

網絡語音保安

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
何謂網絡語音?.....	3
II. 網絡語音規約.....	4
ITU-T H.323.....	4
會話啟動協議 (SIP).....	5
媒體通訊閘控制規約 (MEDIA GATEWAY CONTROL PROTOCOL, MGCP).....	5
III. 網絡語音之保安威脅.....	6
IV. 對策與最佳作業實務.....	8
使用 IPSec、TLS 和 S/MIME 之加密算法.....	8
用戶與設備認證.....	8
控制語音和數據分段 (DATA SEGMENT) 之間的互動.....	8
小包檢驗.....	9
抗電腦病毒軟件與保安修補程式.....	9
網絡語音電話終端用戶之最佳作業實務.....	9

摘要

網絡語音技術（Voice over IP, VoIP）透過互聯網、內聯網或其它小包交接網絡（packet-switched network）之語音內容傳送，來結合全球的話音通訊和數據。住家和企業用戶可使用專用互聯網規約（IP）電話，或是使用運行著 VoIP 軟件的聯網電腦來作為語音直接溝通方式。成本效益成為企業願意從傳統電話系統轉換到 VoIP 的主要誘因。VoIP 基礎建設帶來新的語音附加價值和多媒體服務，為服務提供者創造了豐富的潛在收入，並增加其市場部署。本文討論許多使用 VoIP 科技所引起的相關保安議題，並建議保護 VoIP 網絡和系統的對策。

I. 介紹

何謂網絡語音？

在 VoIP 科技中，首先將語音訊號分成框架（frames），之後儲存成數據小包（data packets），最後透過使用語音通訊規約之聯網規約（IP）網絡來傳送。如今，雖然有少部份 VoIP 系統使用如 SCCP¹之類的專利規約，但大部份 VoIP 系統使用下列其中一個標準：H.323²或是會話啟動協議（Session Initiation Protocol, SIP）³。

¹ <http://www.javvin.com/protocolSCCP.html>

² <http://www.itu.int/rec/T-REC-H.323/e>

³ <http://www.ietf.org/rfc/rfc3261.txt>

II. 網絡語音規約

兩個最廣泛使用的 VoIP 規約是 ITU 標準 H.323 和 IETF 標準 SIP，兩者皆是訊號規約，用來設立、維修和終結 VoIP 通話。此外，Media Gateway Control Protocol (MGCP)⁴ 是提供 VoIP 通訊閘和傳統 PSTN (Public Switched Telephone Network) 通訊閘⁵ 之間的訊號和控制規約。

ITU-T H.323

H.323 隸屬於 ITU-T 規格下的綜合規約，用來在網絡上寄送語音、影像和數據，H.323 規格包含幾項附屬規約：

1. H.225 用來確定通話控制（如：通話設定和 teardown）；
2. H.235 用來確定 H.323 的保安結構和通話設定；
3. H.245 用來確定如終端機能力的 media paths 和 parameter negotiation；
4. H.450 用來確定如通話保留（call hold）和通話等待（call waiting）等補充服務。

H.235 也提供一些保安功能，例如認證、完整性、私隱和支援一些 H.323 通訊內的不可否認性（non-repudiation），其設計是用來與其它規格如 H.245 和 H.225 共同操作。

透過傳輸層保安（Transport Layer Security, TLS）便可安全設定通話。通話設定後，啟動了一個通話控制，使加密算法和媒體通道的資訊進行交涉。H.323 採用實時通訊協定（Real-Time Transport Protocol, RTP）/ 實時控制協定（Real-Time Transport Control Protocol, RTCP），作為其傳輸規約，這些傳輸規約都建立在 UDP 之上。加密算法是由第三者硬件或在其它網絡層的 RTP 小包進行。

在 H.323 下的認證可以是對稱加密式認證（Symmetric encryption-based），或訂閱式認證（Subscription-based）的。對稱加密式認證並不需要通訊實體之間的事先接觸，因該規約使用 Diffie-Hellman 交換鑰匙來產生兩個實體之間的分享秘密（shared secret identity）。參照 H.235 的建議，訂閱式認證需要事先訂立分享秘密，其有三個不同種類；（1）基於密碼與對稱加密算法、（2）基於密碼與雜湊（Hashing）、（3）基於核證與簽署。

⁴ <http://tools.ietf.org/rfc/rfc3435.txt>

⁵ <http://tools.ietf.org/rfc/rfc3525.txt>

會話啟動協議 (SIP)

SIP 是一種文本 (text-based) 應用層規約，針對小包電話網絡中的訊號和會話管理。SIP 定義於 RFC 3261⁶中。SIP 使用類似 HTTP 規約的 request-response 模式，在 SIP 中，認證和授權的處理是「*either on a request-by-request basis with a challenge/response mechanism, or by using a lower layer scheme*」⁷，即認證和授權可在 Request-by-request 形式下的質疑/應答機制處理，又或使用較低層級的方案處理。因 SIP 的保安能力是非常有限的，SIP 請求和應對無法進行點對點的加密，原因是在許多網絡架構中出現的代理伺服器，均須看得見例如請求和路徑的訊息字段，以確保 SIP 請求路徑正確規定，語音數據是透過 UDP 和 TCP 以簡單文本 (Clear text) 來進行傳送的。

雖然 SIP 支援基於 S/MIME 的數碼證書加密方式，但無法對一些使用於請求和應對的標頭字段 (header fields) 進行加密，SIP 規約依賴如 TLS 或 IPSec 等傳輸層保安機制，以提供整個訊息所要求之保安條件。

媒體通訊閘控制規約 (MEDIA GATEWAY CONTROL PROTOCOL, MGCP)

Media Control Working Group 於 RFC 3435⁸報告中發表 MGCP，指出「*MGCP messages will always be carried over secure Internet connections as defined in the IP security architecture as defined in RFC 2401, using either the IP Authentication Header, defined in RFC 2402, or the IP Encapsulating Security Payload, defined in RFC 2406*」⁹，這表示 MGCP 容許數據起源認證、無連接式的完整性和可進行在媒體通訊閘 (Media Gateway, MG) 和媒體通訊閘控制器 (Media Gateway Controller, MGC) 間訊息的抗重播保護。MG 將 circuit-switched traffic 方式轉換為基於小包的運輸方式，而媒體通訊閘控制器 (Media Gateway Controller, MGC) 則決定運輸方式的服務邏輯。

⁶ <http://tools.ietf.org/rfc/rfc3261.txt>

⁷ 同上

⁸ <http://tools.ietf.org/rfc/rfc3435.txt>

⁹ 同上

III. 網絡語音之保安威脅

VoIP 系統依賴數據網絡來進行傳送，即是 VoIP 系統的保安弱點都和任何數據網絡發生的保安漏洞和各式攻擊有關。舉例而言，在傳統電話系統中，線路竊聽（wire-tapping）須要實體接達電話線路或入侵辦公室專用電話交換機（PBX）才可做到。但對 VoIP 而言，將語音轉換成 IP 小包便可能通過許多網絡接達點。因此，入侵者可在攻擊時擷取已暴露的數據便行。事實上，有關 IP 的所有保安風險也對 VoIP 不利，例如電腦病毒、拒絕服務（denial-of-service）和中間人攻擊（man in the middle attack）。

因為針對 PC 系統之攻擊技術日益普及，所以基於個人電腦（PC）操作的 IP 電話也特別易受攻擊。這包括操作系統漏洞、應用系統漏洞、服務漏洞、電腦蠕蟲、病毒等等。基於 PC 操作的 IP 電話也有被針對整個數據分段（data segment）來攻擊的危險。

因語音通訊規約是由會話控制規約（session control protocols）、IP 地址和 TCP/UDP 埠資訊以小包方式封閉，在使用網路位址轉換（Network Address Translation, NAT）技術的網絡中，IP 地址和小包連接埠（port）資訊是無法加密的，因 NAT 設備需要此類資訊以執行轉換功能。這便等於增加了保安限制。

H.323 規約使用 TLS 來保護，事先定義的 TCP 埠 1300 必須用來建立 Call Connection Channel，使首次連結時沒有其它保安機制。此弱點和眾所周知的連接埠可對規約造成保安威脅。

對 SIP 而言，加密算法是建立於使用 S/MIME 的基礎上，只有訊息內特定的訊息標頭已被加密，重要的訊息標頭如「To」、「From」和「Call-ID」等欄位是沒有加密的。

Uncontrolled barge-in 對 MGCP 是眾所皆知的保安威脅。因語音小包可透過適當 UDP 埠導入通訊閘，除非執行了保護措施，否則攻擊者有可能可以聽到語音通訊。為降低威脅，通訊閘應只接受來自事先定義的 IP 地址和 UDP 埠的數據，其缺點便是須要更多處理過程，且 IP 地址可以被仿冒。為對抗仿冒，可設定 MGCP，從啟動通訊閘傳遞 remote session description 至目標通訊閘，以進行檢驗，然而，此舉卻增加通話設定時間。

VoIP 服務也容易被他人濫發（spamming），又稱為濫發網絡電話攻擊（Spam Over Internet Telephony, SPIT）¹⁰，SPIT 在目標 IP 電話中留下非應邀促銷的語音訊息，因語音訊息的數據量通常大於電子郵件的數據量，所以 SPIT 對網絡之影響大大高於一般濫發電子郵

¹⁰ <http://www.voip-news.co.uk/2007/11/01/spam-over-internet-telephony-threat-grows/>

件所造成的影響。

攻擊者也會嘗試攻擊 VoIP 科技，以脅持身份和偷取金錢¹¹。此攻擊與電子郵件的仿冒詐騙（Phishing）攻擊類似，因此稱為語音網絡仿冒詐騙（Vishing 或 VoIP Phishing）。受害者將收到電子郵件或電話，引導受害者至一個顧客服務號碼，受害者在此處將面對許多語音慫恿指示，意圖偷取帳戶號碼、個人身份號碼和其它重要資訊。

¹¹ <http://www.fbi.gov/page2/feb07/vishing022307.htm>

IV. 對策與最佳作業實務

使用 IPsec、TLS 和 S/MIME 之加密算法

加密算法是一種維護傳送訊號保密性的方法，因 SIP 是一項應用層規約，該加密機制可使用於 protocol stack 的較低層次，例如在網絡和傳輸層中，個別使用 IPsec 和 TLS。對 SIP 訊息本身而言，可使用 S/MIME，然而，加密和解密會消耗很多中央處理器的資源，且處理費時，這些因素對傳輸品質皆有影響。假如 VoIP 通話整體延遲時間超過 250 毫秒 (milliseconds)，便會明顯影響通話質素。此外，點對點保安的 SIP 請求和對應並不能完全被加密，因為代理伺服器必須看見一些標頭字段（如 IP 地址、連接埠號碼等等）以選擇數據路徑。

即使用了加密算法，實體接達到 VoIP 伺服器和通訊閘可能容許攻擊者去執行流量分析 (Traffic analysis)，並從加密訊息中得到通話資訊¹²，因此應設立適當的實體保安，以限制接達主要 VoIP 的網絡元件。

用戶與設備認證

一些通話處理伺服器有自動電話註冊功能，利用暫時配置 (temporary configuration) 來引導裝載 (Boostraps) 未知電話，並准許接達網絡，此功能有助於 IP 電話的大量部署，但也存在威脅，因虛假 (rogue) 設備連結至網絡後，便會開始執行未經授權之服務或啟動對抗其它設備的攻擊。使用 IP 電話 MAC 地址的設備認證是解決此問題的其中一個方案，還應取消通話處理伺服器的自動註冊功能。假如一個帶有不知名 MAC 地址的電話試圖從通話處理伺服器中下載網絡配置時，該請求將被拒絕，使這虛假 IP 電話不能獲得網絡配置，因伺服器不能辨認 MAC 地址，致使這些虛假 IP 電話無法連結至網絡。用戶認證 (如用戶 ID、密碼或 PIN¹³) 也是避免通話偽冒 (masquerading) 之有效措施，因其提供一定水平的不可否認性 (non-repudiation) 和通話者身份確定。

控制語音和數據分段 (DATA SEGMENT) 之間的互動

基於 IP 操作的電話透過即有 IP 數據網絡來提供電話通話平台，但是為了維護服務品質 (QoS)，延展性 (scalability)、可管理性 (manageability) 和保安，語音與數據應盡可能使用不同邏輯網絡來分開，把 IP 語音從傳統 IP 數據網絡區分開來，可大大減低 VoIP

¹² http://www.freeswan.org/freeswan_snaps/CURRENT-SNAP/doc/ipsec.html

¹³ http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/3_3_2/ccmcfg/b07user.html

受攻擊的風險。

要語音與數據分段分開，虛擬 LANs (VLANs)、接達控制和狀態檢查 (stateful) 防火牆等科技可提供第三層 (Layer 3) 數據分離 (segmentation)，以分開語音分段和數據分段，且應放置狀態檢查防火牆於數據分段的網絡交匯處。第三層交換器 (Layer 3 switch) 也可透過接達控制和過濾來控制數據分段和語音分段之間的交流。

為了更進一步保護 VoIP 基礎建設，機構也許要考慮封閉式 VoIP 系統，只有機構內合資格用戶方可接達至只作為內部通訊用途的 VoIP 服務。此將完全把 VoIP 服務從互聯網分開，並減低外部網絡攻擊之威脅。

小包檢驗

某些 Network Intrusion Prevention Systems (NIPS)¹⁴可對 VoIP 規約進行語法分析和解析，對推行 NIPS 的 VoIP 系統而言，可偵測和預防針對 VoIP 服務的攻擊。

抗電腦病毒軟件與保安修補程式

使用軟件連結 VoIP 的電腦和其它 VoIP 伺服器與通訊閘時，應以個人防火牆保護。此外，抗電腦病毒和惡性程式軟件也應更新到最新的病毒識別碼和惡性程式碼定義。此將提供數據分段攻擊的基礎保護，此等攻擊亦可能轉換至語音分段。此外，基於 PC 操作之 IP 電話的保安修補程式和 VoIP 伺服器與通訊閘也應隨時更新。

因客戶 PC 病毒威脅日益普遍，VoIP 專屬 IP 硬件電話 (VoIP dedicated IP hardware) 比基於軟件操作 (software-based) 的 IP 電話更好 (即是執行 VoIP 軟件的電腦)。因 VoIP 可能會在企業防火牆上打開數據通道，基於軟件操作的 IP 電話的風險便較高。如軟件被錯誤配置或有保安漏洞，這可能讓未經准許的數據小包通過防火牆。此外電腦病毒、電腦蠕蟲和其它威脅或會從系統其它元件如瀏覽器之類入侵電腦。但是，基於某些原因如電話本身的設計缺點，硬件 IP 電話有時的確有其保安問題。

網絡語音電話終端用戶之最佳作業實務

當使用語音通話而 VoIP 系統失敗時，VoIP 電話用戶須注意和應計劃應變 (Contingencies)。為了保護 VoIP 仿冒詐騙攻擊，用戶不應在進行 VoIP 通訊或對話時，對陌生人公布敏感性資訊如信用卡資料、銀行帳戶或登入憑證等。

對基於軟件操作之 IP 電話用戶而言，其電腦需受個人防火牆保護，並配備安裝了最新

¹⁴ [http://www.icsalabs.com/icsa/topic.php?tid=aeb3\\$347927fc-1ef76edd\\$c11f-5218d1b1](http://www.icsalabs.com/icsa/topic.php?tid=aeb3$347927fc-1ef76edd$c11f-5218d1b1)

病毒識別碼 / 惡性程式碼定義的抗電腦病毒 / 惡性程式碼修復軟件。電腦內的所有軟件，包括 IP 電話軟件，應強制執行一致性和適當的保安修補程式管理和更新。

敏感性數據不應儲存於 IP 電話中，因 IP 電話並無既有的加密系統來保護數據。同時，網路管理員等其他人也可能透過 TFTP 遠端接達 IP 電話中的敏感數據。