IP多媒體子系統之規則式入侵偵測機制
Rule-based Intrusion Detection Mechanism for IP Multimedia Subsystem

陳麒元 Chi-Yuan Chen[1], 趙涵捷 Han-Chieh Chao[2,3], 郭斯彥 Sy-Yen Kuo[1,4], 張凱迪 Kai-Di Chang[3]
[1]國立臺灣大學電機工程學系
[2]國立東華大學電機工程學系
[3]國立宜蘭大學資訊工程研究所與電子工程系
[4]國立臺灣科技大學資訊工程學系
[1]Department of Electrical Engineering, National Taiwan University
[2]Department of Electrical Engineering, National Dong Hwa University
[3]Department of Electronic Engineering and Institute of Computer Science & Information Engineering, National Ilan University
[4]Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology
d96921015@ntu.edu.tw, hcc@mail.niu.edu.tw, sykuo@mail.ntust.edu.tw, kedy@niu.edu.tw

摘要

網際網路興起帶動網路世代迅速發展，使用者對於存取網路服務的需求日益增大。在另一個網路——全球行動通訊系統中，隨著接取技術進步，可讓使用者透過行動通訊網路存取網際網路上的資料和服務，進而促成兩個網路融合。在龐大的融合網路中，所有通訊將以全IP網路為基礎，因此3GPP組織制訂IP多媒體子系統，目標為融合全球行動通訊系統和網際網路，成為提供各式各樣服務的標準開放架構。IP多媒體子系統現階段仍欠缺有效的安全管理機制與策略，因而存在許多風險，包含駭客入侵、惡意使用、假造、偽裝、阻斷服務與SQL Injection等，營運端需要一個有效的入侵偵測機制，以確保用戶正常使用。本論文提出適用於IP多媒體子系統中以規則為基礎的入侵偵測機制，預期達到防止惡意行為出現，確保營運局端在攻擊行為出現時，能即時發現異常行為，保障核心網路正常維運。

關鍵字：IP多媒體子系統、入侵偵測系統、會談起始協定、通用行動通訊系統、全球行動通訊系統。

Abstract

The rise of Internet not only drives the rapid development of network but also makes users' demand for Internet service higher. On the other hand, Global System for Mobile communication allows users access data and service through mobile network due to the advancement of access technology. It facilitates the convergence of Internet and mobile network. To merge the two networks, 3GPP standardized specifications for IP Multimedia Subsystems. It is an open standard architecture, bases on all-IP network and provides a variety of services. At present, there is no sufficient mechanism and strategy to assure the network security of IP Multimedia Subsystem. Thus there are many risks which include hacking, malicious usage, forgery, masquerade, denial of service and SQL Injection. Operators need an effective intrusion detection mechanism to guarantee whole the components operate correctly. In the paper, we purpose a rule-based intrusion detection mechanism for IP Multimedia Subsystem to prevent malicious behaviors, detect abnormal events real-time and ensure the entire core network can keep operating correctly.

Keywords: IP Multimedia Subsystem (IMS), Intrusion Detection System (IDS), Session Initiation Protocol (SIP), Universal Mobile Telecommunications System (UMTS), Global System for Mobile communication (GSM).

1 簡介(Introduction)

全球行動通訊系統（GSM）發展已邁入第三代（3G）的通用行動通訊系統（UMTS）。在前兩代的系統中，最主要提供的功能為語音通話和簡訊傳送。傳送調變技術由類比演進至數位系統，並有泛用無線封包數據服務（GPRS）的基礎數據資料傳送服務。隨著第三代通訊系統已臻成熟，各國電信業者與營運商積極推動3G平台，提供各式服務。業者冀望在第三代行動通訊系統奠定良好根基，展望第四代行動通訊（4G）系統的未來。通用行動通訊系統（UMTS）架構上可分為：電路交換網路（Circuit-switched network, CS）、封包交換網路（Packet-switched network, PS）以及IP多媒體子系統（IP Multimedia Subsystem, IMS）[1-10]。從服務概念來劃分大致上可分別對應至語音服務（Voice Service）、資料服務（Data Service）以及各種利用封包為基礎的多媒體服務（Packet-based Multimedia Service）。最後，整合多種異質網路存取技

術，例如無線區域網路（Wireless LAN）及微波存取全球互通網路（WiMax），提供使用者使用網路上無所不在的服務（Ubiquitous Service），達到下一代通訊網路（NGN）的目標。

另一方面，網際網路無遠弗屆的發展，促成多樣服務興起，加快資訊交換速度，遂成為人類生活不可或缺的一部份。越來越多的場合，使用者除了擁有手持行動電話外，還擁有一台具備網路連線能力的可攜式電腦，以便隨時跟網際網路接軌，獲取最新的資訊。

融合行動通訊與網際網路同時，將帶入網際網路上所有會發生的風險。對於電信網路來說，網際網路是一個開放性高且規模龐大的網路，在行動通訊系統要求極高的安全性下，必然面臨極大挑戰與未知風險，第一個要面臨挑戰的就是IP多媒體子系統（IP Multimedia Subsystem, IMS），以全IP網路為架構，配合會談起始協定（Session Initiation Protocol, SIP）[2]成為使用者管理，驗證、授權、計費、服務存取及信令轉接等的核心網路。過往曾發生在網際網路的各種攻擊模式將發生在IMS，包含IP和SIP協定設計缺失，可能成為攻擊者有心破壞的進入點（Entry Point）。傳統網際網路有各種研究成熟的入侵偵測系統（Intrusion Detection System, IDS）和入侵防禦系統（Intrusion Protection System, IPS），針對各種協定進行分析，然而IMS領域中尚未有成熟的入侵偵測機制被提出。未來IMS發展過程裡，必須利用有效的入侵偵測機制來防護IMS。因此，本論文提出了適用IMS的規則式入侵偵測機制，作為保護IMS及整個核心網路的第一道防線。

本論文結構安排如下：第二段描述本論文相關技術基礎，分別對IMS、IMS監控技術及IMS中會發生的攻擊行為進行介紹，第三段描述本論文提出的入侵偵測機制，第四段針對IMS服務進行建模，第五段進行入侵偵測機制的驗證，證明本入侵偵測機制實務上能達到的成果，最後則是結論和參考文獻。

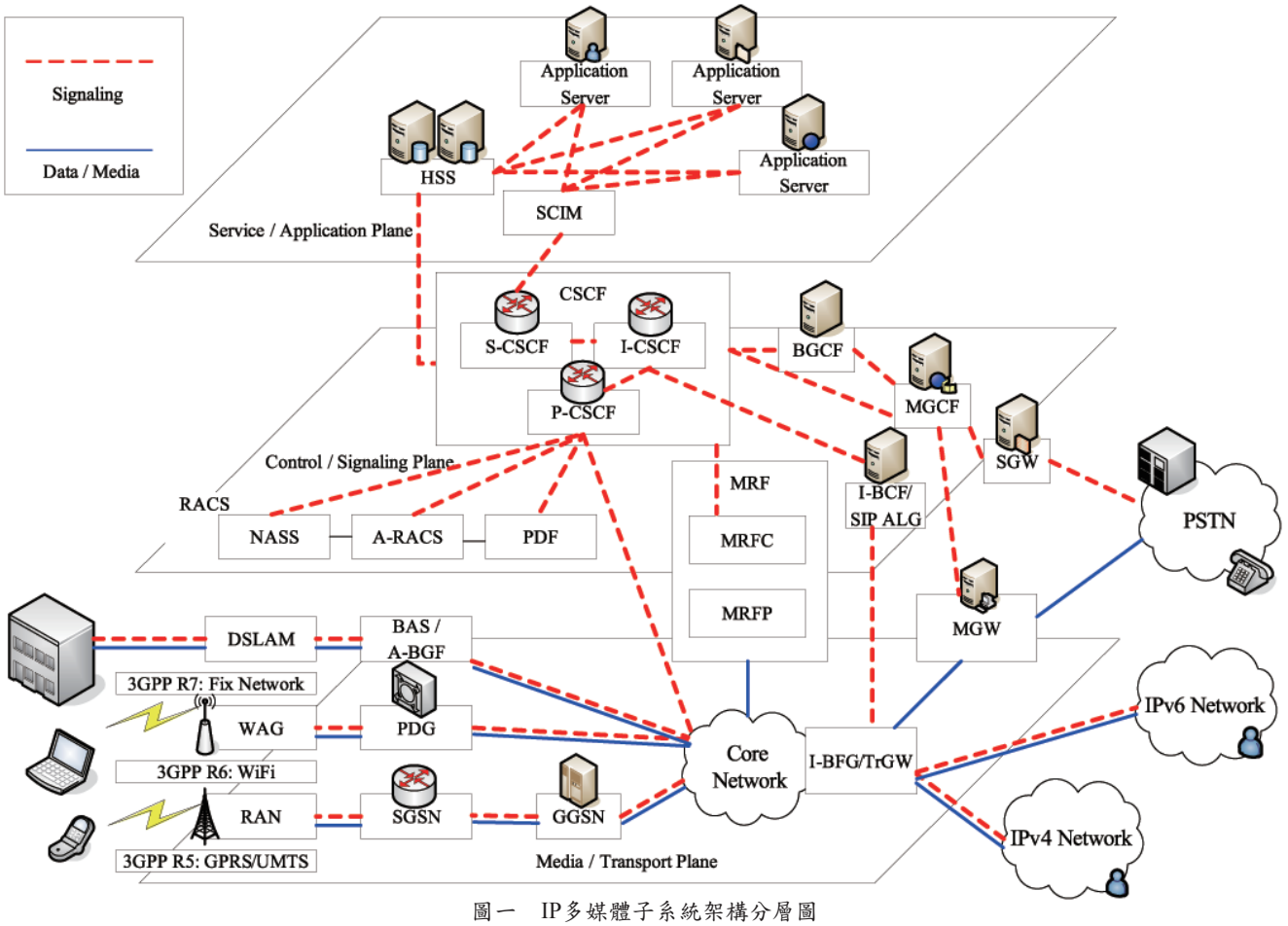
2 背景介紹（Background）

2.1 IP多媒體子系統（IP Multimedia Subsystem）

IMS 主要架構如圖一，可分為三層：媒體與傳輸層、信令與控制層、服務與應用層。

在媒體與傳輸層有著各式各樣不同介接技術（Access Technology），使用者可以透過 IPv4網路、IPv6網路[3]、WiFi、WiMAX、GPRS/UMTS等取得核心網路連線，再連接上 IMS，使用 IMS 提供各式各樣的服務。不管使用者使用的介接技術為何，只要連上核心網路，就能跟IMS連線並使用IMS提供的各種資源。

信令與控制層有IMS核心元件CSCF（Call Session Control Function），主要為Serving-CSCF、Interrogating-CSCF以及Proxy-CSCF，使用者發出的請



圖一　IP多媒體子系統架構分層圖

求信令都會透過本層的元件處理、解析與繞送至正確的目的端，像是把信令繞送到其他營運商的IMS、傳送PSTN建立連線之信令或者向應用伺服器請求服務等，均由本層元件負責。

服務與應用層存在許多應用程式伺服器，提供使用者各式各樣的服務，營運商可以透過標準IMS架構開發應用程式或服務，建置於應用服務層，透過跟IMS信令與控制層連結，就可以提供使用者服務。

2.2 IMS監控技術（IMS Monitoring Technology）

在IMS中，3GPP組織為每個服務制訂相關標準，明確定義各服務正確處理流程，包含應繞送之元件、訊息要求格式，還有各元件對服務要求的處理機制，例如服務的應用伺服器和底層媒體閘道（Media Gateway, MG）溝通協調之工作等。在以IMS架構評估下一代網路可靠度的研究中提出了以系統矩陣（System Matrix）監測各元件間信令狀態的概念[4]。對不同的服務利用標準定義的通訊路徑，建立專屬該服務的系統矩陣，讓營運局端透過系統矩陣，得知路徑上各元件以及會談（Session）運作情況的正確性，經由評估各元件可靠度而提升整體IMS核心可靠度，確保系統和用戶進行的會談能夠正確運作與執行。

本論文利用系統矩陣概念，導入到監控元件中，配合3GPP為各服務制訂的標準，將每個服務建立專屬的規則，在要求進入系統時，就開始將要求與規則比對。

2.3 IMS潛在攻擊（Potential attacks in IMS）

IMS潛在的攻擊涵蓋相當廣泛，由於IMS基於全IP網路和SIP為發展基礎，繼承所有在IP和SIP環境中發生攻擊的可能性與弱點。攻擊主要分成兩大類：時間相依攻擊（例如：Flooding Attack）[5][8]以及非時間相依攻擊（例如：SQL Injection或訊息偽造）[6][9]，本段將簡介IMS可能遇到的攻擊情況。

2.3.1時間相依攻擊：

(1)TCP SYN Flooding Attack：利用TCP三向交握設計上的缺失，在用戶端向IMS發出TCP的SYN訊息時，若假造不存在的來源端，則第一個接入元件P-CSCF會向不存在的來源發出SYN-ACK，之後開啟連結進入等待狀態，若攻擊者同時發出大量假造來源的SYN訊息。P-CSCF的資源（處理器與記憶體容量）可能被大量的SYN訊息耗盡，而失去正常服務能力，讓其他使用者法透過P-CSCF連上IMS核心網路。

(2)時間相依之SIP Flooding Attack：主要為攻擊者短時間內發出大量要求訊息，消耗主機產生回應的資源。例如向IMS註冊之第一個階段，用一台性能優越或多台攻擊跳板工作站短時間內大量發出註冊要求。其攻擊原理為收到第一個401未授權訊息後不發出第二階段註冊回應（Response），在IMS產生大量暫存資源消耗，拖慢IMS效能，讓IMS無法即時反應和正常運作。

2.3.2 非時間相依攻擊：

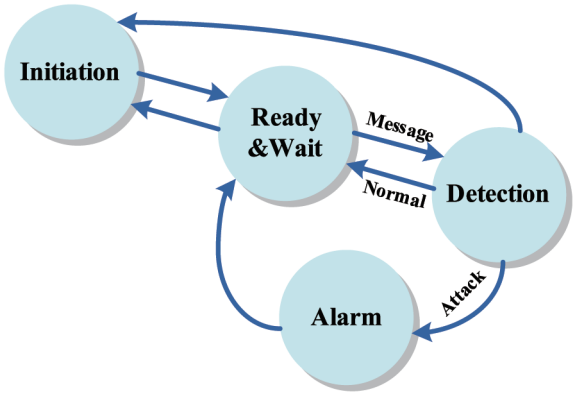
(1)SQL Injection：由於IMS要求訊息是以文字為基礎的訊息，攻擊者利用IMS解析要求訊息的時機，在訊息的SIP標頭或SDP內容加入惡意資料庫攻擊程式碼，利用會向本籍用戶伺服器（Home Subscriber Server, HSS）查詢資料的元件（例如：I-CSCF、S-CSCF或應用伺服器）將惡意程式碼送入HSS，造成資料庫錯誤、資料遺失或竄改資料庫內容。HSS為整個IMS存放使用者資料的資料庫，紀錄使用者公開與私有識別名稱、服務訂閱內容等資訊，若HSS遭任意竄改，將影響整個IMS運作與用戶隱私。

(2)非時間相依之SIP訊息攻擊：在SIP的環境中，會談處於進行階段時，正常情況下能夠利用UPDATE、RE-INVITE訊息對進行中的會談進行參數修改，或者利用BYE訊息結束進行中的會談。因此攻擊者可利用用戶間正常進行的會談時，假造訊息送入其中一用戶之P-CSCF，讓P-CSCF轉送假造訊息給進行會談的使用者。若攻擊者送入假造BYE，進行的會談會單向中斷，造成IMS會談不正常終止；若送入偽造UPDATE或者RE-INVITE則會造成會談狀況改變，例如改變媒體資料傳送目的IP或者連接埠，新增、刪除媒體串流，讓會談成為不對稱狀況，屆時雙方會談已無法正確協商，媒體串流可能被竊取或者轉送往不存在的位址，造成許多ICMP錯誤和網路的負擔。

從入侵偵測的觀點來看，時間相依攻擊可以在特定時間內利用訊息的量分析而偵測出攻擊行為。大部分的攻擊行為模式為針對協定設計缺失進行攻擊，利用漏洞在短時間內發出大量服務要求，藉此嘗試癱瘓服務主機。非時間相依攻擊則無法透過偵測時間內進行相同或類似訊息的數量發現攻擊行為，必須解析資料承載內容，或針對使用者會談進行參數保護來避免發生攻擊。可用來發動攻擊的通訊協定有TCP、UDP、ICMP和SIP等。

3 IMS之入侵偵測機制（Intrusion detection mechanism for IMS）

本論文提出之IMS入侵偵測機制運作流程如圖二的運作狀態機，並將機制建置於Proxy-CSCF，在訊息進入點執行我們提出的入侵偵測機制。首先，入侵偵測機制啟動後，在初始（Initiation）狀態將分析正確IMS服務流程的規則載入到入侵偵測系統中，將規則在系統的記憶體中以資料結構的方式儲存。規則載入完畢後，即進入準備與等待（Ready & Wait）狀態，這時入侵偵測機制已經準備好對任何進入IMS的訊息進行偵測、解析和掃瞄的工作。



圖二 規則式IMS入侵偵測機制運作狀態機

一有訊息進入時，就會觸發偵測（Detection）狀態，系統將依照來源、目的、方向、服務路由和要求的訊息種類等進行解析，與記憶體中合法規則進行比對，同時在Proxy-CSCF中建立專屬於本會談的系統矩陣，追蹤後續會談流程訊息轉遞的過程。若解析後的結果符合合法規則，則狀態機經由正常（Normal）轉回準備與等待繼續等待下一個進入的IMS的訊息，若解析的規則不符合載入記憶體中合法的規則，則由發生攻擊（Attack）轉入警報（Alarm）狀態，對攻擊訊息不進行任何轉遞，並且觸發警報訊息，告知維運人員可能有針對IMS的攻擊產生，詳細記錄來源資訊、時間、觸發警報為何，讓攻擊者無法以協定或標準設計的漏洞，對系統進行任何形式的攻擊。

處理完攻擊訊息後，狀態亦回到準備與等待狀態，繼續處理後續進入IMS的訊息。而當營運商新增加新的服務時，必須新增規則到入侵偵測機制中，以免使用者要求新的服務時，因規則在系統中無法判定為正確程序而被阻擋，有新規則加入後，系統必須重新解析規則並載入記憶體，這時候將由準備與等待狀態或分析攻擊狀態處理完後轉回初始狀態，將重新分析IMS服務流程規則。

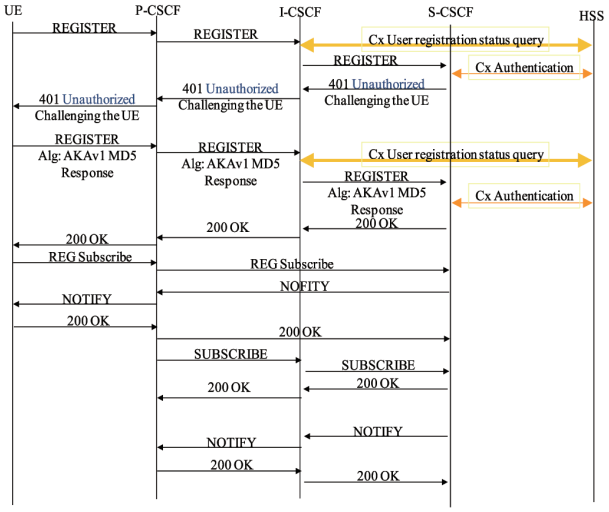
在監測IMS服務方面，以套用系統矩陣的方式對每個會談進行分析並建立屬於該服務的系統矩陣，藉此得知各元件在該會談進行中的狀態。我們針對各種正常IMS服務流程進行分析，建立描述不同服務的IMS規則，規則描述該服務正確流程、訊息傳遞屬於何種元件間溝通關係、以及訊息傳遞的方向、訊息標頭格式等。

4 IMS服務之規則建模（Modeling the rules of IMS service）

IMS為高擴充性開放架構，可以加入各式的應用服務，每個服務運作需要配合的元件不一定相同。因此如何正確建立服務規則，在IMS規則式入侵偵測機制中，是相當重要的議題，不正確的規則無法有效偵測攻擊行為，更可能導致正常服務運作癱瘓。

IMS規則建模步驟大致上可分為三個部分，分別為IMS服務標準分析、服務矩陣建模和建立正常服務規則，本論文以3GPP TS24.228 IMS標準註冊流程[7]為例，說明如何進行IMS服務規則建模。

從圖三得知標準制訂的流程中，註冊必須由UE發起，並且註冊過程中會由P-CSCF、I-CSCF、S-CSCF及HSS進行處理，每個元件間的訊息要求方法（Method）為何，也都有明確的標準，透過如圖四所示之系統矩陣方式，將標準註冊流程建立元件處理的先後關係。



圖三 3GPP IMS標準註冊流程

服務	信令或媒體承載鍊路	局端	ATA	SBC	P-CSCF	I-CSCF	S-CSCF	TAS	HSS	DNSENU	MRF	MGCF	Presence	IPTV
註冊	信令	UAC			●	●	●		●					
		UAS												
	媒體承載鍊路	UCC												
		UAS												

ATA——類比電信轉換　　SBC——會談邊界控制
P-CSCF—— Proxy 會談控制功能　　I-CSCF —— Interrogating 會談控制功能
S-CSCF——Serving 會談控制功能　　TAS ——電信應用伺服器
DNS——域名查詢伺服器　　ENUM——數位號碼映設伺服器
MRF——媒體功能伺服器　　MGCF——媒體閘道控制伺服器

圖四 IMS註冊流程之系統矩陣

獲得系統矩陣內容後，能得知IMS服務運作時所使用的元件類別，這些元件就是在該會談或者服務進行的時候，入侵偵測機制將特別對應和解析訊息的元件。接著按照標準制訂的內容將元件間的溝通以專用編號代替，把訊息標頭簡記，並記錄正確訊息轉遞向量，建立正常服務規則，如圖五所示，建立註冊流程的規則表。

From	To	ID	Vector	Message
UE	P-CSCF	1	Forward	REGISTER
P-CSCF	I-CSC	8	Forward	REGISTER
I-CSCF	S-CSCF	4	Forward	REGISTER
S-CSCF	I-CSCF	4	Back	401 Unauthorized
I-CSCF	P-CSCF	8	Back	401 Unauthorized
P-CSCF	UE	1	Back	401 Unauthorized
UE	P-CSCF	1	Forward	REGISTER
P-CSCF	I-CSCF	8	Forward	REGISTER
I-CSCF	S-CSCF	4	Forward	REGISTER
S-CSCF	I-CSCF	4	Back	200OK
I-CSCF	P-CSCF	8	Back	200OK
P-CSCF	UE	1	Back	200OK
UE	P-CSCF	1	Forward	SUBSCRIBE
P-CSCF	S-CSCF	2	Forward	SUBSCRIBE
S-CSCF	P-CSCF	2	Back	200OK
P-CSCF	UE	1	Back	200OK
S-CSCF	P-CSCF	2	Back	NOTIFY
P-CSCF	UE	1	Back	NOTIFY
UE	P-CSCF	1	Forward	200OK
P-CSCF	S-CSCF	2	Forward	200OK
P-CSCF	I-CSCF	8	Forward	SUBSCRIBE
I-CSCF	S-CSCF	4	Forward	SUBSCRIBE
S-CSCF	I-CSCF	4	Back	200OK
I-CSCF	P-CSCF	8	Back	200OK
S-CSCF	I-CSCF	4	Back	NOTIFY
I-CSCF	P-CSCF	8	Back	NOTIFY
P-CSCF	I-CSCF	8	Forward	200OK
I-CSCF	S-CSCF	4	Forward	200OK

圖五　註冊規則建立表

從規則表歸納出標準服務流程後，就能進一步完成IMS服務規則建模，本論文以圖六之文字延伸標記語言（XML）為基礎，為每種服務建立標準執行規則，依照IMS服務標準分析、服務矩陣建模後可以將合法註冊之規則建模。

透過XML格式的IMS服務規則，入侵偵測機制在初始化階段，能夠快速載入規則到記憶體中。當訊息要進入IMS時，偵測狀態機轉入偵測，並立刻跟載入的規則進行比較，僅放行符合正常規則的會談，並將該會談在系統中建立專屬系統矩陣繼續追蹤監測會談狀態。只要有例外情況發生，該會談將會被終止，並觸發入侵偵測警示。

若在標準流程中夾帶其他資訊（例如：SQL Injection），程序依然會進行，但會有非預期行為發生，若缺乏設計完整的機制，對IMS系統的威脅就會存在。真實環境存在各種標準的服務流程，必須依照不同服務進行XML Profile建模以及套用Service matrix進行規則式入侵偵測，檢測協商程序是否符合標準，並判斷訊息中是否夾帶額外資料，確保IMS系統運作正確無虞。

```
<?xml version="1.0" encoding="utf8" ?>
<!ELEMENT Packet (Time, Vector, Accept, Type,
SourceIP, SourcePort, DestIP, DestPort, Route,
ServiceRoute,SIP-Request-Method)>
<Rule Name = "Register">
<sip-method = "REGISTER">
<service-matrix-vector>1F,8F,4F,4B,8B,1B,1F,8F,4F,4B,8
B,1B,1F,2F,2B,1B</service-matrix-vector>
<service-matrix-message>REG,REG,REG,401,401,401,R
EG,REG,REG,200,200,200</service-matrix-message
<message number>50</message number>
<message interval>60</ message interval>
<alert content="REG Routing Error" From=$UE
Source=$IP>
<sip-method = "SUBSCRIBE">
<service-matrix-vector>1F,2F,2B,1B,2B,1B,1F,2F,8F,4F,4
B,8B,4B,8B,8F,4F</service-matrix-vector >
<service-matrix-message>SUB,SUB,200,200,NOT,NOT,
200,200,SUB,SUB,200,200,NOT,NOT,200,200</service-
matrix-message>
<alert content="SUB Routing Error" From=$UE
Source=$IP>
</Rule>
</xml>
```

圖六　IMS合法註冊規則

5 規則之驗證（Verification the rules）

為了驗證規則式入侵偵測機制能即時偵測攻擊訊息，本論文以IMS非時間相依攻擊中的BYE攻擊為例，驗證本偵測機制。規則之驗證情境為IMS和規則式入侵偵測機制已載入，並進入準備與等待狀態。當使用者進行會談，會談建立完畢、媒體承載資源為進行中的狀態時，若有欲結束會談則會將BYE訊息送給使用者，在BYE規則中能接受的內容如圖七所示。此時，BYE僅能接受的連線向量為1F發起的BYE訊息。從規則建立表可以得知1F為UE向P-CSCF正向遞送訊息，在系統矩陣中若有非UE的攻擊者假造UE發出的BYE訊息，則無法從系統矩陣取得1F的連線向量，並會觸發入侵偵測的警示。

本論文提出的IMS入侵偵測機制能夠有效防止規則以外的攻擊行為發生。從BYE攻擊偵測便能夠驗證本機制在入侵偵測的效果。只要完整將IMS中的服務進行建模，就能夠有效遏止入侵與攻擊的發生，讓IMS處於穩定以及讓使用者會談受到保護。不會遇到攻擊者，輕易地對會談發出偽裝、欺騙的攻擊。

```
<?xml version="1.0" encoding="utf8" ?>
<!ELEMENT Packet (Time, Vector, Accept, Type, SourceIP, SourcePort, DestIP, DestPort, Route, ServiceRoute,SIP-Request-Method)>

<Rule Name = "BYE ">
<sip-method = "BYE">
<service-matrix-vector>1F,1B,1F,2F,7F,5F,6F</service-matrix-vector>
<service-matrix-message>BYE,BYE,200,200,200,200,200</service-matrix-message>
<message number>50</message number>
<message interval>60</ message interval>
<alert content="BYE Attack Alter" From=$Sender Source=$IP>
</Rule>
</xml>
```

圖七　會談中之BYE規則

6 結論（Conclusion）

本論文提出適用於IP多媒體子系統之規則式入侵偵測機制。透過有效的IMS服務規則建模，能偵測出可能在IMS上發生的入侵與攻擊狀況。並依照建模規則將所有的服務模組化並建立專屬於該服務會談的系統矩陣，利用非正常情況蒐集比對，及時攔截不正常動作，確保整個IMS網路運作正常。我們將繼續進行IMS環境中入侵與攻擊的研究，按照提出的規則式入侵偵測機制實作出適用於的規則式IMS入侵偵測系統。期望在實際IMS環境中運作，針對規則解析能力與規則式入侵偵測機制效能進行定量分析（例如: 訊息處理延遲、對系統承載能力的影響），評估規則式入侵偵測機制的系統效能與影響，達到構建完整且安全的IP多媒體子系統目標。

致謝

本研究感謝國科會的資助（計畫編號為NSC 97-2219-E-197-001及NSC 97-2219-E-197-002）。

參考文獻（References）

[1] 3GPP, 3rd Generation Partnership Project; Technical specification group services and systems aspects; IP Multimedia subsystem stage 2, Tech. Spec. 3G TS 23.228 version 6.2.0 (2003 - 06), 2003.

[2] J. Rosenberg, et al., *"SIP: Session Initiation Protocol,"* IETF, RFC 3261, 2002.

[3] J. Wiljakka, J. Soininen, J. Sundquist, and T. Sipilä, *"IPv6 Enabling IMS-based Peer-to-Peer Services in 3GPP and 3GPP2 Cellular Networks,"* Journal of Internet Technology, Vol. 5, No. 2, September 2004, pp. 67-74.

[4] Himanshu Pant, Chi-Hung Kelvin Chu, Steven H. Richman, Ahmad Jrad, and Gerard P. O' Reilly, *"Reliability of Next-Generation Networks With a Focus on IMS Architecture,"* Bell Labs Technical Journal, Vol. 12, No. 4, 2008, pp. 109-126.

[5] Muhammad Sher, Shaoke Wu, and Thomas Magedanz, *"Security Threats and Solutions for Application Server of IP Multimedia Subsystem (IMS-AS), "* IEEE/IST MonAM2006 -- Workshop on Monitoring, Attack Detection and Mitigation, Tuebingen, Germany, September 2006, pp. 28-29.

[6] Muhammad Sher, and Thomas Magedanz, *"Protecting IP Multimedia Subsystem (IMS) Service Delivery Platform from Time Independent Attacks,"* Third International Symposium on Information Assurance and Security (IAS) 2007, United Kingdom, August 29-31, 2007.

[7] 3GPP, 3rd Generation Partnership Project; Technical specification group core network; Signaling flows for the IP multimedia call control based on SIP and SDP; Stage 3, version 5.5.0 (2003–06). 3GPP TS 24.228, 2003.

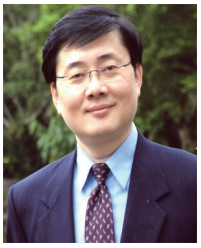
[8] Yacine Rebahi, Muhammad Sher, and Thomas Magdanz, *"Detecting Flooding Attacks Against IP Multimedia Subsystem (IMS) Networks,"* Computer Systems and Applications, 2008. AICCSA 2008, Qatar, March 31-April 4, 2008

[9] M. Mogno, I. Petrilli, and M. Listanti, "*Vulnerability in IMS-Internet interworking: Analysis and Relevant Solutions,"* Networking Workshop 2006, 2006.

[10] Miikka Poikselka, Aki Niemi, Hisham Khartabil, and Georg Mayer, *"The IMS: IP Multimedia Concepts and Services,"* Second Edition, Wiley, 2005.

作者簡歷（Biographies）

Chi-Yuan Chen（**陳麒元**）received his M.S. degree in electrical engineering from National Dong Hwa University, Taiwan, R.O.C. in 2007. He is currently pursuing his Ph.D. degree in electrical engineering at National Taiwan University, Taiwan, R.O.C. His research interests include Personal Communication Service, Software Defined Radio, Cognitive Networks and Network Security.



Han-Chieh Chao（**趙涵捷**） is a jointly appointed Professor of the Department of Electronic Engineering and Institute of Computer Science & Information Engineering, National Ilan University, I-Lan, Taiwan. He also holds a joint professorship of the Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan. His research interests include High Speed Networks, Wireless Networks and IPv6 based Networks and Applications. He received his MS and Ph.D. degrees in Electrical Engineering from Purdue University in 1989 and 1993 respectively. Dr. Chao is also serving as an IPv6 Steering Committee member and Deputy Director of R&D division of the NICI Taiwan, Co-chair of the Technical Area for IPv6 Forum Taiwan. Dr. Chao is an IEEE senior member, IET and BCS Fellows.

Sy-Yen Kuo（**郭斯彥**）is a Chair Professor and Dean of the College of Electrical and Computer Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan. He is also a Distinguished Professor at the Department of Electrical Engineering, National Taiwan University where he is currently taking a leave of absence and was the Chairman at the same department from 2001 to 2004. He received the BS (1979) in Electrical Engineering from National Taiwan University, the MS (1982) in Electrical & Computer Engineering from the University of California at Santa Barbara, and the PhD (1987) in Computer Science from the University of Illinois at Urbana-Champaign. He spent his sabbatical years as a Visiting Professor at the Computer Science and Engineering Department, the Chinese University of Hong Kong from 2004-2005 and as a visiting researcher at AT&T Labs-Research, New Jersey from 1999 to 2000, respectively. He was the Chairman of the Department of Computer Science and Information Engineering, National Dong Hwa University, Taiwan from 1995 to 1998, a faculty member in the Department of Electrical and Computer Engineering at the University of Arizona from 1988 to 1991, and an engineer at Fairchild Semiconductor and Silvar-Lisco, both in California, from 1982 to 1984. In 1989, he also worked as a summer faculty fellow at Jet Propulsion Laboratory of California Institute of Technology. His current research interests include dependable systems and networks, software reliability engineering, mobile computing, and reliable sensor networks.

Professor Kuo is an IEEE Fellow. He has published more than 290 papers in journals and conferences, and also holds several patents. He received the distinguished research award between 1997 and 2005 consecutively from the National Science Council in Taiwan and is now a Research Fellow there. He was also a recipient of the Best Paper Award in the 1996 International Symposium on Software Reliability Engineering, the Best Paper Award in the simulation and test category at the 1986 IEEE/ACM Design Automation Conference(DAC), the National Science Foundation's Research Initiation Award in 1989, and the IEEE/ACM Design Automation Scholarship in 1990 and 1991.

Kai-Di Chang（**張凱迪**）received his B.S. degree in electrical engineering from National Dong Hwa University, Taiwan, R.O.C. in 2007. He is pursuing a Master’s degree in institute of computer science and information engineering at National I-Lan University, Taiwan, R.O.C. His research interests include Voice over IP, IP Multimedia Subsystem and network security.