VoIP網路安全防護

報告人: 張建明

National Ilan University

國立宜蘭大學資工所

VoIP網路安全防護- Outline

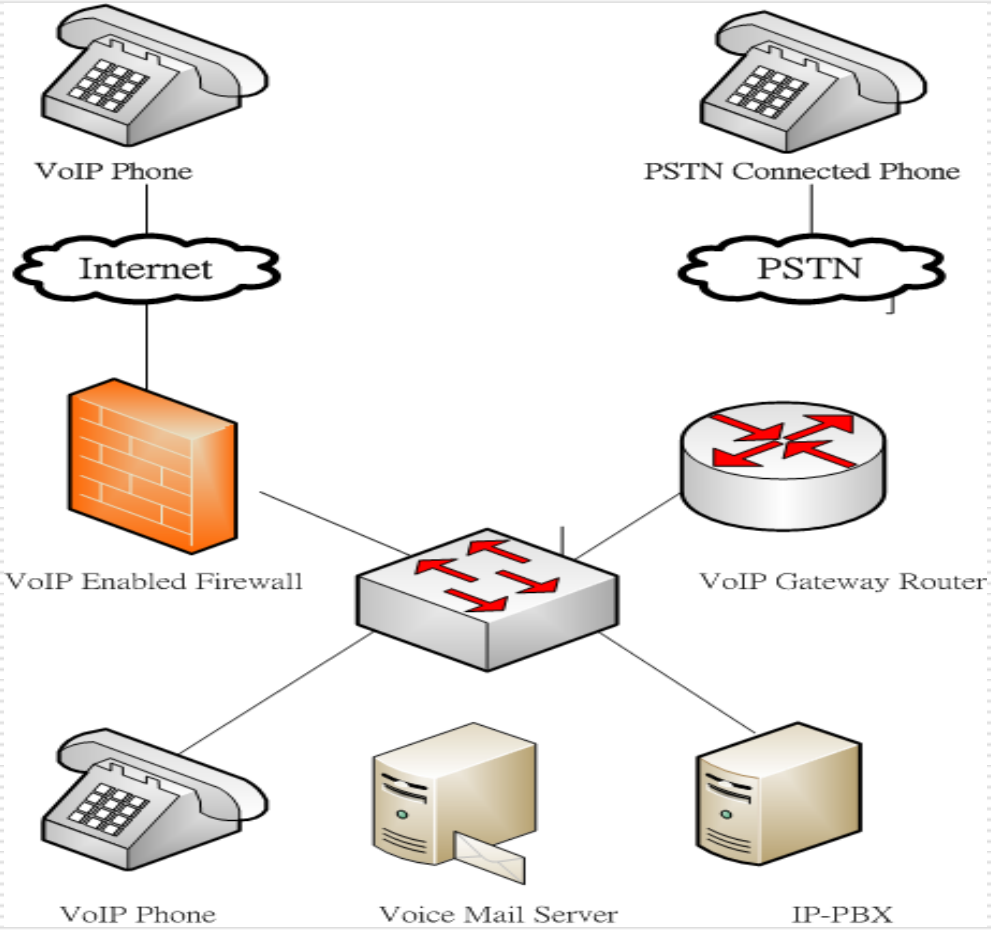
- VoIP 網路之相關技術簡介
- 常見的 VoIP 攻擊
  - Dos
  - Eavesdropping
  - Alteration of Voice Stream
  - Toll Fraud
  - Redirection of Call
  - Accounting Data Manipulation
  - Caller Identification (ID) Impersonation
  - Unwanted Calls and Messages (SPIT)
- VoIP網路之防護策略

VoIP 網路之相關技術簡介

- VOICE over Internet Protocol (VoIP)
  - 網路語音通訊技術
  - 利用網路無所不在的特性，在企業或家庭的網路環境部署VoIP的裝置，取代傳統的電話系統。
  - 使用 IP-base 網路進行語音通訊
  - VoIP軟體可安裝在桌上型電腦、行動 IP 電話或網路閘道器上。

- VoIP網路架構
  - Endpoints (VoIP Phone)
  - Control Nodes
  - Gateway Nodes (VoIP Gateway Router)
  - IP-base 網路
  - Public Switched Telephone Network (PSTN)

VoIP 網路之相關技術簡介



VoIP 網路之相關技術簡介

- VoIP 通訊流程
  - 撥號 (signaling)
  - 編碼 (encoding)
  - 傳送 (transport)
  - 控制閘道 (gateway control)

- VoIP的使用者在進行語音通訊之前必須先撥號(*signaling*)，待通訊線路被建立後，接著VoIP系統會將語音資料先進行編碼(*encoding*)，再透過網路傳送給接收端，若接收端是使用傳統電話系統，則需要透過控制閘道(*gateway control*)進行格式轉換。

VoIP 網路之相關技術簡介

- 撥號 (signaling)
  - H.323

    ITU-T於1996年提出的VoIP標準，一開始是應用在以區域網路爲基礎的視訊會議，後來被廣泛應用於網路電話。
  - SIP (Session Initial Protocol)

    被廣泛使用作爲VoIP通訊的標準，可用於建立多方多媒體通訊(Multiparty Multimedia Communications)系統，SIP也規範通話建立與結束所使用的命令方式與訊息傳輸的協商機制等。

VoIP 網路之相關技術簡介

- 編碼與傳送 (encoding & transport)
  - 編碼
    - 將類比訊號 (使用者的語音) 轉成數位信號 (VoiceData)
  - 傳送
    - 將 VoiceData 封裝 (encapsulation) 成串流封包，才能經由網路即時(real time)送到接收端。
  - 當接收端收到串流封包時，需將串流封包解封裝 (decapsulation) 回VoiceData，再數位信號解碼成類比訊號 (語音) 。

- 控制閘道 (gateway control)
  - VoIP Phone若要與一般 PSTN 的電話進行通訊時，需要透過控制閘道進行格式轉換。

常見的 VoIP 攻擊

- 目前在 VoIP 系統常發生的安全性問題如下表所示

Security Concern	Confidentiality	Integrity	Availability
Denial of Service			X
Eavesdropping	X		
Alteration of Voice Stream	X	X	
Toll Fraud		X	
Redirection of Call	X	X	X
Accounting Data Manipulation	X	X	
Caller Identification Impersonation		X	
Unwanted Calls and Messages		X	X

Denial of Service (DOS)

- Denial of Service (Dos) 阻斷服務癱瘓攻擊
  - 破壞系統的可用性
  - 耗盡目標主機的網路頻寬或系統資源
  - 讓使用者無法撥電話或無法接電話

Denial of Service (DOS)

- Dos 攻擊手法
  - 駭客可以對IP PBX電話交換機、語音閘道器、或客戶端數據機等不同目標進行DOS攻擊。
  - 有心人士可以送出大量的 SIP 要求（例如邀請、註冊、再見或 RTP 封包）佔據 VoIP 系統所需要的資源，讓 VoIP 系統完全不能處理其他使用者的要求，讓 VoIP 系統降低服務品質(如強迫使用者提前掛斷電話等) ，嚴重時 VoIP 系統甚至無法正常提供網路電話服務。

Denial of Service (DOS)

- Dos 攻擊手法
  - 從攻擊方法和破壞效果來看，阻斷服務癱瘓攻擊是一種既簡單又有效的攻擊方式，攻擊者向伺服器發送相當多帶有虛假IP 的服務請求，伺服器會等不到回傳的消息，就會耗盡所有資源，以阻止合法使用者存取伺服器或服務。

Eavesdropping

- Eavesdropping
  - 破壞通訊的隱私性。
  - Internet 爲一開放式架構，有心人士可以輕易做到監聽 VoIP 電話內容。
  - 利用後門或木馬程式進行竊聽。

Eavesdropping

- Eavesdropping 攻擊手法
  - 監聽 VoIP 和傳統監聽網路資料不太一樣，監聽 VoIP 除了需要攔截建立連線使用的信號訊息外，亦要攔截之後包含語音的媒體資料流(Media stream)。
  - 信號訊息通常使用SIP (Session Initiation Protocol)通訊協定來傳遞， SIP可使用不同的傳輸層(例如 UDP或TCP) ，通訊協定的埠號由VoIP軟體自行決定。
  - 媒體資料流(Media stream)一般使用 UCP 搭配 RTP (Real Time Protocol)。目前利用SIP 和 RTP通訊協定傳送的封包並沒有被加密，有心人士可以利用相關工具(例如Ethereal)來側錄封包，除了達到監聽的目的，還可以得知通話者的身份、註冊資訊和SIP統一資源標識符號(Uniform Resource Identifier:例如電話號碼)等個人資料。

Alteration of Voice Stream

- Alteration of Voice Stream (取代攻擊)
  - 破壞隱私性以及完整性
  - Man-in-the-middle
  - 當通話雙方彼此不認識時，攻擊者攔截通訊的語音封包，同時假冒雙方與另一端進行通訊。
  - 當通話雙方彼此互相認識時，此種攻擊較難成功，除非攻擊者能產生通話雙方的相似聲波，或事先錄下某一方的聲音來欺騙另一方，但這還是有困難度存在。

Toll Fraud

- Toll Fraud (話費詐欺)
  - 破壞完整性
  - 誘騙使用者撥打高付費電話

    (在使用者的通訊設備上留下電話號碼，並要求使用者回電，當使用者一回電就需付高額的通話費。)
  - 欺騙電話系統

    (攻擊者可以利用 Replay 或是 Impersonate 的方法去偽冒成系統的合法使用者，之後攻擊者撥打高付費電話時，付錢的不是攻擊者本身而是被假冒的受害者。)

Redirection of Call

- Redirection
  - VoIP在設計時，爲了方便讓caller能夠透過一組號碼找到位於不同位置或使用不同接話設備的callee，提供了Redirection的服務，當caller撥號至callee號碼時，可以redirect到callee的手機、室內電話或VoIP Phone等的任何通訊設備。

Redirection of Call

- Redirection of Call
  - 破壞隱私性及完整性
  - 有心人士可以藉由修改redirect的資訊，將號碼redirect至有心人士所預定的號碼(如：高付費電話、或攻擊者本身的電話)。

Accounting Data Manipulation

- Accounting database
  - 用來存放 call data records (CDR) 資訊
  - CDR 包含每一通電話的撥號端號碼、接話端號碼、日期時間與通話時間等等。
- Accounting Data Manipulation
  - 破壞完整性
  - CDR 被用來當做收費的依據，若攻擊者得到修改 CDR database 的權限時，便可以竄改或刪除通話記錄，藉此進行盜打或犯罪等不法行爲。

Caller Identification Impersonation

- Caller Identification (ID) Impersonation
  - 破壞完整性
  - 攻擊者假冒成別的合法使用者 ID 來撥打電話或接電話。

Caller Identification Impersonation

- Caller Identification (ID) Impersonation
  - 身分僞造是在網路上隱藏真正的身份且建立假的身份，攻擊者必須在封包中使用僞造來源來取代真實位址。身分僞造可用來隱藏攻擊的原始來源或愚弄網路存取控制清單，無法讓別人追蹤到欺騙封包的原始傳送者。
  - 駭客在一段很短的時間內一直發出REGISTER 要求，除了嘗試登錄系統竊取使用者帳號資訊以盜撥電話，也能癱瘓一定程度的代理伺服器處理效能。

Unwanted Calls and Messages

- Unwanted Calls and Messages (SPIT)
  - 破壞可用性及完整性
  - SPIT 指的是 SPAM over Internet telephone
  - 攻擊者藉由大量的垃圾語音訊息塞爆合法使用者的 voice mail box ，使其無法接收其他的語音訊息。

Unwanted Calls and Messages

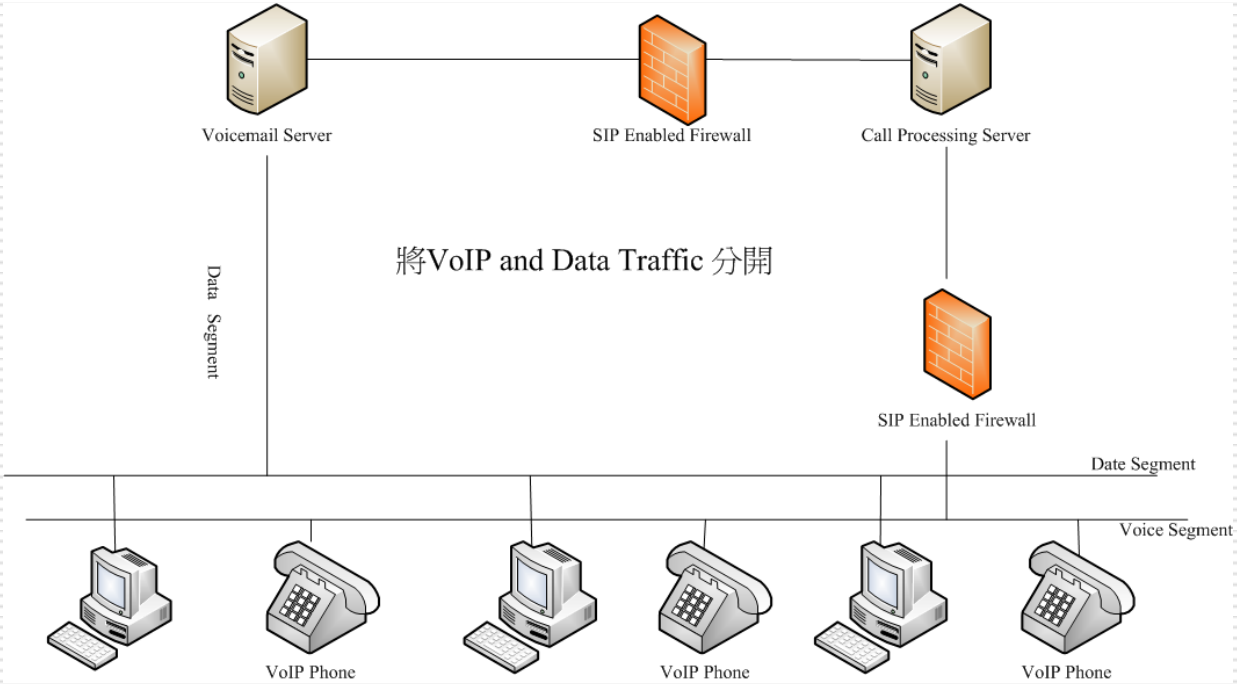
- Unwanted Calls and Messages (SPIT)
  - 如同網路的垃圾電子郵件(SPAM)，垃圾網路電話是一些來路不明的網路電話，沒有顯示來電號碼(Caller-ID)，內容大多是推銷、騷擾或詐騙。
  - 如果是垃圾電子郵件，只要將一堆垃圾郵件刪除不讓信箱塞爆即可，但是如果是一天接到數通垃圾網路電話，工作時接到、睡覺時接到、吃飯時接到，甚或是在人生中最重要的時刻接到壞了自己大好的前程，這都會使接到許多垃圾網路電話的使用者不堪其擾。

VoIP網路之防護策略

- 用來解決前面所敘述之攻擊的防禦方法有下列四種：
  - 將 VoIP and Data Traffic 分開
  - 設定身份驗證機制
  - 撥號時進行雙方身份驗證
  - 語音訊息需做加密

VoIP網路之防護策略

- 將 VoIP and Data Traffic 分開
  - 我們可以將VoIP的封包與Data Traffic做區隔，以防止其他人藉由網路封包監聽器來進行竊聽。

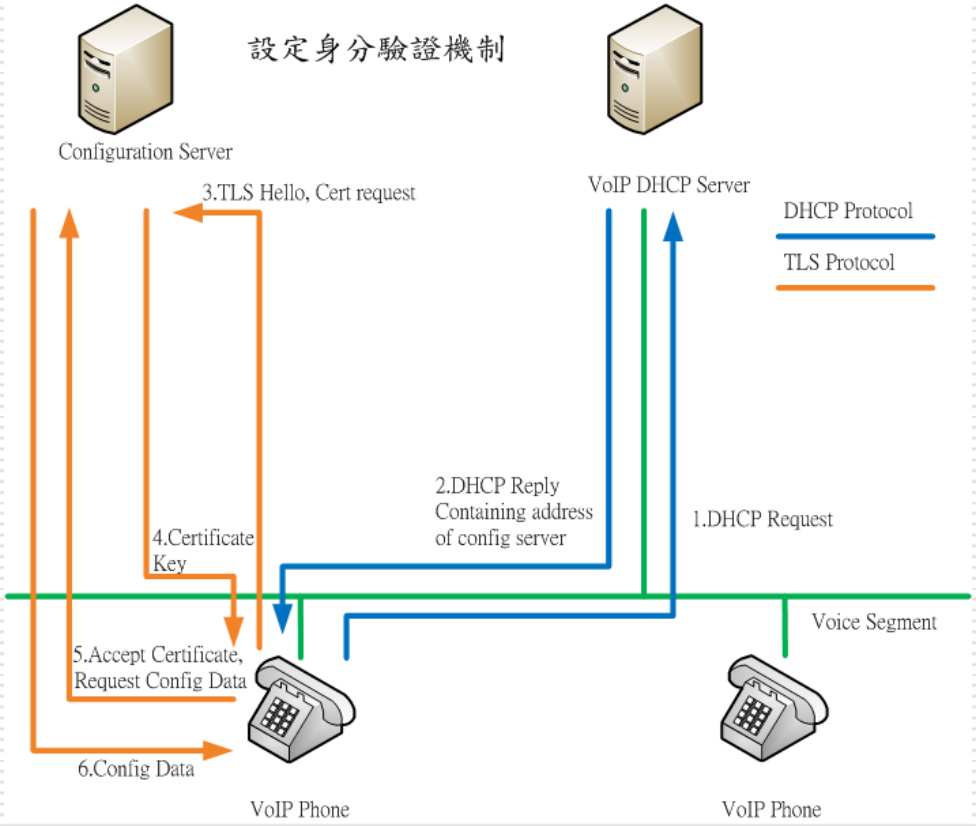


VoIP網路之防護策略

- 設定身份驗證機制
- 管理者可以透過一台Configuration Server來控管使用者，如下圖，當使用者要使用VoIP服務時，會先向DHCP Server取得自身要使用的IP與Configuration Server的IP；接著，Configuration Server會對VoIP Phone進行身份驗證，確認VoIP Phone的身份後，再給予啓用VoIP Service的設定檔，VoIP Phone再藉由此設定檔，進行VoIP連線。

VoIP網路之防護策略

- 設定身份驗證機制



VoIP網路之防護策略

- 撥號時進行雙方身份驗證
- 我們需要在撥號的同時，執行撥號端與接話端之間的相互身份認證，待互相確定對方之身份後，再建立一條加密通道，傳送語音。

- 語音訊息需做加密
- 利用現有的加解密系統，對語音資訊進行加密，如此一來，除非竊聽者破解密碼系統或取得通訊時所使用的金鑰，否則，將無法竊聽通話內容。

VoIP網路之防護策略

- 最近幾年VoIP的安全問題已慢慢浮現，針對這種情況，AVAYA、賽門鐵克、西門子等在 2005 年 2 月成立了 VoIP 安全聯盟(VOIPSA)，雖然目前VoIP相關的攻擊事件並不多，但其潛在的危險性仍不容忽視。

VoIP網路之防護策略

- 雖然有了很多的保護機制，駭客攻擊的方式仍在不斷的變動或更新，除了做好基本的防禦工作外，平時使用也要小心。當然，定期的去更新防禦駭客的方式也是一種方法。
- 雖然駭客可能還是有辦法入侵，不過有防禦的動作，就會降低駭客想要攻擊的可能性。畢竟越多的防護，要破解也就越難，這時駭客到不如去找那些沒有防護的電腦去攻擊，才比較可能成功。

參考資料

- 「安全資訊管理.ppt」。
- 「 http://www.voipsa.org/」, VOIPSA。
- 「http://www.voip-news.com:80/」, VoIP-NEWS。
- 「Security Challenge and Defense in VoIP Infrastructures 」, Butcher, D., Xiangyang Li, Jinhua Guo, IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 2007。
- 「 Strategies to Keep Your VoIP Network Secure」, Wesley Chou, IT Professional, Volume 9, Issue 5, Sept.-Oct. 2007 Page(s):42 – 46。

感謝聆聽　敬請指教