網路電話之安全性分析

(The Security Analysis of VoIP)

黃秀園　李正吉　楊竣吉
亞洲大學
電腦與通訊學系
台中縣霧峰鄉柳豐路 500 號
cclee@asia.edu.tw

摘要

由於現行網際網路的方便性，人們可以利用網際網路的便捷，與在世界的另一端互通語音，再者傳統公眾電話網路〈PSTN〉費用不低，因成本考量，人們期望可以透過網路來進行交談，在本文中，我們將說明在網際網路上，使用網路電話時，目前可能所遭遇到的攻擊，並且指出一些安全技術，以抵擋在網際網路上使用網路電話時，所遭遇到安全威脅。

關鍵詞：網路電話、SIP、認證

Abstract

By the convenience of the current Internet, people can use the Internet to interflow the voice with each other in the world. Due to the cost of using traditional public telephone network <PSTN>, people hope to talk through the Internet. In this paper, we shall introduce some threats about VOIP (Voice over Internet Protocol), and point out some security technologies to withstand these threats. We analyze some protocols on VOIP.

Keyword；Authentication, SIP, VOIP.

一、前言

VoIP〈Voice over IP〉被稱為網路電話，是一種透過網際網路以數位化的方式傳送語音封包的技術，此技術需先把語音由類比訊號轉換成數位化訊號，再將資料經由編解碼器進行處理後，由 IP 技術傳送，使得雙方建立通話通道，此時彼此間的線路是屬於專線性質。

VoIP 的源由，早期網際網路興盛時，一些開發人員便著手於如何利用 IP 技術透過網際網路來發展網路電話，只是當時網際網路的軟、硬體技術尚處於雛型，透過網際網路來傳輸語音的效果並不佳，僅限於實驗階段。[1, 5]

1995 年二月，由以色列 Vocaltee 公司率先開發出網路電話軟體，此套軟體可以讓同樣在網際網路上的各地網友們，實現了可同時在網際網路上撥打電話的語音通訊與資料傳送的服務，而不像以往需透過公眾電話網路〈PSTN〉來交談，再者撥打網路電話費用只需一般網路使用費遠低於一般國際或長途電話的費用，雖然當時的語音品質尚處於不佳，但仍然造成全球各地網友們廣泛的興趣。[1, 5, 6]

隨著網路電話的發展，有網路業者於 1996 年推出了網際網路閘道器〈IT Gateway，ITG〉使得網路電話可與傳統一般公眾電話網路〈PSTN〉相連結，也就是使用者可以不需再借助 PC，只需有一具網路電話，即可與傳統的話機交談。而後一

些網路業者發現網路電話可帶來的商機，於1998年陸續建立相關網路電話的通訊協定：H.323、SIP〈Session Initiation Protocol〉會談啟始通訊協定、MGCP〈 Media Gateway Control Protocol〉媒體閘道器控制通訊協定等等，主要是以PC to PC 來點對點的通訊傳輸為主。[1,5.6]

網路電話盛行至今，其仍有許多問題等待解決，如語音的傳輸品質、服務品質、安全性與緊急電話服務等，尚未達到傳統一般公眾電話網路〈PSTN〉的水準。本文所探討主要是其安全性議題，Voice over IP Security Alliance〈VoIPSA〉[8]網路電話安全聯盟也於2004年二月成立，主要任務為把影響網路電話的各種安全威脅加以區分及描述。可預期的，網路電話的安全威脅，會因網路電話的發展與日遽增，如何去確保網路電話通話時的安全性，將是目前相當重要的議題，並且從眾多協定中，選定SIP來加以探討。

本文主要共分成七個部份，第二部份介紹網路電話主要的部份協定；第三部份探討網路電話之安全威脅及安全需求；第四部份就其相關研究安全技術介紹；第五部份為相關分析；第六部份為結論；第七部份為一些參考文獻、資料。希望能對於網路電話安全性議題有興趣者，能透過此篇文章，更加了解網路電話的安全問題。

二、網路電話協定

網路電話由眾多協議共同組成起來，從早期的H.323到SIP、MGCP至MEGACO/H.248分別或共同由ITU-T及IETF所制定，ITU-T 屬於電信通訊〈Tele-Communication〉協定，IETF則是屬於資料通訊〈Data-Communication〉協定，下列會分別介紹電網電話協定：

(一)、H.323

由國際電信聯盟〈International Telecommunications Union，ITU〉第16研究組於1996年6月起訂定是屬於一系列的標準協定，主要是用以在網路上利用封包使用視訊電信〈Video Telephony〉和多媒體會議〈Multimedia Conferencing〉；而後1998年1月國際電信聯盟ITU制定H.323 Version 2；1999年制定H.323 Version3，主要是為合併先進的功能及新的概念以使H.323有能力在現有的網際網路中使用網路電話。

2000年11月17日為符合市場遽增的需求，國際電信聯盟ITU又制定新的標準H.323 Version 4增加新的功能，主要是強調可調整性〈Scalability〉、可靠性〈Reliability〉和彈性〈Flexibility〉，以增加有彈性的調整閘道器〈Gateway〉及多端控制器單元〈Multipoint Controller Unit，MCU〉；2003年因網路電話與系統的互通性及需求的增加，又制定H.323 Version 5，以包含更多功能，新的版本也陸續在進行中。

至今，H.323已被定義成可設定閘道器來進行語音和視訊的編、解碼以及封包化操作，並且提供所需的定址功能、通話信令、控制功能、資料交換功能和多媒體管理和寬頻管理來解決多媒體網路傳送時的及時性及連續性問題；而因H.323也衍生出其他通訊協定：H.235系列、H.246、H.248、H.332、H.450系列、H.460系列、H.510、H.530等。

H.323並不依賴於網際網路結構中，而是個別獨立於作業系統與硬體的平臺上，來支援多端功能、組播跟頻寬的管理，其具備相當高的靈活性，可支援包含不同功能節點間和不同網域間的多媒體會談；但H.323並不支援群播協定只可採用多端點控制單元〈MCU〉來構成多端點會議，所以只有有限的多端點用戶；其也不支持呼叫轉移。

(二)、SIP

由網際網路工程事務小組〈Internet Engineering Task Force，IETF〉於 1999 年二月為改進 H.323 系列協定無法滿足現行網際網路的多樣化服務，而制定了可整合傳統一般公眾電話網路〈PSTN〉與網際網路〈Internet〉相結合的會談起始通訊協定〈Session Initiation Protocol，SIP〉，是一種多媒體通訊的控制協定，其協定制定沿革也仍然在陸續制定中，如表 2-1 所示。

表 2-1 SIP 協定的制定沿革

編號	制定日期	功能、事件
RFC2543	1999 年 2 月	SIP 協定
RFC2616	1999 年 6 月	HTTP/1.1
RFC2617	1999 年 6 月	HTTP 認證
RFC2976	2000 年 10 月	SIP 資訊方式
RFC3261	2002 年 6 月	SIP 協定
RFC3262	2002 年 6 月	SIP 暫時性回應的可靠度
RFC3263	2002 年 6 月	位置伺服器
RFC3264	2002 年 6 月	提議 / 回應模型
RFC3265	2002 年 6 月	特殊事件的告知

SIP 是以一種近似 HTTP 本文為基礎的主從式 Client-Server 協定，具有是採用 SIP 規則資源定位語言敘述〈SIP Uniform Resource Locators〉，可方便修改或測試作業，比 H.323 更具有靈活性與擴充性，其主要功能是用來建立、修改跟結束多媒體會談，並且整合語音、視訊和一些即時性訊息傳送的交談式通訊服務。

SIP 同時也支援群播與單點播送〈Unicast〉的功能，即使用者可隨時加入正在進行的視訊會議中，而在網路 OSI 中，屬於應用層協議，可透過 UDP 或 TCP 協定來進行傳送。

(三)、MGCP

由網際網路工程事務小組〈Internet Engineering Task Force，IETF〉於 1999 年 10 月發表 RFC2705 的媒體閘道器控制通訊協定〈Media Gateway Control Protocol，MGCP〉是利用軟式交換〈Softswith〉技術的主從式〈Master-Slave〉架構的通訊協定，有別於 H.323 與 SIP 協定是專門對於網路電話提出的二套各別獨立的標準，二者間並不相通與相容，反觀，MGCP 可同時支援 H.323 及 SIP，因為 MGCP 只牽涉到閘道器分解的問題。

MGCP 主要組成是由數個負責媒體流處理的媒體閘道器〈MG〉，和一個掌控呼叫建立與控制整個通話過程的媒體閘道控制器〈MGC〉所建構成，其中 MG 是負責將語音封包化並加以傳送，而 MGC 又被稱為通話代理人〈Call Agent〉，當通話連線建立時，相關的通話訊息內容都會傳送到 MGC，以控管整個通話過程，而 MG 也在 MGC 的管控下，實現了跨網域的多媒體電信會談。

(四)、MEGACO / H.248

2000 年 11 月由 ITU-T〈Telecommunication Standardization Sector of International Telecommunication Union〉與 IETF 為擴充 MGCP 功能而共同訂定，提供更有彈性的介面，來允許媒體閘道控制器〈MGC〉可對媒體閘道器〈MG〉進行動態的控制與管理，或更多媒體閘道器〈MG〉的所有操控；此協

定，IETF 稱作 MEGACO，ITU 稱作 H.248，而 MGCP 與 MEGACO 均在訊號〈Signaling〉傳送過程中支援 IPsec，MEGACO 在封包標頭〈Header〉使用認證〈Authentication〉的功能，以加強語音通訊的安全性。在語音資料傳送過程方面，語音資料內容與來源位址中 MGCP 與 MEGACO 均支援加密功能，以防範非通話者、有心人士的偷聽與竊取。

三、網路電話之安全威脅及安全需求

由於網路電話的便利，人們可以更方便與遠方溝通，但也因方便所相對衍伸出許多問題，早期網路電話面臨的安全威脅主要有下列四種：[5]

1. 阻斷式服務〈DoS〉攻擊
2. 非法存取
3. 話費詐欺
4. 竊聽

我國有國內學者，自己也歸納出下列幾項影響安全的問題：[2]

1. 建置和安全是二件事
2. IPT 網路淺藏許多安全問題
3. 網路電話機可能就是弱點所在
4. 遠端使用者的安全問題
5. 認證與授權所潛藏的風險
6. 如何強化 VoIP 主機或設備
7. 安全設備可能影響通話品質

而真正世界公認的安全威脅標準，由網路電話安全聯盟〈VoIPSA〉[8]於 2005 年十月二十四日宣佈了 VoIP Security Threat Taxonomy ，把會影響網路電話的安全威脅分成四大類：

1. 不實的回應、服務否定與非法的訊號
2. 不斷重複傳送單一請託訊息而耗盡資源、流量修正
3. 電話氾濫、服務濫用
4. 資訊劫取、在未經同意的狀況下攔截訊號或使其繞道甚至修改。

而後，十一月十一日，有國內學者通訊分析師指出，「未來十年所有電信將都會是 VoIP，但目前，大部分的通訊設置是 VoIP 與傳統電話服務共存。而我不清楚到哪一刻，你會想捨棄掉傳統電話服務」，還表示，公司在下列六種情況下，應還是要採用傳統電話服務而非 VoIP，或至少是 VoIP 與傳統電話服務共存[3]：

1 、品質為重、連線可靠：

傳輸語音時，品質及可靠度為其最關鍵的部份；雖然透過語音來通訊對所有企業皆非常重要，但因為網路頻寬的問題，導致可能漏接關鍵電話或話質不佳，對一些企業而言更是吃不消。

2 、額外功能、網路邊際：

企業需要的功能，VoIP 卻無法全部提供：雖然一些已開始有緊急電話服務的提供，但以總體而言屬少數。

3 、網路速度、資金費用：

網際網路的使用量近乎滿載：即便企業已經取得足夠的寬頻，然而，企業的寬頻可能會因其他因素，導致無法提供 VoIP 充足的頻寬資源，特別是正在使用大量串流視訊流，或其他極耗頻寬的應用程式時。此問題雖可藉由傳輸速度的升級而獲得解決，但選擇升級傳輸速度時，主要的還是有關資金的花費：雖然 VoIP 保證會比傳統電話服務省錢，但 VoIP 先前的建置成本可能就需極高的花費來建構。

四、相關研究

網路電話協定有 H.323、SIP、MGCP 跟 MEGACO / H.248，其本身都各自有其安全性議題，本文主要是就有關 SIP 的方面，來加以討論。

SIP 本身提供了許多種不同的中繼點(Hop-by-hop)與端點對端點(End-to-end)的加

密機制，使封包的標頭及訊息本體受到保護，而傳輸或網路層會針對 SIP 訊息流進行加密，保持訊息的機密及完整。一般說來，IP Security(IPSec)是一個普遍使用的網路安全機制，以提供傳輸層的網路安全。

以現行 VoIP 的網路架構而言，SIP 的保密性是無法維護的，因為 SIP 在傳送時其標頭欄位的訊息是以一般文字格式方式存在，通常都是利用 TLS 傳輸層加密（Transport Layer Security）而加以加密，而現有的防火牆是無法提供 TLS 傳輸層加密的機制；而 SIP 本身也具有聊天、檔案傳輸、遠端控制以及應用與分享等功能，此意指著，在這些應用上幾乎是沒有任何限制的，因此相對地會導致一些嚴重的私密問題。例如：

1. 透過認證辨明使用者或伺服器身份

在通話進行中，攻擊者可能偽裝為正常使用者或者伺服器，為了辨別使用者或伺服器是否為合法需要一個機制來辨明，此種機制一般稱為認證機制。在 SIP 網路中，認證可發生在使用者代理人(User Agent)和代理伺服器間，代理伺服器在進行傳輸「訊息要求」前，需要 User Agent 認證。同樣地，User Agent 可向代理伺服器或重複向伺服器要求認證以辨明身分。

SIP 定義封包表頭是使用的認證方式。認證表頭包含一個經 SIP 訊息運算值的 Signature，此標頭在代理伺服器間傳送時不會改變表頭，而且包含 Nonce 值、範圍(The realm)、命令的模式(Request method)(由 User Agent 調度訊息要求的型態)、要求型態的版本與授權類型。且 SIP User Agent 所使用的 Proxy-authorization 表頭可以辨明身份，此包含了認證的類型、User Agent 的憑證及要求資源的範圍。

根據認證決定授權程度一旦認證完成，必須決定此身份是否可以使用所要求的服務。雖然經安全的認證，但是某部分的服務的存取仍需更進一步的認證。

2. IPSec 提供安全的通道環境

IPSec 為開放性的標準，在 IP 層提供了安全功能、認證及加密。

在 IPSec 執行時有三種協定被使用：

・Encapsulating Security Payload(ESP)協定：為一種安全協定，可提供數據安全傳輸、認證及重送偵測的防護。ESP 可完全壓縮數據，並可單獨使用或與認證表格同時使用。

・Authentication Header(AH)協定：可單獨使用或與 ESP 共同使用。AH 提供封包有關認證的服務。

・Internet Key Exchange 協定：一種混合性的協定，Internet Security Association and Key Management Protocol(ISAKMP)的框架下使用部分的 Oakley 和 SKEME。IKE 用來建立分享性安全政策及服務認證的金鑰(如 IPSec)。

在任何 IPSec 流量行經任一路由器、防火牆或主機時，必須要查證其群組的身份。此可以手動進入雙方主機中預先分享的金鑰來執行，或藉由認證授權(Certification Authority)服務或透過 DNS Secure(DNSSec)。

以下就幾篇討論 SIP 認證論文來加以介紹：

(一)、自行發展 SIP 的安全機制［4］

此篇主要介紹一個自行發展強化 SIP 安全性的安全機制，此篇的主要架構中需增加二個元件：認證伺服器(Authentication Server，AS)和註冊伺服器(Registration Server，RS)，來提供安全的認證機制，其相互認證的基本概念是在使用者代理人檢查 AS 是否為合法伺服器的同時 AS 也會檢查使用者的身份是否正確。而相互認證主要是保證動態攻擊者不能夠從伺服器端或著是使用者端獲得任何有關於使用者的資訊。

其相互認證機制的基本準則，在於使用者代理人和其伺服器端資料庫共同使用

一個”金鑰K”，而此主要金鑰K在任何情況下，都僅在使用者代理人和伺服器端資料庫之間傳，絕不可外流出去，以免資料外洩。

再者，AS在每個各別的認證中會傳送一個取得認證的訊息要求給使用者。這個訊號包含認證的兩個參數：RAND和AUTN。使用者需用主要的金鑰K和參數AUTN和RAND來當做輸入並且完成同樣類似在AS產生認證向量的計算。這個產生認證向量的過程包含許多演算法的執行。對於計算的結果，使用者能夠驗證這個參數AUTN是否的確是由一個合法的AS所產生的。並且同時，UA會計算出來參數RES在認證的回覆訊息中送回給AS。藉著此一認證的回覆，AS能使用認證向量來對使用者的認證回覆的RS與AS所預期的回覆的XRES做比較。如此便完成相互的認證。

其認證流程如下：

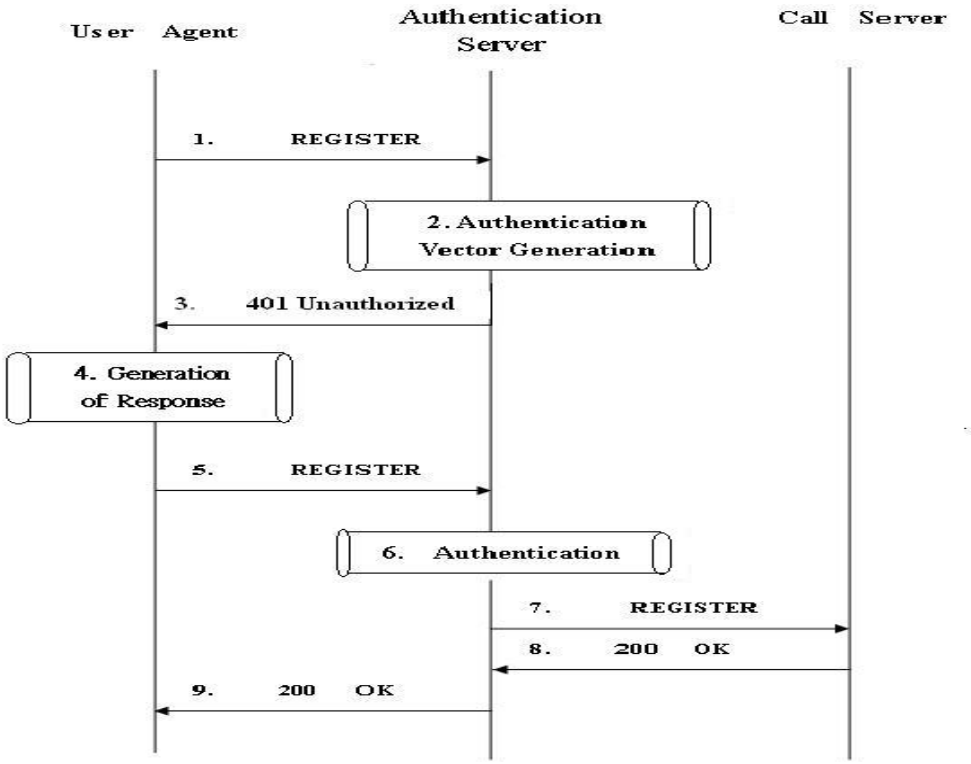
1、位置註冊流程：如圖一

使用者註冊位置資訊的過程。註冊時是由AS來認證。如果認證的過程成功，AS會知會通話伺服器此新註冊UA的位置。

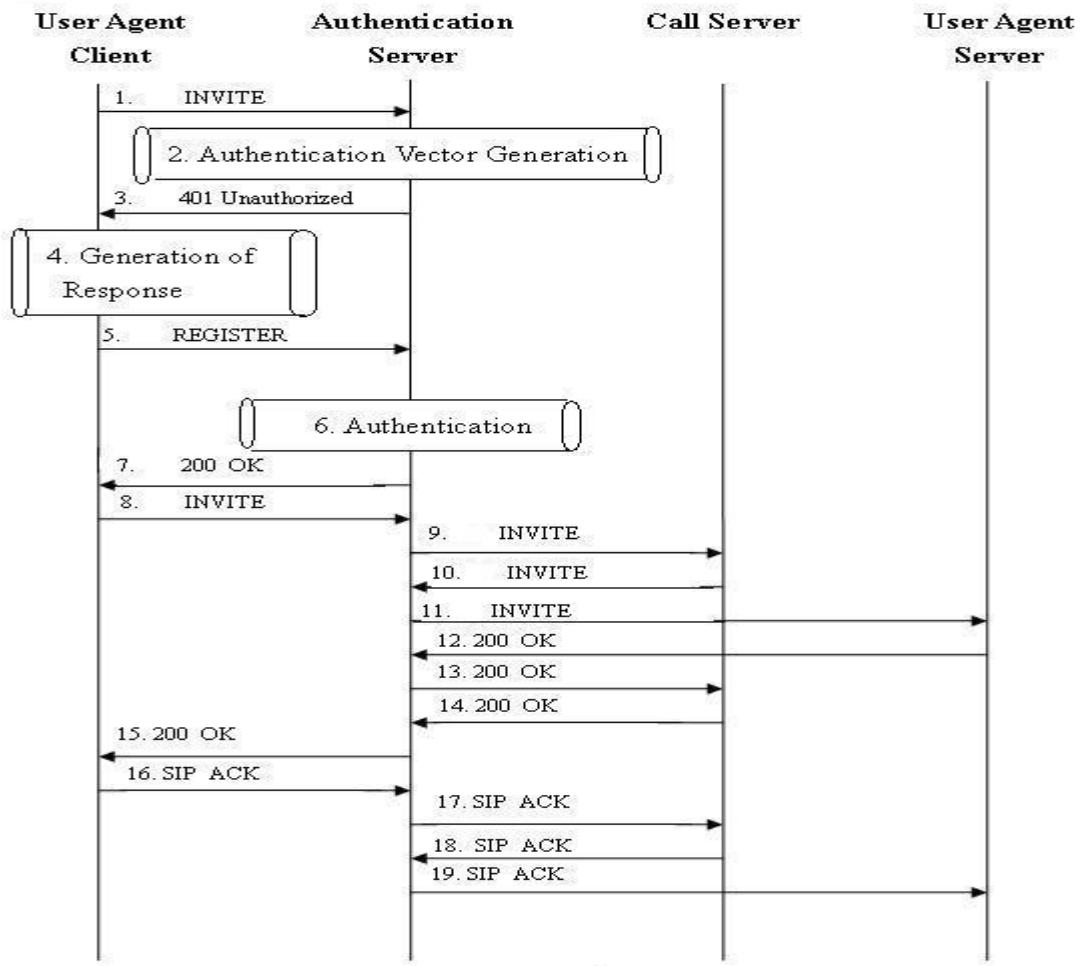
2、通話產生的流程：如圖二

通話建立訊號交握的過程。使用者的代理用戶端UA(UAC)向使用者代理伺服器(UAS)要求建立通話連線時，需要先完成認證以確保身分，再完成通話建立訊號傳遞。訊號交換的過程剛開始的時候(步驟1至7)，AS會要求UAC它開使認證的程序，就如同我們在A所提到的註冊過程。第二個階段(步驟8至19)是平常SIP產生連結的過程。

因為公開金鑰系統最容易於第一次交換金鑰時遭遇MITM(Man in the middle)式的攻擊，而此架構事先就分享金鑰以避免MITM的攻擊。



圖一 [4]



圖二［4］

（二）、Yang 等人的 SIP 認證法［7］

其流程如圖三所示，其基本是基於 Diffee-Hellman 的概念取決於困難離散的對數，步驟如下：

第 1 步：

Client：請求 REQUEST{username,t1⊕F(pw)}

第 2 步。

Server： (realm, t2⊕F(pw), F(t1,K))

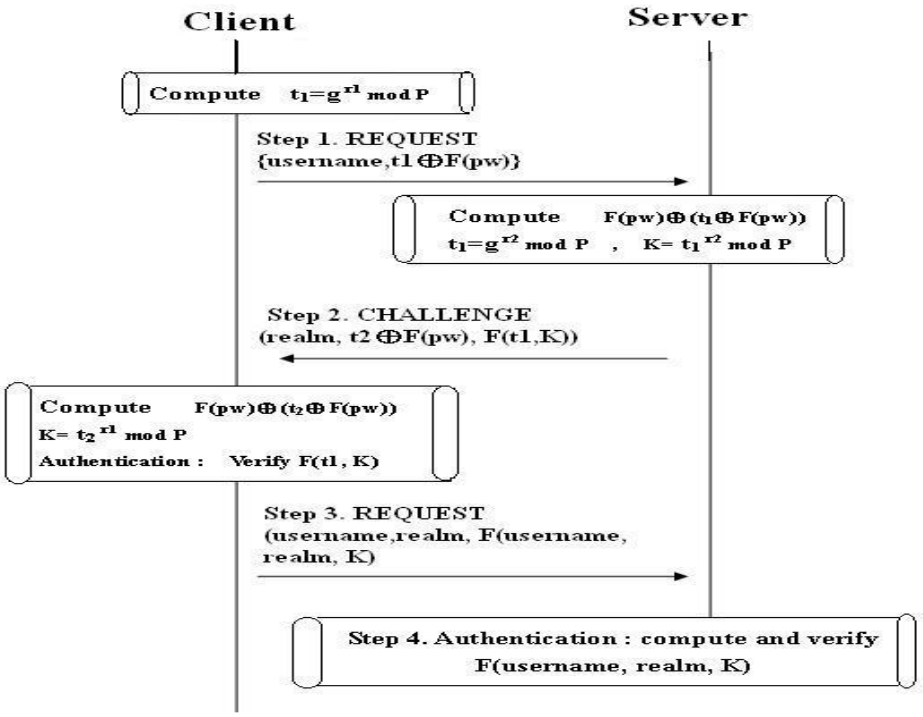
第 3 步：

REQUEST (username,realm, F(username, realm, K)

第 4 步：

Authentication: compute and verify F(username, realm, K)

此計劃可以抵禦重複攻擊，主要是因為如果一個攻擊者重複對 Server 傳送 {username,t1⊕F(pw)}，Server 將(realm, t2⊕F(pw)與 F(t1, K)}回傳，但因攻擊者並沒有 F(pw)，而在第三步驟時無法回傳 RESPONSE 給 server 因此此計畫是安全的。



圖三［7］

此計劃也可預防離線的密碼猜測攻擊與伺服器欺騙攻擊，理由是：

1、離線的密碼猜測攻擊：

〈1〉攻擊者可能會猜測偽造一個密碼 pw´並 計算 F(pw′).

〈2〉然後計算 t1′= F(pw)⊕(t1⊕F(pw))及 t2′=⊕F(pw)⊕4(t2⊕F(pw)).

〈3〉因為面對離散對數的困難，攻擊者不能計算出 K 所以無法對 Server 回應，因此，離線的密碼猜測攻擊不能在此計畫裡攻擊。

2、伺服器欺騙預防：

在此計畫，伺服器先計算 F(pw)而後獲得 F(pw)⊕(t1⊕F(pw))，然後伺服器計算$K=t1^{r2} \bmod p$ 與 F(pw)⊕(t2⊕F(pw))並與 F(t1, K)一起傳送給使用者

，使用者收到後運算 F(pw)⊕(t2⊕F(pw))與$K=t2^{r1} \bmod p$ 然後與使用者所傳送的F(t1, K)相認証，使用者就能證實身分，因模指數可知攻擊者不能扮演伺服器來欺詐用戶。

五、分析

SIP 所需的基本網路安全包含：維持傳輸訊息的機密及完整性、避免重送攻擊〈Replay attack〉及訊息偽裝、提供授權服務、保障通話進行中每位使用者的隱私權及 SPIT〈Spam for Internet Telephony〉垃圾網路電話[1, 5]。

SIP 還是像現今網路存有的問題一樣，目前現今一般討論網路電話 SIP 安全性的論文，主要都是就其認證方面，來加以分析，去比較其認證的效率時間性，並利用認證來解決上述所提的一些問題，像是避免重送攻擊〈Replay attack〉及訊息偽裝等問題，但也有就各種不同的 OSI 層分別比較，其認證的效率優缺點好壞等；而也有其他論文主要是研究硬體部分，比較屬於實作，有實驗結果例如閘道器加密實作，或者話機加密，至於軟體方面，則是屬於談話介面軟體設計，也是使用加密認證軟體來實作，其安全性仍需再加強中，而就整體網路電話也有許多論文在探討服務品質保證〈QOS〉方面。

六、結論與未來研究方向

網路電話盛行，但仍有其風險存在，網路加密軟體 PGP 的發明人 Phil Zimmermann 在 2005 年黑帽會議 The Black Hat conference 上曾發表他對未來產品佈局的看法[3]，他也同時表示網路電話上的安全加密將成為他下一個研究目標。他認為網路電話將繼電子郵件後，成為駭客攻擊的下一個目標；把網路電話資料加密，目前技術上辦得到。不過，今天的技術是使用公開鍵值加密系統(public key infrastructure；PKI)，也就是藉提供數位身分認證給通話的雙方，以確保通話的安全性。但是架構和管理公開鍵值加密系統的工程是十分浩大。Zimmermann 他希望成立一家公司，所創的系統不用 PKI；再者，網路電話因還在發展，所以其安全性仍然在建構中，其風險性仍有可能增加中，其安全議題可能仍有許多問題有待解決，國內有學者彙整提出最大限度的保障網路電話應用安全的幾項策：將用於語音和資料傳輸的網路進行隔離、將 SIP 服務做為一種應用程式來看待、選擇合適的產品和解決方案、語音資料流程的加密、合理規範企業員工的撥號許可權限 [1]。但這些也只是一些治標的方面，因為網路電話是運行於一般網路上，甚至跟傳統電話網路相接合，可能會有更多危險會出現，而現行的安全策略只能做到此些安全防護，未來也有可能出現其他新的風險。

七、參考文獻

[1] 賈文康編著，SIP會談啟始協議操典，民九四，初版，臺北：文魁資訊股份有限公司

[2] 資策會, http://www.find.org.tw/find/home.aspx

[3] 資傳網, http://cpro.com.tw/

[4] 郭大維, 林風, 楊佳玲等，“虛擬家網路環境：即時行動交談之設計與實作”，資訊工程系，資訊網路與多媒體研究所，國立台灣大學

[5] 戴江淮, 姜玲鳳編著，網路電話 SIP 原理與應用，民九四，臺北：儒林圖書有限公司

[6] 陳宏宇編著，VoIP網路電話技術，民九四，初版，臺北：文魁資訊股份有限公司

[7] Chou-Chen Yang, Ren-Chiun Wang, Wei-Ting Liu, “Secure authentication scheme for session initiation protocol”, ELSEVIER , Computers & Security 24, pp. 381- 386, 2005

[8] VoIPSA , http://www.voipsa.org/