

開放源碼保安

2008 年 2 月

© 香港特別行政區政府

這份文件的內容為香港特別行政區政府的財產，未經香港特別行政區政府的明文批准，不得轉載全部或部份文件內容。

免責聲明：政府盡力確保本文資料準確，但不明示或隱含保證資料準確無誤。對於因使用本文資料而引致或與之有關的任何錯誤或遺漏，香港特別行政區政府概不承擔任何法律責任。

目錄

摘要.....	2
I. 介紹.....	3
何謂開放源碼軟件？	3
開放源碼軟件之使用趨勢	3
開放源碼與商業軟件的比較	3
II. 使用開放源碼軟件作為保安工具	5
III. 開放源碼系統之軟件保安	6
IV. 如何在機構內安全地使用開放源碼產品	7
V. 結論.....	8

摘要

有人認為開放源碼軟件在本質上，通常較封閉式源碼軟件或專利軟件更加安全，也有人持相反意見，兩方意見持續爭辯著。原始碼的開放提供機會給攻擊者和防衛者去讀取詳細編碼，並分析軟件保安漏洞。

另一方面，封閉式源碼軟件迫使用戶只接受供應商選擇提供的保安水平。本文討論如何從開放源碼軟件得到關於資訊科技保安的優勢，此外，也將列出幾項由開放源碼用戶社群推薦之開放源碼保安的最佳作業實務，並指出在機構內安全地使用開放源碼產品應注意的重點。

I. 介紹

何謂開放源碼軟件？

開放源碼軟件通常指的是軟件的原始碼是開放的，准許任何人讀取、使用和改寫。根據開放源碼促進會（Open Source Initiative）¹的說法，「開放源碼軟件」這個專有名詞必須符合該促進會訂出的十項標準²，其中頭三項簡述如下：

1. 可自由地不斷散佈該軟件
2. 可散佈軟件的原始碼和編譯版本
3. 其執照（license）准許修改原始碼和由原始碼衍生而出的程式

符合該促進會的軟件執照名單可在 [Opensource.org](http://opensource.org)³網站中找到，幾個範例包括 Apache Software License、GNU General Public License（GPL）、IBMPublic License 和 Microsoft Public License（MS-PL）。

「免費軟件」（Freeware）此專有名詞指的是不用成本便可使用的軟件，開放源碼軟件在本質上是免費軟件，但是免費軟件並非必然准許大眾使用其原始碼。

開放源碼軟件之使用趨勢

近來開放源碼軟件已漸漸獲得接受，即使是企業營運下的環境也接受這趨勢，在 2006 年時，Unisys 預測開放源碼軟件將會持續獲得企業客戶的接受，企業客戶可把這些軟件作為部署企業應用程式的工具，並將驅使企業成長和進行低交易成本的革新⁴。

在歐洲，有人認為開放源碼是改善 ICT 業界競爭力的工具⁵。事實上，早在 2005 年便有報告指出將近一半的歐洲當地政府機構已使用開放源碼軟件⁶。

開放源碼與商業軟件的比較

開放源碼和商業軟件最明顯的差別就是可否檢視原始碼，因開放源碼軟件的原始碼是開放給社會大眾的，基本上可免費使用。基於經濟上的原因，許多小型和中型規模的企業

¹ <http://opensource.org/>

² <http://opensource.org/docs/osd>

³ <http://opensource.org/licenses>

⁴ http://www.unisys.com/about__unisys/news_a_events/11288732.htm

⁵ <http://blogs.the451group.com/opensource/2007/11/22/europes-open-source-opportunity/>

⁶ http://www.theregister.co.uk/2005/10/21/opensource_government/

已選擇或正考慮選擇使用開放源碼軟件。

有人認為開放源碼免費和開放的特性對於軟件保安有幫助，因社群之間對原始碼的檢查可快速地找出軟件錯誤（bugs）或保安漏洞，但並非所有人皆同意此論點。

商業軟件大部份是封閉源碼，表示原始碼並非開放給大眾。因為不開放原始碼，攻擊者便需通過重重關卡以取得編碼，即使漏洞的確存在，利用原始碼保安漏洞來攻擊的可能性也較低。然而，並非所有人皆同意此說法，因為尚未報告或尚未確認的錯誤（bugs）並不代表該程式毫無缺點。

到底開放源碼保安比較好，還是封閉源碼保安比較好，現在尚未得到一致性的結論。兩方的論點皆頗具說服力⁷，有人預期該爭論將會持續一段時間。

⁷ <http://www.acmqueue.com/modules.php?name=Content&pa=showpage&pid=453>

II. 使用開放源碼軟件作為保安工具

開放源碼用戶社群開發了一系列保安工具。以下是在業內較受歡迎的部份開放源碼保安工具，這些工具分為四大不同類別：

1. 防火牆，如：iptables
2. 入侵檢測系統，如：Snort
3. 網絡監察工具，如：Multi Router Traffic Grapher（MRTG）
4. 保安評估工具，如：作為掃描網絡伺服器的 Nikto

因開放源碼工具尚未獲得官方正式支持，所以必須特別注意使用該類軟件可能帶來的風險，在部署該類軟件於機構之前，必須獲得管理階層的同意。

III. 開放源碼系統之軟件保安

如前所述，開放源碼軟件其中一項特點是原始碼開放給大眾，連同潛在罪犯和攻擊者也包括在內。攻擊者可讀取原始碼並更快地攻擊因編碼弱點造成的保安漏洞。此外，開放源碼應用程式通常由互聯網團體與社群自願地共同開發，攻擊者也可能經這途徑提供該軟件的部份編碼。編碼的保安程度通常依賴可信賴的系統維護者或其他貢獻者所作出的檢視。然而，封閉源碼軟件也可能會面對類似問題，例如心存不滿的員工在系統放置 **backdoors**，把原始碼外洩給公眾。

開放源碼用戶社群已致力於改善軟件安全和品質，以減低包括開放源碼軟件在內的應用程式和系統之保安漏洞。一般而言，開放源碼軟件保安可從以下最佳作業實務著手⁸：

1. 維護一份關於所有使用過的軟件清單，包括開放源碼軟件，該清單也應詳細記錄版本和雜湊值 (**hash value**) (例如 MD5 或 SHA-1)，以作為原始碼完整性的核對，並記錄下載該軟件的網站。
2. 定期檢查開放源碼軟件有效的保安更新和錯誤 (bugs) 修正，如此一來，修補程式管理流程便可定期執行，使開放源碼軟件保安漏洞也減少了。
3. 應盡快改變安裝後的開放源碼軟件中所有預設的保安設定，透過取消不想要的服務功能，來以最安全的方法設定該產品。
4. 以編碼分析器 (code analysers) 或審計工具 (auditing tools) 來測試和掃描原始碼，例如 BOON (Buffer Overrun Detection)⁹、Flawfinder¹⁰、RATS (Rough Auditing Tool for Security)¹¹ 等工具，開發者也須執行整合編譯 (compiler-integrated) 工具，例如 IBM 的 ProPolice¹² (或是 Stack-Smashing Protector (SSP))，該工具可把保護碼自動插入原始碼中，從而保護編譯程式¹³。
5. 假如應用程式要求打開防火牆埠，應確定開放源碼應用程式完全遵守既有的網絡結構，當引進新應用程式時，此舉將可避免違反機構的防火牆規則和保安政策。

⁸ http://searchsmb.techtarget.com/tip/0,289483,sid44_gci1271530,00.html

⁹ <http://www.cs.berkeley.edu/~daw/boon/>

¹⁰ <http://www.dwheeler.com/flawfinder/>

¹¹ <http://www.fortifysoftware.com/security-resources/rats.jsp>

¹² <http://www.trl.ibm.com/projects/security/ssp/>

¹³ Cowan, C., "Software Security for Open-Source Systems", Security & Privacy Magazine, IEEE, Volume 1, Issue 1, Jan.-Feb. 2003 pp.38-45.

IV. 如何在機構內安全地使用開放源碼產品

為了安全使用開放源碼產品，機構必須考慮以下幾點：

1. 制定完善記錄的保安政策，並確定嚴格執行該政策。當企業需要改變時，也須修訂該政策。
2. 只從可信任的網站下載開放源碼產品，例如軟件開發者的官方網站，以避免事先置入惡性程式碼的潛在風險。
3. 下載原始碼，而非編譯過的套裝軟件，如此，可核對原始碼是否符合 MD5/SHA-1 校驗和 (checksum)，並分析保安漏洞，和進行編譯，以求符合機構的特殊需求。
4. 詳細研讀產品文件，以獲得保安配置參數的詳細說明。
5. 假如發現產品的保安漏洞，便應檢查是否有既定的通報程序，並確定妥善維護和處理該產品的所有保安議題。
6. 定期檢查一般保安漏洞資料庫，例如 CVE (Common Vulnerabilities and Exposure)¹⁴，此類資料庫發布任何有關開放源碼產品保安漏洞的資訊。
7. 採用縱深防禦 (defence-in-depth) 策略，可完全應付開放源碼產品和網絡之間不同水平所引起的威脅。
8. 對機構內員工提供適當訓練，以支援和維護開放源碼產品。把所有作業實務和配置程序進行合適的文件記錄，以避免因職務調動或離職而引起的問題。

¹⁴ <http://www.cve.mitre.org/about>

V. 結論

在當今市場中，一些機構試圖以最少的資源得到最多的利益，而未有考慮品質或保安問題。然而，機構採用開放源碼並不應只簡單地從網站下載和執行免費程式，在機構進一步踏入開放源碼世界之前，有許多保安考慮是值得注意、評估和決定的，此外，個人和機構雙方都須留意開放源碼用戶社群所建議的最佳作業實務，至於考慮使用開放源碼解決方案的企業也須留意本文所述的各項要點。