公司(NERC)也提供成員關於如何抵擋實體與網路威脅的安全指引，這些章節包含了遠端存取硬體、員工背景篩選以及事件回應與復原等規範。

在2009年初期，SANS組織與MITRE聯合發表了前25大的程式設計錯誤問題(Top 25 Coding Error)，這個部份提供給其他組織一個很好開始，去理解軟體常犯的一些錯誤。同樣來自SANS組織所提供的共識稽核指南(Consensus Audit Guidelines)可用來協助其他組織符合2002年的FISMA法案；換言之，CAG 可以協助組織對抗不好的軟體問題，但是卻很少著墨於底層的問題。

當微軟(Microsoft)在2002年成立信賴運算計劃(Trustworthy Computing Initiative)時，其內部就開始運作安全軟體開發生命週期(SSDL)流程，並持續很多年。這個流程已經產生了許多升級至Windows Vista/Windows Server2003/Windows 7與Windows 2008等軟體在安全、隱私以及可靠度方面有形的效益。這樣的微軟SSDL流程其實與Adobe、DTCC、EMC、Google、QUALCOMM與Wells Fargo公司所使用的流程是很相似的。最近在Fortify與Cigital的研究人員所提出的理論 - Building Security in Maturity Model也是同樣可以評估軟體安全成熟度的一種開放方法之理論。

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461 台北市中山區德惠街 9 號 5 樓　TEL：(02)2586-7890　FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 315 號 13 樓之 3　TEL：(07)586-6195
海外據點：上海、北京、東京　www.gss.com.tw

美國政府機關的案例

政府機關有其自身的軟體安全指引。跨所有聯邦機構的依據其實就是國土安全部(Department of Homeland Security)國家網路安全辦公室（National Cyber Security Division）的軟體保證計劃的軟體開發與採購的標準－此標準可用來減少與降低軟體的安全弱點，與提升軟體開發與佈署方面的品質。同時，國家標準與技術中心(NIST)提供一種被DHS與其它單位使用作為開發度量的SSA技術之專案計劃「軟體保證度量與工具評估(SAMATE)」。

某些州政府已依據上述標準著手進行屬於自己的SSA，例如：所有州政府使用的應用程式的Alabama標準、加州針對所有電子投票系統的標準、華盛頓州針對所有Web應用程式標準以及在維吉尼亞州有著更多普遍性的資訊科技的標準。

通常SSA專屬於單一機構，例如：加州的健康服務部(Department of Health Services)、密西根州的勞動力發展與退休管理(Workforce Development and Retirement Administration)以及馬里蘭州交通運輸部(Department of Transportation)。以聯邦政府層級來看，美國健康和社會福利部門醫療保險與醫療輔助計劃服務中心提供可足夠作為CMS應用系統的需求。而在內部收入服務單位它的手冊也提供了IRS應用系統開發的指引。並且在其能源部門裡未分類之資訊系統安全控制手冊裡，也勾勒出結構化與安全程式碼審核的流程。甚至在美國陸軍司令部通信電子資訊處也擁有獨立的軟體品質保證實驗室(SWAL)的需求。

美國空軍應用軟體卓越保證中心(ASACoE)的SSDL正雄心勃勃地展開中。其軟體由主從架構(Client-Server)轉換至Web-based的軟體，ASACoE正在找尋強化其安全與可靠度的方法。從2007年建立至今，ASACoE正在思考一種可以提升安全嚴重等級與改變網路威脅本質的主動回應方案。

建議

為了減輕未來的軟體安全威脅，聯邦政府和各個機構需要按照美國空軍的例子，積極主動進行SSA活動。新的CTO必須要求所有的政府單位把安全優先建立至軟體流程內部，而不是把它擱在一邊。這種新的「安全文化」應該全面考慮簽約開發、委外開發、SaaS、開放源碼以及內部自行開發的軟體，並且，它必須重新配置資源，甚至是必須以新的思維來進行。

此外，組織必須：

- **為了安全有效地組織任命底下三種角色人員：**
  - 領導者(Leader)：組織中需有人負責整體資安流程，從供應商合約的法律角度到員工的教育訓練、到軟體弱點之評估。
  - 專家(Expert)：組織內應該指派一位直接負責安全流程、技術與人事方面的軟體安全的專業人員。
  - 把關人員：組織內也應該指派一位安全專家來識別以風險為基礎的安全流程以及預期的弱點衡量指

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461 台北市中山區德惠街 9 號 5 樓　TEL：(02)2586-7890　FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 315 號 13 樓之 3　TEL：(07)586-6195
海外據點：上海、北京、東京　www.gss.com.tw

標，然後檢驗並使其符合軟體安全標準。把關人員將設立、維護與監督安全衡量指標並且產生符合法規標準之報告，特別是從未修正的安全問題。組織應授權這位把關人有權暫停未符合安全標準的產品或產出之上線或交付。

- **實施預防式而非運營型的安全標準**：組織不應只是單單讓使用軟體方面符合標準而已，應該還必須將開發或取得新軟體的過程納入標準。既有的州立、聯邦或非官方的指引應該被統一，最好能將基準做法提供為參考。
- **定義取得安全軟體的流程：**不僅是挑選作業平台或是軟體在組織內的角色而已，應該還要關心採購的第三方軟體、簽約取得或是開放源碼的軟體，這些都需要經過嚴格的安全審查。第三方軟體廠商應該闡明他們的開發人員在軟體安全方面盡了什麼努力。廠商應該接受簽約以示負責。開放原始碼的專案不應該變成一個預設的選項 - 只因它成本低廉 - 但便宜並未能使它降低風險。
- **進行全面的教育訓練：**組織應規劃舉辦可以強化專案經理與開發人員瞭解軟體安全、以及讓開發人員可實施最佳安全實踐之相關程式語言的訓練課程。教育訓練是可以解決在軟體開發過程的所有階段中的安全問題之重要關鍵，以及組織應該訓練軟體開發經理瞭解衡量指標的意義。訓練開發人員如何修復問題，以及要求所有人員理解安全需求。
- **舊型系統(legacy systems)問題處置：**組織也應該進行舊型系統的安全問題之處置活動，或者用更安全的程式碼（語言）來取代。

更多的相關資源

1 http://www.ffiec.gov/ffiecinfobase/booklets/information_security/04_05_systems.htm
2 http://www.occ.treas.gov/ftp/bulletin/2008-16.html
3 http://www.ncua.gov/corporatecu/corpletters/2004/2004-03.pdf.
4 https://www.pcisecuritystandards.org/
5 http://www.nerc.com/page.php?cid=6|69.
6 http://cwe.mitre.org/top25/
7 http://www.sans.org/cag/
8 http://www.microsoft.com/mscorp/twc/default.mspx
9 http://bsi-mm.com/
10 http://www.dhs.gov/xabout/structure/editorial_0839.shtm
11 http://samate.nist.gov/index.php/SAMATE_About.html
12 http://isd.alabama.gov/policies/new_format/Policies/Policy_660-03_Appl_Secy_Testing.pdf
13 http://www.sos.ca.gov/elections/vs_conditions.htm
14 http://isb.wa.gov/tools/webguide/testing.aspx
15 http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/IT_Security_Standard_SEC501_01.pdf
16 https://www.vita.virginia.gov/uploadedFiles/Library/PSGs/ITSecurity_Standard_501_01.pdf
17 http://www.dhcs.ca.gov/provgovpart/rfa_rfp/peap/Documents/DHCSCDHSWebApplicationArchitectureV5.pdf

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461 台北市中山區德惠街 9 號 5 樓　TEL：(02)2586-7890　FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 315 號 13 樓之 3　TEL：(07)586-6195
海外據點：上海、北京、東京　www.gss.com.tw

18 http://www.michigan.gov/documents/Attachment_1_Bus_Req_169789_7.doc
19 http://doit.maryland.gov/contracts/Documents/cats_torfp_status/torfpwebsptservices42606.pdf
20 http://www.cms.hhs.gov/InformationSecurity/Downloads/test_approach.pdf
21 http://www.cms.hhs.gov/transmittals/downloads/R9SS.pdf
22 http://www.irs.gov/irm/part10/index.html/
23 http://www.directives.doe.gov/pdfs/doe/doetext/neword/205/m2051-7.pdf
24 http://www.sec.army.mil/secweb/facilities_labs/swal.php
25 http://www.hanscom.af.mil/news/story.asp?id=123076592

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461 台北市中山區德惠街 9 號 5 樓 TEL：(02)2586-7890 FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 315 號 13 樓之 3 TEL：(07)586-6195
海外據點：上海、北京、東京 www.gss.com.tw