



澳門城市大學
Universidade da Cidade de Macau
City University of Macau

計算機科學導論



主講人 |

姓名 張琪

Name Zhang Qi


澳門城市大學

City University of Macau



第七章 計算機信息安全基礎

本章學習要點：

- 1 計算機信息安全概述
 - 2 計算機病毒及其防治
 - 3 防火牆技術
 - 4 計算機職業道德
- 

7.1 計算機信息安全概述

7.1.1 計算機信息安全的基本概念

- 系統信息安全的定義為：
- 確保以電磁信號為主要形式的、在計算機網絡化（開放互連）系統中進行自動通信、處理和利用的信息內容，在各個物理位置、邏輯區域、存儲和傳輸介質中，處於動態和靜態過程中的機密性、完整性、可用性、可審查性和抗抵賴性
- 與人、網絡、環境有關的技術安全、結構安全和管理安全的總和
- 其中，人是指信息系統的主體，包括各類用戶，支持人員，技術管理和行政管理人員
- 網絡是指計算機，網絡互聯設備，傳輸介質，信息內容和操作系統，通信協議等
- 環境是系統的穩定和可靠運行所需要的保障體系，包括建築物，機房，動力保障等



7.1 計算機信息安全概述

7.1.1 計算機信息安全的基本概念

- 信息系統安全唯一和最終目標是保障信息內容在任何地方，任何時候，任何狀態下的機密性，完整性和可用性
- 機密性 (Security)，指系統中的信息只能由授權用戶訪問
- 完整性 (Integrity)，指系統中的資源只能由授權用戶進行修改，以確保信息資源沒有被篡改
- 可用性 (Availability)，指系統中的資源對授權用戶是有效可用的





7.1 計算機信息安全概述

7.1.1 計算機信息安全的基本概念

- 根據一些惡意用戶攻擊他人的目的和方式，可以將威脅手段分為以下兩種：
- **主動攻擊**：指修改信息或創建假信息，一般采用的手段有重現、修改、破壞和偽裝。例如，利用網絡漏洞破壞網絡系統的正常工作和管理
- **被動攻擊**：指通過偷聽和監視來獲得存儲和傳輸的信息。例如，通過收集計算機屏幕或電纜輻射的電磁波，用特殊設備進行還原，以竊取商業、軍事和政府的機密信息





7.1 計算機信息安全概述

7.1.2 計算機信息安全技術

- 總的來說，計算機信息安全技術主要包含以下幾個方面

1．實體安全技術

- 指為保證計算機設備、通信綫路以及相關設施的安全而採取的技術和方法

2．數據安全技術

- 指為保證計算機系統中的數據庫或數據文件免遭破壞、修改、竊取而採取的技術和方法





7.1 計算機信息安全概述

7.1.2 計算機信息安全技術

- 總的來說，計算機信息安全技術主要包含以下幾個方面

3 · 軟件安全技術

- 指爲了保證計算機軟件系統中的軟件免遭破壞、非法複製、非法使用或避免軟件本身缺陷而採取的技術和方法

4 · 網絡安全技術

- 指爲了保證網絡及其結點安全而採取的技術和方法

5 · 安全評價技術

- 計算機系統的安全性是相對的，不同的系統、不同的任務對信息系統安全具有不同的要求，因此需要一個安全評價標準作爲系統安全檢驗的依據





7.1 計算機信息安全概述

7.1.3 信息安全法規

1. 計算機犯罪的定義

- 指在信息活動領域中，利用計算機信息系統或計算機信息知識作為手段，或者針對計算機信息系統，對國家、團體或個人造成危害，依據法律規定，應當予以刑罰處罰的行為

2. 計算機犯罪的定義類型

- 破壞計算機系統罪
- 非法侵入計算機信息系統罪
- 計算機信息系統安全事故罪



7.1 計算機信息安全概述

7.1.3 信息安全法規

3．軟件知識產權與計算機安全的法律法規

(1) 什麼是軟件知識產權？

- 知識產權，指人類通過創造性的智力勞動而獲得的一項智力性的財產權，是一種典型的由人的創造性勞動產生的“知識產品”
- 軟件知識產權，指的是計算機軟件版權

(2) 計算機安全相關的法律法規

- 爲了依法打擊計算機犯罪，加強計算機信息系統的安全保護和國際互聯網的安全管理，我國制定了一系列有關法律法規
- 經過多年的實踐，已形成了比較完整的行政法規和法律體系



7.2 計算機病毒及其防治

- 隨著計算機和Internet的日益普及，計算機病毒已經成為了當今信息社會的一大頑症
- 由于計算機病毒極強的破壞作用，因而它嚴重地干擾了人們的正常工作，企業的正常生產，甚至對國家的安全都造成了巨大的影響
- 網絡防病毒技術已成為計算機網絡安全研究的一個重要課題



7.2 計算機病毒及其防治

7.2.1 計算機病毒的概念

1. 計算機病毒的定義

- **計算機病毒**，是指編制或者在計算機程序中插入的破壞計算機功能或者破壞數據，影響計算機使用并且能够自我複製的一組計算機指令或者程序代碼





7.2 計算機病毒及其防治

7.2.2 計算機病毒的特徵

計算機病毒都是人爲製造的、具有一定破壞性的程序，它不同于日常生活中所說的傳染病毒。計算機病毒具有以下一些基本特徵：

- 傳染性

- 計算機病毒能通過各種渠道從已被感染的計算機擴散到未被感染的計算機，而計算機中被感染的文件又會成爲新的傳染源，再與其他機器進行數據交換或通過網絡接觸，使病毒傳播範圍越來越廣

- 隱蔽性

- 計算機病毒往往是短小精悍的程序，若不經過代碼分析，病毒程序和普通程序是不容易區分開的。正因爲如此，才使得病毒在被發現之前已進行廣泛的傳播



7.2 計算機病毒及其防治

7.2.2 計算機病毒的特徵

計算機病毒都是人爲製造的、具有一定破壞性的程序，它不同于日常生活中所說的傳染病毒。計算機病毒具有以下一些基本特徵：

- 潛伏性

- 計算機病毒程序進入系統之後一般不會馬上發作，可以在幾周或者幾個月內甚至幾年內隱藏在合法文件中，對其他系統進行傳染，而不被人發現

- 觸發性

- 觸發病毒程序的條件較多，可以是內部時鐘，系統的日期和用戶名，也可以是網絡的一次通信等。一個病毒程序可以按照設計者的要求，在某個計算機上激活并發出攻擊

- 破壞性

- 計算機病毒的最終目的是破壞系統的正常運行，輕則降低速度，影響工作效率；重則刪除文件內容、搶占內存空間甚至對硬盤進行格式化，造成整個系統的崩潰

7.2 計算機病毒及其防治

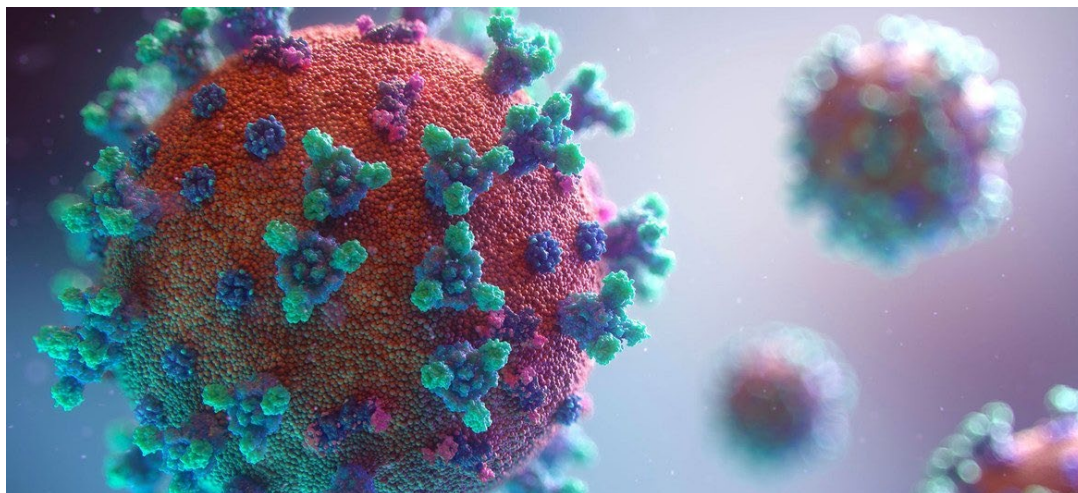
7.2.2 計算機病毒的特徵

計算機病毒都是人爲製造的、具有一定破壞性的程序，它不同于日常生活中所說的傳染病毒。計算機病毒具有以下一些基本特徵：

- 衍生性

- 計算機病毒本身由幾部分組成，所以它可以被惡作劇者或惡意攻擊者模仿，甚至對計算機病毒的幾個模塊進行修改，使之衍生爲不同于原病毒的另一種計算機病毒

➤ 類比一下，現實世界裏的病毒，他們是不是比較類似？





7.2 計算機病毒及其防治

7.2.3 計算機病毒的分類

目前，全球的計算機病毒有幾萬種，對計算機病毒的分類方法也存在多種，常見的分類有以下幾種：

(1) 按病毒存在的媒體分類

● 引導型病毒

- 引導型病毒，指寄生在磁盤引導區或主引導區的計算機病毒
- 此種病毒利用系統引導時，不對主引導區的內容正確與否進行判別的缺點，在引導系統的過程中侵入系統，駐留內存，監視系統運行，待機傳染和破壞





7.2 計算機病毒及其防治

7.2.3 計算機病毒的分類

目前，全球的計算機病毒有幾萬種，對計算機病毒的分類方法也存在多種，常見的分類有以下幾種：

(1) 按病毒存在的媒體分類

● 文件型病毒

- 文件型病毒是計算機病毒的一種
- 文件型病毒是對計算機的源文件進行修改，使其成為新的帶毒文件。一旦計算機運行該文件就會被感染，從而達到傳播的目的
- 針對文件型病毒是通過文件進行傳播，所以當使用來歷不明文件的時候，先用最新升級過的殺毒軟件進行檢查，確認沒有文件型病毒之後方可使用。切記不要雙擊打開或複製



7.2 計算機病毒及其防治

7.2.3 計算機病毒的分類

目前，全球的計算機病毒有幾萬種，對計算機病毒的分類方法也存在多種，常見的分類有以下幾種：

(1) 按病毒存在的媒體分類

● 混合型病毒

- 指具有引導型病毒和文件型病毒寄生方式的計算機病毒，所以它的破壞性更大，傳染的機會也更多，殺滅也更困難
- 這種病毒擴大了病毒程序的傳染途徑，它既感染磁盤的引導記錄，又感染可執行文件
- 當染有此種病毒的磁盤用于引導系統或調用執行染毒文件時，病毒都會被激活
- 因此在檢測、清除複合型病毒時，必須全面徹底地根治，如果只發現該病毒的一個特性，把它只當作引導型或文件型病毒進行清除。雖然好像是清除了，但還留有隱患，這種經過消毒後的“潔淨”系統更賦有攻擊性



7.2 計算機病毒及其防治

7.2.3 計算機病毒的分類

目前，全球的計算機病毒有幾萬種，對計算機病毒的分類方法也存在多種，常見的分類有以下幾種：

(2) 按病毒的破壞能力分類

- 良性病毒

- 計算機良性病毒是不破壞計算機的數據或程序。它是一種只占用計算機資源來執行而不會導致計算機系統癱瘓的計算機病毒

- 惡性病毒

- 計算機惡性病毒是指破壞系統數據，刪除文件，甚至摧毀系統的危害性很大的病毒



7.2 計算機病毒及其防治

7.2.3 計算機病毒的分類

目前，全球的計算機病毒有幾萬種，對計算機病毒的分類方法也存在多種，常見的分類有以下幾種：

(3) 按病毒傳染的方法分類

- 駐留型病毒

- 駐留型病毒感染計算機後，把自身的內存駐留部分放在內存（ RAM ）中，這一部分程序挂接系統調用并合并到操作系統中去，他處于激活狀態，一直到關機或重新啓動

- 非駐留型病毒

- 非駐留型病毒在得到機會激活時并不感染計算機內存，一些病毒在內存中留有小部分，但是并不通過這一部分進行傳染，這類病毒也被劃分爲非駐留型病毒

7.2 計算機病毒及其防治

7.2.3 計算機病毒的分類

目前，全球的計算機病毒有幾萬種，對計算機病毒的分類方法也存在多種，常見的分類有以下幾種：

(4) 按照計算機病毒的鏈接方式分類

- 源碼型病毒

- 源碼型病毒攻擊高級語言編寫的程序，病毒在高級語言編寫的程序編譯之前插入到源程序中，經編譯成功後成為合法程序的一部分

- 嵌入型病毒

- 嵌入型病毒，指病毒是將自身嵌入到現有程序中，把計算機病毒的主體程序與其攻擊的對象以插入的方式鏈接
- 這種計算機病毒是難以編寫的，一旦侵入程序體後也較難消除

7.2 計算機病毒及其防治

7.2.3 計算機病毒的分類

目前，全球的計算機病毒有幾萬種，對計算機病毒的分類方法也存在多種，常見的分類有以下幾種：

(4) 按照計算機病毒的鏈接方式分類

- 外殼型病毒

- 外殼型病毒常附著在主程序的首尾，在文件執行時先行執行此病毒程序，從而不斷的複製，使計算機工作效率降低，最終使計算機死機

- 操作系統型病毒

- 操作系統型病毒會用它自己的程序加入操作系統或者取代部分操作系統進行工作，具有很強的破壞力，會導致整個系統癱瘓
- 這種病毒在運行時，會用自己的程序片斷取代操作系統的合法程序模塊。根據病毒自身的特點和被替代的操作系統中合法程序模塊在操作系統中運行的地位與作用，以及病毒取代操作系統的取代方式等，對操作系統進行破壞

7.2 計算機病毒及其防治

7.2.4 計算機病毒的威脅及傳播途徑

1. 計算機病毒的威脅

- 隨著互聯網的發展，近幾年來計算機病毒呈現出異常活躍的態勢，特別是針對用戶計算機和移動設備的惡意攻擊，比前幾年大大增加
- 目前已有若干軟件平臺頻繁受到病毒的攻擊，例如微軟的IE瀏覽器、Adobe Reader、甲骨文的Sun Java、Office辦公軟件等，此外Java和ActiveX技術的廣泛應用也為病毒攻擊創造了條件





7.2 計算機病毒及其防治

7.2.4 計算機病毒的威脅及傳播途徑

2. 計算機病毒的傳播途徑

- 將磁盤帶到網絡上運行後，使網絡感染上病毒
- 訪問網絡電子廣告牌（BBS）時感染的病毒
- 從軟件商的演示光盤中帶來的病毒
- 從系統維護盤中帶來的病毒
- 從公司之間交換的磁盤中帶來的病毒





7.2 計算機病毒及其防治

7.2.5 計算機病毒的防治

近年來，全球計算機病毒猖獗，爲了有效地防禦計算機病毒、蠕蟲病毒和特洛伊木馬等病毒，一般可采取以下措施

- 提高警惕，不打開來歷不明的郵件及附件
- 首次安裝防病毒軟件時，務必對計算機進行一次全盤掃描
- 使用光盤、優盤、移動硬盤等外存儲器設備時，一定先進行病毒掃描
- 不從不可靠渠道下載軟件
- 使用基于客戶端的防火牆或過濾措施
- 禁用Windows Scripting Host

➤ 舉個計算機病毒傳播的例子



思考題

- 計算機病毒的分類主要有哪些？請簡要說明。
- 計算機病毒的特徵主要有哪些？請簡要說明。
- 計算機信息安全技術主要包含哪幾個方面？

休息一下

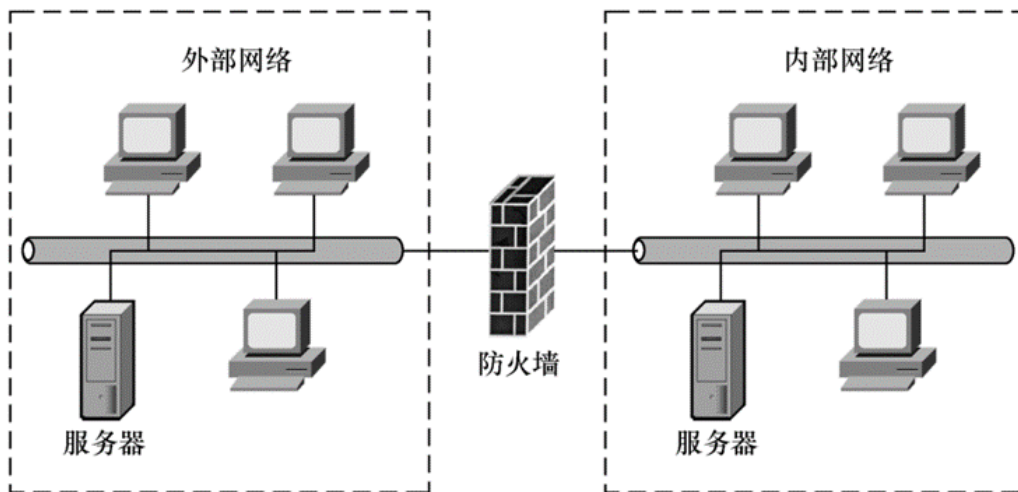
Take a break

7.3 防火牆技術

7.3.1 防火牆的基本概念

1. 防火牆的基本概念

- “防火牆” (Fire Wall) 是用來連接兩個網絡并控制兩個網絡之間相互訪問的系統
- 它包括用于網絡連接的軟件和硬件以及控制訪問的方案
- 防火牆用于對進出的所有數據進行分析，并對用戶進行認證，從而防止有害信息進入受保護網，為網絡提供安全保障





7.3 防火牆技術

7.3.1 防火牆的基本概念

2. 防火牆的主要功能

- 集中的網絡安全
 - 防火牆允許網絡管理員定義一個中心（阻塞點）來防止非法用戶進入內部網絡，禁止存在不安全因素的訪問進出網絡，并抗擊來自各種綫路的攻擊
- 安全警報
 - 通過防火牆可以方便地監視網絡的安全性，并產生報警信號
- 重新部署網絡地址轉換（NAT）
 - 接入Internet的機構，可以通過網絡地址轉換（NAT）來完成內部私有地址到外部注冊地址的映射，而防火牆正是部署NAT的理想位置





7.3 防火牆技術

7.3.1 防火牆的基本概念

2. 防火牆的主要功能

- 監視Internet的使用情况
 - 防火牆也是審查和記錄內部人員對Internet使用的一個最佳位置，可以在此對內部訪問Internet的情況進行記錄
- 向外發布信息
 - 防火牆同樣還是部署WWW服務器和FTP服務器的理想位置。它允許Internet上的其它用戶訪問上述服務器，而禁止訪問內部受保護的其它系統





7.3 防火牆技術

7.3.1 防火牆的基本概念

3. 防火牆的局限性

防火牆并非萬能，影響網絡安全的因素很多，對於以下情況它無能為力：

- 不能防範繞過防火牆產生的攻擊
- 不能防範由于內部用戶不注意所造成的威脅
- 不能防範受到病毒感染的軟件或文件在網絡上傳輸
- 很難防止數據驅動式攻擊



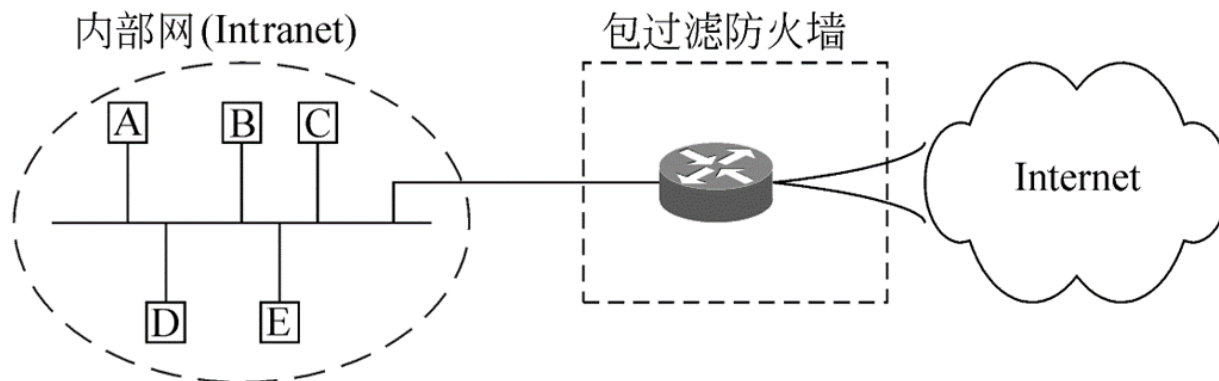
7.3 防火牆技術

7.3.2 防火牆的基本類型

典型的防火牆系統通常由一個或多個構件組成，相應地，實現防火牆的技術包括以下四大類：

1. 包過濾防火牆 (Packet Filtering Firewall)

- 包過濾防火牆，又稱網絡級防火牆，通常由一台路由器或一台充當路由器的計算機組成
- Internet/Intranet上的所有信息都是以IP數據包的形式傳輸的，包過濾路由器負責對所接收的每個數據包的IP地址，TCP或UDP分組頭信息進行審查，以便確定其是否與某一條包過濾規則匹配



7.3 防火牆技術

7.3.2 防火牆的基本類型

典型的防火牆系統通常由一個或多個構件組成，相應地，實現防火牆的技術包括以下四大類：

1. 包過濾防火牆 (Packet Filtering Firewall)

- 包過濾防火牆檢查每一條過濾規則，如果找到一個匹配，且規則允許該數據包通過，則該數據包根據路由表中的信息向前轉發；如果找到一個匹配，且規則拒絕此數據包，則該數據包將被捨棄
- 包過濾防火牆對用戶來說是全透明的，其優點是只需在一個關鍵位置設置一個包過濾路由器就可以保護整個網絡，使用起來非常簡潔、方便，且速度快、費用低
- 包過濾防火牆也有其自身的缺點和局限性，例如它只檢查地址和端口，對應用層上的黑客行為無能為力；包過濾規則配置比較複雜；包過濾沒法檢測具有數據驅動攻擊這一類潛在危險的數據包等

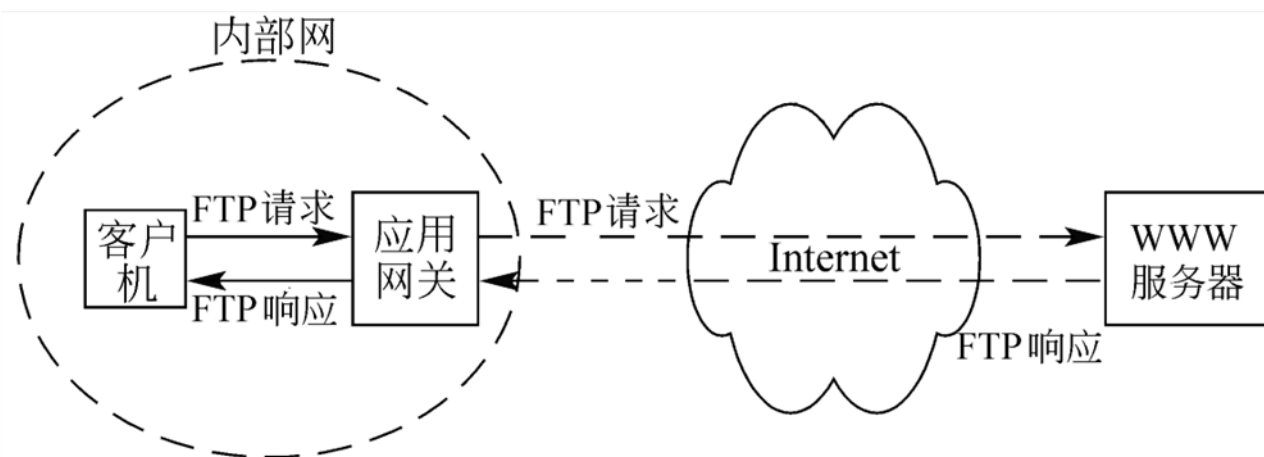
7.3 防火牆技術

7.3.2 防火牆的基本類型

典型的防火牆系統通常由一個或多個構件組成，相應地，實現防火牆的技術包括以下四大類：

2. 應用層網關 (Application Level Gateway)

- 應用層網關主要控制對應用程序的訪問，它能够對進出的數據包進行分析、統計，防止在受信任的服務器與不受信任的主機間直接建立聯繫。而且它還提供一種監督控制機制，使得網絡內、外部的訪問請求在監督機制下得到保護





7.3 防火牆技術

7.3.2 防火牆的基本類型

典型的防火牆系統通常由一個或多個構件組成，相應地，實現防火牆的技術包括以下四大類：

2. 應用層網關 (Application Level Gateway)

- 和包過濾防火牆一樣，應用層網關也是僅僅依靠特定的邏輯判斷來決定是否允許數據包通過。一旦防火牆內外的計算機系統建立起直接聯繫，它外部的用戶便有可能直接瞭解防火牆內部的網絡結構和運行狀態，這有利于實施非法訪問和攻擊
- 應用層網關具有較強的訪問控制功能，是目前最安全的防火牆技術之一。但其每一種協議都需要相應的代理軟件，實現起來比較困難，效率不如網絡級防火牆高，而且對用戶缺乏“透明度”



7.3 防火牆技術

7.3.2 防火牆的基本類型

典型的防火牆系統通常由一個或多個構件組成，相應地，實現防火牆的技術包括以下四大類：

3. 電路層網關 (Circuit Level Gateway)

- 電路層網關通常工作在OSI參考模型中的會話層上，它只依賴于TCP連接，而并不關心任何應用協議，也不進行任何的包處理或過濾。它就像電綫一樣，只是在內部連接和外部連接之間來回拷貝字節。由于連接要穿過防火牆，因而其隱藏了受保護網絡的有關信息
- 電路層網關往往不是一個獨立的產品，它要和其它一些應用級網關結合在一起使用。其最大的優點是主機可以被設置成混合網關，內部用戶使用起來很方便，另外，電路層網關還可將所有內部的IP地址映射到一個防火牆專用的、安全的IP地址

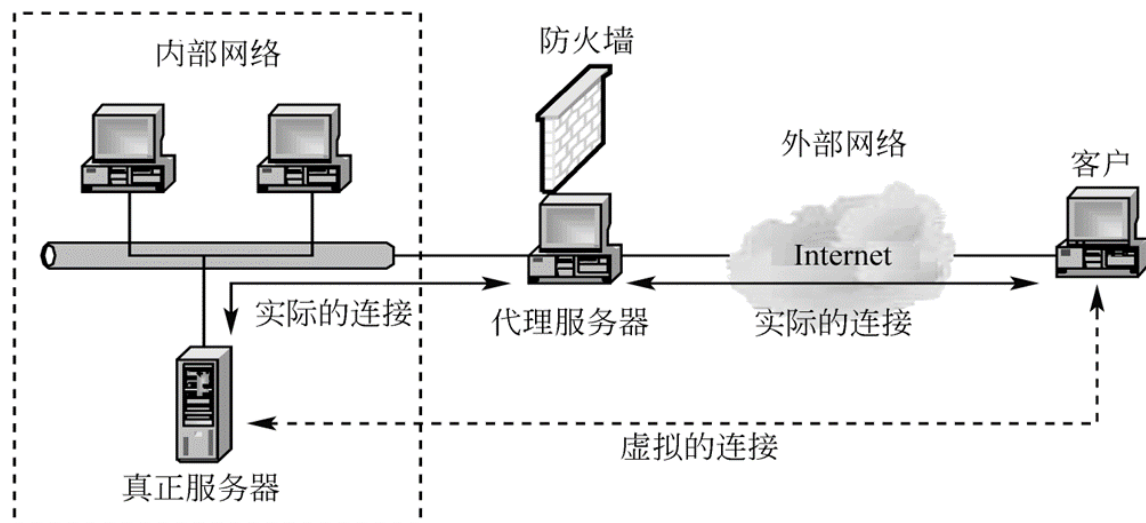
7.3 防火牆技術

7.3.2 防火牆的基本類型

典型的防火牆系統通常由一個或多個構件組成，相應地，實現防火牆的技術包括以下四大類：

4. 代理服務防火牆 (Proxy Sever Firewall)

- 代理服務防火牆工作在 OSI 參考模型的最高層——應用層，有時也將其歸為應用層網關一類。代理服務器 (Proxy Sever) 運行在Intranet和Internet之間，是內、外網絡的隔離點，起著監視和隔絕應用層通信流的作用



7.3 防火牆技術

7.3.2 防火牆的基本類型

典型的防火牆系統通常由一個或多個構件組成，相應地，實現防火牆的技術包括以下四大類：

4. 代理服務防火牆 (Proxy Sever Firewall)

- 代理服務器收到用戶對某站點的訪問請求後，便立即檢查該請求是否符合規則。若規則允許用戶訪問該站點，代理服務器便會以客戶身份登錄目的站點，取回所需的信息再發回給客戶
- 代理服務器將所有跨越防火牆的通信鏈路分為兩段，外部用戶只能看到該代理服務器而無法獲知任何內部資料，如IP地址，從而起到了隔離防火牆內、外計算機系統的作用
- 代理服務軟件要分析網絡數據包並作出訪問控制決定，從而在一定程度上影響了網絡的性能，且代理服務器需要為每個網絡用戶專門設計，安裝使用較複雜，成本也相對較高

7.3 防火牆技術

7.3.3 防火牆的基本類型

- CheckPoint FireWall
- NetScreen 防火牆
- Cisco PIX 防火牆





7.4 計算機職業道德

7.4.1 計算機職業道德的基本概念

- **計算機職業道德**：是指在計算機行業及其應用領域所形成的社會意識形態和倫理關係下，調整人與人之間、人與知識產權之間、人與計算機之間，以及人與社會之間關係的行為規範的總和
- 計算機職業道德是在計算機信息系統及其應用所構成的社會範圍內，經過一定時期的發展，經過新的社會倫理意識與傳統的社會道德規範的衝突、平衡、融合，最終形成的一系列計算機職業行為規範





7.4 計算機職業道德

7.4.2 計算機職業道德教育的重要性

- 不僅有利于計算機信息系統的安全，而且有利于整個社會對個體利益的保護
- 保障計算機網絡的良好秩序和計算機信息的安全性，減少網絡陷阱對青少年的危害
- 對計算機的學習不僅要重視技術理論的學習，而且還要加強對計算機職業道德問題的學習



7.4 計算機職業道德

7.4.3 信息使用的道德規範

美國計算機倫理協會總結、歸納了以下計算機職業道德規範，稱爲：[計算機倫理十戒](#)

- 不應該用計算機去傷害他人
- 不應該影響他人的計算機工作
- 不應該到他人的計算機裏去窺探
- 不應該用計算機去偷竊
- 不應該用計算機去做假證明
- 不應該複製或利用沒有購買的軟件
- 不應該在未經他人許可的情況下使用他人的計算機資源
- 不應該剽竊他人的精神作品
- 應該注意你正在編寫的程序和你正在涉及的系統的社會效應
- 應該始終注意，你使用計算機是在進一步加強你對同胞的理解和尊敬

思考題

- 防火牆有哪些局限？請簡要說明。
- 防火牆的基本類型主要有哪些？請簡要說明。
- 信息使用的道德規範主要有哪些？

休息一下

Take a break



感謝觀賞

Thank you for listening.