資安實務與技術

information security: practice and technologies

第11章 資訊安全管理實務

11.1 惡意程式與病毒防治

了解到底惡意程式與電腦病毒是什麼、由什麼構成、如何產生危害，有了這些認識之後才能夠進一步地防治惡意程式與電腦病毒可能產生的危害

認識惡意程式(Malware)

「Malware is able to compromise information systems.」，中文的意思就是「惡意程式可以讓資訊系統妥協」，簡單地說，惡意程式可以讓資訊系統不再堅持原來的安全原則，也就是說惡意程式能夠開始為所欲為

01 惡意程式並不像一般人想像的那麼神秘，只有技術高超的駭客能夠駕馭

02 由於各種硬體平台在軟體上的相容性越來越高，也使得惡意程式能夠滲透到各種硬體設備上

03 由於惡意程式的功能單純又專一，讓系統防不勝防，對於有犯罪動機的人來說，這種犯罪方式太誘人了

04 病毒程式的內容沒有像一般的資訊系統那麼龐大，可是必須針對軟體系統的漏洞來開發

惡意程式出人意料的一面

病毒程式開發者對於電腦系統要有一定程度的了解，當然，也少不了背後邪惡的目的，因此有可能需求很簡單，但是會因為攻擊的系統太穩固而使病毒程式的開發難度變高了

惡意程式作用的方式

01

惡意程式會執行或是將自己安裝在系統中，原因可能是軟體本身的錯誤或是設定上的缺失，讓駭客有機可乘。這一類的漏洞需要在被發現之後修補起來

02

有的惡意程式需要與使用者之間有某種程度的互動，例如滑鼠在網頁上的點按、打開電子郵件的附檔，或是經由超連結前往另外一個網站

惡意程式的傳播媒介

所謂的惡意程式的傳播媒介(propagation vector)是指惡意程式傳遞到各種裝置上所運用的電子資訊方法。為什麼強調「電子資訊方法」呢？基本上這是傳送電腦病毒最有效的方法，因為病毒程式其實就是資料而已，而電子媒介的傳遞有光速那麼快，一下子就可以把病毒傳送到世界各地

11.1.1

電腦病毒與惡意程式

電腦病毒是指讓電腦不舒服的東西嗎？它有生命嗎？「電腦病毒(computer virus)是一種電腦程式，有複製自己並且傳播到其他電腦上的能力。」

電腦病毒與惡意程式的差異

惡意程式(malware)」同樣是電腦程式，但是未必有複製自己的能力。一般認為「惡意程式可以在一個資訊系統中造成損害、造成其他資訊系統的損害，或是將這些系統導引向其他的功能，不再正常地運作。」

電腦病毒是惡意程式

電腦病毒是惡意程式，但是惡意程式未必符合比較嚴格的電腦病毒的定義

電腦病毒可複製與傳播

電腦病毒是「程式」，產生的作用是惡意的，電腦病毒可透過寄主散佈到其他電腦上

電腦病毒的感染力強

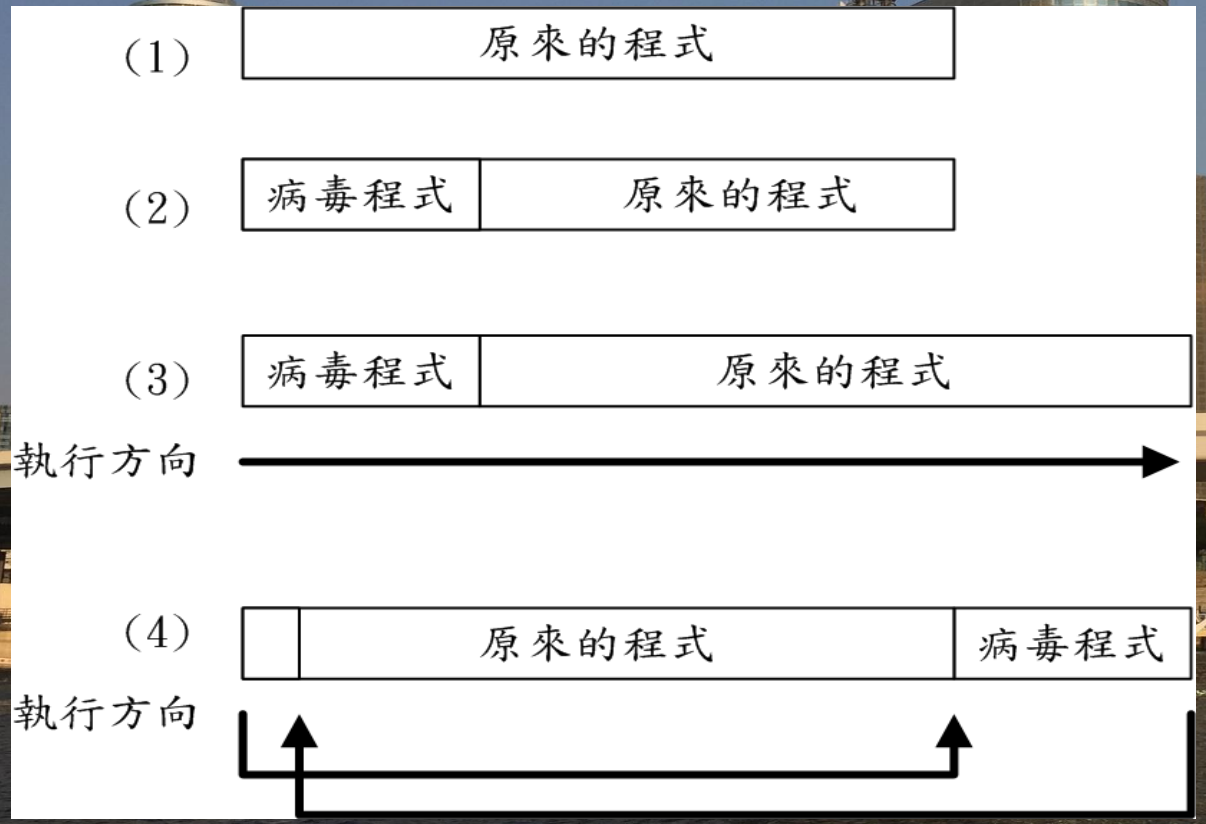
有時候電腦病毒會先感染電腦或是網路上的檔案，再透過這些檔案的散佈來傳播

電腦病毒的組成與結構

電腦病毒的組成與結構五花八門，可以從病毒的作用來區分一個病毒程式通常會具備的組成要素，先不管裡頭詳細的結構。一般病毒都具有典型的組成結構

- 標記(Mark)
- 感染機制(Infection mechanism)
- 觸發條件(Trigger)
- 破壞內涵(Payload)

程式檔案病毒(program file virus)可能存在的結構



第1種情況是原來的程式，處於正常的狀態，檔案大小是固定的。第2種情況是病毒程式覆蓋到原來的程式，程式檔案大小沒有改變。第3種情況是病毒程式加到原來的程式開始的地方，沒有改變原來的程式，不過檔案的大小改變了，當程式執行時會直接執行病毒程式。第4種情況是把病毒程式加到檔案後頭，也會改變檔案的大小，不過檔案前面也要加入一段控制執行方式的程式碼，讓執行的控制權轉移到病毒程式

11.1.2

惡意程式的攻擊

惡意程式也常被稱為惡意軟體（malicious software），惡意軟體運用電腦系統的弱點來發動攻擊或是產生破壞，這是電腦系統最複雜的一種威脅

病毒程式的生命週期

01 潛伏期

Dormant phase

在這個時期病毒沒有活動，必須等到觸發的事件發生才會離開此時期，例如某個日期、某個程式或是檔案產生時，或是磁碟空間超過某個限度時

02 傳播期

Propagation phase

病毒會將自己複製到其他的程式中，或是儲存磁碟上的系統區域，被感染的程式也會因為含有病毒而陸續進入傳播期

03 觸發期

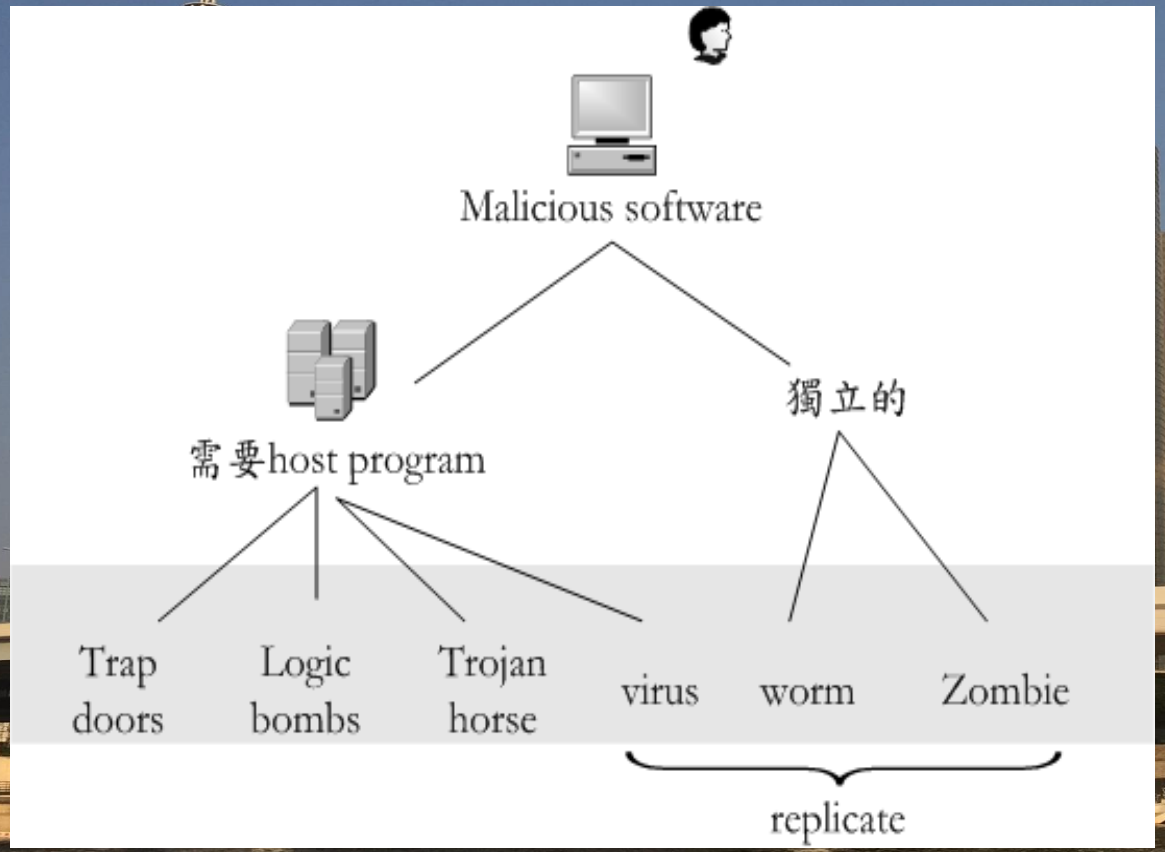
Triggering phase

當病毒被觸發時會執行原來預定執行的功能，觸發期可能會因為各種系統的事件而啟動，例如病毒本身被複製的次數達到某個數字

04 執行期

Execution phase

此時期會執行其本身所被賦予的功能，不見得會造成損害，有的病毒執行後只會顯示特定的訊息在螢幕上，有的病毒執行後會破壞電腦中的程式與檔案



惡意軟體的分類

需要寄主程式（host program）的惡意軟體多半屬於程式片段，獨立的惡意軟體則可直接在作業系統的安排下執行。這裡顯示的分類並沒有完全描述各種惡意軟體，只是透過簡單的歸類讓大家了解惡意軟體的一般類型，Logic bombs與Trojan horse有可能是virus或worm的一部分

常見的惡意軟體(1/6)

病毒（viruses）

病毒程式可以感染其他的程式，所謂的感染其實就是修改的意思。被感染的程式會進一步地感染其他的程式，病毒本身有辦法透過複製來繁衍，這也是電腦病毒作用的模式，當然病毒也有破壞的能力，像開機病毒與巨集病毒都是有名的實例

蠕蟲（worms）

網路蠕蟲程式可以透過網路連線來散佈，一旦存在於系統中，就會像病毒一樣漫延。蠕蟲程式可經由電子郵遞、遠端執行與遠端登入等方式來傳播

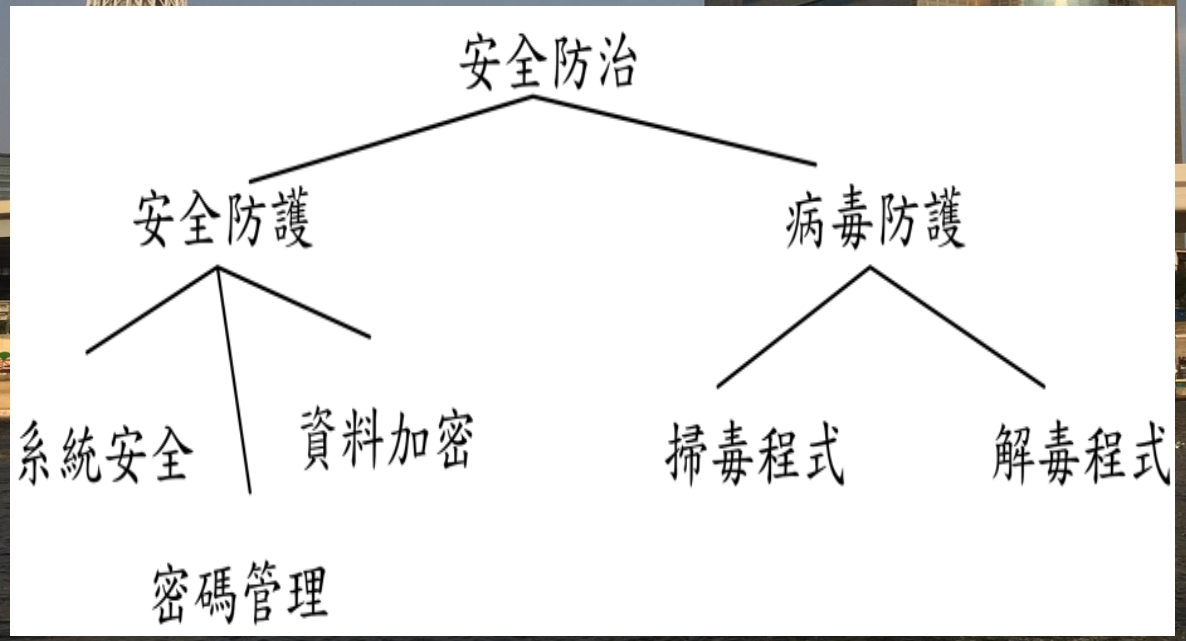
11.1.3

惡意程式的防治

惡意程式的防治可以透過防護的軟體，包括作業系統提供的工具，或是專門用來對付病毒程式的防毒軟體，不過同樣重要的是個人與機構的警覺，以及安全的電腦使用習慣的養成

安全防治軟體的分類

防毒軟體可以幫助電腦系統進行病毒的防護，或是針對網際網路的安全漏洞加以補強，有的防毒軟體還內建防火牆。目前市場上有幾個主要的開發防毒軟體的公司，針對個人SOHO族、小型、中型與大型企業提供的防毒方案



關於防毒軟體的迷思

電腦病毒的防治跟生物病毒的防治都是一塊很大的市場，但是防毒軟體的使用不見得會解決所有的問題，平時除了要經常更新病毒碼之外，還要養成良好的電腦使用習慣

- 安裝了防毒軟體之後電腦會變得很慢
- 電腦上的私人照片已經刪除卻在送修時依然流傳出去
- 社群網站的功能單純肯定不會有問題

Getting to know computer virus

病毒分析方法的類型

靜態分析
(static analysis)
運用各種工具來分析病毒內容的特徵，例如字串分析、反向工程與二元可執行檔的分析等

動態分析
(dynamic analysis)
可在病毒執行時從很多角度來觀察病毒行為，例如對檔案的存取、產生的執行程式、網路通訊，以及對系統登錄(registry)的更動。可透過除錯減慢病毒執行的速度