會談邊際控制器於網路電話架構下的安全性實證研究

潘森豪[1*] 劉興華[2] 伍台國[3]

[1]國防大學管理學院資訊管理學系

[2]聲威網際科技

[3]國防大學管理學院資訊管理學系

論文編號：NM-43-02-01
來稿2022年4月8日→第一次修訂2022年5月4日→第二次修訂2023年1月16日→
同意刊登 2023 年 3 月 1 日

摘要

VoIP 於通資整合技術大幅提升的優勢下獲得了大量的應用，展現於近兩年全球新冠疫情嚴峻，以 VoIP 為核心技術的雲整合通訊服務 UCaaS(Unified Communication as a Service)引領居家辦公成為另一種工作型態。UCaaS 是基於 Internet 網際網路連結的服務架構，於通訊傳輸上存在安全的風險。本研究根據近年來網路語音設備製造商所提出的會談邊際控制器(SBC)，依照其提供協議轉換、資料加密、身份鑑別、防止惡意攻擊等安全防護機制，架設實際的通信環境；分別在 Azure 雲端服務平台安裝軟體版本的 SBC-SWe，及本地端安裝實體的 SBC，打造一個簡易的 UCaaS 通信環境以實作方式驗證。研究結果可作為產品改善的依據，也藉此提升客戶使用意願。

關鍵詞：會談邊際控制器(SBC)、整合通信服務(UCaaS)、協議轉換、傳輸層安全協定(TLS)、安全及時傳輸協定(SRTP)

*聯絡作者：潘森豪 email:pansenhaw@gamil.com

An Empirical Study of Security of SBC(Session Border Controller)in VoIP Networks

Pan, Sen-Hao [1]* Liu, Hsing-Hua [2] Woo, Tai-Kuo [3]

[1]Department of Information Management, National Defense University, *Taiwan, R.O.C*

[2] Hivocal Technologies

[3] Department of Information Management, National Defense University, *Taiwan, R.O.C*

Abstract

VoIP has lots of applications due to the advantages of the greatly improved integration of information and communication technology. It has been shown in the severe global Covid-19 epidemic in the past two years. Cloud-integrated communication service UCaaS (Unified Communication as a Service) using VoIP as the core technology has led the work-from-home to another work style. The service of UCaaS is based on the service structure of Internet connection, and there is a risk of security in communication transmission. This study is based on the Session Border Controller (SBC) proposed by the manufacturer of Internet voice equipment in recent years. According to SBC provides security protection mechanism such as protocol conversion, data encryption, identity authentication, prevention of malicious attacks, etc., to set up the real communication environment. Install the software version of SBC-SWe on the Azure cloud service platform and install the physical SBC on the local side whitch it creates a simple UCaaS communication environment to verify by implementation. The research results can be used as a basis for product improvement, and enhance customers' willingness to use.

Keywords: Session Border Controller(SBC), Unified Communication as a Service(UCaaS), Protocol conversion, Transport Layer Security(TLS), Security Real-time Transport Protocol(SRTP)

* Corresponding Author: Pan, Sen-Hao email:pansenhaw@gmail.com

一、前言

Covid-19疫情蔓延全球，對人類的生命造成威脅，衝擊了全球的經濟，也影響了人們的生活。台灣因為本土疫情持續嚴峻，政府於110年5月19日提升全國疫情警戒至第三級，企業為了維持正常運作並降低集體染疫風險，採取居家辦公模式(Work From Home, WFH)，創造出了一種新的工作型態。在此期間UCaaS(Unified Communication as a Service)成為了企業在語音、視訊、會議等即時通訊的解決方案，讓員工即使在居家辦公，依然可以使用行動分機、視訊會議與同事及客戶溝通。其中行動分機這項技術就是以VoIP為核心技術所發展的，因必須透過網際網路傳輸所以存在著風險，因此會談邊際控制器(Session Border Controller, SBC)在這個領域扮演著守護企業語音安全的重要角色。

隨著網路頻寬的穩定性提升，帶動了網路電話的普及應用，網路電話所面臨的挑戰是屬於安全性上的議題，語音閘道器、IPPBX、IP Phone、Softphone等構成VoIP通信的元件，皆須與網路連接，通話時必須依靠網路傳輸，因此也伴隨著網路帶來的風險，包含阻斷攻擊與身分竊取造成盜打甚至竊聽語音封包等資安威脅。SBC就是因應網路電話的安全性所發展出的標準，SBC的主要功能為防止惡意攻擊、會話管理、QoS(Quality of Service)監控和報告以及對服務的安全訪問，在語音及視訊服務的日益普及，這些功能對於確保網路電話與IMS(IP Multimedia Subsystem)服務的可行性非常重要，SBC將在IP通信時代的網路安全中扮演著關鍵的角色(Kaul & Jain, 2018)。

新一代的傳輸技術讓VoIP過去因語音品質如通話時的語音抖動(Jitter)、延遲(Delay)以及語音封包遺失(Packet Loss)已有良好的改善，新的問題發生如VoIP被盜打的事件卻時有所聞，駭客經由網際網路入侵VoIP系統，撥打國際電話，產生高額的通話費，使企業造成損失。因駭客有利可圖，故此類問題層出不窮(McInnes, Wills, & Zaluska, 2019)。SBC是部署在VoIP與網際網路之間的設備，其核心功能包含IP語音及視訊等其它即時通訊(Real Time)會談處理、訊令(Signaling)和媒體(Media)提供控制功能外，同時在網路邊緣對所處理的媒體內容進行安全保障（防攻擊、VPN隔離、防火牆等），因此在業界有語音防火牆之稱。

本文將建立VoIP與SBC於UCaaS的通信環境，並對其進行安全實證測試，驗證SBC在VoIP通訊環境中之間的所能提供的安全防護，以提升使用意願。

二、文獻探討

2.1 整合通訊服務(UCaaS)

UCaaS 為雲端服務的新應用型態，是將語音與視訊等多媒體服務置於雲伺服器內。UCaaS 供應商將 Application Server 託管在雲端平台如 AWS、Azure、Google cloud...等，用戶可以下載專屬軟體到個人設備上，也可以通過 Web 瀏覽器使用 WebRTC 插件(Plug-in applet)。透過網際網路便可獲得語音（電話）、會議（視訊或語音）、即時通訊、電子郵件、文件共享等的整合通訊服務(Lazar, 2020)。

2.2 VoIP 的威脅概述

隨著VoIP服務的日益普及，而它正面臨著危險的漏洞和安全威脅。由於VoIP部署在Internet上，因此它承襲了Internet開放環境的傳統威脅(Al Saidat, 2019)。安全性是VoIP系統必須面臨的挑戰之一。VoIP中主要使用的協議為會談發起協議SIP(Session Initiation Protocol) (Rosenberg, Schulzrinne, Camarillo, Johnston, Peterson, Sparks, & Schooler, 2002)，最初設計時的重點放在提供開放式服務以及簡易理解通訊交握程序，但忽略了系統從註冊、通話呼叫甚至通話期間的安全性(Karopoulos, Portokalidis, Domingo-Ferrer, Lin, Geneiatakis & Kambourakis, 2015)。SIP協議常見的攻擊包括竊聽(Eavesdropping)、通話詐欺(Fraud)、註冊劫持(Registration Hijack)和DoS(Denial of Service)攻擊(Ghafarian, Seno & Dehghani, 2016)。通話詐欺可分為幾個階段，如圖2. 1所示(Machens, Gebauer & Wermser, 2018)。基於維也納和埃森獨立誘補系統的大規模驗證中，註冊劫持為最常見的攻擊，如圖2. 2所示；經過詳細分析後，確定了攻擊者的目的，例如，在成功的註冊劫持攻擊之後，攻擊者試圖建立與PSTN(Public Switched Telephone Network)網路的電話通話，以進行通話詐欺。(Gruber, Hoffstadt, Aziz, Fankhauser, Schanes, Rathgeb & Grechenig, 2015)。

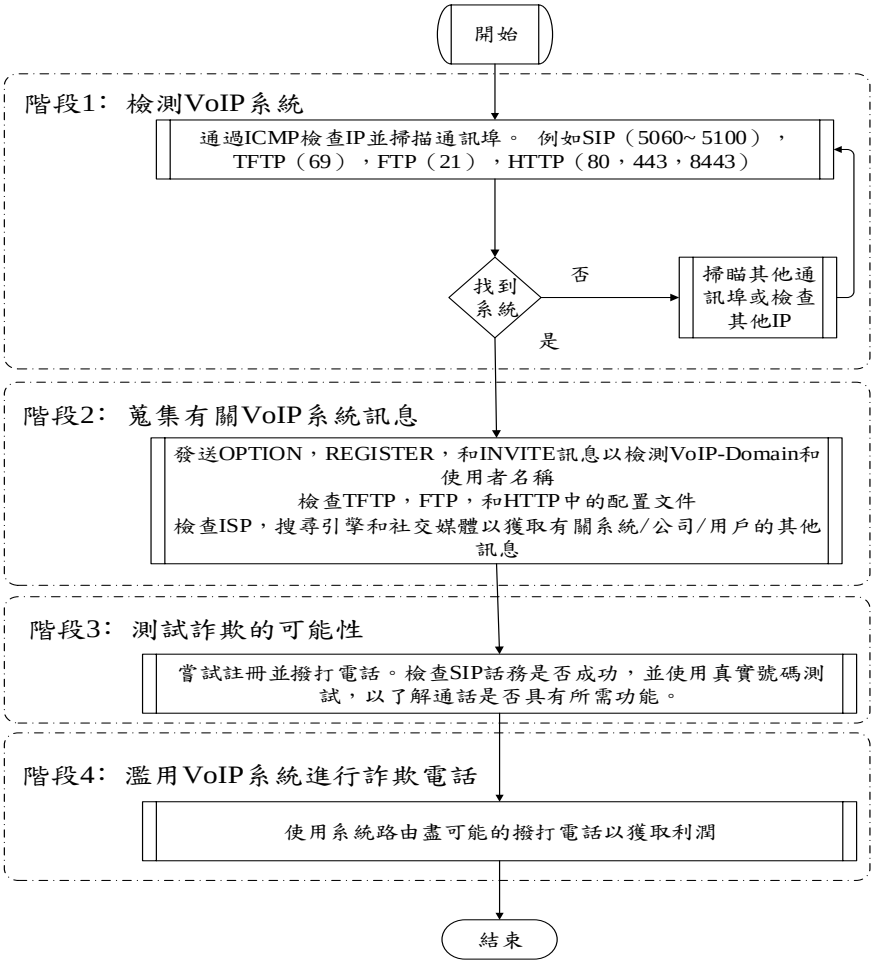

圖 2.1 詐欺階段模型

資料來源：Machens, Gebauer & Wermser, 2018

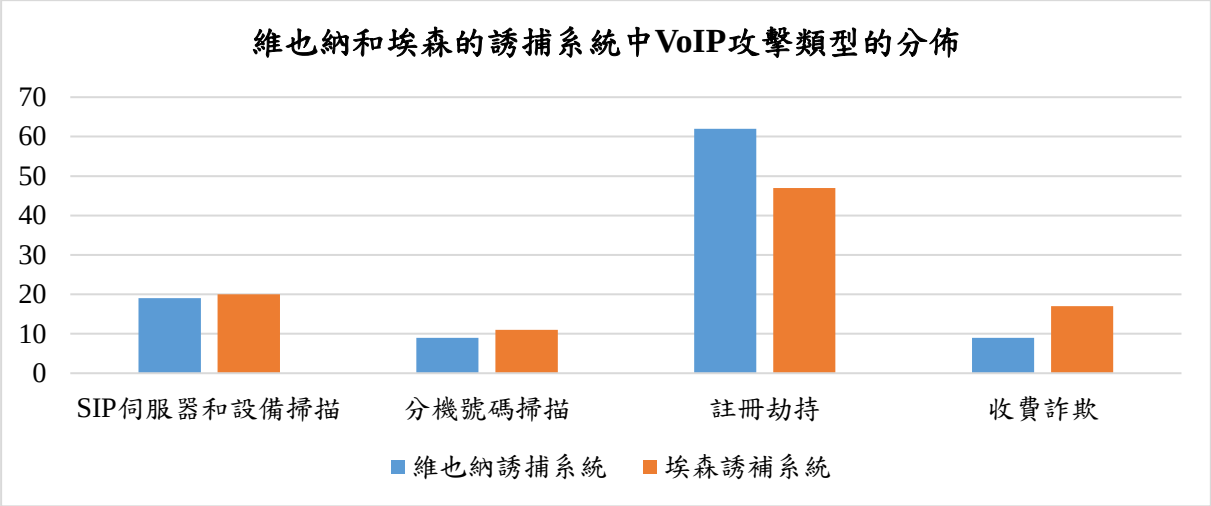

圖 2.2 維也納和埃森的誘捕系統中 VoIP 攻擊類型分佈
資料來源：Gruber et al., 2015

2.3 VoIP 的網路安全機制

面對網路上對 VoIP 帶來的威脅，許多學者提出各種的保護機制來加強 VoIP 的安全性。當前的大多數解決方案都集中在監視和分析、訊令(Signaling)路徑保護、身份鑑別(Authentication)、誘捕系統(Decoy System)、機密性(Confidentiality)和真確性(Integrity)保護以及防禦所有 SIP 攻擊的防火牆(Naeem & Missen, 2020)。對使用者進行身分驗證可防止攻擊者的非法入侵，媒體加密可防止 VoIP 通訊被竊聽及竄改資料，使用專用的防火牆可減少 DoS 攻擊(Hasan & Hussain, 2017)。

針對VoIP網路的安全性及漏洞可實施的安全措施，例如網路拓樸隱藏(Topology Hiding)、更改標準Port、更新和修補程式、實施TLS、配置SIP專用防火牆、IP tables、部署會談邊際控制器(SBC)等，可以緩解組織中VoIP基礎結構可能遭受的漏洞和風險。SBC的功能與防火牆相似，差別在於SBC是專屬設計給SIP的安全解決方案，SBC的功能至少可以減緩DoS攻擊，點對點加密等(Carino, Del Giorgio, Abeledo, Bullian, Gonzalez & Hencek, 2018)。

2.4 會談邊際控制器(SBC)

會談邊際控制器(Session Border Controller, SBC)，顧名思義，就是在網路邊際對 SIP 會談進行控制。根據字面意思就基本上了解了 SBC 的作用和功能：

一、Session（會談）：是指用戶之間的即時通訊連接，通常是語音/視訊通話。

二、Border（邊際）：彼此之間不完全信任的網路接口，這裡的邊界是指內網和外網之間的區域。類似於防火牆一樣，部署在網路的邊界區域就可以實現安全設置。

三、Controller（控制器）：SBC（允許、拒絕、變更、結束）控制每個越過邊界的會話能力(Benitez, 2017)。

SBC 沒有特別標準化或定義，依各家廠商所提供的功能略有不同。SBC 部署於內網與外網中間同時處理訊令和媒體，邏輯架構如圖 2.3 所示。SBC 提供多種功能可增強與

保護會談的多媒體服務（IP 語音/視訊）(Hautakorpi, Camarillo, Penfield, Hawrylyshen & Bhatia, 2010)。

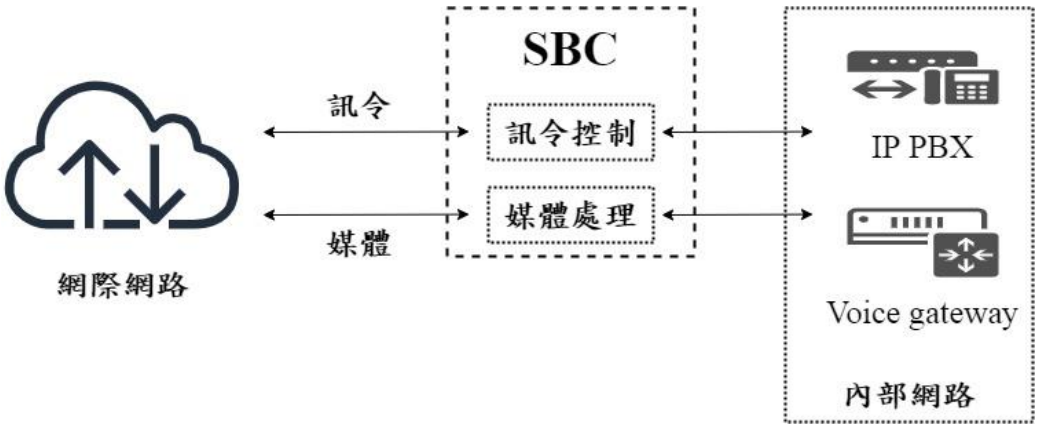

圖 2.3 SBC 架構
資料來源：Hautakorpi et al., 2010

SBC的主要功能

一、隱藏網路拓撲：SBC 使用網路地址轉換(NAT)來隱藏內部網路詳細信息。
二、語音的防火牆：防止分佈式阻斷服務攻擊(DDoS)、收費欺詐和服務盜竊。
三、加密：SBC 使用傳輸層安全協議(TLS)及安全實時傳輸協議(SRTP)對訊令和媒體進行加密。
四、協議轉換（例如，在 SIP 和 H.323 之間）
五、語音編碼協議轉換(Transcoding G.711/G.729/G.726/iLBC/OPUS/SILK)
六、頻寬管理：SBC 可以獨立管理每個通信會談的頻寬。SBC 在每個連接的設備上，跨所有通信模式（視訊、語音、串流媒體等）提供頻寬管理。
七、訪問控制：由於 SBC 處理所有的通信會談，因此能夠基於頻寬限制、使用的協議、來源/目標 IP 位址、SIP 身分等對訪問進行允許、拒絕、變更、結束等控制。
八、基於 QoS 的控件：SBC 可以監控通信會談的狀態。此外，某些 SBC 可以進行調整頻寬以解決通話品質問題(Benitez, 2017)。

2.5 受保護的 SIP 連線

SIP 為建立 VoIP 會談(Session)時的主要訊令協議。RTP 是用於 VoIP 通話時對語音資料進行傳輸的主要協議。TLS 用於加密 SIP 的訊令及 SRTP 對稱加密時的公鑰，SRTP 使用的對稱加密演算法為 AES，相較於 DES、3DES 等可提供更快的加解密速度及安全性(Abdullah, A. M, 2017)，保護通話時的 RTP 資料。TLS/SRTP 連線可為 VoIP 提供身份驗證、訊令及消息的完整性和機密性，以建立安全的 VoIP 會話。圖 2.4 說明了兩端的用戶使用 TLS 及 SRTP 通過 SIP Proxy Server 進行 SIP 訊令交換的過程(Subramanian & Dutta, 2010)。

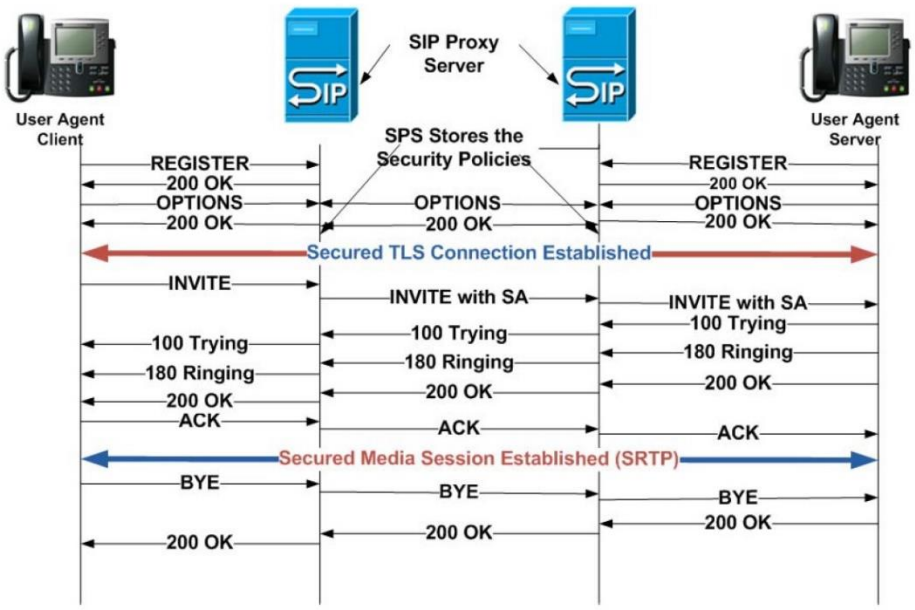

圖 2.4 受保護的 SIP 連線

資料來源：Subramanian & Dutta, 2010

三、實驗系統架構設計

3.1 環境設計

本研究即是在驗證 UCaaS 環境下的通訊安全議題，在實驗環境中於本地端部署實體 SBC，並且於雲端(Microsoft Azure)安裝 SBC 的軟體版本(SBC-SWe Lite)，雲端與地端之間是經由網際網路接取(Internet Access)，並於兩端的 SBC 上，註冊各類型的網路電話終端做為通話建立的驗證裝置，環境設計的架構如圖 3.1 所示。

實驗環境分為五大部分。第一部份是位於雲端所安裝的 SBC，我們採用 Ribbon 與微軟合作的 UCaaS 平台(Ribbon SBCs Support Microsoft Operator Connect)，主將其視為 SIP Proxy Server，亦驗證使用雲端總機時的安全性。第二部分為本地端的 SBC，即模擬一般企業用戶所使用的通信環境，通常企業用戶會將 SBC 與公司內的 IP 交換機或者語音閘道器介接，但本文目的為 SBC 的安全驗證，故將其省略。第三部分為雲端 SBC 的網路電話終端，使用者經由 Internet 向雲端的 SBC 註冊，便可將網路電話終端變成行動分機。第四部分為本地端的網路電話終端，使用者可以由內部網路或者 Internet 向地端的 SBC 註冊，為本地端分機。當雲端 SBC 的行動分機與地端的 SBC 分機進行通話時，可擷取並分析雲端及地端的 SBC 通信時的封包，以驗證 SBC 在 VoIP 通信環境中的安全性。第五部分為攻擊主機與監控電腦；攻擊主機從網際網路分別對地端及雲端的 SBC 進行各項測試；監控電腦於地端擷取 SBC 的封包，對 SBC 進行監控及分析。

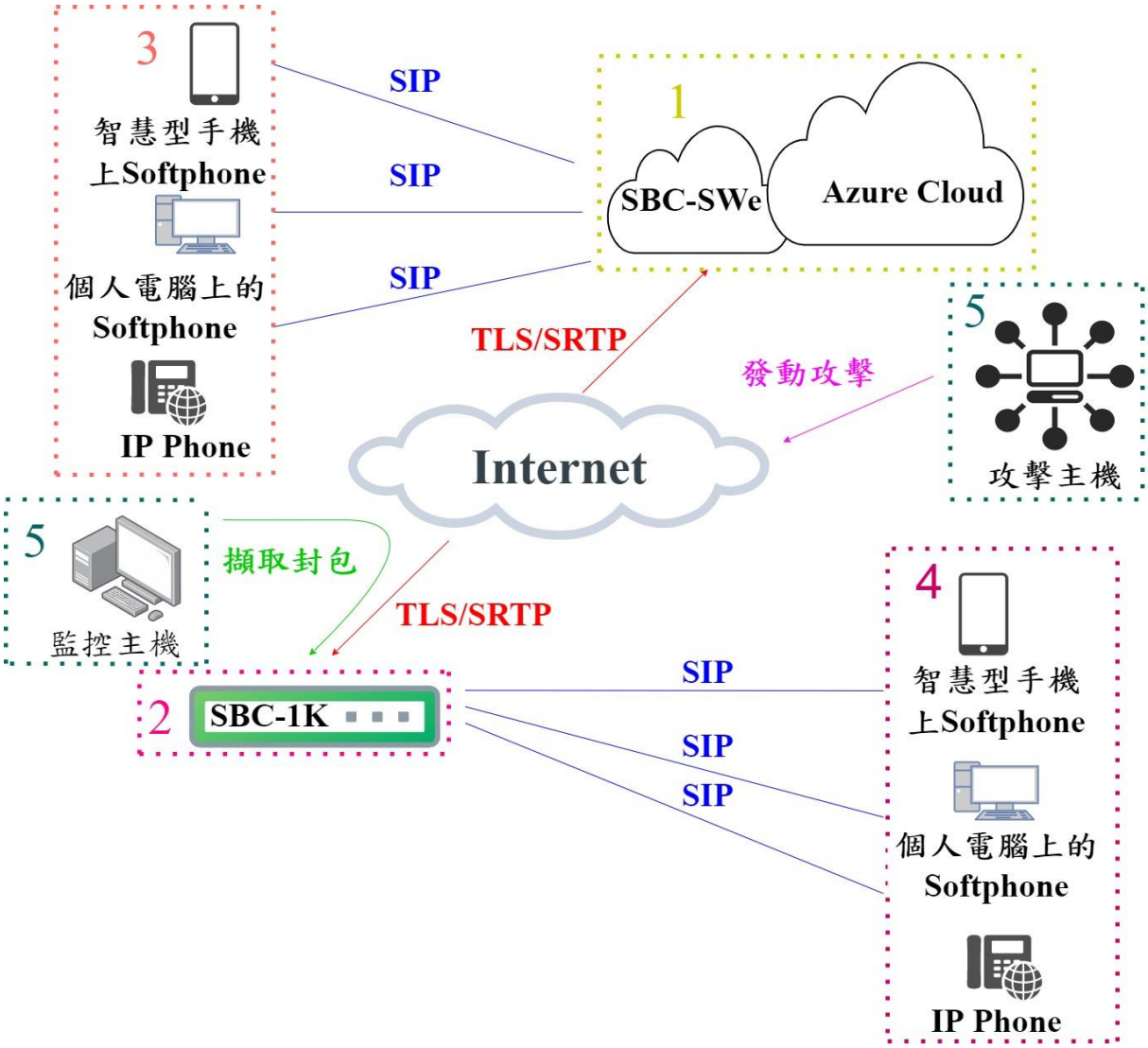

圖 3.1 模擬環境設計

3.2 工具介紹

Azure簡介：Azure是Microsoft的雲端運算服務平台，它提供了包含IaaS、PaaS、SaaS等200多項的產品及服務。

Ribbon SBC：Ribbon是即時語音安全通信領域的全球領導者，為全球通信服務提供商、企業、獨立軟體供應商、合作夥伴和系統集成商提供軟體和雲端網路產品和解決方案，本研究於雲端平台安裝Ribbon SBC SWe，地端安裝Ribbon SBC 1k。

SIPVicious：SIPVicious是一組測試基於SIP的VoIP系統的套件，由svmap、svwar、svcrack、svcrash、svreport等五個工具組成。

SIPp：SIPp 是一個測試 SIP 協議性能的工具軟體，可以簡單用來測試 SIP 協議。

Wireshark：Wireshark是一個免費的開源網路封包分析軟體，能在Windows、Linux、macOS、Solaris、FreeBSD、NetBSD 和許多其他平台上運行。

Kali Linux：這是一個高級滲透測試Linux發行版，用於滲透測試、道德駭客攻擊和網絡安全評估，本研究使用的版本為2020.3。

3.3 測試步驟及項目

本研究的測試內容將針對 2.2 節中 VoIP 常見及嚴重的威脅進行測試，步驟將參考圖 2.1 詐欺階段模型中的各階段進行，使用工具為 3.2 節中介紹之工具，流程如圖 3.2 所示，測試項目如表 3.1 所示。

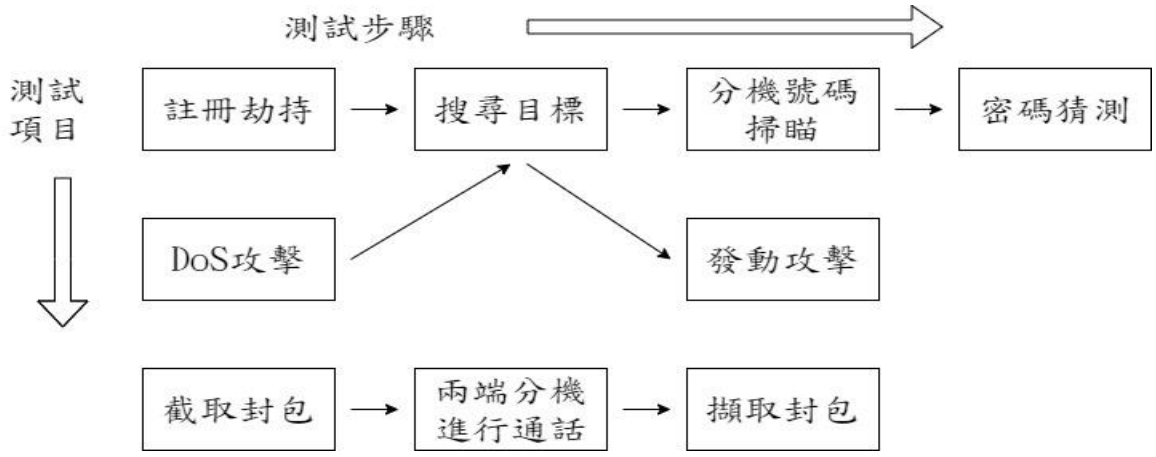

圖 3.2 測試步驟流程圖

表3.1測試項目

測試項目	目的	工具
搜尋目標	找出本次研究安裝於地端及雲端的 SBC。	svmap
分機號碼掃瞄	找出 SBC 內存在的分機號碼，以作為密碼猜測的目標。	svwar
密碼猜測	猜測分機號碼註冊時所需的密碼，嘗試註冊劫持的可能。	svcrack
DoS 攻擊	阻斷 SBC 服務，檢測 SBC 抵禦 DoS 的能力。	SIPp
封包擷取	擷取網路電話通訊時的封包，檢視封包，進行分析。	Wireshark

四、安全性測試與成果

4.1 探測 SIP 設備

對網際網路進行掃描，探測是否有SIP設備存在，是對SIP進行攻擊的第一步，目的在於確定設備類型，作業系統及版本，開放的通訊埠等。

首先攻擊主機使用svmap對IP:210.201.89.1/24進行掃描（假設攻擊者對網路進行隨機掃瞄），操作指令如圖4.1所示，掃描結果發現IP:210.201.89.1/24的網段有2台SIP設備，但是並非本次研究所安裝的SBC。

```
pansenhaw@kali:~$ svmap 210.201.89.1/24 -v
```

圖 4.1 svmap 掃描 IP:210.201.89.1/24 操作指令

使用svmap對IP:13.70.35.1/24進行掃瞄，操作指令如圖4.2所示，掃瞄結果並未發現任何SIP設備。

```
pansenhaw@kali:~$ svmap 13.70.35.1/24 -v
```

圖 4.2 svmap 掃瞄 IP:13.70.35.1/24 操作指令

因為svmap預設掃瞄的Port為5060，本次研究安裝的SBC所設定SIP Listen Port為7890，所以無法探測到本次安裝的設備。

以下以IP:210.201.89.1/24再次進行掃描，並添加掃瞄Port範圍5000-8000（本次研究將SIP Listen Port改為7890，為縮短掃瞄時間，所以將範圍設定為5000-8000），操作指令如圖4.3所示；掃描結果即發現出了本次研究安裝於地端的SBC。

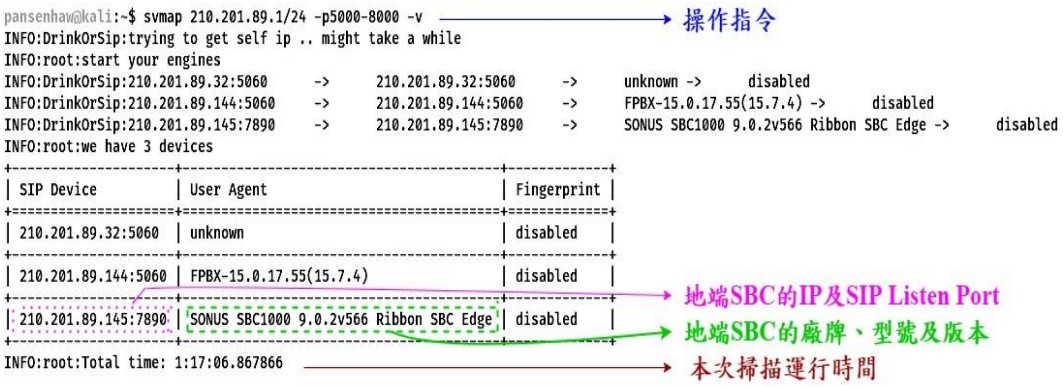

圖 4.3 svmap 對 IP:210.201.89.1/24 Port 5000-8000 掃描結果

再次對IP:13.70.35.1/24進行掃描，並添加掃瞄Port範圍5000-8000，掃描結果出現了3台SIP設備，本次研究安裝於雲端的SBC也出現在掃描結果內，結果如圖4.4所示。

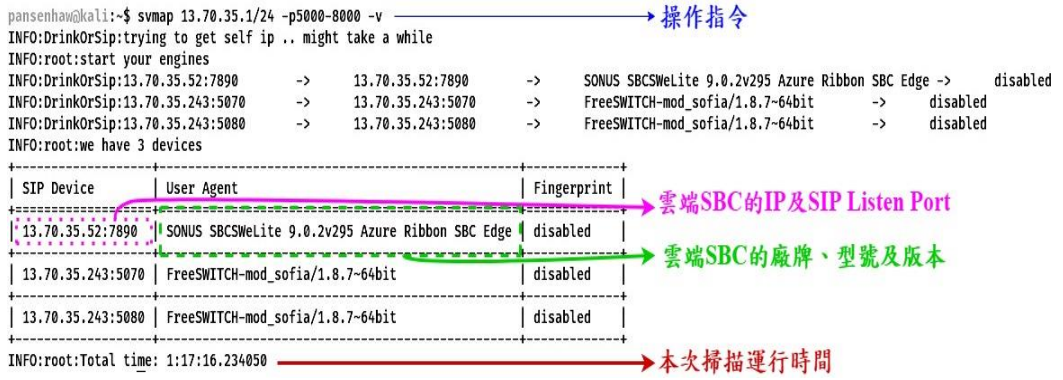

圖 4.4 svmap 對 IP:13.70.35.1/24 Port 5000-8000 掃描結果

本階段的掃描結果如表4. 1所示，由此得知，當攻擊主機對整個Class C網段進行掃描時，如果SIP設備的SIP Listen Port使用預設的5060，將會輕易的被發現（攻擊主機僅掃描每個IP的5060 Port，因此掃瞄速度非常快）。如果SIP設備不使用預設Port，以本次測

試為例，攻擊主機的掃瞄範圍為每個Class C網段IP的5000-8000 Port，範圍越大所需的時間越多，所以如果不使用預設的5060 Port，可以增加探測的困難度。

表 4.1 探測 SIP 設備結果

掃瞄範圍	掃瞄預設Port	指定掃瞄Port範圍(5000-8000)
IP:210.201.89.1/24	發現SIP設備，但並非地端SBC	發現地端SBC
IP:13.70.35.1/24	未發現任何設備	發現雲端SBC

根據本階段的探測結果，假設攻擊者已發現本次研究所安裝的 SBC，接下來的安全性測試將如圖 4.5 所示。

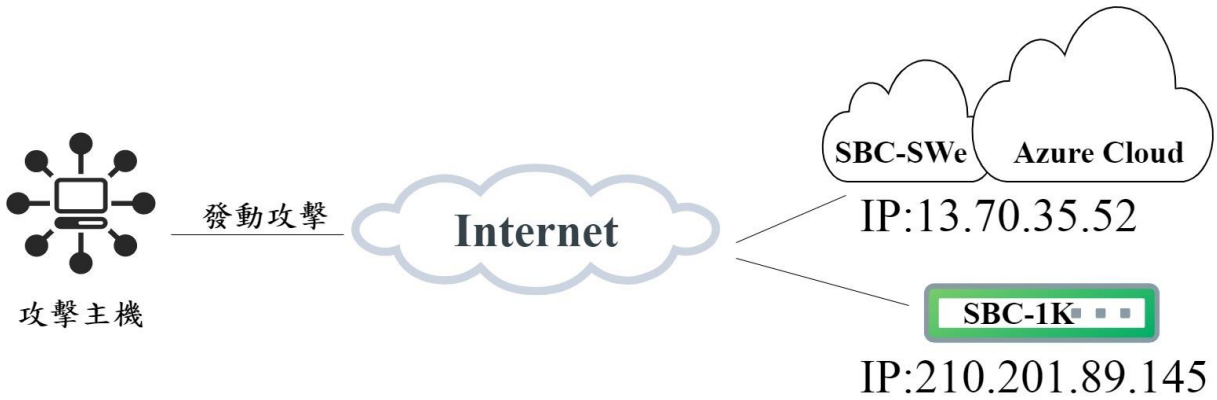

圖4.5 網路拓譜圖

4.2 分機號碼掃瞄

此階段為攻擊者對SBC進行分機號碼掃描，試圖找出SBC上的分機號碼。攻擊主機使用svwar掃描地端SBC，操作指令如圖4.6所示，預設的掃描方式為攻擊主機對SBC發出REGISTER的請求，使用的指令 -D意思為使用腳本內的分機號碼，這些號碼為常用的分機號碼，例如：1000、2000、3000等，掃描結果並未發現任何分機。

```
pansenhaw@kali:~$ svwar --force -D 210.201.89.145 -p7890
```

圖 4.6 svwar 對地端 SBC 進行分機號碼掃描操作指令

再次對地端的SBC進行掃描，並加入 -m INVITE指令，操作指令如圖4.7所示，將攻擊主機對SBC的請求改為INVITE，結果亦未發現任何分機。

```
pansenhaw@kali:~$ svwar --force -D 210.201.89.145 -p7890 -m INVITE
```

圖 4.7 svwar –m INVITE 對地端 SBC 進行分機號碼掃描操作指令

攻擊者對雲端的SBC進行分機號碼掃描，操作指令如圖4.8所示，結果並未發現任何分機。

```
pansenhaw@kali:~$ svwar --force -D 13.70.35.52 -p7890
```

圖 4.8 svwar 對雲端 SBC 進行分機號碼掃描操作指令

再次對雲端的SBC進行掃描，並加入 -m INVITE指令，操作指令如圖4.9所示，結果亦未發現任何分機。

```
pansenhaw@kali:~$ svwar --force -D 13.70.35.52 -p7890 -m INVITE
```

圖 4.9 svwar –m INVITE 對雲端 SBC 進行分機號碼掃描操作指令

本階段掃描結果如表4.2所示。svwar的掃描方式為對SBC發出REGISTER或者INVITE的請求；以地端SBC為例，當攻擊主機使用腳本內的分機號碼對SBC發出REGISTER請求時，這個請求是不包含密碼的，所以不論這個分機號碼是否存在SBC中，SBC都給予401 Unauthorized的回應。當攻擊主機對SBC發出INVITE訊息時，SBC認為這個訊息的來源並不是來自雲端或地端的合法分機號碼，所以不論腳本內的分機號碼是否存在SBC中，SBC也是給予401 Unauthorized的回應，由Wireshark中可觀察到當SBC接收到不明的REGISTE及INVITE訊息時的反應，如圖4.10所示。svwar無法判斷分機號碼是否存在，因此本次掃描並未發現任何存在於SBC的分機號碼。

表 4.2 分機號碼掃描結果

掃瞄目標	掃瞄預設Port	添加掃描指令(-m INVITE)
地端SBC IP:210.201.89.145	未發現任何分機	未發現任何分機
雲端SBC IP:13.70.35.52	未發現任何分機	未發現任何分機

Source	Destination	Protocol	Length	Info
112.104.74.42	210.201.89.145	SIP	464	Request: REGISTER sip:210.201.89.145
210.201.89.145	112.104.74.42	SIP	527	Status: 401 Unauthorized
112.104.74.42	210.201.89.145	SIP	422	Request: REGISTER sip:210.201.89.145
112.104.74.42	210.201.89.145	SIP	419	Request: REGISTER sip:210.201.89.145
210.201.89.145	112.104.74.42	SIP	485	Status: 401 Unauthorized
210.201.89.145	112.104.74.42	SIP	482	Status: 401 Unauthorized

Source	Destination	Protocol	Length	Info
112.104.74.42	210.201.89.145	UDP	60	46533 → 7890 Len=4
112.104.74.42	210.201.89.145	SIP	468	Request: INVITE sip:1267824600@210
210.201.89.145	112.104.74.42	SIP	506	Status: 401 Unauthorized
112.104.74.42	210.201.89.145	SIP	423	Request: INVITE sip:1000@210.201.8
112.104.74.42	210.201.89.145	SIP	419	Request: INVITE sip:1100@210.201.8
210.201.89.145	112.104.74.42	SIP	473	Status: 401 Unauthorized

圖 4.10 地端 SBC 回應不明 REGISTER 及 INVITE

4.3 密碼猜測

此階段假設攻擊者已透過方法(例如：社交工程)獲得地端SBC的分機號碼82269968，及雲端SBC分機87650001，將對這兩個分機以暴力破解(Brute-force Attack)的方式進行密碼猜測，以嘗試註冊劫持的可能性。攻擊主機首先使用svcrack對此82269968進行密碼猜測，密碼範圍為1-9999，操作指令如圖4.11所示，結果並未找出任何密碼。

```
pansenhaw@kali:~$ svcrack -u82269968 -r1-9999 -z4 210.201.89.145 -p7890 -v
```

圖 4.11 svcrack 對 82269968 進行密碼暴力破解操作指令

攻擊主機使用svcrack對此87650001進行密碼猜測，密碼範圍為1-9999，操作指令如圖4.12所示，結果並未找出任何密碼。本階段的密碼猜測結果如表4.3所示。

```
pansenhaw@kali:~$ svcrack -u87650001 -r1-9999 -z4 13.70.35.52 -p7890 -v
```

圖 4.12 svcrack 對 87650001 進行密碼暴力破解操作指令

表4.3密碼猜測結果

破解目標	結果
IP:210.201.89.145（82269968）	未發現任何密碼
IP:13.70.35.52（87650001）	未發現任何密碼

4.4 DoS 攻擊

本階段將測試 SBC 抵禦 DoS 攻擊的能力，首先攻擊主機使用 SIPp 對雲端的 SBC 發出大量的 INVITE 訊息，SIPp 預設值攻擊的 Port 為 5060，因為使用手冊上並未說明 SIPp 能發送訊息速率的最大量，為了讓攻擊主機能以最大的速率發送訊息，因此將速率設定為每毫秒 10000 個，操作指令如圖 4.13 所示。監控主機使用 SBC 專屬的日誌記錄軟體 LX 接收訊息。同時於遭受攻擊期間使用雲端分機 87650001 及地端分機 82268868 相互通話。以驗證 SBC 抵禦 DoS 攻擊的能力。

```
pansenhaw@kali:~$ sipp uac -r 10000 -rp 1 13.70.35.52
```

圖 4.13 發送 INVITE 訊息給雲端 SBC 的操作指令

當雲端 SBC 遭受攻擊期間，雲端分機及地端分機依然可以正常撥打，如圖 4.14 中所示，SBC 於 LX 留下了當時撥打的紀錄。同時於 SBC 的管理界面中觀察到，SBC 待機時 CPU 的使用率為 5%，如圖 4.15 所示；遭受攻擊期間 CPU 的使用率為 6%，如圖 4.16 所示，相較於待機時並無太大改變。此次攻擊並未對 SBC 系統造成負擔。

Calls | End To End Calls | Debug Subsystems | Call Statistics

ID	Protocol	Direction	Received Time	Peer IP	Peer Port	SBC IP	SBC Port	Calling #	Called #	Meth...
8	SIP	Received	2021-10-14 16:26:49:348	112.104.74.46	52788	10.3.0.5	7890	87650001	82269968	INVIT...
11	SIP	Received	2021-10-14 16:26:49:389	112.104.74.46	52788	10.3.0.5	7890	87650001	82269968	INVIT...
12	SIP	Sent	2021-10-14 16:26:49:457	210.201.89.145	5070	10.3.0.5	24577	87650001	82269968	INVIT...
14	SIP	Received	2021-10-14 16:26:49:893	112.104.74.46	52788	10.3.0.5	7890	87650001	82269968	INVIT...

圖 4.14 雲端 SBC 遭受攻擊時分機呼叫日誌

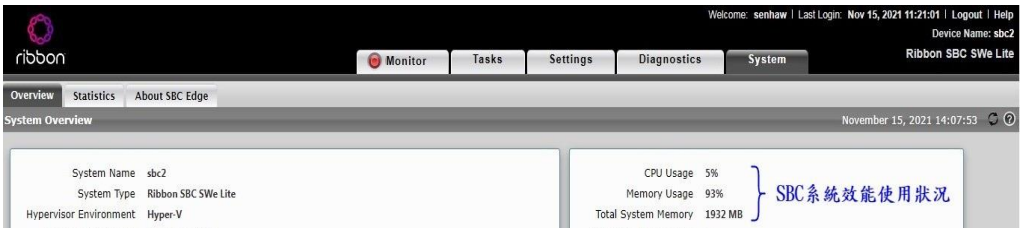

圖 4.15 雲端 SBC 待機時的系統資訊

圖 4.16 雲端 SBC 遭受攻擊時的系統資訊

再次攻擊雲端 SBC，並且指定攻擊 Port 為 7890，發送速率為每毫秒 10000 次，操作指令如圖 4.17 所示。在此同時雲端分機也無法撥打電話給地端分機，管理界面中也無法再更新系統資訊。

```
pansenhaw@kali:~$ sipp uac -r 10000 -rp 1 13.70.35.52:7890
```

圖 4.17 發送 INVITE 訊息給雲端 SBC Port 7890 的操作指令

攻擊主機使用 SIPp 對地端的 SBC 發出大量的 INVITE 訊息，速率設定為每毫秒 10000 個，操作指令如圖 4.18 所示。

```
pansenhaw@kali:~$ sipp uac -r 10000 -rp 1 210.201.89.145
```

圖 4.18 發送 INVITE 訊息給地端 SBC 的操作指令

當地端的 SBC 遭受攻擊期間，分機依然可以正常撥打，SBC 在 LX 留下了當時呼叫的紀錄，如圖 4.19 中所示。同時於 SBC 的管理界面中觀察到，期間 CPU 及 Memory 的使用率並無太大改變，如圖 4.20 所示。此次攻擊並未對 SBC 系統造成負擔。

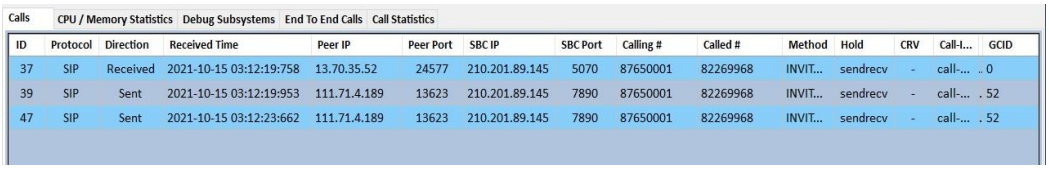

圖 4.19 地端 SBC 遭受攻擊時分機呼叫日誌

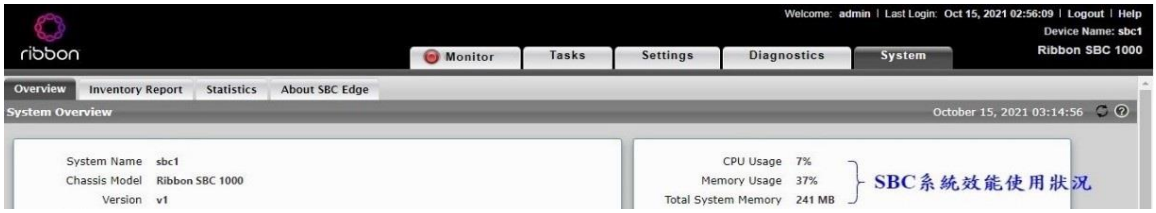

圖 4.20 地端 SBC 遭受攻擊時的系統資訊

再次對地端 SBC 發起攻擊，並且指定攻擊 Port 為 7890，發送速率為每毫秒 10000 次，操作指令如圖 4.21 所示。在此同時雲端及地端分機也無法互打，管理界面中也無法再更新系統資訊。

```
pansenhaw@kali:~$ sipp uac -r 10000 -rp 1 210.201.89.145:7890
```

圖 4.21 發送 INVITE 給地端 SBC Port 7890 的操作指令

本階段的攻擊結果如表4.4所示。由Wireshark中可以觀察到，當攻擊主機使用預設值攻擊時，SBC在接收到第六次INVITE訊息時，就不給予回應，如圖4.22所示，因此不對系統造成影響。而針對Port 7890攻擊時，SBC接收到多少個INVITE訊息，即回應多少個401 Unauthorized訊息，如圖4.23所示，以本次攻擊為例，SBC接收大量的INVITE訊息後，已超過SBC系統所能負擔的處理能力，也因此阻斷了SBC的服務。

表4.4 DoS攻擊結果

攻擊目標	預設攻擊Port（5060）	指定攻擊Port（7890）
雲端SBC IP:13.70.35.52	未對SBC系統造成負擔（圖4.15）	阻斷了SBC的服務
地端SBC IP: 210.201.89.145	未對SBC系統造成負擔（圖4.19）	阻斷了SBC的服務

Source	Destination	Protocol	Length	Info
84.17.34.78	192.168.1.104	TCP	60	443 → 1070 [ACK] Seq=11325 Ack=554114 Win
Fortinet_03:3a…	Broadcast	ARP	60	Who has 192.168.2.14? Tell 192.168.2.1
112.104.66.184	210.201.89.145	SIP/SDP	1112	Request: INVITE sip:100@210.201.89.145
210.201.89.145	112.104.66.184	ICMP	590	Destination unreachable (Port unreachable
112.104.66.184	210.201.89.145	SIP/SDP	1112	Request: INVITE sip:100@210.201.89.145
210.201.89.145	112.104.66.184	ICMP	590	Destination unreachable (Port unreachable
112.104.66.184	210.201.89.145	SIP/SDP	1112	Request: INVITE sip:100@210.201.89.145
210.201.89.145	112.104.66.184	ICMP	590	Destination unreachable (Port unreachable
112.104.66.184	210.201.89.145	SIP/SDP	1112	Request: INVITE sip:100@210.201.89.145
210.201.89.145	112.104.66.184	ICMP	590	Destination unreachable (Port unreachable
112.104.66.184	210.201.89.145	SIP/SDP	1112	Request: INVITE sip:100@210.201.89.145
210.201.89.145	112.104.66.184	ICMP	590	Destination unreachable (Port unreachable
112.104.66.184	210.201.89.145	SIP/SDP	1112	Request: INVITE sip:100@210.201.89.145
210.201.89.145	112.104.66.184	ICMP	590	Destination unreachable (Port unreachable
112.104.66.184	210.201.89.145	SIP/SDP	1112	Request: INVITE sip:100@210.201.89.145
112.104.66.184	210.201.89.145	SIP/SDP	1112	Request: INVITE sip:100@210.201.89.145
112.104.66.184	210.201.89.145	SIP/SDP	1112	Request: INVITE sip:100@210.201.89.145
112.104.66.184	210.201.89.145	SIP/SDP	1112	Request: INVITE sip:100@210.201.89.145

圖 4.22 Wireshark 觀察 SIPp 預設值攻擊 SBC

Source	Destination	Protocol	Length	Info
112.104.74.231	210.201.89.145	SIP/SDP	1112	Request: INVITE sip:100@210.201.89.145
112.104.74.231	210.201.89.145	SIP/SDP	1112	Request: INVITE sip:100@210.201.89.145
112.104.74.231	210.201.89.145	SIP/SDP	1112	Request: INVITE sip:100@210.201.89.145
112.104.74.231	210.201.89.145	SIP/SDP	1112	Request: INVITE sip:100@210.201.89.145
112.104.74.231	210.201.89.145	SIP/SDP	1112	Request: INVITE sip:100@210.201.89.145
112.104.74.231	210.201.89.145	SIP/SDP	1112	Request: INVITE sip:100@210.201.89.145
112.104.74.231	210.201.89.145	SIP/SDP	1112	Request: INVITE sip:100@210.201.89.145
112.104.74.231	210.201.89.145	SIP/SDP	1112	Request: INVITE sip:100@210.201.89.145
112.104.74.231	210.201.89.145	SIP/SDP	1112	Request: INVITE sip:100@210.201.89.145
112.104.74.231	210.201.89.145	SIP/SDP	1112	Request: INVITE sip:100@210.201.89.145
210.201.89.145	112.104.74.231	SIP	512	Status: 401 Unauthorized
210.201.89.145	112.104.74.231	SIP	512	Status: 401 Unauthorized
210.201.89.145	112.104.74.231	SIP	512	Status: 401 Unauthorized
210.201.89.145	112.104.74.231	SIP	512	Status: 401 Unauthorized
210.201.89.145	112.104.74.231	SIP	512	Status: 401 Unauthorized

圖 4.23 Wireshark 觀察 SIPp 攻擊 SBC Port 7890

4.5 使用 TLS 的 SIP Listen Port

由於 SIP 承襲了 Internet 的傳統威脅，因此 SIP 的 Listen Port 不論使用 TCP 或者 UDP 的 Protocol 都會容易受到攻擊；本研究將 SIP 的 Listen Port 設定為 7890 使用 Protocol 為 UDP，遭受攻擊時的表現並不突出。接下來將 SIP Listen Port 的 Protocol 改成 TLS 再次進行測試，項目及步驟與 4.1~4.4 節相同，由於 4.1~4.4 節的測試中雲端及地端 SBC 的結果並無差別，因此後續的測試僅以雲端 SBC 為例。

首先使用 svmap 對 IP:13.70.35.1/24 進行掃描，掃瞄 Port 範圍 5000-8000，結果未發現任何 SIP 設備。第二步對雲端 SBC 進行分機掃瞄，掃描方式與 4. 2 節所使用的相同，在兩種掃描方式都使用的情況下，結果並未發現任何分機。第三步對 SBC 進行密碼猜測，使用的工具及操作指令與 4.3 節相同，結果並未找到任何密碼。最後對雲端 SBC 進行 DoS 攻擊，使用工具及指令與 4.4 節相同，SBC 遭受攻擊期間 CPU 使用率為 30%，如圖 4.24 所示，使用率雖有上升，但是系統還可正常運作。

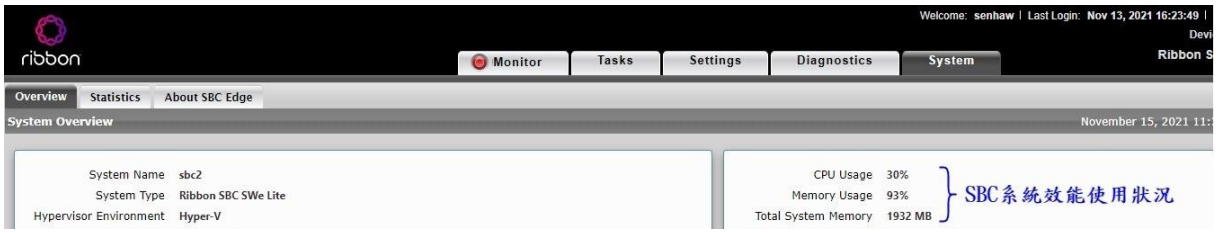

圖 4.24 雲端 SBC 受攻擊時的系統使用狀況

由 Wireshark 中可觀察到 SBC 受到 DoS 攻擊時的反應如圖 4.25 所示。其間攻擊主機無法與雲端 SBC 建立 TLS 連線，因此 SBC 對於之後攻擊主機所發出的訊息一律不回應，也因此抵擋了 DoS 的攻擊。

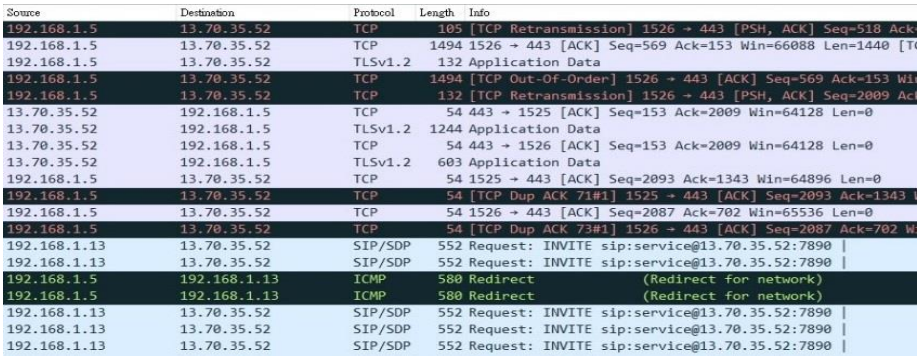

圖 4.25 Wireshark 觀察雲端 SBC 受攻擊時的狀況

本階段的測試結果如表 4.5 所示，探測 SIP 設備這個項目結果與 4.1 節比較，已找不到雲端的 SBC，分機號碼掃描與密碼猜測這兩個項目，結果與 4.2 及 4.3 節相同，在 DoS 攻擊這個項目中，由 SBC 的系統資訊中發現這次攻擊未對 SBC 造成太大影響，因此 SIP Listen Port 的 Protocol 使用 TLS 可以提供更安全的防護。

表 4.5 測試結果

測試項目	結果
探測 SIP 設備	未發現任何設備
分機號碼掃瞄	未發現任何分機
密碼猜測	未找到任何密碼
DoS 攻擊	CPU 使用率雖有上升，但是系統可正常運作（圖 4.24）

4.6 封包擷取

本階段將使用地端分機 82269968 與雲端分機 87650001 進行通話，由監控主機使用 Wireshark 擷取通話時的封包，如圖 4.26 所示，並檢視封包，驗證 SBC 能夠保護語音通訊的機密性與真確性。

Source	Destination	Protocol	Length	Info
210.201.89.145	13.70.35.52	ICMP	93	Destination unreachable (Port unreachable)
13.70.35.52	210.201.89.145	RTCP	132	Sender Report
210.201.89.145	13.70.35.52	ICMP	160	Destination unreachable (Port unreachable)
210.201.89.145	13.70.35.52	TLSv1.2	1163	Application Data
13.70.35.52	210.201.89.145	TCP	60	24577 → 5070 [ACK] Seq=2528 Ack=3418 Win=501 Len=0
13.70.35.52	210.201.89.145	TLSv1.2	827	Application Data
210.201.89.145	13.70.35.52	TCP	56	5070 → 24577 [ACK] Seq=3418 Ack=3301 Win=441 Len=0
13.70.35.52	210.201.89.145	RTP	224	PT=ITU-T G.711 PCMA, SSRC=0x48F7EF96, Seq=23, Time=1772807569, Mark
210.201.89.145	13.70.35.52	CLASS…	86	Message: Binding Request
210.201.89.145	13.70.35.52	CLASS…	86	Message: Binding Request
210.201.89.145	13.70.35.52	RTP	224	PT=ITU-T G.711 PCMA, SSRC=0x2443A858, Seq=1920, Time=3749724241
13.70.35.52	210.201.89.145	RTP	224	PT=ITU-T G.711 PCMA, SSRC=0x48F7EF96, Seq=24, Time=1772807729
210.201.89.145	13.70.35.52	RTP	224	PT=ITU-T G.711 PCMA, SSRC=0x2443A858, Seq=1921, Time=3749724401

圖 4.26 擷取分機通話時的封包

由擷取的封包中發現，當兩端分機從通話建立到結束都未發現 SIP 封包，僅發現 TLS 的 Application Data 及 RTP 的語音封包。由此可見 SIP 訊令已被 TLS 加密保護，而 Wireshark 並無顯示 SRTP 封包。當嘗試播放此次擷取到的 RTP Streams 時，發現 Wireshark 無法解析出封包的音頻格式及內容，所以無法播放，如圖 4.27 所示。因此可判斷 RTP Streams 是經過加密的。而解密的密鑰也被 TLS 的加密保護，無法直接於封包內發現。即使封包被攻擊者擷取了，也無法輕易解析封包內容。

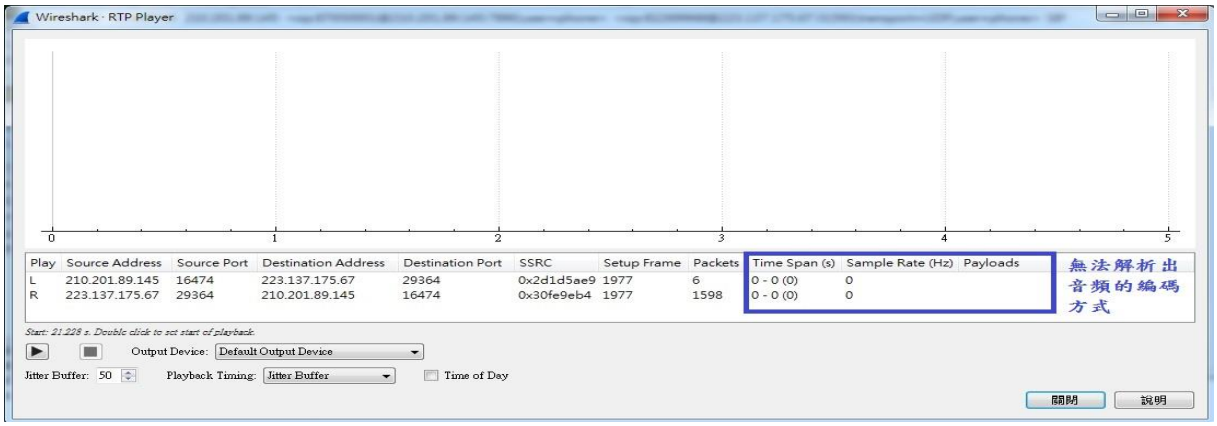

圖 4.27 無法播放 RTP Streams

五、結論與建議

5.1 研究結論

本文透過系統的實作，建立 UCaaS 與地端 VoIP 的通訊環境，對 VoIP 裡常見的威脅進行測試，驗證了雲端及地端的 SBC 的安全性。兩端的 SBC 建立了 TLS/SRTP 連線，SBC 使用憑證互相對彼此的身分進行鑑別，完成後， SIP 的訊令及 SRTP 加解密所需的密鑰都使用非對稱加密保護著，通話內容經則過 AES 的加密。SBC 確實提供了 VoIP 通信時資料的機密性(Confidentiality)、完整性(Integrity)和身分鑑別(Authentication)。

VoIP 通信建立前，必須經由 SBC 進行身分鑑別，若無法通過鑑別，SBC 對於陌生的 INVITE 都不給予回應，如圖 4.24 所示，通信即無法建立，可防止語音釣魚及通話轉

址的風險。訊令及通話內容已被加密，可降低通話被攔截時，內容被竄改(中間人攻擊)與竊聽的可能性。

SBC 的部署位置是在 VoIP 系統與 Internet 之間，IP PBX、語音閘道器(Voice Getaway)安裝於內網，與 SBC 介接，因此僅有 SBC 暴露於 Internet 上。當攻擊者進行掃描時，只會發現 SBC，不會發現安裝於內網的其他設備，將整個 VoIP 的拓樸(Topography)隱藏了起來。

當 SBC 遭受到 DoS 攻擊，若攻擊者攻擊的 Port 並非 SBC 的 SIP Listen Port，SBC 則不給予回應，因此對系統並不造成太大影響。當攻擊者針對 SBC 的 SIP Listen Port 發動攻擊時，將會對 SBC 的系統造成負擔（根據攻擊的量及時間決定負擔的大小）。

4.5 節中將 SIP Listen Port 使用的協議由原本的 UDP 改為 TLS，而在接下來的測試中發現，在探測 SIP 設備時已無法探測到雲端 SBC，當遭受 DoS 攻擊時系統還可以正常操作，可成功抵禦 DoS 攻擊。

5.2 建議

本次研究於 4.1 節，對網路進行掃描時，在圖 4.3 的掃描結果內發現一台 SIP 設備(210.201.89.32:5060)，並未掃描出該設備可能的廠牌及版本。攻擊的手法日新月異的同時，能夠被攻擊者發現資料越少越好，本次研究結果將回報於原廠，建議原廠隱藏設備資訊，以增加攻擊的困難度。

4.5 節的測試結果發現當 SBC 的 SIP Listen Port 使用的 Protocol 為 TLS 時，除了可以抵擋 DoS 攻擊外，也增加了 SBC 在 Internet 被發現的困難度；因此最佳設定的方式為使用 TLS 的 SIP Listen Port。如果 SIP Listen Port 的 Protocol 無法使用 TLS 時，可使用如同 Asterrisk 的方式，將 Fail2ban 作為預設的 IPS 系統，它可讓多次連線失敗的 IP 禁止訪問，保護 SBC 免受 DoS 及暴力破解的攻擊。

5.3 未來研究方向

本文以 UCaaS 為研究背景，驗證了 SBC 對語音部分的安全性，而 UCaaS 應用廣泛，服務品質也是非常重要的一環，未來研究可朝如何在安全的環境下提供良好的服務品質，不僅是語音部分而已。

國防領域之應用

作戰靠指揮，指揮靠通信，在國防領域裡，通信最重要就是資料的機密性與完整性，才能確保指揮命令完整的傳達。本文驗證了 SBC 於 UCaaS 網路電話中安全性，在國軍使用整合通訊系統的同時，將有、無線電系統整合，透過公共網路傳輸，為了建構安全及可靠的通信，SBC 對通話加密、身分的鑑別、防攻擊等功能，在此有著不可或缺的地位。

參考文獻

Abdullah, A. M. (2017). Advanced encryption standard (AES) algorithm to encrypt and decrypt data. *Cryptography and Network Security, 16*(1), 11.

Al Saidat, M. R. S. (2019). A Design of an Enhanced Redundant SIP Model for Securing SIP-Based Networks. In *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*, 1-6. IEEE.

Benitez, R., A. (2017). Market Guide for Enterprise SBC. From https://www.patton.com/guides/gartner-esbc-market-guide.pdf (retrieved on December 14, 2021)

Carino, F. M., Del Giorgio, H. R., Abeledo, M. C., Bullian, P., Gonzalez, J., & Hencek, M. (2018). Detection and analysis of vulnerabilities in convergent network platforms. In *2018 Congreso Argentino de Ciencias de la Informática y Desarrollos de Investigación (CACIDI),* 1-5. IEEE.

Ghafarian, A., Seno, S. A. H., & Dehghani, M. (2016). An empirical study of security of VoIP system. In *2016 SAI Computing Conference (SAI)*, 1031-1036. IEEE.

Gruber, M., Hoffstadt, D., Aziz, A., Fankhauser, F., Schanes, C., Rathgeb, E., & Grechenig, T. (2015). Global VoIP security threats-large scale validation based on independent honeynets. In *2015 IFIP Networking Conference (IFIP Networking),* 1-9. IEEE.

Hasan, M. Z., & Hussain, M. Z., (2017). Collective Study On Security Threats In VOIP Networks. *International Journal of Scientific and Technology Research, 6*(1).

Hautakorpi, J., Camarillo, G., Penfield, R., Hawrylyshen, A., & Bhatia, M. (2010). Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC). From https://datatracker.ietf.org/doc/rfc5853/ (retrieved on December 14, 2021)

Karopoulos, G., Portokalidis, G., Domingo-Ferrer, J., Lin, Y. D., Geneiatakis, D., & Kambourakis, G. (2015). Security and privacy in unified communications: Challenges and solutions. *Computer Communications, 100*(68). 1-3.

Kaul, S., & Jain, A. (2018). Study On: Session Border Controllers and Impact on Voice and Video Conferencing. *IJRAR- International Journal of Research and Analytical Reviews, 5*(2), 61-67.

Lazzez, A. (2014). VoIP Technology: Investigation of QoS and Security Issues. *architecture, 19*, 22.

Machens, B., Gebauer, O., & Wermser, D. (2018). Fraud Attacks in VoIP-Based Communications Systems-Risk Analysis, Prevention, Protection, Detection. In *Titel: Proceedings of the 5th International Conference on Applied Innovations in IT, Volume Nr. 5*. Bibliothek, Hochschule Anhalt.

McInnes, N., Wills, G., & Zaluska, E. (2019). Analysis of threats on a voip based pbx honeypot. *Infonomics Society*. 113-118.

Naeem, M. M., Hussain, I., & Missen, M. M. S. (2020). A survey on registration hijacking attack consequences and protection for Session Initiation Protocol (SIP). *Computer Networks, 175*, 107250.

Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., & Schooler, E. (2002). SIP: session initiation protocol (No. rfc3261). From https://www.rfc-editor.org/rfc/rfc3261 (retrieved on December 14, 2021)

Subramanian, S. V., & Dutta, R. (2010). Comparative study of secure vs. non-secure transport protocols on the SIP proxy server performance: An experimental approach. In *2010 International Conference on Advances in Recent Technologies in Communication and Computing,* 301-305. IEEE.