Security Analysis of the Evolved Packet Core for LTE Networks

A thesis

submitted in partial fulfilment

of the requirements for the degree

of

Master of Science (MSc)

at

The University of Waikato

by

SIMON WADSWORTH

THE UNIVERSITY OF
WAIKATO
Te Whare Wānanga o Waikato

Abstract

Originally cellular networks handled calls and short messages only. Today, this has been extended to handle packet data services. However now the world is moving towards an entirely IP based mobile service based on LTE and the Evolved Packet Core. Security becomes even more important than before. Cellular networks will be using the same technology that runs the Internet, which could leave them open to a range of threats from the air interface side of the network, especially with the popularity of smart phones and USB "Mobile Broadband" modems. This thesis investigated a range of network protocols used in the Evolved Packet Core, as well as the possibility of attacks against these networks and their protocols and whether such attacks can be achieved, especially from cheap handheld devices. Further this thesis presents results showing that these network protocols are free from serious flaws in their specification.

Acknowledgements

I would like to thank my friends and family who supported me and encouraged me to pursue my masters and who dealt with me when I was stressed and grumpy. I would like to offer thanks to Dr Tony McGregor and Dr Richard Nelson for supervising me, their guidance and support has been invaluable. I must give thanks to all the Lecturers from the Computer Science Department who have lectured me over my time at The University of Waikato, especially Tony, Richard and Dr Mathew Luckie who together taught me more than any other lecturer, and without their knowledge and guidance I would not be where I am today. I also would like to thank Endace Technologies for giving me an internship in the summer before my Thesis, which sparked my interest in this area, and motivated me to investigate it further.

Contents

List of Figures

Chapter 1

Introduction

Early mobile networks used what were essentially dumb terminals, able to make calls and send SMS messages. These devices were simple, and difficult to compromise meaning that security was essentially overlooked in these older networks. This was not only because these devices could not be used for malicious purposes, but also because the networks were owned by a few large telecommunication companies and interconnections were done over secure private networks, which greatly reduced the chance of attack from outside of the network. However as mobile devices developed and the need for mobile data services developed, it became clear that security was going to become an issue. In this modern mobile world, smartphones and even computers via USB modems can be connected to the mobile networks. Not only does this create massive amounts of data to be carried across the networks, it provides platforms that can be used maliciously. For the first time mobile networks were required to connect to public data networks, such as the internet, requiring firewalling and security to protect the mobile core from attack from outside of

the network.

However with these new devices, new threats exist from the radio access network. This thesis focuses on the mobile core of the network, specifically the protocols used, and what attacks may be launched against the core network from the radio access network. A decision was made early on in the investigation, to limit the scope of the thesis to the core of the mobile network and to mostly ignore the radio access network part of the infrastructure. While some consideration of how the radio access network works and how it interfaces with the core is required, overall security concerns regarding the radio access network are mostly un-investigated in this thesis. As a result of this decision, only those protocols which are used within the fixed line core of the network (that is anything that is not the radio access networks, so if a provider is using microwave back links, this is considered as part of the core and for the purposes of this thesis, fixed line), and no testing or further investigation into the radio access network of LTE is undertaken. Investigations into security issues surrounding the radio access networks have previously been undertaken in second and third generation networks with results indicating that security issues are being addressed as the network technologies mature. This is discussed briefly in Section 2.1

The thesis consists of the following sections. Chapter 2, The Background Section discusses the 2G Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), 3G Universal Mobile Telecommunications System (UMTS) and 4G Long Term Evolution (LTE), the 3GPP consortium network technologies used in Mobile Networks and the also an overview

of the physical design of the Mobile Networks. Chapter 3, The Protocol Investigation explains and describes GPRS Tunnelling Protocol (GTP), Mobile IPv6 (MIPv6), Proxy Mobile IPv6 (PMIPv6), Diameter and the IP Multimedia Subsystem (IMS), the protocols that were identified as being important to 3GPP mobile network cores. They were extensively investigated and researched as part of this thesis. Chapter 4 describes a list of network attacks that was developed and that were considered, followed by a description of the lab environment and a description of the methods used to undertake the testing of some of the protocols. Chapter 5 presents the results from the testing and also present some recommendations to provide additional security to the networks against unwanted traffic. Chapter 6 offers discussion of the results and some recommendations on where this work could be expanded and ideas for other areas of investigation.

Chapter 2

Background

2.1 Related Work

Previous investigation has been undertaken regarding the radio access network technology of the mobile networks and considered the security implications. These consider the impact of Mobile Equipment sending large amounts of data to the network in an attempt to use all available bandwidth on a cell, thereby overload the network and denying access to other users. This was also achieved exploiting the scheduling algorithms in mobile networks to hold network channels open, causing resource starvation essentially committing a denial of service attack (Racic, Ma, Chen, & Liu, 2008). There has also been some investigation into potential man in the middle attacks against cellular architecture, showing that it is possible for an intruder to impersonate a GSM/UMTS base station allowing an intruder to eavesdrop on a users traffic(Meyer & Wetzel, 2004). This area is not the focus of the thesis, and is not discussed in detail.

Previous research has been undertaken in the area of vulnerabilities in the General Packet Radio Service (GRPS) backbone (Xenakis & Merakos, 2006), however this research focuses purely on GTP, and GSM networks, ignoring newer 3rd generation, 4th generation networks and the Evolved Packet Core. This is an important area where this thesis varies. This thesis looks specifically at the Evolved Packet Core developed for the 4th Generation LTE networks. It is true that when GSM and GSM EDGE Radio Access Network (GERAN) were developed there was no need to protect the traffic in the core, as these networks were owned by a small number of institutions. With the introduction of GRPS, signalling and user plane traffic started running over publically accessible and open protocols providing an attack vector. However the previous work was undertaken before the new standards were defined and therefore doesn't acknowledge the newer requirements for the network to be a separate secure network. This means that the security concerns raised around running the GRPS network alongside other networks are no longer an issue. The paper further raises issues around roaming, and forwarding traffic between networks, indicating that traffic may be sent in unsecured tunnels. In the Evolved Packet Core, IPSec is used to provide security for users data, ensuring that man in the middle attacks cannot be employed to read the users traffic. However if a network is interconnected via a secure transport network the use of extra security such as IPSec is not always required. Further the research presented in this thesis, especially with the use of Proxy Mobile IPv6 shows that it is easy to protect against signalling attacks, even with spoofed source addresses. The paper also suggests attacks when a GPRS Peering Exchange is used. It is

understood that carriers choose who to peer with and merely use the exchanges as ways to reduce the amount of interconnectivity required, and would in these situations use the IPSec Encapsulated Security Payload method for protecting the signalling and users traffic.

2.2 Mobile Network Technologies

The following section describes several Mobile Technologies that are commonly in use today. It excludes non-3GPP protocols such as CDMA, as Long Term Evolution and the Evolved Packet System were designed by the 3rd Generation Partnership Project. It first presents and describes the early Global System for Mobile Communications service, followed by the General Packet Radio Service additions, before moving into discussing third generation UMTS and High Speed Packet Access, followed finally by Long Term Evolution.

2.2.1 Global System for Mobile Communications

Global System for Mobile Communication (GSM), along with CDMA, were two early second generation mobile technologies. The first call made via GSM was in 1991, and GSM was the dominant technology eventually expanding to be used in most markets worldwide. It originally provided voice and SMS message services only, later providing circuit switched packet data services. GSM was developed and deployed when devices were simple, and did not use advanced features. As a result of this the network was entirely circuit-switched, meaning that two nodes (be it a cell phone, or landline) establish a dedicated channel of communication. This makes sense for phone calls, where voice data

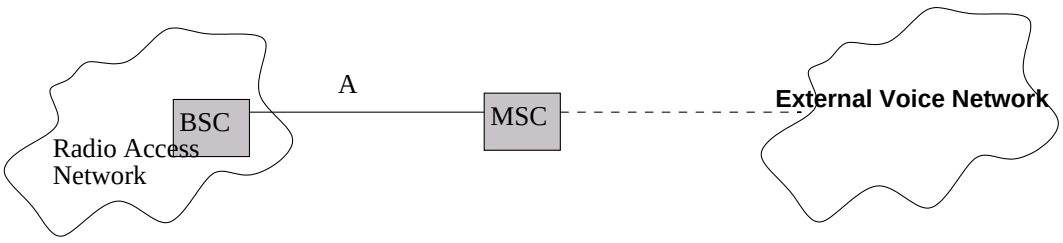

Figure 2.1: High level overview of a GSM network

is constantly flowing in either direction, as using circuit-switched allows for bandwidth to be reserved for the call allowing better quality of service to the customer.

Figure 2.1 shows a GSM network without data. It shows the Base Station Controller (BSC), which connects to many Base Transceiver Stations (BTS) under its control. These devices form the base station subsystem. For the purposes of simplicity the BTS are not shown. The BSC connects to the Mobile Switching Centre (MSC) inside the core, which is responsible for handling and routing calls and SMS messages. The MSC also handles charging and pre-paid account monitoring, as well as dealing with mobility and roaming of the device during a call. Not shown in the diagram is the Home Location register, which is used to hold data about SIM cards and phone numbers.

2.2.2 General Packet Radio Service

Circuit Switched data networks hold connections through the network, open for long periods of time. This is undesirable as while these connections are open, the bandwidth is unavailable to another user even if there is no traffic flowing across the connection. With the evolution of the internet, a need developed for mobile networks to support packet switched data services, where

all communication between two nodes are across a medium that may be shared. The commodity internet is a good example of a packet switched network.

To provide packet switched data services, the 3GPP developed the General Packet Radio Service (GPRS), an extension to 2G circuit switched networks. The first GRPS service being launched in 2000. To support this new service, changes to the mobile core architecture were required, specifically the addition of the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN) as shown in figure 2.2. The SGSN is where the mobile device is first terminated inside the network core for packet data. It is important to note that in this system, calls and messages are still sent via the circuit switched network. The SGSN acts as a kind of router, encapsulating user traffic and tunnelling it through the network to the GGSN. This tunnelling, as discussed in the next section, is what allows data mobility within and data roaming between mobile networks. The GGSN provides access to the packet data networks which the telecommunications provider connects to. In most cases this will be the commodity internet, but could also be a corporate network for example. GPRS supports IP, Point-to-Point Protocol and X.25. GPRS provided always on internet access (this is somewhat variable. Many devices will switch off GPRS while using the GSM service to make a call or send an SMS message).

Original GPRS networks provided downstream speeds up to 60kbit/s, which was later improved to up to 236.9kbit/s with the development of Enhanced data rates for GSM evolution or EDGE.

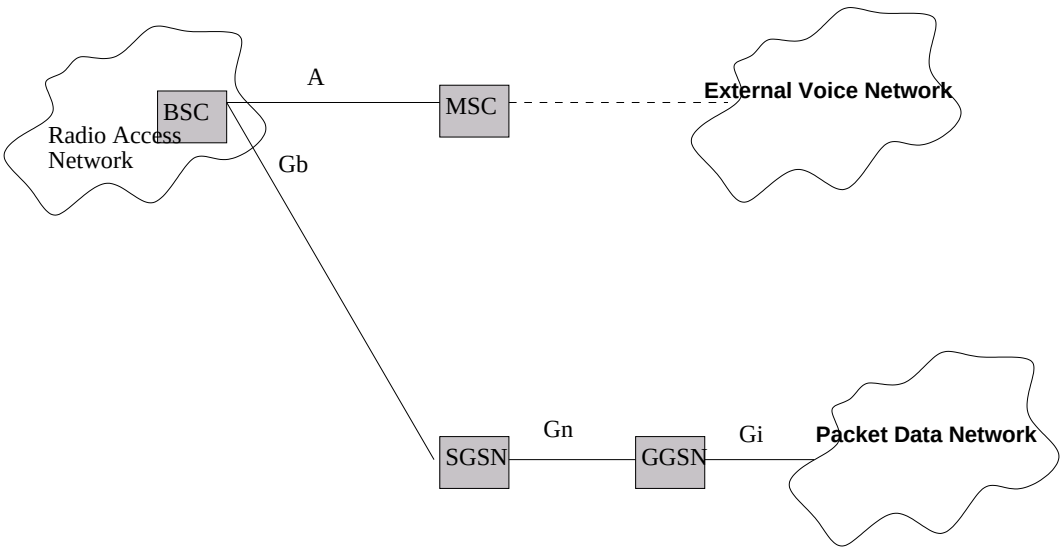

Figure 2.2: High level overview of a GSM network with GPRS additions

2.2.3 Universal Mobile Telecommunications System

As networks evolved the Universal Mobile Telecommunications System (UMTS) was developed. This is the first of 3G cellular technologies, and uses Wideband Code Division Multiple Access as its radio access technology. This provides greater bandwidth to network operators. With this increased bandwidth came the opportunity to provide faster packet data services. As part of the upgrade to UMTS, new cells are needed. These are known as NodeBs and are attached to a Radio Network Controllers (RNC). These RNCs communicate with the SGSN from the GRPS system for handling data as shown in figure 2.3. The RNC also communicates with the MSC in the circuit switched side to handle voice calls and SMS services.

High-Speed Packet Access

A desire to increase speeds on 3rd generation networks lead to the development of the High-Speed Packet Access (HSPA) family of protocols, and further

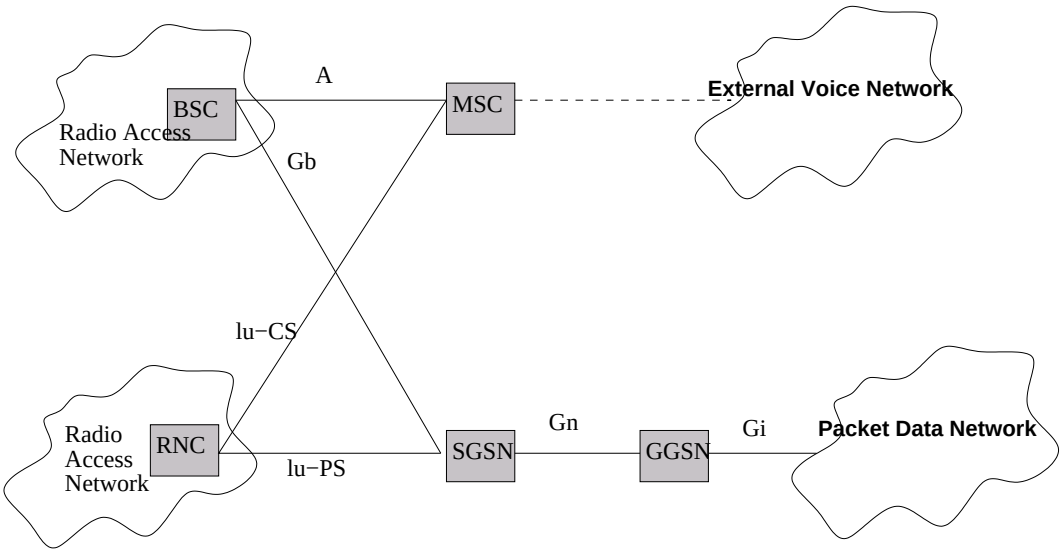

Figure 2.3: High level overview of a GSM and UMTS network

to the Evolved HSPA (HSPA+) family of protocols. High-Speed Downlink Packet Access (HSDPA) is the first step in upgrading the network to HSPA. This improves downlink speeds to 14Mbit/s and much lower latency. Fortunately upgrading the HSPA can be achieved with a software upgrade, requiring little or no investment in hardware upgrades, reducing the cost for providers and allowing them to easily provide better services to their customers. High-Speed Uplink Packet Access (HSUPA) applies similar methods to improve the upstream rate. Some mobile operators (such as Vodafone in New Zealand) throughout the world deploy a system known as Dual-Carrier HSDPA which uses multiple cells to provide more bandwidth and an even faster connection, up to 42Mbit/s.

2.2.4 Long Term Evolution and the Evolved Packet Core

Long Term Evolution (LTE) is the first of the 4G Mobile technologies. Although LTE is commonly referred to as 4G, it is technically 3.75G, not formally

meeting the requirements laid out by the 3GPP to be fully 4th Generation. There requirements include being all IP, and specify items such as data rates and bandwidth among others. The new LTE Advanced standard does meet the requirements to be 4th generation, and to differentiate between LTE and LTE Advanced, LTE Advanced is labelled as True 4G. LTE requires an entirely new Radio Access Network. The new cells are known as eNodeB's as shown in figure 2.4, the e for evolved, and are interconnected together to reduce latency between devices. They can perform handoffs very quickly, reducing the time a mobile node needs to switch towers. These eNodeBs are no longer controlled by a RNC instead all controlled by the Mobility Management Entity.

LTE is designed to be extremely fast, providing speeds of up to 300Mbit/s downstream and 75.4Mbit/s upstream. Depending on the frequency, a mobile node can be moving at up to 350km/h or 500km/h and still maintain an active connection (Motorola, 2007). This is good for areas where high speed trains are in use such as Japan. Further the new Evolved UTRAN cells can support up to 4x the capacity of cells used in the older HSPA system, providing greater bandwidth.

The Evolved Packet Core (EPC) was developed alongside the LTE system. One of the main goals of LTE and the EPC is to be all IP. This means from end to end then architecture uses IP technology. This means that common IP nodes are needed such as routers and firewalls. However specific to EPC are the requirements for the new Serving Gateway (S-GW) and the Packet Data Network Gateway (PDN-GW). The S-GW and PDN-GW replace the SGSN and GGSN respectively. However in many cases both are capable of providing

the older SGSN and GGSN services, allowing backwards compatibility with older networks.

Figure 2.4 shows an WCDMA and GSM network interconnecting with the newer LTE networks. Not all network elements are featured in this figure, of special notice is the Mobility Management Entity (MME). The MME is responsible for all signalling and handling of all User Equipment on the network. This connects to the eNodeB via the S1-MME interface. The figure shows the S4 and Gn interfaces. These interfaces are optional, but are used to allow older networks to connect to the Evolved Packet Core (Olsson et al., 2009). There are two ways of doing this. Either the GGSN can be replaced with the PDN GW which will provide GGSN functionality and have all traffic flow via the SGSN and then to the S-GW over the S4 interface or the SGSN can bypass the S-GW and connect directly to the PDN-GW and forward traffic via this. The method that is used is dependent on the network operator, and different options can make roaming easier. Another option is to leave the GGSNs in place, and have older 2G/3G traffic use the GGSNs, and LTE capable terminals use the newer PDN Gateway.

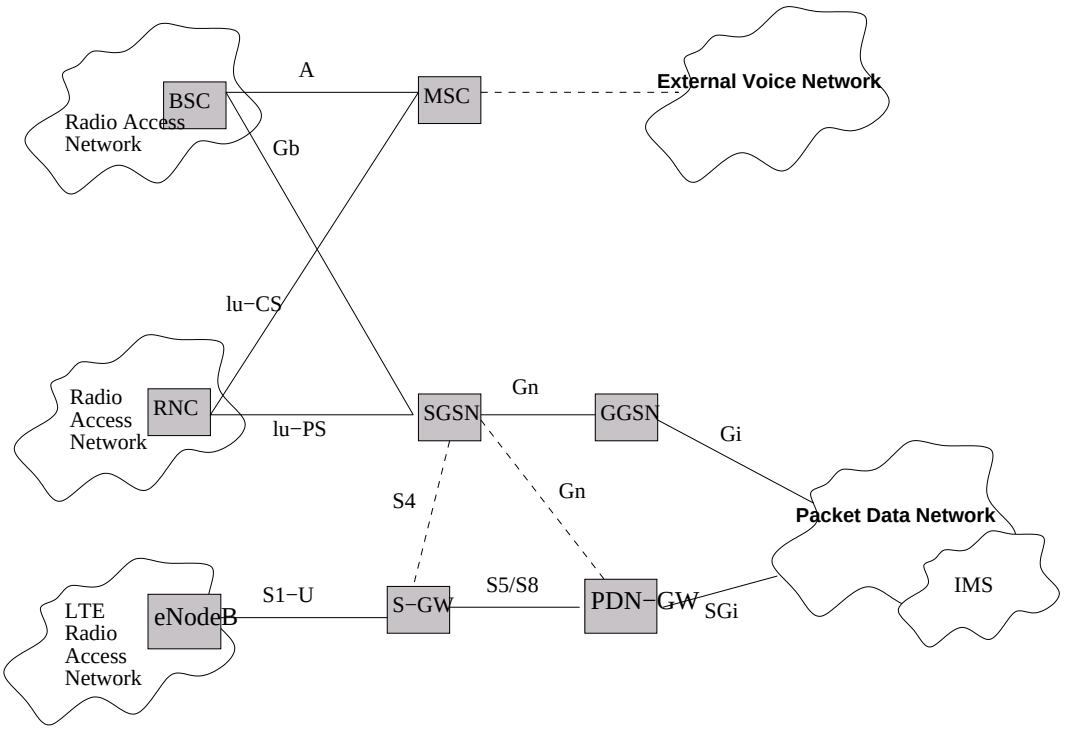

Figure 2.4: High level overview of a WCDMA and GSM network interfacing with LTE

Chapter 3

Protocol Investigation

There are many protocols involved in the Evolved Packet Core, however some of these are of greater importance than others. For example IP has been thoroughly investigated and reported on by others and even as it is the base protocol for the Evolved Packet core, higher level protocols are more important to the functionality of the network. The following sections detail protocols which were determined to be of high importance to the operation of the Evolved Packet core. As a result these protocols were investigated in depth to learn of their functionality and operation. The protocols are the GPRS Tunnelling Protocol, Mobile IPv6, Proxy Mobile IPv6, Diameter and the IP Multimedia Subsystem.

3.1 GPRS Tunnelling Protocol

GPRS Tunnelling Protocol (GTP) is a core protocol and of great importance to the functionality of the Evolved Packet Core. GTP is the mobility protocol between GPRS Support nodes in the mobile core. The GTP protocol defines

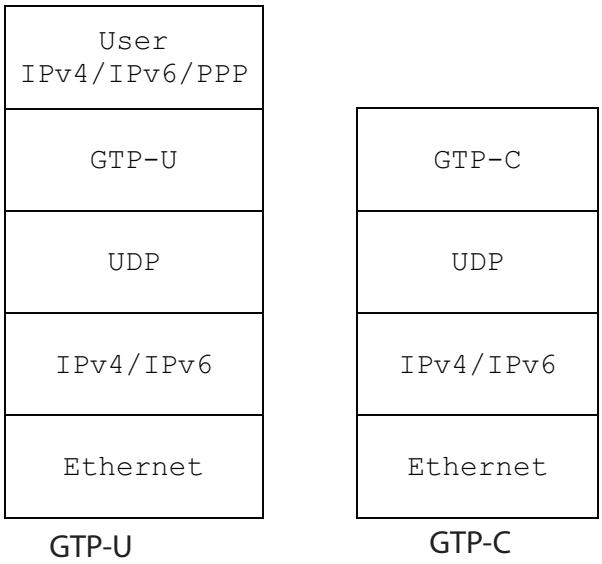

Figure 3.1: GTP-U and GTP-C stack

both a GTP Control and User plane for the Gn interface, which is the interface between Support nodes in the same PLMN, and for the Gp which is the interface between GSNs in different PLMNs. GTP-C is not defined for the lu interface between the SGSN and the Radio Access Network. In this situation the Radio Access Network Application Part protocol handles the control function for the user plane (3GPP, 2012a).

GTP runs over IP for addressing, making use of UDP (required since version 1) at the transport layer, and can transport packets of IPv4, IPv6 or PPP format. Figure 3.1 shows how GTP fits into the stack.

GTP' is a protocol which is used for charging, when the Charging Gateways are located separate from the GSNs.

The ultimate use of GTP is to allow the tunnelling of multiple protocols across the network, being used by SGSNs and GGSNs in the core and BSC and RNCs in the RAN. SGSNs and GGSNs must implement the GTP-C protocol, however no other systems in the network need to be aware of GTP. Mobile

devices connect to the SGSN without needing GTP. This is handled by the network side of the Radio Access Network.

To allow mobility, GTP assumes that there will be a many-to-many relationship between SGSNs and GGSNs. For example a single SGSN may connect to multiple GGSNs to provide access to multiple networks(Olsson et al., 2009). Further a single GGSN may provide access to multiple SSGNs in separate geographic locations (a large mobile network is likely to have multiple SSGNs and GGSNs purely for load balancing purposes).

With the development of LTE and EPC, a new version of GTP-C has been developed. GTPv2 is a new version designed to support new features and network components (3GPP, 2012b). GTP-Uv1 is still used for users traffic between the P-GW and S-GW, and from the S-GW to the eNodeB's. Control Plane traffic between the Evolved Packet Core and the E-UTRAN (eNodeBs) uses S1AP (3GPP, 2013). It is important to note that even if PMIPv6 as described in section 3.3 is used between the P-GW and S-GW, GTP-Uv1 is still used to tunnel traffic between the S-GW and the eNodeB's.

3.2 Mobile IPv6

Mobile IPv6, while isn't necessarily a core protocol for the Evolved Packet Core, its behaviour is important for the understanding of Proxy Mobile IPv6 in section 3.3, and can be used by the Evolved Packet System for mobility, if non 3GPP technologies are being mixed with 3GPP technologies. Mobile IPv6 (MIPv6) allows a mobile node to move between access mediums and networks and maintain active (such as TCP) connections and IP addresses. Maintaining

IP addresses is important as many transport protocols, such as TCP, rely on a tuple to match connections, usually involving the source/destination address. If the address was to change while moving across a network, these connections would be closed and have to be reopened, potentially causing issues for the end user.

This requires the node to implement a MIPv6 stack and handle MIPv6 signalling correctly. MIPv6 makes use of the IPv6 Routing Extension Header. This header was originally designed to allow the source node to specify a list of addresses that the packet must be passed to. There are two types of Routing Headers. Type 0 was the original header, however it could be used for a simple but very effective denial of service attack, and therefore has been deprecated. It is expected that all routers and hosts would ignore this header. Type 2 is designed for use with MIPv6, and contains a single IPv6 address.

When a Mobile Node travels into a foreign network it needs to get a new address belonging to that network. This is known as the care-of-address. Once the mobile node receives this address it must perform a binding update with its home agent which is located inside the home network.

MIPv6 can operate in two modes. There is bi-directional mode and route optimization mode. Bi-directional mode involves a tunnel between the Home Agent and the Mobile Node. This tunnel is established when the Mobile Node sends a binding update. This is essentially an IP-in-IP tunnel as shown in figure 3.2. It works by tunnelling all traffic through the home agent, this has an advantage that the correspondent node (any node in another network on the internet) does not need to know about the care-of-address used by the

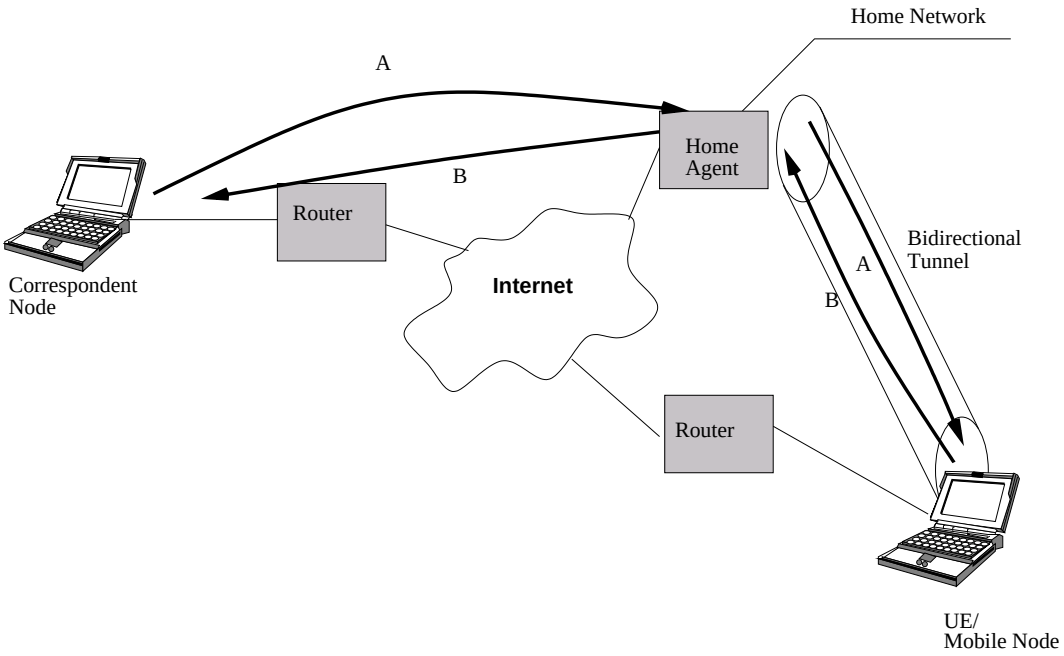

Figure 3.2: MIPv6 Bi-directional Mode

Mobile node. It can simply address the Mobile node with its IPv6 address as it normally would.

Route optimization mode is more complex. It requires the correspondent node to have knowledge of the care-of-address. While this means that traffic can be sent directly between the two nodes, without proper support in the correspondent node, it would have the unfortunate side effect of breaking TCP layer connections if the care-of-address changes, as the correspondent node's TCP stack would have no associated flows, and therefore require a new TCP connection. To resolve this route optimization mode makes use of the IPv6 Routing Header and Destination Options headers. When a mobile node sends a packet to the correspondent node, it includes a Destination options header, which contains its home address. The source address on this packet is the Mobile nodes care-of-address. When a correspondent node wants to communicate with the Mobile node, it attaches a Routing Header with the Mobile nodes

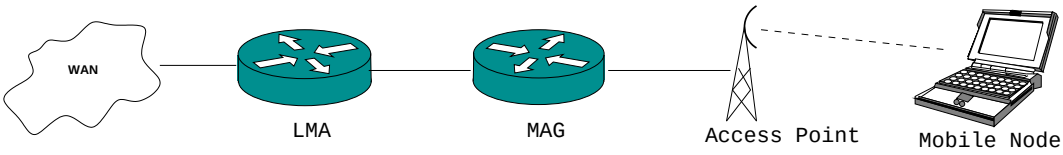

Figure 3.3: Abstract view of a PMIPv6 network

home address in it, and addresses the packet to the care-of-address as normal. When the packet arrives at the Mobile node it substitutes the source address of the packet, for the one stored in the routing extension header.

When using multiple 3GPP and non-3GPP access networks, such as CDMA (a 3GPP2 protocol) and LTE, MIPv6 must be used by the mobile nodes to maintain connectivity when moving between these two networks.

3.3 Proxy Mobile IPv6

Proxy Mobile IPv6 (PMIPv6), an IETF protocol as defined in RFC5213, is a core protocol, interchangeable with GTP between the Serving Gateway and PDN Gateway, developed for mobility in networks. It allows a device to move between access nodes and maintain a constant connection to the network with the same IPv6 address allowing network connections to remain open, however in contrast to Mobile IPv6, the mobile node is unaware this is happening and does not need to implement anything extra, therefore reducing the complexity of a Mobile node.

PMIPv6 introduces a Local Mobility Anchor (LMA) and a Mobility Access Gateway (MAG). These two nodes sit inside the core of the network and handle all of the mobility signalling and control for mobile nodes.

The mobile nodes communicate with access points as they normally would

in a wireless network. These access points are then connected to MAGs. These MAGs must have the same link-local IPv6 address, to hide the fact that the mobile node is moving. Generally a MAG will be associated with one access point. When a packet arrives from the access network, the MAG tunnels it through to the LMA for the network. This is usually an IP-in-IP tunnel. However it is possible to use IPSec tunnels if tunnelling across unsecured networks.

The MAG performs another important role. In MIPv6 the mobile node is required to perform binding updates, however in PMIPv6 this responsibility falls onto the MAG, when a new mobile node completes an attach procedure to the access network, the MAG will perform a Proxy Binding Update to the LMA. The Proxy Binding Update is used to establish a binding between the mobile node's home network prefix and its current proxy care-of address. The format of a Proxy Binding Update is shown in figure 3.4.

There are some changes to the message format when compared to the original Mobile IPv6 message formats. One of these changes is the addition of the P flag, this flag is used to indicate a proxy registration, it is set as zero if the Binding Update is directly from a mobile node as in Mobile IPv6 (Gundavelli et al., 2008). There are also some new options defined. These include the Home Network Prefix Option which is used for exchanging information regarding the mobile node's home network prefix. The Handoff Indicator Option which is used to indicate the method of handoff, for example whether the mobile node was a handoff between MAGs for the same mobile node interface, or whether it was a new attachment. Further there is the Access Technology type option, which specifies the type of access network whether it be Ethernet or Wireless

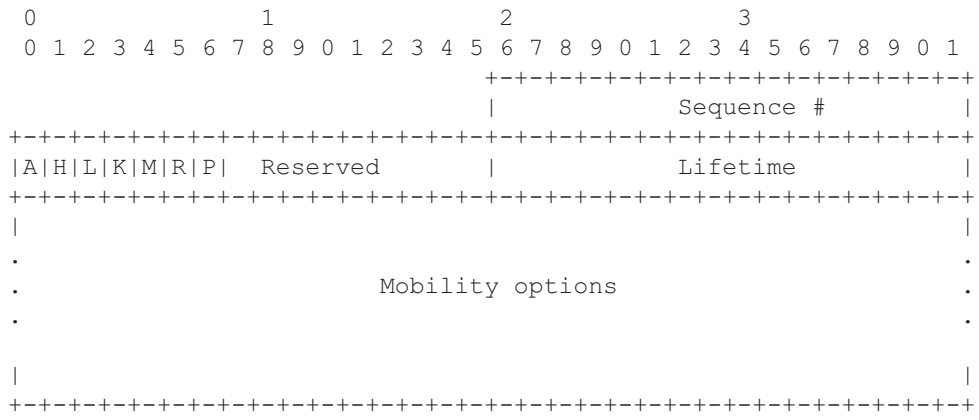

Figure 3.4: Proxy Binding Update Message Format (Gundavelli et al., 2008)

Lan etc. Another new option is the Mobile Node Link-layer Identifier option which is used to exchange information regarding the link-layer identifier which is used to identify the device uniquely. Some access links do not use link-layer addresses in which case this option is unused. Similar to this option is the Link-local address option which is used for exchanging link-local address information of the Mobile Access Gateway. Finally there is the timestamp option, which is used to transport a 64 bit timestamp.

A Proxy Binding Acknowledgement is sent from the LMA to the MAG which is simply a response packet to the Proxy Binding Update message. It is possible in this situation to have the LMA provide the MAG with an address or a prefix that the mobile node should use. The MAG would then advertise this to the mobile node, using something like ICMPv6 Router Advertisements or DHCPv6, after which the mobile node would then configure itself accordingly.

While in a PMIPv6 network, there may be many MAGs, there is typically only one LMA. This LMA is used as the anchor point within the network. All traffic is forwarded through the machine. When traffic is received from the

WAN it is sent through the LMA. The LMA inspects the destination address, and is able to determine which MAG it needs to be tunnelled to. The MAG then sends the packet to the mobile node across the access network. However it is important to note that the MAG may connect to an LMA in another network to provide cross network roaming services.

3.3.1 PMIPv6 in the Evolved Packet Core

The previous section described PMIPv6 in a more abstract sense. It is important to discuss how PMIPv6 fits into the EPS and consider any differences.

EPS is likely to be connected to a 3GPP access network such as LTE or WCDMA. In this case, then eNodeBs in LTE and the NodeBs in WCDMA will send packets to the Serving Gateway. This Serving Gateway acts as the PMIPv6 MAG (Laganier, Higuchi, & Nishida, 2009).

As described in 2.2.2 the Serving Gateway forwards packets through to the Packet Data Network Gateway (P-GW). The P-GW acts as the PMIPv6 LMA. It acts as the anchor in the network which all traffic must pass through.

The Evolved Packet core also makes use of the Generic Routing Encapsulation (GRE) protocol to support the tunnelling of users traffic. GRE is an encapsulation protocol in which the users IP packet is encapsulated in a GRE packet, which is then further encapsulated in another IP packet for delivery. This ensures that to the end user the route that the packet takes appears as one hop. This creates the illusion of virtual point-to-point connections. There is no requirement for the packet being encapsulated in GRE to be IP, however in this situation it will almost certainly be IP.

In this thesis, it is mostly assumed that PMIPv6 is being used to allow roaming between cell towers, rather than roaming between networks. While the latter is supported it is currently not extensively deployed.

3.4 IP Multimedia Subsystem and Multimedia Telephony

One of the aims of the move to LTE and the Evolved Packet Core, was to develop an all-IP system, therefore the networks no longer provide dedicated circuit switched channels. Cellular devices need another method to make voice calls and send SMS messages. Currently there are two methods that can be used. The first is circuit switch fall back (CSFB) which results in the device dropping back to older generations, usually UMTS to make the phone call. Another option, and the ultimate goal is for providers to provide an IP Multimedia Subsystem (IMS) that allows for Voice over LTE calls. These IMS services are based on IP, and are not limited to just voice calls and SMS messages, they can be used to provide a whole range of services such as Push to Talk, however for the purposes of this thesis only Voice over LTE is considered.

Voice calls would now handled by a system known as Voice over LTE (VoLTE), which is essentially an implementation of Voice over IP (or VoIP) a well known and deployed protocol for providing communications over the internet. Many telecommunications providers now offer VoIP services in New Zealand, and it is becoming a viable option for voice calling. [1]. The full system for providing the voice service is known as Multimedia Telephony (MMTel). It

[1] 2talk, Slingshot, Orcon are examples in New Zealand

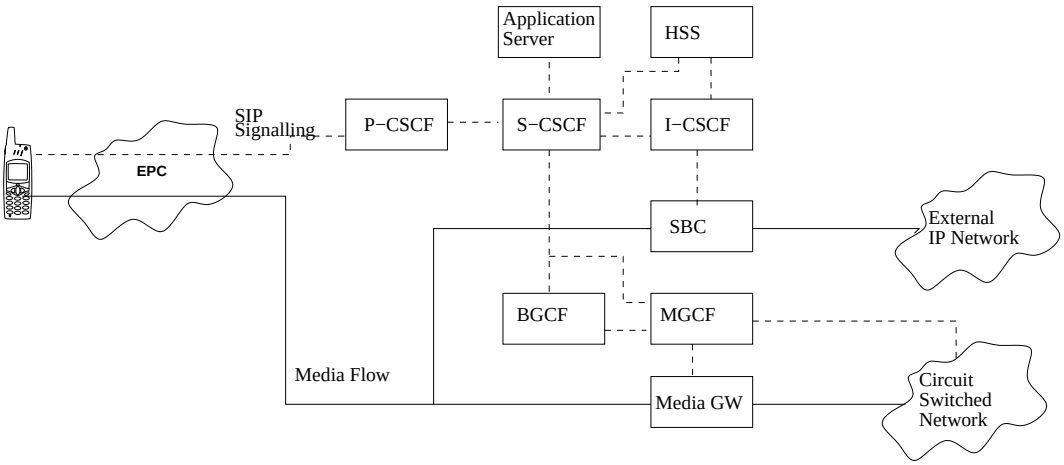

Figure 3.5: Diagram showing IP Multimedia Subsystem Architecture adapted from (Olsson et al., 2009)

allows for full duplex speech, real time video, text communication, file transfer and more. However it is entirely optional for User Equipment to decide what capabilities they support (3GPP, 2011).

The IMS core is complex, to provide voice services, several elements are needed. The first is the IMS Call Session Control Function (CSCF). This device contains the Serving CSCF, is the session control entity and maintains state for all sessions, as well as interfacing with the HSS for subscriber data. The Proxy CSCF is the first point to IMS for devices. It forwards SIP messages from the UE towards the users home Serving CSCF and is also responsible for providing quality of service functions. There is also an interrogating CSCF which is responsible for interfacing SIP requests with other networks, and selecting a Serving CSCF to handle the SIP session.

The Session Border Controller (SBC) is an IP gateway between the IMS domain and an external IP network. This contrasts with the next device which is responsible for interfacing with circuit switched networks. The SBC man-

ages SIP sessions and manages security and quality of service. The Breakout Gateway Control Function (BGCF) is an entity is the system component that selects the network and handles the routing for calls that are towards circuit switched networks. The BGCF usually selects a Media Gateway Control Function (MGCF) especially if this breakout to a circuit switched network is to occur within the same network. The MGCF provides for IMS interconnecting with circuit switched networks. and also controls the actions and behaviour of the Media Gateway. The Media Gateway is responsible for forwarding traffic through to the circuit switched network and transcoding different formats, for example converting IP based voice into circuit switched voice.

A SIP Application Server is used to implement one or more services inside the IMS. MMTel is an example of such a service. Further these services are defined within 3GPP, however there is no requirement for services to be standardized within 3GPP (Olsson et al., 2009).

MMTel allows several extra services, some such services that it can provide are Hold services, call waiting services, conference services etc, which are services that most telecommunications companies currently charge extra for due to the difficult nature of supplying these services. With MMTel being based on SIP a lot of these services are easily supplied allowing mobile carriers to provide a more feature packed service.

3.5 Diameter

Diameter is a core protocol used in the Evolved Packet Core for Authentication, Authorization and Accounting. In the days of Dial Up internet access, a

user would provide their username and password which would be authenticated by the Remote Authentication Dial-In User Service (RADIUS) protocol. The server that was providing this service could therefore be in a more secure location hidden away from the network access systems. Often user information was stored in a Lightweight Directory Access Protocol (LDAP) server. However it is possible for this information to be stored in a text file etc, and RADIUS to access this. This system continued into the use of Broadband Internet access. With the development of IMS it was determined that RADIUS was unable to cope with the new requirements of IMS.

Diameter first and foremost is an Authentication, Authorization and Accounting system. Authentication is the process of authenticating the user and ensuring they are who they say they are, Authorization is the process of ensuring the user is allowed to access the service they are trying to access, and Accounting is used to count the amount of service used, whether this be minutes, or data etc.

Diameter is built from RADIUS. However it is designed differently to allow for easy extension while keeping the protocol generic. Applications that use the Diameter protocol are free to define their own extensions on top of Diameter.

Diameter is designed as a peer-to-peer service, this meaning that a Diameter node may act as a client, server or agent. There are three types of Diameter agents, Relay agent, Proxy agent and Redirect agent. The Relay agent is used to forward messages to an appropriate destination. So it is possible to configure a network access server to use a specific Diameter node, that node could be a Relay agent, which would then forward the requests onto remote Diameter

nodes, perhaps based on Realm (the Diameter node might belong to another company etc). This can greatly reduce the amount of reconfiguration needed if for some reason a Diameter node changes location etc. A Proxy Agent is similar to the Relay agent however it can modify the message content. This may be useful to enforce policy, or perform administration. A Redirect Agent acts as a centralized repository for other Diameter nodes. When it receives a request it will look up its internal routing table, and returns a message that contains the redirection information needed. This is useful as not all Diameter nodes need to keep a copy of this table, they can simply query a Redirect Agent when needed.

Chapter 4

Methodology

4.1 Network Attack List

To look at each protocol and their potential for attack, it was necessary to build a generic lists of attacks and systematically work through it investigating potential for issues. There are lists already out there but many focus on specific attacks (Microsoft, 2012) (Bunter, 2011). The aim here is to develop a more general list but list specific applications to protocols involved in the Evolved Packet Core.

4.1.1 Hijacking

Hijacking is a method of taking over a users session in progress. In the general sense session hijacking is used to refer to the theft of a cookie used to authenticate a user to a remote server/service. The protocols used within the network however, use hijacking in several different ways.

Session Hijacking

For the security of GTP and PMIPv6 it is important that no session hijacking can be carried out. This includes but is not limited to, appearing as another user and sending and receiving traffic as this user, and killing another users session.

VoLTE Hijacking

Many of the issues that surround VoLTE come from that of SIP, the VoIP protocol. VoLTE is essentially a way of running VoIP over an LTE network. This makes use of the IP Multimedia subsystem described earlier.

4.1.2 Spoofing

Address spoofing or identity spoofing is a method of changing or forging a source address in a packet to make the packet appear to come from another location. This can be especially useful, as a packet can appear to come from inside the secure network, and if the correct security measures are not taken then packets may be allowed through into the network that should normally be blocked.

4.1.3 Denial of Service

Cap Exhaustion

While this is not entirely related to the protocols, it is an important security issue. Issues around this relate to whether another user can trick the network

into costing another user money [1]. This could potentially be caused by sending large amounts of unsolicited data to the device.

Further the issue of whether a node could send large amounts of data destined for Mobile nodes on the same cell, and cause the cell to become overloaded and stop providing service. Similar tests have been performed in 2G and 3G networks, attacking to control plane and causing resource starvation and bringing the RNC or BSC inside the network down resulting in mass outages for network users.

4.2 PMIPv6 Testing

To test the behaviour of PMIPv6 and to run security analysis on the protocol, a test network is needed. The preferred network would have been hardware routers with PMIPv6 support, Wireless APs and a Mobile Node. Unfortunately only specific Cisco, Alcatel-Lucent and some LTE manufacturers provide PMIPv6 capability in their hardware, and the only hardware available is Juniper hardware. To compensate for this, a virtualized network was constructed made of KVM virtual machines using Ubuntu 12.04 running a custom compiled Linux kernel with extra Mobile IP and tunnelling features enabled. Instead of using simple KVM networking, the virtual machines are connected to a instance of VDE switch. This decision was made as VDE switch includes support for VLANs. As it was unfeasible to connect the virtual machines to real wireless access points, which require SYSLOG functionality and MAC masquerading, the decision was made to entirely virtualise the mobile side in

[1] by say spending all their prepaid credit

the test network. In this test network there are no access points, the movement between MAGs being controlled by the VDE switch, having the "radio access network" side of the MAGs being on separate VLANS. This means that the Mobile Node can be switched between MAGs without having to reconfigure the MN, which is the important characteristic of PMIPv6.

Linux offers no support for PMIPv6, as a result of this a third party implementation of PMIPv6 was needed. There are several available, but the best at the time is the implementation written by OpenAirInterface (*OpenAirInterface Proxy Mobile IPv6 (OAI PMIPv6) — Open Air Interface*, 2012). It requires a special kernel as mentioned above. One of the advantages of using the OpenAirInterface implementation is that it has been thoroughly tested and shown to work in their test bed network. An implementation of Freeradius is supplied with the OpenAirInterface implementation of PMIPv6, with modifications needed for it to work correctly with their implementation. In a true LTE and EPC network, this would be provided by a Diameter server, not a RADIUS server, but the distinction between the two for the purpose of this testing is negligible.

OpenAirInterface PMIPv6 has multiple different modes. Each LMA and MAG needs to be running PMIPv6 in the correct mode. The LMA runs it in LMA mode, which allows for multiple MAGs to connect to it, and for it to keep track of the location for each Mobile Node. The LMA is also running the Freeradius server. This could be on a separate machine, but for the purpose of this testing is unnecessary. The LMA communicates with the RADIUS server to obtain a prefix and authentication information for the connecting Mobile

Node.

The MAGs are running an instance of PMIPv6 in MAG mode. This allows them to connect to the MAG, but they also listen to SYSLOG messages. OpenAirInterface PMIPv6 is designed to use SYSLOG messages from connected access points to determine when a device is connected to it, however as there are no access points in this network, we are forced to use a python script to send the SYSLOG messages. For the purpose of this we run the python script on the Mobile Node, but this does effect the running of the network, as the machine sending the SYSLOG messages need not be the Mobile Node. There is an important difference here between the test network and a real life LTE network. In an LTE network, there are documented attach procedures that the air network performs when a Mobile node connects to the network. It is in these attach procedures that inform the MAG that a device has connected. Unfortunately it was impossible to test this as it requires an LTE network, and at the time, mid 2012, there were no usable LTE networks in New Zealand.

When the test network is running and VDE switch has the link between the MAGs and Mobile node configured to one of the MAGs, the Mobile Node can send a SYSLOG message. The PMIPv6 implementation running on the MAG receives this message and can authenticate it with the LMA via the RADIUS server running on the LMA. This is achieved via a Proxy Binding Update message which also serves to inform the LMA of the Mobile Nodes location. These LMA responds with a Proxy Binding Acknowledgement and these two machines form a bidirectional IP-in-IP tunnel. All of the mobile node's traffic now flows through this tunnel. For traffic to flow however the

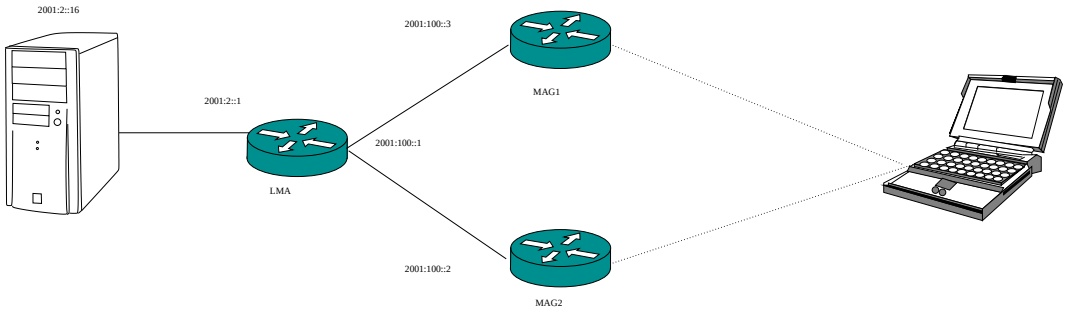

Figure 4.1: The PMIPv6 test network

Mobile Node needs some address information. To facilitate that the modified RADVD daemon that is part of the MAG implementation, sends a ICMPv6 Router Advertisement message to the Mobile Node. This message contains the IPv6 Prefix that the Mobile node should use on the network. Correspondent nodes in the network forward all traffic destined for the Mobile node through to the LMA.

With VDE switch it is possible to change the VLAN that the Mobile Node is on, and this is transparent to the Mobile Node. In an ordinary network with Access Points, this change would be notified to the MAGs by the access point, however in the test network the Python script must be used. This method is now essentially the same as moving between two access points. The MAG that the mobile node is now connected to sends a Proxy Binding Update message to the LMA, and as before a Proxy Binding Acknowledgement is generated from the LMA to the MAG. The LMA deletes the IP-in-IP tunnel that was configured with the previous MAG and sets up a new one with the new LMA, causing all traffic to now flow through the new path. In this test network the prefix 2001:100::/48 is used by the core and /64s are assigned to the Mobile nodes, with 2001:2:: being used by correspondent nodes.

```
a=IP6(src=2001:100:1::a, dst=2001:100::3)/ICMP()
b=IP6(src=2001:100::2, dst=2001:100::1)/a
send(b)
```

Figure 4.2: Scapy commands used to send a packet addressed to another MAG tunnelled inside a packet appearing to be from the MAG the User Equipment is connected to

4.3 Method of performing tests

To test the protocols, especially where packets are able to be sent, several tools are needed. The first tool used is a Python package known as Scapy. Scapy is an extremely power and flexible packet manipulation program and library. Scapy offers the ability to create and decode packets, and send them on the network (BIONDI, 2007). It allows for very low level packet testing, allowing the creation of odd packet combinations and assembling packets in a specific way. This allows for easy testing of potential issues such as sending IPv6 packets with spoofed addresses and other such anomalies. Not only can Scapy send packets it can also match return packets with the source packets. This makes it easy to identify responses to spoofed packets and packets with anomalies.

The other tool used in testing were the simple network tools NMAP, tcpdump and traceroute. The use of traceroute meant that it was possible to see the devices that the packet past through in the path. To allow determination of paths a constant address was tested, to ensure that the path towards the address outside of the mobile network was essentially the same, therefore restricting any variance to the mobile core itself, allowing to determine what addresses were changing. NMAP allowed more thorough testing of addresses

found in the core network, resulting in the determination of whether an address was a core router or another machine. To determine whether these machines were GPRS Support Nodes, the GTP ports were scanned for responses. Finally the use of tcpdump was used on the interface that was connected to a mobile broadband USB modem, allowing viewing of the packets being sent via the modem.

Chapter 5

Results and Recommendations

5.1 GTP Issues

Unfortunately configuring a GTP network in a lab environment was impossible, as a result only some simple testing against a mobile network was undertaken. There are limited to simple traceroutes and address range scans. The aim was to determine if GTP as a protocol would allow packets to be routed to machines inside the core.

Interestingly enough some of the addresses that responded were private addresses. This was determined by running a traceroute command to known servers from a USB modem. Some of these servers included www.waikato.ac.nz and www.google.com. Several addresses were listed in the path including 172.21.38.11, 172.21.38.21 and 172.21.41.11, which are within the 172.16.0.0/16 address block (addresses ranging from 172.16.0.0 to 172.31.255.255). As the address assigned to the User Equipment was a global routable address, it suggests that these core routers are forwarding packets with private addresses into

areas assigned with global addresses. It is recommended that providers using GTP, with private address spaces, ensure that these private address machines do not respond to non private address space (Rekhter, Moskowitz, Karrenberg, de Groot, & Lear, 1996). Further these machines were open to port scanning, soliciting responses from ports including SSH port 22 and Telnet port 23.

5.2 PMIPv6 Issues and Recommendations

Initial investigation of PMIPv6 showed that packets will be routed to any address that a packet is sent to. This includes devices within the core network. One of the requirements for EPC is that the core be a secured private network. With PMIPv6 allowing this functionality in the default state, it breaches this requirement. It was observed that an MAG will send all traffic from a Mobile Node through a tunnel to the LMA, even if this traffic is directly addressed to another core device, it will instead be forwarded through the tunnel. It is important to note that the EPC standards allow for an MAG to route traffic between Mobile Nodes directly, however this functionality does not involve PMIPv6, and uses other mobility protocols between the MAG and the cell towers.

As a result of this observation, it provides a single point where filtering can be implemented. The LMA is the focal point for all traffic being forwarded in and out of the network. It also handles traffic coming in from the WAN. While not a direct line of investigation, the recommendations made in the following provide protection against attacks from the WAN as well. Unfortunately simply blocking all traffic to the prefix used by the core is impractical, but by

using forwarding rules, we can block traffic from outside of the core prefix from being forwarded to addresses inside the core prefix. It is important to note that many networks will provide DNS servers that may be inside this core prefix. Care needs to be taken to allow packets to be sent to these machines. It would be recommended that only packets destined for the DNS port on these machines be allowed through in this situation. By applying firewall rules, in this situation using the prefixes from section 4.2, by blocking all packets destined for 2001:100::/64 unless they are from 2001:100::/64, stops Mobile nodes sending packets to machines in the core. This was tested and observed to work as expected.

Unfortunately the following only works when the Mobile node is using its own prefix. It offers no protection against an address spoofing attack. Through experimentation is was found that packets could be sent to nodes within the core network, simply by faking the source address. By spoofing a source address in the 2001:100::/64 prefix, packets tunnelled through to the LMA appear as if they are being sent from inside the core itself. This is a very serious issue, as it could be possible if an attacker knew the address of a MAG, something that is possible unless precautions discussed in 5.3 are taken, to falsify PMIPv6 control messages. A malicious Mobile node could send a Proxy Binding Update message to the LMA which tells it that another Mobile node has moved to another MAG therefore disrupting service to the other user and hijacking their session. Fortunately due to the way that PMIPv6 works, the new MAG would have no knowledge of the Mobile node, and any traffic destined for that node would simply be discarded. This is because as the MAG

has itself not initiated the Proxy Binding Update, it will not allow a tunnel to be established and will not create routing rules for that node. While this means that users traffic cannot be intercepted from the radio access network, it is important that LMAs and MAGs only accept control messages from each other. For this reason it is important to address the address spoofing problem.

There are two solutions to the spoofed address problem. One can either implement source based routing on the MAG, or implement interface specific firewall rules on both the MAG and the LMA. Experimentation showed that due to the nature of Source Based routing it was an impractical solution and did not work. Packets were still routing with spoofed addresses even with source based routing enabled. Therefore the required action to prevent an attack from spoofed addresses is to enable firewall rules. In the test environment, packets coming in on an interface that were destined for the MAG and also being forwarded that had source addresses belonging to the core network prefix were dropped. This meant that control messages received from the LMA to the MAG were still received as the rule is only being applied to the ingress interface on the MAG (i.e. the interface facing the radio access network). Figure 5.1 shows the iptables firewall rules applied to the MAG, and figure 5.2 shows the firewall rules applied on the LMA.

5.2.1 Routing Header security

Another potential issue is that of the Routing Header in IPv6. While not a direct weakness of PMIPv6, it does have some relation. There are two main types of Routing Header, Type 0 and Type 2. RFC5095 deprecates the type 0

```
Chain INPUT (policy ACCEPT 124 packets, 9848 bytes)
 pkts bytes target  prot opt in   out  source         destination
    2    96 DROP    all      eth1 *    2001:100::/64  ::/0

Chain FORWARD (policy ACCEPT 52 packets, 5408 bytes)
 pkts bytes target  prot opt in   out  source         destination
    0     0 DROP    all      eth1 *   2001:100::/64  ::/0

Chain OUTPUT (policy ACCEPT 147 packets, 11944 bytes)
 pkts bytes target  prot opt in   out  source         destination
```

Figure 5.1: Firewall rules applied to MAG

```
Chain INPUT (policy ACCEPT 127K packets, 11M bytes)
 pkts bytes target  prot opt in   out  source         destination

Chain FORWARD (policy ACCEPT 1034 packets, 104K bytes)
 pkts bytes target  prot opt in   out  source         destination
   12  1248 DROP   all  *  *   ::/0          2001:100::/64

Chain OUTPUT (policy ACCEPT 127K packets, 10M bytes)
 pkts bytes target  prot opt in   out  source         destination
```

Figure 5.2: Firewall rules applied to LMA

routing header (RH0), further it states that IPv6 nodes must not process the packet and should instead treat it as an unrecognised routing type. Further to this IPv6 implementations are no longer required to implement RH0 (Abley, Savola, & Neville-Neil, 2007). Previously RH0 would have allowed a device to specify multiple hops that must be taken in the path. This could theoretically allowed a malicious user to get traffic to nodes within the core network. Unfortunately blocking all routing headers is against RFC5095 and would have implications for the future development of IPv6. As a result networks should filter and block only routing header type 0 (Ferguson & Senie, n.d.) (Baker & Savola, 2004). Mobile IPv6 makes use of type 2 routing headers. These are essentially the same as type 0, however they only allow a single address to be included as is required by the MIPv6 standard (Johnson, Perkins, & Arkko, 2004). As RFC5095 states that firewalls must permit forwarding of Type 2 routing headers, it is impractical to block all of them, especially when using mixed non-3GPP networks as MIPv6 is required. If only 3GPP network types are being used then it is highly recommended to block packets destined for core network devices with these headers. They could potentially be processed by the MIPv6 stack in the core nodes and result in packets being sent to devices otherwise filtered by the network.

5.3 ICMPv6 considerations

ICMPv6 is a version of the Internet Control Message Protocol for IPv6. As with all protocols ICMP is preceded by an IPv6 header and zero or more extension headers. The value used to identify ICMPv6 differs from that of

ICMP for IPv4 (Conta, Deering, & Gupta, 2006). The ICMPv6 packet however maintains the same format as ICMP for IPv4. With the creation of IPv6 several protocol changes were made, one important one was the replacement of the Address Resolution Protocol with Neighbour Discovery Protocol, a protocol that runs on ICMPv6. This is used to discover the physical address of machines on the network. As a result of some of the newer tasks assigned to ICMP, to ensure the security of the Mobile core and connected devices, some ICMPv6 packet filtering may be required.

The following section looks at some of the more important ICMPv6 message types, describing their usage and whether filtering is recommended or required. Filtering some of these packets may result in adverse effects, where this occurs is mentioned.

5.3.1 Type 1 - Destination Unreachable

These packets need to be allowed through the network. These packets are essential for the correct operation of internet protocols. They are used to advise clients that the address/port they are trying to connect to could not be reached. Without these clients would be relying on timeouts, creating unnecessary latency, and is unwanted given one of the core objectives of LTE and EPC is reduced latency.

5.3.2 Type 2 - Packet Too Big

Packet too big messages are required for the correct functionality of Path MTU Discovery. Path MTU Discovery is an algorithm used to determine

the Maximum Transmission Unit of a link, that is the maximum size that a packet can be to a destination without fragmentation. However PMTUD is considered unreliable due to firewalling of ICMP packets (Luckie & Stasiewicz, 2010). Therefore if networks block the forwarding of these packets, then clients may not be able to determine the MTU of the link, and therefore may result in suboptimal performance. This is especially true with the large amount of tunnelling currently in use for IPv6 connectivity. While other methods based on TCP and other protocols may have been developed (Mathis & Heffner, 2007), forwarding this packet provides no adverse affects and it is recommended to allow this packet through.

5.3.3 Type 3 - Time exceeded

In IPv6, the Time Exceeded message is used to indicate when the hop limit has been exceeded. It is probably wise to disable response of these on core routers, but unwise to disable forwarding, as Time exceeded messages will be used for traceroute.

5.3.4 Type 4 - Parameter Problem

The Parameter problem message is used when IPv6 next headers are unknown or there is an unusual header field. This provides no security issues, however it is unlikely to cause too many issues if blocked, although it will result in nodes not being informed that their packet wasn't accepted.

5.3.5 Type 128 - Echo Request and Type 129 - Echo Response

These packets depend entirely on network policy, however it is recommended that the core routers and machines inside the network Echo Responses be disabled. It is unwise to disable forwarding, as there are often used to determine whether a connection is active. While this eliminates one method of scanning, there are many others out there such as TCP SYN scanning, and so alone is not enough to prevent network scans, however this is beyond the scope of this report.

5.3.6 Type 133 - Router Solicitation

These packets need to be received by the MAGs, but they should not be forwarded. The destination addresses of these packets should be the All Routers multicast address, if it is not it is recommended that they are dropped

5.3.7 Type 134 - Router Advertisement

Only the MAGs should send these inside the network. They should never be forwarded and should be dropped if received from a handset, this is because if a MAG received one of these packets, it could potentially start sending all traffic via a users handset.

5.3.8 Type 135 - Neighbor Solicitation

As per the ICMPv6 RFC, this packet should never be forwarded outside of a link, and compliant implementations should not forward these anyway, so no

extra filtering should be required.

5.3.9 Type 137 - Redirect Message

These must be blocked. It is incredibly important and would be disastrous to the security of the network if a node could inform another node that its new first hop should be something else, these could result in a type of Denial of Service attack against Mobile nodes if forwarding is allowed.

Chapter 6

Discussion

The original aim of the thesis was to investigate the network protocols used within the Evolved Packet Core, and see if there were any security flaws in the protocols that could be exploited for gain. However the protocols used in LTE and the Evolved Packet Core have been developed recently, within the last 10 years. As a result of this, security was a major consideration during the design phase of the protocols used in the Evolved Packet Core. This contrasts with original internet protocols such as IP and SMTP, where these protocols had to be adapted as their use increased, and security issues became apparent. For example, when SMTP was originally defined, it was not expected that the system would be abused. As use of the internet grew it was clear that this was not the case and SMTP as a protocol has severe security issues. Due to the ability to easily impersonate an SMTP server, several security features had to be built on top of the original protocol, and not all of these security features may be supported by different servers and clients. The issues that can be caused by not taking the appropriate security considerations in the protocol

design phase (such as incompatibilities with versions implementing different security features), led to increased consideration of security issues during the new protocol design phases. This resulted in many of the security flaws that are evident in older protocols being considered and therefore non-existent in these protocols, therefore greatly reducing the amount of issues that can be discovered in protocols used in fourth generation networks. As part of the original thesis aim was to see if there were any security flaws, with the hope of uncovering a big security flaw, it is disappointing personally to conclude that these are no major security flaws in the protocols. However this result is comforting to protocol designers, service providers and end users as it shows the networks they are designing and using are essentially secure and free from major flaws. This does not mean they can be ignorant of security issues and need to take appropriate steps to deal with issues discussed in this thesis.

One clear conclusion is no matter how well a protocol may be defined, it does not mean that proper firewalling is not required. This firewalling needs careful consideration and needs to be undertaken my someone with some expertise in this area. It is not something that just anyone can correctly and accurately do. Further, there is no one size fits all solution, and firewalling needs to be customized to the individual network environment, especially in regard to IP addresses and IPv6 prefixes in use. This relates to the core as well as prefixes being used by User Equipment. There also needs to be careful consideration of what packets network operators should filter. It would be responsible for network operators to carefully develop rule sets for protocols such as ICMP, that are targeted to specific packet types rather than a protocol

wide ban as is common with ICMP filtering.

This thesis has presented network protocols used within the Evolved Packet Core, as well as investigation into the security of some of the protocols. It presents recommendations for firewall rules and filtering to ensure maximum security of the core network from attacks originating from devices on the radio access network. How this filtering is implemented is up to the network operator, and may be implemented by a firewall or an network intrusion detection system such as Snort. Most of the recommendations need no knowledge of state so could easily be applied in a stateless manor, inspecting individual packets without having to track traffic flows.

6.0.10 Limitations

A possible limitation arising from using an implementation of PMIPv6 inside a virtualized environment is it may not behave exactly as it would inside a production LTE network. This is especially evident in how the network is informed of the devices connectivity. While the control messages between the two nodes using PMIPv6 should be the same, it is impossible to know if the network attach procedure used in LTE would have any effect. Unfortunately, testing was only able to be performed within a restricted lab environment limiting the testing to Linux virtual machines. In an attempt to minimize these problems, the protocol operation itself was inspected, and individual bugs in an implementation of the protocols have been ignored rather than considering these issues to be weaknesses in the protocol. While any specific implementation issues are a problem, these are outside of the scope of this thesis. The issues

discovered are believed to effect any PMIPv6 system correctly implementing the protocol as described in the RFC.

This work only considered PMIPv6 as a IPv6 protocol. While not discussed in this thesis, PMIPv6 is capable of acting in a dual-stacked mode and carrying IPv4 packets for devices that require it. This may present other flaws through the use of IPv4, however this is unlikely as similar firewall rules can be applied, and the operation of PMIP is essentially the same.

6.1 Future Work

One obvious possibility for future work is to apply the investigation to a real life LTE and EPC network. This would allow any issues surrounding differences in a production environment and a lab environment to be determined. Possible security issues could exist where the GTP networks becomes PMIPv6, where GTP is used on the S1-U interface and S5/S8 is used on the S5/S8 interface. It seems unlikely, due to the security considerations taken when developing the new networks, that signalling attacks could be performed against the network. It may be possible to trick a Serving Gateway into believing that the packet sent from the Mobile Node was in fact from a eNodeB, although it would require knowledge of the IP addresses used by the eNodeB, of which there is no easy way to determine.

This thesis did not look at specific bugs in implementations of PMIPv6. An interesting area for further investigation would be to investigate particular implementations of PMIPv6. This could relate to packet fuzzing and other such methods to determine if these implementations have any security holes

related to the way they have been developed. There is potential here to uncover bugs in code that result in unusual behaviour, not expected in a fully compliant bug free implementation.

Another further area of investigation is to run testing of VoLTE on an actual LTE and IMS infrastructure. The lab environment prohibited testing of VoLTE, instead only having access to VoIP environments. This therefore means it was impossible to determine any weaknesses related to using it in the IMS system. While security is in place within the core, it is possible that signalling for VoLTE calls may be delivered over the core, and therefore cause a connected device to think it is getting an incoming call, or for a User Equipment to impersonate another device and make calls as that user.

References

3GPP. (2011). *3gpp ts 22.173: 3gpp ip multimedia core network subsystem (ims) multimedia telephony service and supplementary services; stage 1.* 3GPP, http://www.3gpp.org/ftp/Specs/html-info/29173.htm.

3GPP. (2012a). *3gpp ts 29.060: General packet radio service (gprs); gprs tunnelling protocol (gtp) across the gn and gp interface.* 3GPP, http://www.3gpp.org/ftp/Specs/html-info/29060.htm.

3GPP. (2012b). *3gpp ts 29.274: 3gpp evolved packet system (eps); evolved general packet radio service (gprs) tunnelling protocol for control plane (gtpv2-c); stage 3.* 3GPP, http://www.3gpp.org/ftp/Specs/html-info/29274.htm.

3GPP. (2013). *3gpp ts 36.413: Evolved universal terrestrial radio access network (e-utran); s1 application protocol (s1ap).* 3GPP, http://www.3gpp.org/ftp/Specs/html-info/36413.htm.

Abley, J., Savola, P., & Neville-Neil, G. (2007). *Rfc 5095, deprecation of type 0 routing headers in ipv6.* IETF Network Working Group, http://www.ietf. org/rfc/rfc5095.txt.

Baker, F., & Savola, P. (2004). *Rfc 3704 (best current practice): Ingress filtering for multihomed networks.*

BIONDI, P. (2007). *Network packet manipulation with scapy.*

Bunter, B. (Ed.). (2011, January). *List of wireless network attacks.* Retrieved from `http://www.brighthub.com/computing/smb-security/articles/53949.aspx`

Conta, A., Deering, S., & Gupta, M. (2006). *Rfc 4443: Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6) specification.* IETF Network Working Group, http://www. ietf. org/rfc/rfc4443.txt.

Ferguson, P., & Senie, D. (n.d.). Rfc-2827 network ingress filtering: Defeating denial of service attacks which employ ip source address spoofing, 2000. *See also BCP0038. Obsoletes RFC2267. Status: BEST CURRENT PRACTICE*.

Gundavelli, S., Leung, K., Devarapalli, V., et al. (2008). *Rfc 5213: Proxy mobile ipv6.* IETF Network Working Group, http://www. ietf. org/rfc/rfc5213.txt.

Johnson, D., Perkins, C., & Arkko, J. (2004). Rfc 3775: Mobility support in ipv6. *IETF, June*.

Laganier, J., Higuchi, T., & Nishida, K. (2009). Mobility management for all-ip core network. *NTT DOCOMO Technical Journal*, *11*(3), 34-39.

Luckie, M., & Stasiewicz, B. (2010). Measuring path mtu discovery behaviour. In *Proceedings of the 10th annual conference on internet measurement* (pp. 102–108).

Mathis, M., & Heffner, J. (2007). *Rfc 4821: Packetization layer path mtu discovery.* IETF Network Working Group, http://www. ietf.

org/rfc/rfc4821.txt.

Meyer, U., & Wetzel, S. (2004). A man-in-the-middle attack on umts. In *Proceedings of the 3rd acm workshop on wireless security* (pp. 90–97).

Microsoft. (2012, October). *Common types of network attacks.* Retrieved from `http://technet.microsoft.com/en-us/library/cc959354.aspx`

Motorola, L. (2007). A technical overview. *Technical White Paper*.

Olsson, M., Sultana, S., & Rommer, S. (2009). *Sae and the evolved packet core: Driving the mobile broadband revolution.* Academic Press.

Openairinterface proxy mobile ipv6 (oai pmipv6) — open air interface. (2012, June). Retrieved from `http://www.openairinterface.org/openairinterface-proxy-mobile-ipv6-oai-pmipv6`

Racic, R., Ma, D., Chen, H., & Liu, X. (2008). *Exploiting opportunistic scheduling in cellular data networks.*

Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., & Lear, E. (1996). *Rfv 1918: Address allocation for private internets.* IETF Network Working Group, http://www. ietf. org/rfc/rfc1918.txt.

Xenakis, C., & Merakos, L. (2006). Vulnerabilities and possible attacks against the gprs backbone network. *Critical Information Infrastructures Security*, 262–272.