最佳實踐：
如何建立高安全的應用程式(上)

概述

軟體版權問題已經成為一個流行的話題。軟體商業聯盟(BSA)與國際數據資訊有限公司(IDC)在第二屆全球軟體盜版研討年會中指出，全球電腦中所安裝的軟體大約有 35% 被破解與複製，導致在 2004 年的損失約高達 300 億美金。本文主要探討時下流行的軟體破解手法，以及如何有效地去防止此類軟體遭破解的安全事件發生。同時，我們也列出幾個最佳實踐的案例，來描述如何實現這方面的軟體版權安全防護技術。

威脅風險評估

為了確認與評選應用程式的最適當軟體版權安全保護解決方案。首先，你必須評估應用程式目前所面臨的威脅。有一個經常被大家誤解的認知是許多組織或單位，認為先前文中所提及的軟體業者因軟體被破解，所產生的損失約 300 億美元，就已經是目前軟體業者全部的損失。實際上，很多軟體的使用者，雖然他們只有買一個授權，但是他們仍然隨意地去在許多機器上，複製他們想要的軟體來使用，無形之中造成軟體業者極大的損失，而至今仍無法估計實際損失。

很不幸地，有很多駭客認為破解軟體保護是一種很有趣且具有挑戰性的腦力激盪遊戲。甚至其中，有一些人透過販售其破解過的軟體來獲利。他們破解應用程式或軟體後，把無保護的軟體放在網路提供收費下載服務，或者燒錄成 CD/DVD 片在大街上販賣。這些囂張且惡意的駭客利用各種管道，違法地販售各大軟體公司的盜版產品。另一方面，有一群盜版者的行為更囂張，通常被稱為 ”Cracker”。這些人在破解社群或論壇上，公開地把軟體保護機制移除，並重新整合包裝回原版軟體內。他們不追求個人的收入利益，卻把破解後的軟體放到點對點的網路上提供給使用者下載。透過網路廣泛的下載連結，將導致這樣免費的已破解軟體版本很容易被取得。雖然 Cracker 可能沒有賺到錢，但是這樣的行為將對軟體廠商的收入造成極大的損失。

GSS 叡揚資訊 Galaxy Software Services 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

對敵策略

現在我們已經知道這些盜版者的動機與目標後，就可以檢查他們的戰術並建立對應的相關策略。以下幾點是 SafeNet 針對目前最流行的軟體破解技術，所提出的幾項反盜版措施:

驅動程式取代或模擬

這種破解手法是在應用系統與軟體金鑰間溝通程序中，直接取代軟體保護驅動程式或模擬其主要的動作。

重播

這種破解手法，是駭客針對應用系統，進行監控進而複製應用程式與硬體金鑰間的溝通行為，然後在其存取應用軟體或程式時，將其複製的動作重現出來，讓軟體認為是正常的存取行為。

暴力破解攻擊

暴力破解攻擊手法是一種可以透過不同的字元、數字或符號排列組合，並利用系統反覆性地嘗試不同的組合去測試其軟體保護的密碼，直到正確的組合被找出的方式。

反(組譯)向工程

反(組譯)向工程是一種利用除錯器或反組譯工具去移除軟體保護機制的破解手法。這些工具早期開發出來，是被使用者執行去瞭解應用系統的運作方式與架構。除錯者或反組譯者不僅可以把把程式碼傾印出來，也可以針對程式碼進行局部取代，進而移除其對硬體裝置的呼叫程式碼，來達到破解的目的。

竄改時間

竄改時間的攻擊手法主要是把系統時間回溯到較早的時期，當應用系統使用期限到期，而無法正常運作時，這樣的方法可以欺騙應用系統其時間仍然還在有效期限，因而繼續正常執行，通常這種破解手法被應用於軟體的試用版本。

GSS Galaxy Software Services 叡揚資訊 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

建立安全的防護

實際上，沒有一家軟體廠商可以採用最高安全等級的軟體防護機制。最高等級安全防護方式就像在每一套出售的軟體上，佈滿了裝備著強力武器如坦克與手榴彈的武裝警衛來幫忙保護其軟體的版權。這樣的保護方式的確可以保證沒有任何軟體版本，在沒有經過授權的情況下，可以被複製或安裝到每一台 PC 上。姑且，我們先不討論這樣的方案是否可行。除此之外，我們仍然需要繼續去尋找最有可能且合理的其他方式來保護你的應用程式。

在軟體保護的市場中，許多廠商提供了大量的解決方案，其中包含了各層面的安全保護機制來防止軟體的非法使用。其中軟體式授權保護方式，雖然不是最安全的保護方法，卻可以有效地降低因被隨意複製所造成的損失。通常這種行為往往是導致軟體廠商收入損失的主要原因，而不是蓄意地盜拷軟體所造成的。透過此種簡單方式可以有效提醒使用者，不要進行非法的使用其軟體，進而降低使用者因忽略所造成的盜版行為。軟體式授權也有提供最強大且彈性的選項，並且可以與硬體結合提升軟體保護的強度。然而，這種方式並沒有完整地考量到軟體的運行環境及其安全性，因為授權是儲存在機器上，而不是一個額外的裝置。因此，軟體式授權並無法針對破解的行為，建立一個無法被攻破的防禦機制。

特殊武器

當然如果引用了高安全的保護機制，因此帶來過高的額外成本是一個不合理的解決方案，我們所設定的目標是要讓使用者破解軟體的成本高於其購買的成本。外接硬體式解決方案提供了目前最高安全等級的保護方式。硬體式的權杖(Token)常被用來保護高價值的軟體，因此有許多使用者已經習慣這樣的軟體使用方式。有一些軟體，是靠無線網路或者網際網路連線，或者利用其他方式來進行授權驗證，這些方式對使用者在軟體使用上造成較大的影響，甚至覺得不便。硬體式的權杖(Token)其不至於對使用者習慣造成極大的影響，進而影響到其銷售。傳統的硬體保護鎖通常使用 USB 或者是 25-pin 序列埠的 Key Pro 來進行對軟體的保護。利用其搭配的軟體開發套件來整合你的應用程式去檢查硬體鎖的存在，進而保護應用程式。而在軟體執行時，會根據軟體保護的策略讀取硬體鎖中的授權資料。

加強的防護機制

<待續>

GSS Galaxy Software Services 叡揚資訊 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787