行政院及所屬各機關出國報告
(出國類別：實習)

赴新加坡諾基亞公司實習
『無線語音數據整合服務評估平台技術』報告

服務機關：中華電信研究所
出國人　職　　稱：助理研究員
姓　　名：林信志

出國地區：新加坡
出國期間：90 **年** 12 **月** 2 **日至** 91 **年** 1 **月** 24 **日**
報告日期：91 **年** 2 **月** 25 **日**

摘要

由於Internet (網際網路)的蓬勃發展，商業行為轉移到Internet上逐漸增加。網路駭客的技術手段越來越高明，一半左右的中、小商家將在2003年成為這種新型犯罪活動的受害者。安全保密的考量跟以前比起來變得愈來愈重要。

而GPRS(整合封包無線電服務技術)及3G(第三代無線行動通訊)的封包核心網路(Packet Core Network)都是採用IP技術做為核心網路，所以在Internet上所遭遇到的Security問題，如今也同樣會發生在無線數據行動通信的網路上。

GPRS和3G核心網路骨幹有數個設備，這些設備處理複雜的存取控制程序並內存著使用者的使用資訊(Profile)。此外，由於網路安全與核心網路骨幹設備是否被照著廠商所提供的文件制式被正確的設定與網路安全有著極大相關，而且如果一部設備被惡意地侵入，那整個網路都會陷入極大的風險，所以這些設備設定必須被詳細地確認。

在本篇中主要針對通訊網路安全風險分析(Security Risk Analysis)來討論。在完成所有的風險評估後，接下來的相關部份如：安全保護評量(Security Audit)、災害應變(Recovery)及回復(Fallback)可依此為基礎做更深入的探討。

本報告包括：

◆前言

◆行程及實習內容紀要

◆第三代無線行動通訊的網路安全

◆實習心得與建議

目　　錄

1. 前言

行動電話已逐漸成為用戶行動中不可或缺的通訊工具，而目前行動電話仍然是以語音服務占大多數。國際電信聯盟（ITU）統計，2001年全球行動電話門號數增加40%，即將超過10億支，預計不久後手機數量將超過固定電話數量。另外根據市場分析公司International Data Corp. (IDC)的執行長Kirk Campbell，在IDC的亞太地區IT論壇上發表演說時指出，亞洲地區將會達成許多IT與電訊產業的記錄，包括：

◆行動電話用戶人數將會超過三億人口，佔全球總數約30%。

◆Internet用戶人數將會達到1.2億人口，佔全球總數約20%。

再依據市內有線電話語音及數據服務的比率、日本i-mode以及全球行動電話簡訊資訊量愈來愈大三種趨勢推估，行動數據服務將日益重要。

而無論是GPRS無線數據行動通信或3G的封包核心網路(Packet Core Network)，也都因應Internet潮流，採用IP技術做為主要的介面規範(Protocol)。但因為Internet的快速發展，商業行為轉移到Internet上逐漸增加，使得愈來愈多意圖不良份子覬覦這個利益，且網路犯罪的技術手段越來越高明。所以在Internet上所遭遇到的Security問題，如今也同樣會發生在無線數據行動通信的網路上。因此未來第三代無線行動通訊業者極可能成為下一波的侵襲目標。

根據《Internet Security》的一項調查報告，公司企業網路安全系統的攻擊者，除了外來惡意侵入者之外，還有企業內部蓄意搗亂的僱員以及與公司有生意來往的合作夥伴者的員工。因此除了防範外在的攻擊者外，在內部網路上亦須建立安全政策(Security Policy)，以建置更安全更令使用者安心的網路。

網路安全政策主要保障業者服務的持續性、提昇投資效益及降低風險免於被攻擊。網路安全是需要由應用一組合適的安全政策；實踐

網路政策、程序、組織架構及軟體功能。

值得注意的是，每一次的網路攻擊事件所產生的不只是當次攻擊的營業損失，還要包含後續所造成難以估計的名譽損失，所以網路安全除了針對病毒、駭客、資訊洩露和篡改等問題，做評測與監管外，網路服務提供業者如何在其網路上建立安全政策，如何提供一個夠安全的網路服務，在成本花費及風險管理上做一個評量，才能讓使用者能夠有足夠的信心，安心地租用服務。

Nokia公司除了擁有無線行動通訊的技術外，在網路安全也與Checkpoint公司合作防火牆設備，累積了相當多的經驗，近來更開始提供網路安全評估服務，在這項服務是以ISF(Information Security Forum)所提供的安全保密方法學來做更詳細的檢查列(check lists)並以此來協助網路服務業者評量3G及GPRS網路安全性。

2. 行程及實習內容紀要

為對『無線語音數據整合服務評估平台技術』最新發展趨勢和電信公司網路架構應用方式與提供服務與業務之方式的瞭解；以及為配合本公司對引進第三代無線通訊技術的服務，奉中華電信公司九十年十一月二十六日信人二字第90A3002726號函核准職前往新加坡Nokia公司技術支援中心，實習『無線語音數據整合服務評估平台技術』，實習期間(含行程)自民國九十年十二月二日至九十一年一月二十四日為期五十四天。本次實習課程計有：

◆研習Nokia Security元件。

◆研習GPRS及3G IP核心網路技術，及SGSN、GGSN、BG、CG、LIG資料。

◆研習GGSN與其他元件結合，如SGSN (focus on Gn internface)。

◆參與Security Audit研討。

3. 為什麼需要考量網路安全?

「美國白宮網站受到駭客攻擊」、「駭客攻擊雅虎Yahoo、eBay、Amazon.com」、「駭客破壞的網站包括美國聯邦調查局和微軟公司的網站」等駭客攻擊事件時有所聞。國際知名網路資訊集團 mi2g Intelligence Unit 發布2001年駭客攻擊網路報告，該報告指出2001年政治動機之網路駭客顯著增加的趨勢，網路駭客動機包括，向社會挑戰、對人事的不滿、政治動機(包括意識型態的差異)及犯罪行為。而該報告亦指出兩岸的僵局及美國與中國大陸軍機爭端，導致我國與中國大陸網站遭駭客「毀容」數量大幅增加，佔全球的8.7% 。「.tw」網域遭駭客「毀容」案件 由106件，增加至1355件，增加1178%，中國大陸則由91件增加至1298件，達1326%。另美國「.com」網域佔2001年全球遭駭客「毀容」案件的30%，「.gov」 網域及「.mil」網域分別為37% 及128% 的高成長率。然而這些數據只是純粹就網站攻擊事件而已。另外在2000年2月，有一個受到攻擊的網址是全國經紀人集團(NDB)；駭客攻擊使該網站關閉了一個多小時。全國經紀人集團有二十多萬客戶。由於駭客攻擊，該公司的銷售額下降了百分之二十五。由這個例子可以想見每一次的網路攻擊事件所產生的不只是當次攻擊造成的業務停擺及營業損失，客戶對網路服務提供業者的信心喪失及後續所造成的名譽損失，其所影響更是難以估計。另外如果駭客成功地攻擊進入某一個網路元件時，其後的安全問題就如同滾雪球一般，藉由該設備再去攻擊其他設備或系統。

為什麼3G需要考量到網路安全性的問題呢?原因在於無論是GPRS無線數據行動通信及3G的封包核心網路，均採用IP技術做為主要的介面規範，而IP技術基本上是設計在一個被信任的網路環境，因此並沒有足夠的安全控管。且因為Internet的快速發展，商業行為轉移到Internet上逐漸增加。某些不法的駭客覬覦Internet中商業行為內部

的利益，加上網路犯罪的技術手段越來越高明，所以在Internet上所遭遇到的Security問題，如今也同樣會發生在無線數據行動通信的網路上，因而在第三代無線行動通訊IP網路安全是變成了一個重要的考量。因此未來第三代無線行動通訊業者極可能成為攻擊者下一波的侵襲目標。

因此什麼是網路安全檢查呢？網路安全檢查主要意義是在確保電腦主機及其內部資訊和網路的安全，為了考量網路安全我們必須要做一個安全評量檢查；而安全評量檢查所檢測的系統可以是包含一台(或多台)電腦及一個(或多個)網路所產生的檢查清單。而網路安全是經過一個處理、程序或者是一個工具確保資料進入主機及其後被取出時都是由被授權過的人才能做。程序應額外被包含在系統中，當某個人是未經授權地取出、篡改或破壞資料時將會違反安全管制，而當有人試圖非法穿越安全管制時，系統管理者將會收到通知。[1]

所以網路安全除了針對病毒、駭客、資訊洩露和篡改等問題，做評測與監管外，網路服務提供業者如何在其網路上建立安全政策，如何提供一個夠安全的網路服務，在成本花費及風險管理上做一個評量，才能讓使用者能夠有足夠的信心，安心地租用服務。

4. 行動數據網路名詞解釋

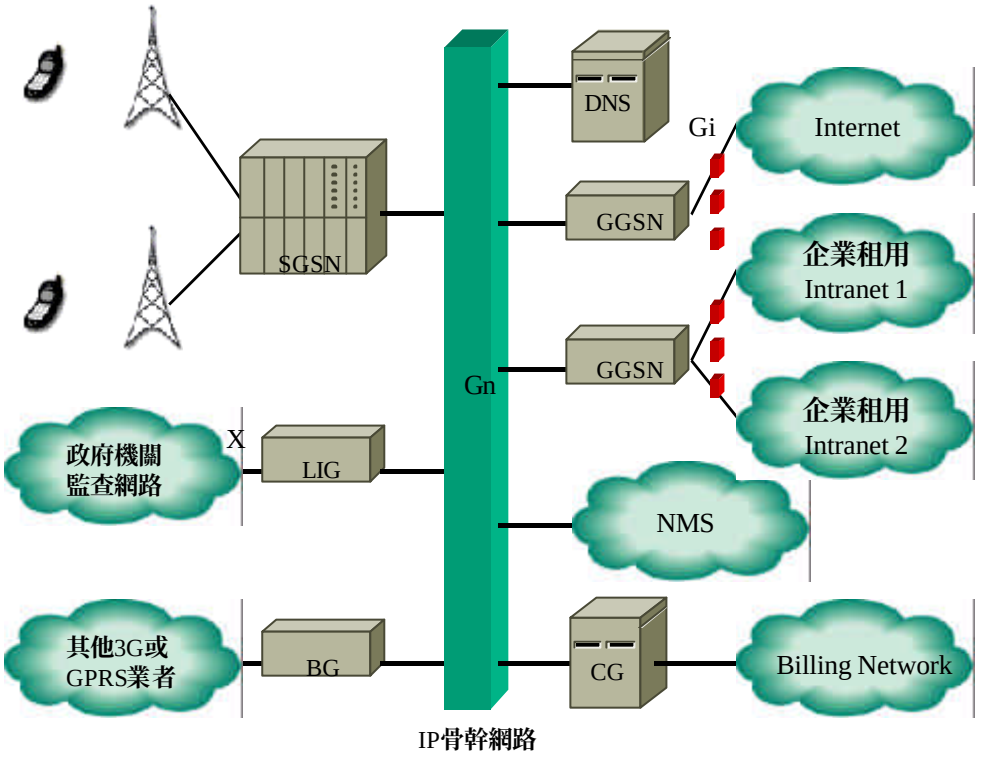

圖4.1. 行動數據網路示意圖

GGSN (Gateway GPRS Support Node)

第一個G 是指 Gateway，**代表GGSN是行動數據與外界網路的一個閘道，所以GGSN能將外界網路的封包傳送進行動數據網路，或將行動數據網路內的封包傳出到外界的**Internet**上。**[2]

SGSN (Serving GPRS Support Node)

在GSM網路中，一個BSC同時連接許多 BTS，BSC**與**BTS**的所在區域即組成GSM網路的一個服務區域，位於服務區域內的手機使用者都能使用GSM通訊網路。行動數據網路增加的另一個節點SGSN，會佈設在網路內的各個服務區域內，**SGSN**負責紀錄在服務區域內有哪些使**

用者，若是使用者傳送的是屬於封包的資料，經由BSC**的判斷，會將封包的資料傳給**SGSN**，由**SGSN**做封包的交換與傳輸。**[2]

BG (Board Gateway)

與其他業者簽訂國際漫遊時，連接兩個的GPRS**或**3G**網路需要透過**BG**。可以是一個路由器或者是防火牆。**BG**提供兩個不同網路的一個直接的**GPRS Tunnel**。**

CG (Charging Gateway)

收集從SGSN**及**GGSN**傳送來的帳務資料並將之處理後轉送後端帳務系統。**

LIG (Lawful Interception Gateway)

政府警政系統監察行動數據網路使用者行為時的設備。

GTP (GPRS Tunneling Protocol)

GTP**是**GPRS**骨幹網路上，兩個**GSN**間用來相互傳送使用者資料及控制訊號的通道協定，它必須在兩個**GSN**間提供資料傳送的機制。在**GTP**之下，使用**UDP**透過**IP**骨幹網路，來提供**GTP**協定單元的傳送服務。**

DNS (Domain Name Server)

在Internet**上的一個應用層規範，主要是將一個易記的文字名字**(Domain Name)**轉換成**IP**位址。如將** gprs.chttl.com.tw = 140.116.123.45**。**

APN (Access Point Name)

APN可視為一個標記，用戶設定在手機上，由此網路端可向DNS查詢該透過那個GGSN連到外界網路。

5. 無線行動網路的攻擊者

Internet上的攻擊者一般就認知而言，就是駭客。而在本篇中我們所定義的攻擊者除了外部惡意攻擊的使用者，還討論到內部操作人員。分述這兩大類如下：

- 外部惡意攻擊的使用者又可區分為下面5種：
  - 不懷善意的行動電話使用者；
  - Internet上的駭客；
  - 透過BG利用其他網路服務業者來攻擊；
  - 透過LIG與外部連線的侵入者；
  - 其他無法獲得網路服務業者正式授權操作網路但蓄意侵入操作的人。[3]
- 內部操作人員又可區分為下面3種：
  - 允許進入操作維護之機房人員；
  - 廠商及其配合廠商(Third Party)的工程師；
  - 其他被允許進入操作的人員。[3]

6. 網路上的安全威脅

在安全威脅上主要包含三個對象，分別為攻擊者、目標主機及受信任的系統主機，分述如下：

- 攻擊者：未經合法授權嘗試進入目標主機存取、篡改資料者。
- 目標主機：攻擊者的目標。

- **受信任的系統主機：可合法存取目標主機的遠端，通常是攻擊者偽裝的對象。**

在攻擊上大致可以區分四種方式，分別為IP Spoofing、Sniffering、Session Hijacking**及**Man-in-the-middle**，分述如下：**

6.1. IP Spoofing

攻擊者假裝成受信任的系統主機IP**位址欺騙目標主機，使主機相信他是網路上合法的成員。而最終的目標是與目標主機建立連線使得攻擊者能獲得管理者的使用權限，並在目標主機上安裝後門，之後便可以利用該漏洞進入系統。**

IP spoofing**屬於瞎眼攻擊**(Blind Attack)**，意思就是說攻擊者被認為是受信任的遠端主機，而目標主機認為是一般”正常”的封包在傳送，但實際上都是由攻擊者的主機所假造的資料，如果在上層的應用程式不須回應**(Handshaking)**時，攻擊者和受信任的主機並無不同，然而如果在上層的應用程式須回應時，由於封包會往回送給該受信任的系統主機**IP**位址，所以攻擊者將無法直接看到封包內容。因此攻擊者必須很聰明而且知道在傳送？一個偽造的封包後，目標主機會回應什麼資料，下一步會需要什麼資料。因此攻擊者就像瞎著眼睛在操作系統一樣。**[4]

所以攻擊者通常會先自行模擬後，再做一連串的script**，在目標主機上安裝後門，然後再用”正常“程序進入。**

6.2. Sniffering

Sniffer**原本是設計用來做共享式媒體(如：**Ethernet)**的網路分析、**

除錯(Trouble Shooting)的工具，但這個工具功能強大，可以抓取到任何在網路上所穿過的封包，當然包含利用Telnet等遠端控制軟體的封包，所以如使用者密碼(Password)等機密資料，一旦Sniffer架上該段網路上，其間所送的資料就予取予求，而且隱藏在網路中竊聽，不易被發現，因此Sniffer成為駭客最愛的工具。

6.3. Session Hijacking

攻擊者首先竊聽網路上的封包，一旦封包內含受信任的使用者或主機所傳送的資料或者使用者已進入管理者權限狀態時，接著就假造封包將受信任的系統主機塞爆並讓該主機當機，然後攔截受信任的使用者或主機的IP，重新發peer-to-peer arp “is-at”的封包，將IP對應的MAC位址轉成攻擊者所使用的主機，最後攻擊者就可以用該使用者身分在目標主機做任何事。[5]

6.4. Man-in-the-middle

這是一種最複雜的攻擊方式，攻擊者會同時使用上述的三種方式複合式的嘗試並攻擊。攻擊者使用竊聽受信任的使用者所傳送的封包、接著偽冒為該使用者假造封包，然後攔截，而使用者和目標主機除了中間連線有部份時間發生問題外，並沒有感到任何異狀，但是攻擊者已在其中修改封包內的資料並將偽造的資料送回給使用者和目標主機兩者。[6]

7. 駭客攻擊的路徑

由於GPRS及3G有許多的網路設備，駭客攻擊的目標可以依駭客

的喜好自由決定。如果攻擊者打算中斷服務可以選擇攻擊SGSN，當然如果有機會，還可以透過這個設備存取到NMS (網管系統)的網路。

然而一般而言攻擊者通常會想在不影響正常服務的運作下，偷偷地侵入網路，那通常會選擇CG當作目標，而使自己能夠使用免費的網路資源，或者是侵入LIG中監視網路上所有活動的進行，而藉此謀利。

由於封包核心網路有路由器、DNS、GGSN及SGSN等極多的目標。攻擊者有時為了獲得最後目標的存取權限，會鎖定多個設備攻擊。例如攻擊者可能會進入SGSN或自建一個假的SGSN，然後藉由這個SGSN卸下網路服務業者在GGSN、CG等設備的防護措施。然後再透過這些被攻擊的設備再去侵入其他目標。因為GGSN通常會把SGSN當做是一個可信任的設備，這種攻擊方式通常也較一般直接侵入的方式容易。所以安全漏洞就像是滾雪球一樣，一個設備一旦被侵入，接著下一個就會被攻擊，整個網路也就將會被逐漸地蠶食。

在這部份我們討論到一個封包核心網路所有可能的攻擊路徑，主要可區分成下面三大類：IP攻擊、GTP攻擊及穿越式攻擊。分述如下：

7.1. IP 攻擊：

在封包核心網路因為使用IP技術做為主要的介面規範，所以只要是Internet所會遭遇到的攻擊相同地在3G封包核心網路網路層也同樣會發生。而Gi介面的防火牆擔負了保護的重要責任。接下來？述的6個攻擊路徑是IP攻擊的途徑。[7]

7.1.1. 從 Internet 攻擊手機。

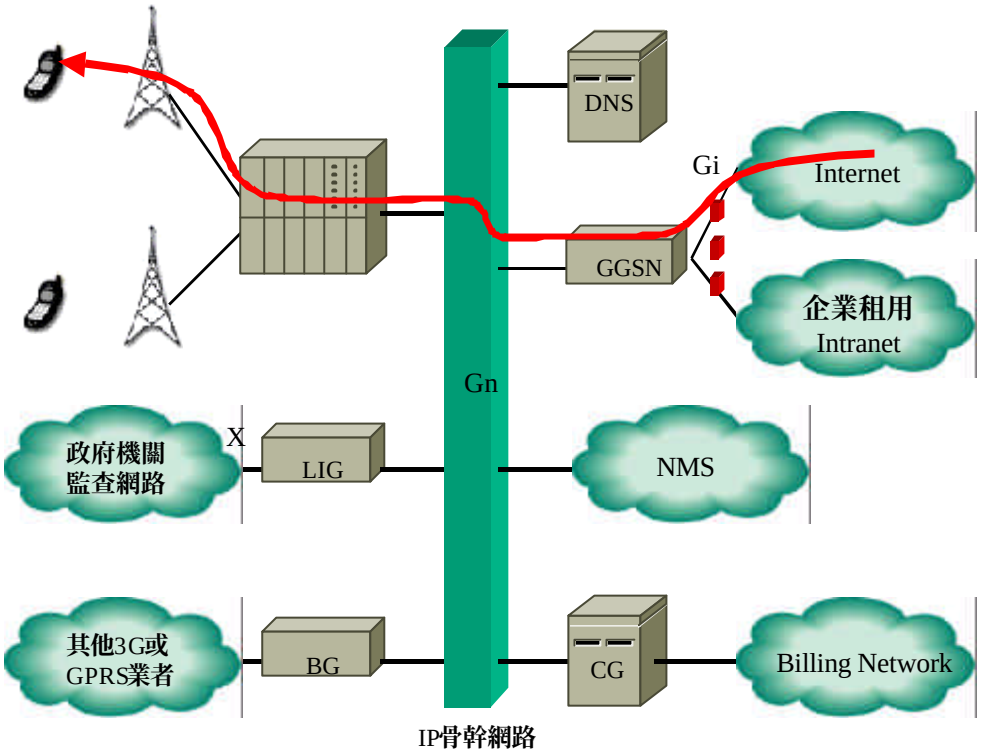

圖7.1.1. 從Internet攻擊手機

如圖7.1.1.所示，由於手機在Internet上而言也可看成是Internet的一個主機，同樣擁有一個IP位址，從Internet的駭客攻擊手機，實際上就和Internet的駭客攻擊某台主機的意義相同。

攻擊者可能是Internet的駭客。使用的方式可能是IP Spoofing、Sniffering、 Session Hijacking和Man-in-the-middle。利用IP Spoofing駭客可以把手機或手機後端的筆記型電腦塞爆，使手機或手機後端的筆記型電腦當機。Sniffering、 Session Hijacking和Man-in-the-middle用來竊取或修改手機使用者與Internet上的伺服器連通時的密碼或資訊。

7.1.2. 從 Internet、企業租用戶的網路或手機經由 GGSN 侵入 IP 骨幹網路。

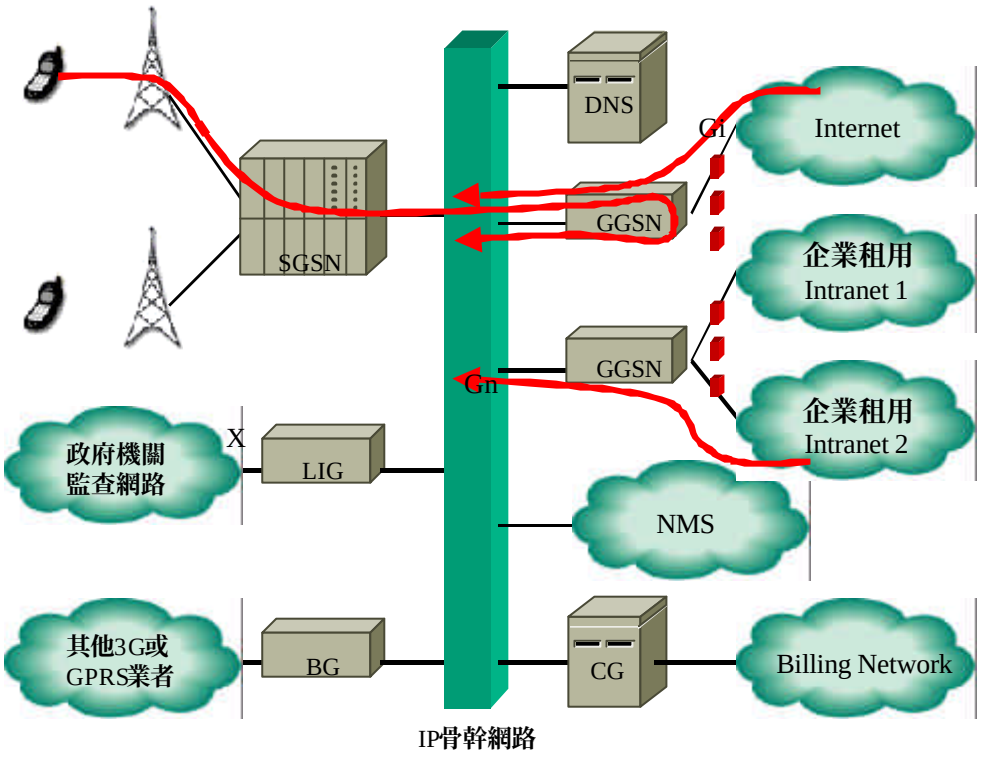

圖7.1.2. 從Internet、企業租用戶的網路或手機經由GGSN侵入IP骨幹網路

如圖7.1.2.所示，以IP網路的角度來看GGSN在3G封包核心網路上簡單的說可以視為是網路上的一個路由器，而路由器的觀念就是會轉送所有的封包去目的位址，除非在防火牆設定Rule (存取規則)，GGSN設定ACL(存取控制列)。從Internet或企業租用戶的網路經由GGSN侵入IP骨幹網路。而其目標可以是核心網路中IP骨幹的任一設備，包含SGSN、CG、BG、LIG、中間的Switch (交換機)及其他的GGSN。雖然這種方式依據3G標準是不會發生的，但GGSN設備做法因各家而

異，如果網路管理者未將GTP層上下IP層的路由表分開，這種情形就有可能產生，當然由手機端也可以直接連上IP骨幹的設備。而這三種方式又以從企業租用戶的網路端攻擊最為容易, 因VPN Tunnel通常是由GGSN建至企業端，中間的防火牆也是開一個洞使資料能夠進出，所以在防止不懷善意的企業租用戶的員工並無太大功用，僅能從GGSN設ACL來防止惡意入侵。

攻擊者可能是Internet的駭客、不懷善意的企業租用戶的員工或是手機使用者。使用的方式可能是IP Spoofing。利用IP Spoofing駭客可以將SGSN、GGSN、CG、BG、LIG及中間的交換機Switch塞爆，使這些網路設備無法順利運作，或者獲取這些網路設備管理者權限，以為下一步的攻擊做準備。

7.1.3. 從 Internet 或企業租用戶的網路透過防火牆侵入 NMS 網路

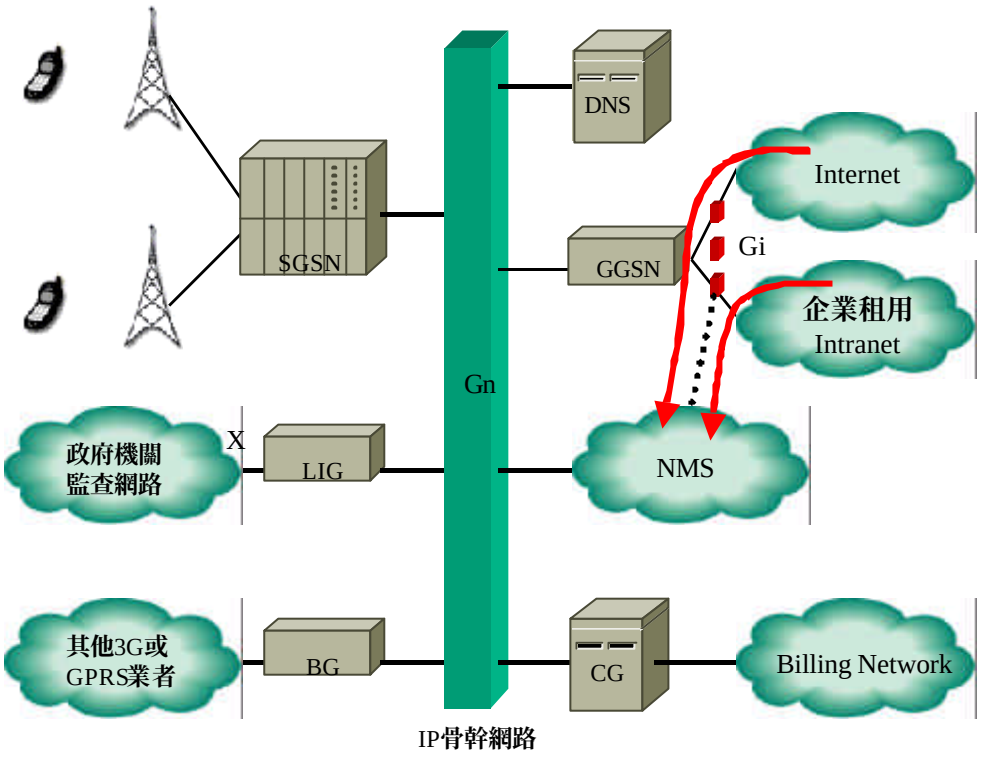

圖7.1.3. 從Internet或企業租用戶的網路透過防火牆侵入NMS網路

如圖7.1.3.所示，在Gi介面上的防火牆因為要管理，所以會與NMS有連接。而防火牆通常是Internet駭客第一個攻擊的目標，一旦防火牆有漏洞或程式不常更新(Patch)等，外部攻擊者便有機會侵入NMS。

攻擊者可能是Internet的駭客或是不懷善意的企業租用戶的員工。使用的方式可能是IP Spoofing。IP Spoofing駭客可以把手機或手機後端的筆記型電腦塞爆，使手機或手機後端的筆記型電腦當機。利用IP Spoofing駭客可以將防火牆塞爆，使之無法正常的運作或使用阻斷服務方式(DOS)攻擊，或者獲取這些網路設備管理者權限，侵入

NMS以為下一步的攻擊做準備。

7.1.4. 在相同的 APN 時，從手機攻擊手機

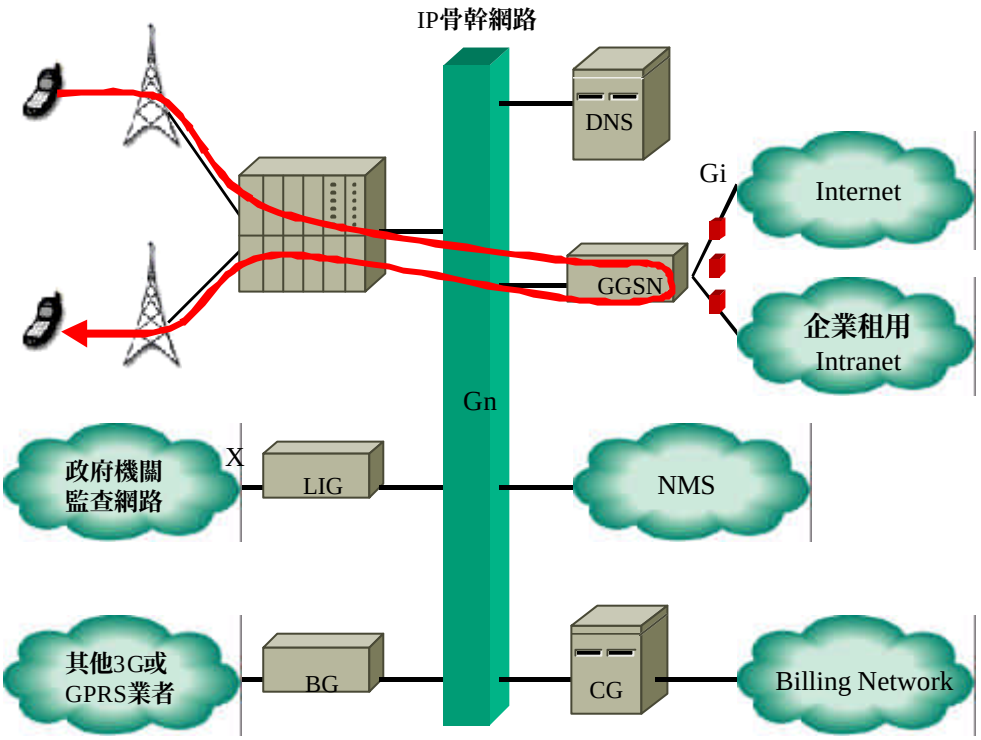

圖7.1.4. 在相同的APN時，從手機攻擊手機

如圖7.1.4.所示，兩台手機連在相同的APN上，其中一台手機攻擊另一台。如果其中一台手機知道另一台手機的IP位址，而且GGSN允許手機彼此互通時，GGSN會將封包互送到對方，而且Gi介面上的防火牆將無法阻擋這類攻擊。目前而言通常不允許兩台手機互傳資料，如果需要這種服務，如MMS(Multimedia Message Service)也是透過中間的伺服器來轉送，但未來這種直接傳送的服務應該也會開放。這類攻擊網路服務業者極難防止。

攻擊者是不懷善意的手機使用者。使用的方式可能是IP Spoofing、Session Hijacking和Man-in-the-middle。利用IP Spoofing攻擊可以把手機或手機後端的筆記型電腦塞爆，使手機或手機後端的筆記型電腦當機。Session Hijacking和Man-in-the-middle用來竊取或修改手機使用者與Internet上的伺服器連通時的密碼或資訊。

7.1.5. 從其他 3G 或 GPRS 業者的封包網路內經由 BG 攻擊

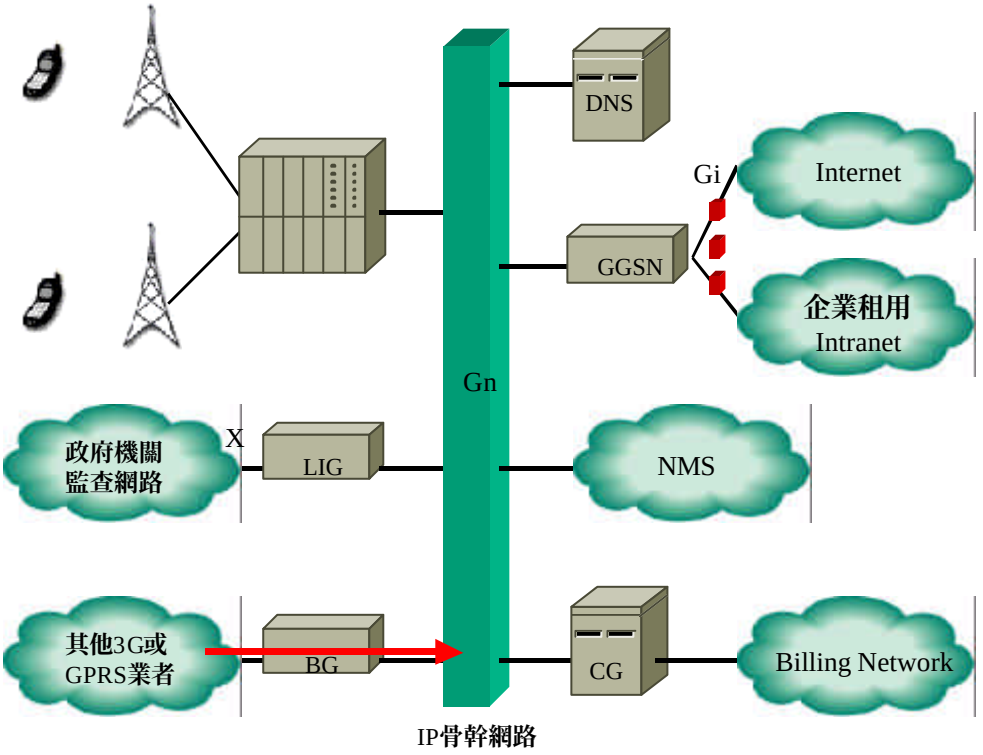

圖7.1.5. 從其他3G或GPRS業者的封包網路內經由BG攻擊

如圖7.1.5.所示，從其他3G或GPRS業者的封包網路內經由BG攻

擊。有可能是因為其他3G或GPRS業者的封包網路內設備被侵入，或者是其中有假造的SGSN利用國際漫遊與本地的網路連接的方式來攻擊。

攻擊者可能是不懷善意的其他3G或GPRS業者或是其配合廠商的員工。使用的方式可能是IP Spoofing。利用IP Spoofing駭客可以將BG塞爆，使之無法正常的運作或使用阻斷服務方式攻擊，或者獲取這些網路設備管理者權限，侵入以為下一步的攻擊做準備。

7.1.6. 由政府機關監查網路經由 LIG 攻擊

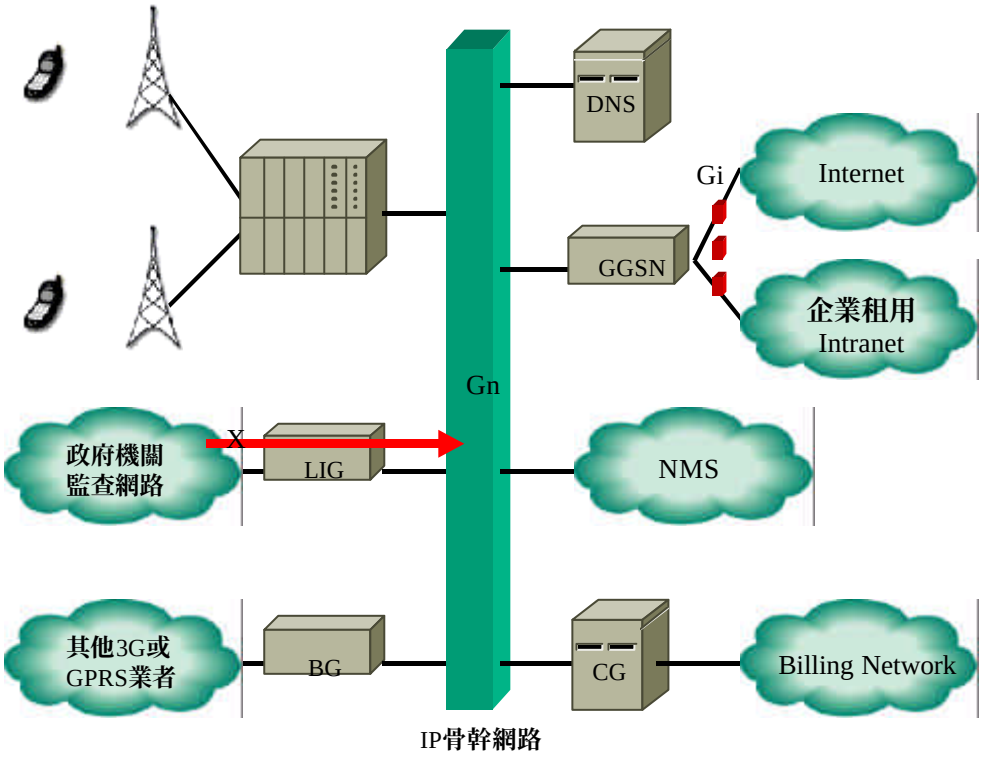

圖7.1.6. 由政府機關監查網路經由LIG攻擊

如圖7.1.6.所示，從政府機關監查網路經由LIG攻擊。通常這是非

常難以做到。由於法令的需要，X介面是有著極強大的保護措施而且也不會接受未經授權的指令。但如果這個介面是利用VPN透過Internet傳送時就會有這樣的風險。

攻擊者可能是X介面間的惡意侵入者。使用的方式最可能是IP Spoofing。

7.2. GTP 攻擊

3G封包核心網路的骨幹由於3GPP標準的制定上是設計成私有網路而且對使用者而言是不可見，但是仍可由其他網路與核心網路連接的介面來攻擊。接下來？述的5個攻擊路徑是利用GTP攻擊的途徑。[7]

7.2.1. 由 Internet 主機假造 GTP 封包攻擊核心網路

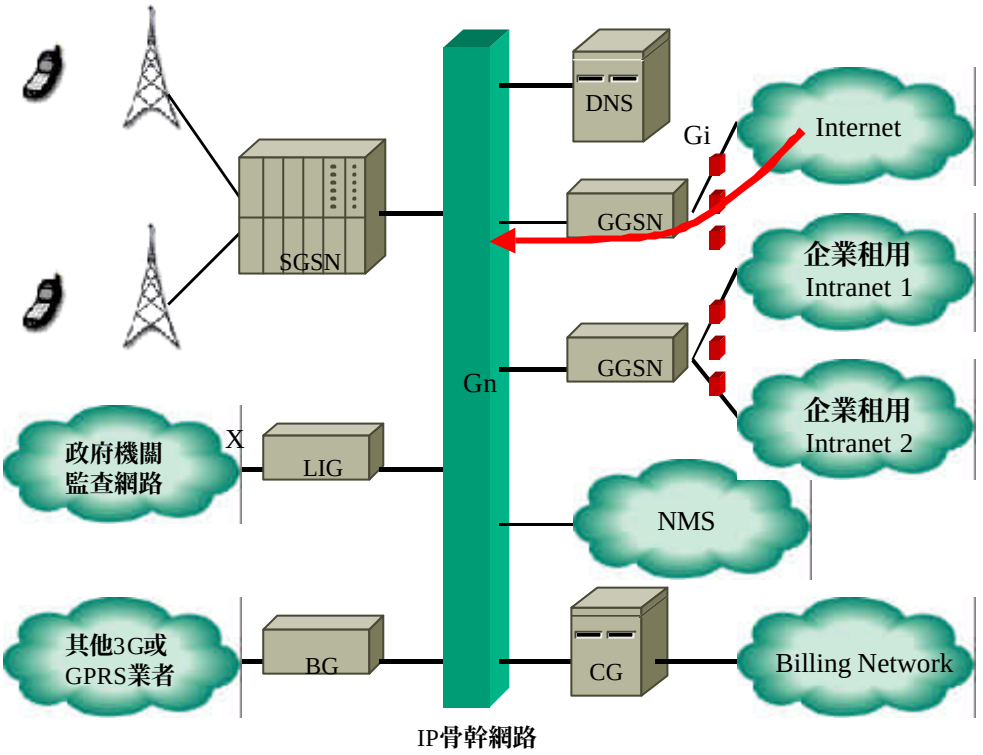

圖7.2.1. 由Internet主機假造GTP封包攻擊核心網路

如圖7.2.1.所示，由Internet主機假造GTP封包攻擊核心網路與攻擊路徑7.1.2.最大不同就是駭客假造GTP封包，而最有可能攻擊的目標是CG。

攻擊者可能是Internet上的駭客。使用的方式可能是IP Spoofing。利用IP Spoofing駭客可以將CG塞爆或Buffer Overflow等，使之無法正常的運作或使用阻斷服務方式攻擊，或者獲取這些網路設備管理者權限，進而修改帳務資料等。

7.2.2. 從 Internet或企業租用戶的網路攻擊其他 3G或 GPRS 業者

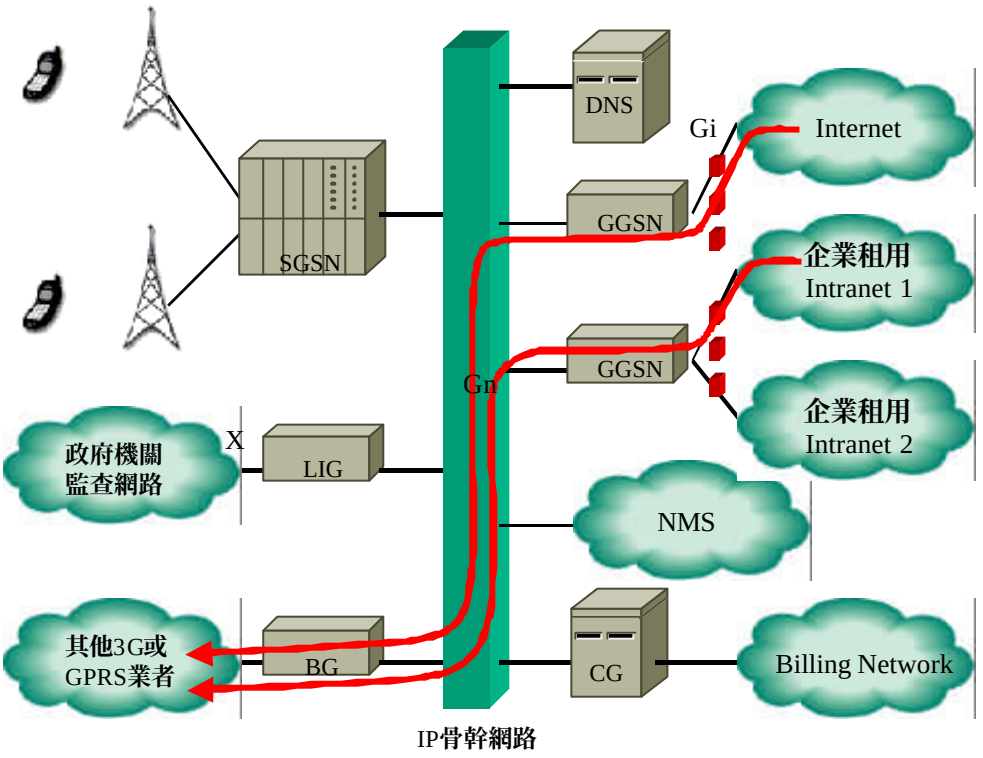

圖7.2.2. 從Internet或企業租用戶的網路攻擊其他3G或GPRS業者

如圖7.2.2.所示，從Internet或企業租用戶的網路攻擊經由BG攻擊其他3G或GPRS業者。從Internet或企業租用戶的網路假造GTP封包，如果GGSN未做完善的設計或操作時，透過BG連到其他3G或GPRS業者的封包網路內的GGSN，會使其他與本地網路簽訂漫遊的業者困擾，或者是其中有假造的SGSN利用國際漫遊與本地的網路連接的方式來攻擊。

攻擊者可能是Internet上的駭客或是不懷善意的企業租用戶的員工。使用的方式可能是IP Spoofing。利用IP Spoofing駭客侵入目標可

能是其他3G或GPRS業者的GGSN，或者獲取這個網路設備管理者權限，以為下一步的攻擊做準備。

7.2.3. 從 IP 骨幹網路中製造假的 GTP 封包攻擊手機或其他 3G 或 GPRS 業者

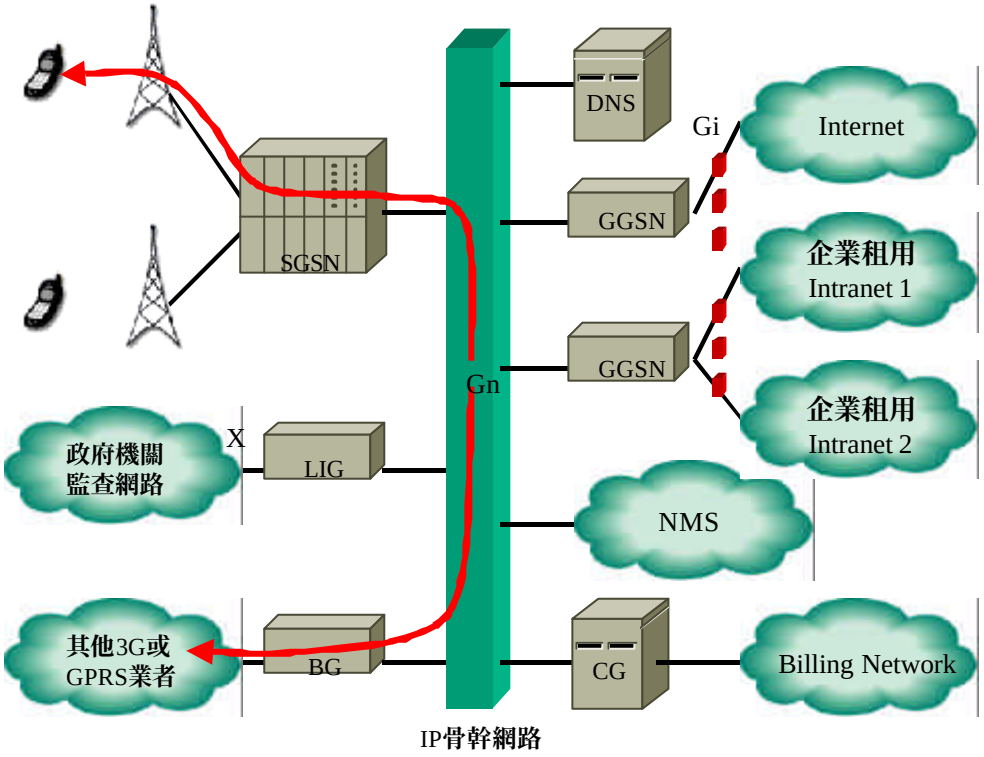

圖7.2.3. 從IP骨幹網路中製造假的GTP封包攻擊手機或其他3G或GPRS業者

如圖7.2.3.所示，與攻擊路徑7.2.2.相類似，但危險性更高。在IP骨幹網路中，攻擊者主機偽裝成一台合法的SGSN，製造假的GTP封包攻擊經由BG其他3G或GPRS業者攻擊其他3G或GPRS業者。另一方

向是攻擊者主機偽裝成一台合法的GGSN，製造假的GTP封包攻擊手機。如果封包核心網路IP骨幹中，有未經合法安裝的程式或主機，裏面包含有SGSN或GGSN的模擬程式，就會有這種情形發生。

攻擊者可能是已入侵成功的Internet上駭客、不肖的機房人員、廠商及其配合廠商的工程師或被允許進入機房的操作人員。使用的方式可能是IP Spoofing、Sniffering、 Session Hijacking和Man-in-the-middle。利用IP Spoofing侵入目標可能是其他3G或GPRS業者的GGSN，或者獲取這個網路設備管理者權限，以為下一步的攻擊做準備。Sniffering、 Session Hijacking和Man-in-the-middle用來竊取或修改任何在IP骨幹上連通時的密碼或資訊等。

7.2.4. 從手機製造假的 GTP 封包透過另一台 GGSN 攻擊企業租用戶的網路

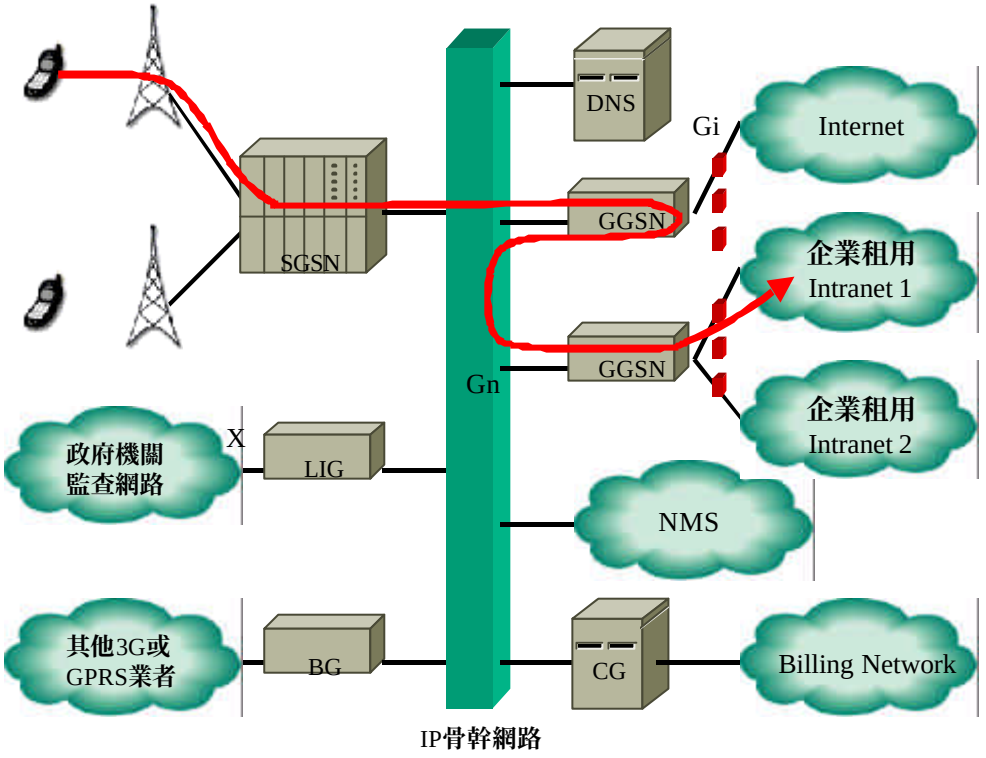

圖7.2.4. 從手機製造假的GTP封包透過另一台GGSN攻擊企業租用戶的網路

如圖7.2.4.所示，從手機製造假的GTP封包透過另一台GGSN攻擊企業租用戶的網路。從手機或手機後端的筆記型電腦上假造GTP封包，如果GGSN未做完善的設計或操作時，當解開GTP封包後，又轉送到另一台GGSN，會使這一台GGSN認為是由SGSN送來的GTP封包，再將封包解開後轉送給企業租用戶的網路。所以攻擊者在假造封包時會包兩次的GTP並了解所欲攻擊的企業租用戶的網路，所連接的

GGSN其IP位址。雖然在3GPP的標準上，GGSN必須主動丟掉未上線的封包，但仍依廠商是否有依據標準做到這項功能來決定。

攻擊者可能是不懷善意的企業租用戶的員工利用其手機來做入侵。使用的方式可能是IP Spoofing。利用IP Spoofing駭客侵入目標可能是企業租用戶的網路內的某部伺服器，獲取管理者權限，竊取或修改伺服器上的密碼或資訊。

7.2.5. 從手機製造假的 GTP 封包攻擊其他 3G 或 GPRS 業者

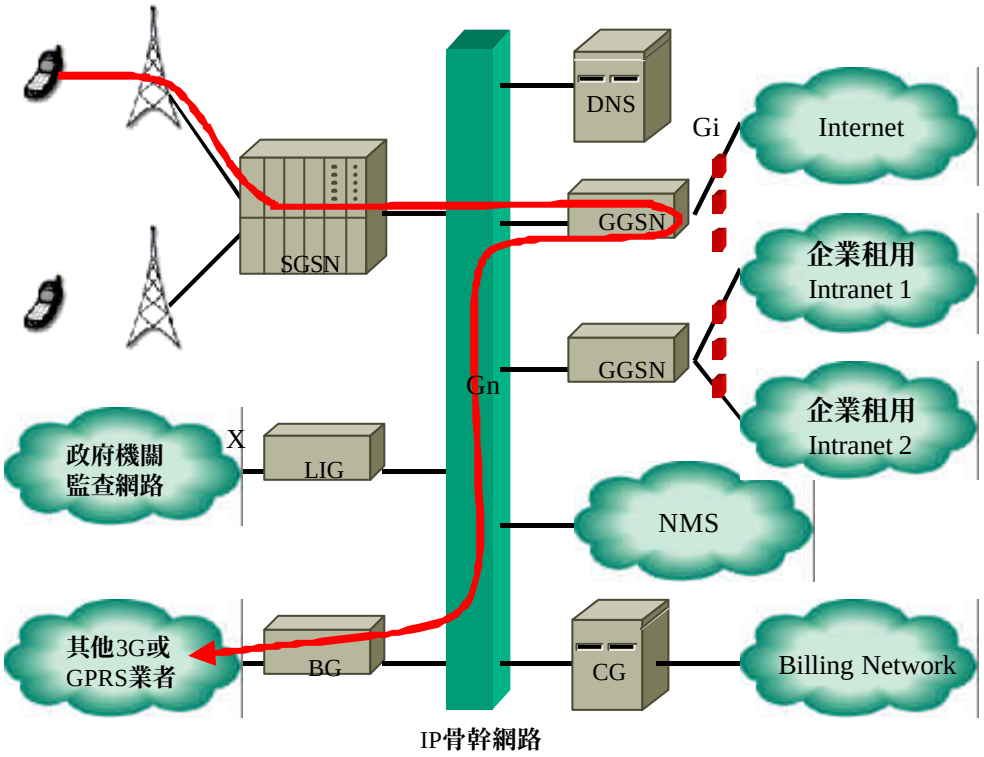

圖7.2.5. 從手機製造假的GTP封包攻擊其他3G或GPRS業者

如圖7.2.5.所示，與攻擊路徑7.2.4.非常類似。從手機製造假的GTP封包，由GGSN解開GTP封包後，GGSN發現裏面又包了另一個GTP，透過BG轉送到其他3G或GPRS網路業者的GGSN上。攻擊者從手機或手機後端的筆記型電腦上假造GTP封包，如果GGSN未做完善的設計或操作時，當解開GTP封包後，發現裏面又包了另一個GTP，再轉送BG連到其他3G或GPRS網路業者的GGSN，會使這一台GGSN認為是由SGSN送來的GTP封包，再將封包解開後轉送被攻擊的目標設備。所以攻擊者在假造封包時會包兩次的GTP並了解所欲攻擊的其他3G或GPRS網路業者的GGSN其IP位址。雖然在3GPP的標準上，GGSN必須主動丟掉未上線的封包，但仍依廠商是否有依據標準做到這項功能來決定。

攻擊者可能是不懷善意的手機使用者。使用的方式可能是IP Spoofing。利用IP Spoofing駭客可能是其他3G或GPRS網路業者的SGSN、GGSN、CG、BG、LIG及中間的交換機Switch塞爆，使這些網路設備無法順利運作，或者獲取這些網路設備管理者權限，以為下一步的攻擊做準備。

7.3. 穿越式攻擊

有時攻擊者只是把封包核心網路內的設備當做是中間的跳板來攻擊其他的目標。[7]

7.3.1. 從一家企業租用戶的網路透過 Gi 介面攻擊另一家企業租用戶的網路

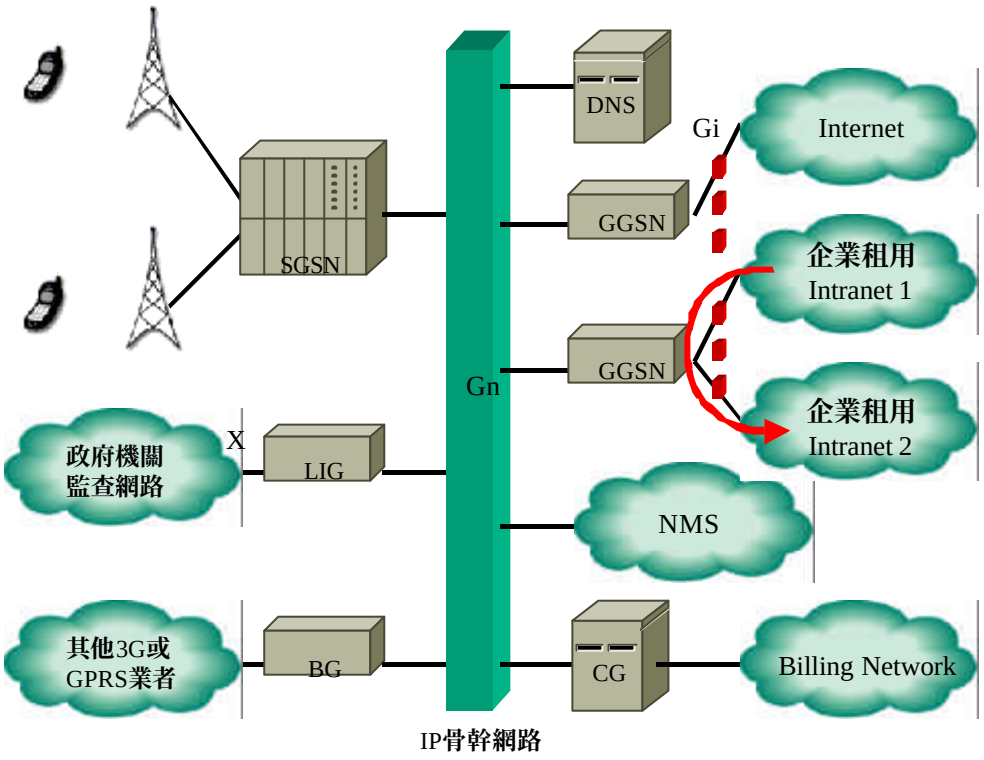

圖7.3.1. 從一家企業租用戶的網路透過Gi介面攻擊另一家企業租用戶的網路

如圖7.3.1.所示，如果沒有定好GGSN後端Gi的防火牆其內的存取規則，就很有可能而且很容易地從一家企業租用戶的網路透過Gi介面攻擊另一家企業租用戶的網路。

攻擊者可能是某一家企業租用戶的員工攻擊另一家企業租用戶的網路。使用的方式可能是IP Spoofing。攻擊者侵入目標可能是企業租用戶的網路內的某部伺服器，獲取管理者權限，竊取或修改伺服器上的密碼或資訊。

7.3.2. 透過封包核心網路攻擊 SS7 網路

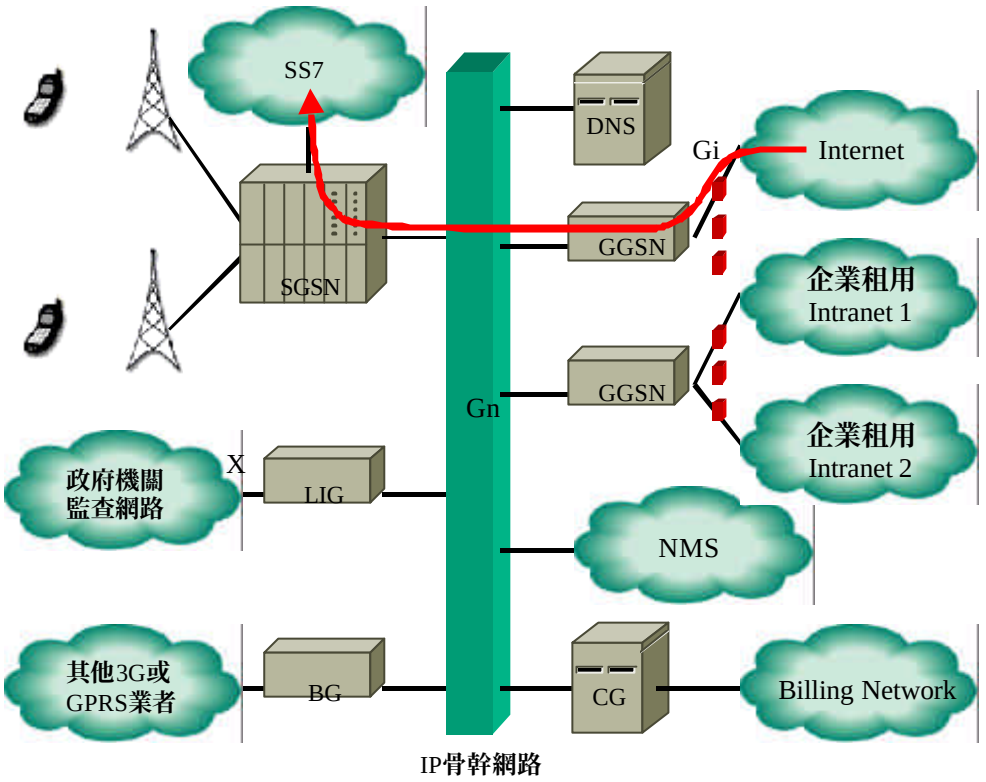

圖7.3.2. 透過封包核心網路攻擊SS7網路

如圖7.3.2.所示，由於3G封包核心網路中的SGSN與SS7網路直接連接。而SS7在安全保密性上不夠強韌，一旦被入侵電話系統將會受到影響。而是否會被攻擊就得看廠商的SGSN是如何設計。

7.3.3. 從手機發起攻擊透過另一部手機當跳板來攻擊企業租用戶的網路

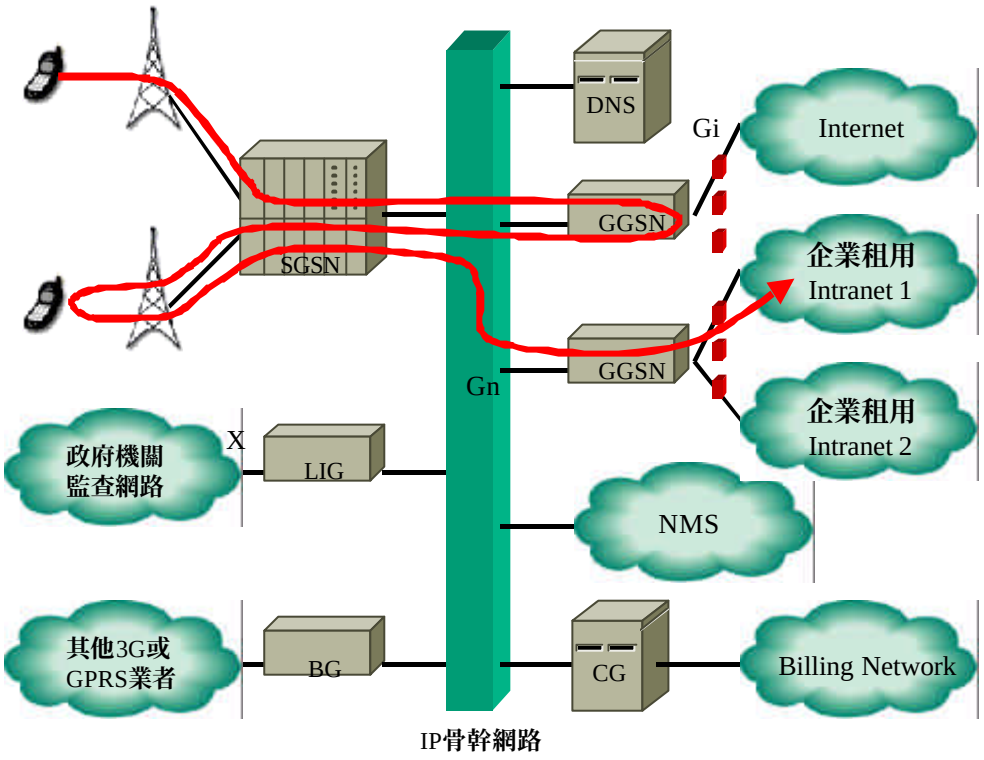

圖7.3.3. 從手機發起攻擊透過另一部手機當跳板來攻擊企業租用戶的網路

如圖7.3.3.所示，從手機發起攻擊透過另一部手機當跳板，而這種情形最有可能是手機或手機後端的筆記型電腦已經被安裝了木馬程式。而由攻擊者的手機在遠端遙控，來攻擊企業租用戶的網路。可能是企業租用戶的網路的內部員工想要得到更高權限的存取使用權，如該企業的董事長、總經理或網管系統者的網路識別身份等。

8. 安全評估的方向

在完成上述的攻擊路徑後，每個GPRS及3G的網路都需要做安全評估以確保網路內的資訊、系統及服務的安全。依據資訊安全評估(Information Security Audit)的方法分析網路安全分析的方式亦可依3個分析方向：機密性(Confidentiality)、可靠性(Availability)及資料完整性(Data Integrity)；檢驗四個部份：認證(Authentication)、資料保密(Confidentiality)、資料完整(Data Integration)、備援或危機應變(Redundancy or Risk Recovery)及存取控制(Access Control)。

機密性意思是指網路內的資訊、系統及服務只提供給有權力使用的人，避免網路內的資訊洩漏。機密性定義為

- 拒？未經授權存取。
- 使用認證授權及依各不同帳號訂定存取權限。
- 使用網路安全機制(Network Security Protocol)建立安全的通訊通道(Channel)。

可靠性意思是指網路內的資訊、系統及服務在使用者需要服務時就可以隨時提供。可靠性定義為

- 備援、備份及容錯。
- 確保存取網路及服務的連續性。

資料完整性定義為

- 完整及未經修改的內容。
- 確保是由信任的來源主機送出。
- 在來源及目的端主機使用認證數位簽章建立訊息鏈路。

9. 安全分析方法學

在完成了一個網路的網路威脅分析後，針對網路各設備易受攻擊的安全威脅處分析(詳細資料參考附件)、組織架構、維運人員帳號管理等一一探討，再依此做詳細的檢查列(check lists)**。範例如下：**

編號	**問題**	**危險程度(Rating)**				
(No.)	**(Question)**	0	1	2	3	4
1	Is the network scanned periodically for vulnerabilities?					
	建議評估測試 **(Suggested audit tests)**	**完成日期及註記** **(Completed date)**				
	1. verify that there is a process in place that details how network vulnerability assessment is to be conducted.					
	2.Confirm that tools used for scanning (eg NAI Cybercop, ISS Internet Scanner) are properly maintained and are capable of detecting the latest known vulnerabilities.					
	3.Check that responsibility for conducting vulnerability assessments has been formally assigned.					
	4.Make sure that the individuals responsible for conducting vulnerability assessment are properly trained in the user of the tools.					
	5.Ascertain if the results of network vulnerability assessments are acted upon (eg request a copy of the most recent assessment and discuss the actions that have been initiated).					
	備註(Comment)	**其他參考頁(WP ref.)**				

再完成所有的檢查項目後，再實際到現場逐項驗證。完成驗證報告後，再依此做建議及改善網路安全。

10. 實習心得與建議

據IDC的統計，到公元2003年將有43%的通訊將在IP網路上進行，這將是通訊產業的重大轉變。無論是在語音、數據或多媒體通訊，資料在網路中如何確保機密性、安全性及資料完整性，將成為各電信公司的重要議題。

就此次至新加坡諾基亞技術支援中心實習，該中心除了做各項電信產品做技術支援服務外，並以Information Security Forum的Information Security Audit Frame Work為基礎，針對GPRS、3G及一般IP網路提供安全評量(Security Audit System)的解決方案。先針對網路做安全風險分析(Security Risk Analysis)，分析組織、維運方法及程序(GAP; Group Algorithm and Procedure)與網路所有元件的安全威脅，列出檢查項目(Check Lists)，依需求建立測試樣本(Test Cases)，最後提出建議報告包含維運存取權限控制、災害應變計畫等(access control, change control, emergency recovery plan)。

上述分析雖然有外面廠商可以幫忙做，接下來是我們需要多安全呢？在大部份的系統安全的代價會是花多少錢、效能、容易使用的程度、複雜性及額外的管理。一個具有成本效益的安全保障建立後，剩下來的風險只是維運管理的問題。而網路的安全風險由於新的攻擊方式、威脅增加或者網路擴展變化等，應該要定期的重新檢驗，才足以確保。

所以就一個大型電信服務公司而言，其內部亦需培育相關人才，決定要花多少錢要多安全，並定時定期與機房維運人員配合，做安全控管工作，如此才能真正確保網路安全。

未來電信市場目前比費率的競爭，創意、服務均不可或缺。網路安全就是電信服務重要的一環。如何提供客戶一個安全穩定的網路平台，使客戶能在網路安心使用，不受駭客侵擾。所以除了新技術的引

入(如：3G網路)之外，現行已存在的網路安全(如：HiNet的IP網路、GPRS網路等以IP為骨幹的網路)，其網路安全均需妥善地考量，所以網路安全的課題也是一個除了提供客戶良好的QoS時，亦應同時並進的目標。

11. 參考資料

[1] “Security: What is it and how much do I need? ”, James W. Meritt, CISSP.

[2] “http://www.ericsson.com.tw/ericsson/technology/t0204.htm” , ERICSSON.

[3] “GPRS Network Elements Threats Analysis (draft) ”, NOKIA.

[4] “Introduction to IP Spoofing”, Victor Velasco, SANS Institute.

[5] “Analysis of a Telnet Session Hijack via Spoofed MAC Addresses and Session Resynchronization”, Ed Norris, SANS Institute.

[6] “Man-in-the-middle Attack- A Brief”, Bhavin Bhansali, SANS Institute.

[7] “Implementing the GPRS IP Backbone”, NOKIA.