SECURE TRANSPARENT MOBILITY
Secure Mobility Infrastructure using Mobile IP

Mark W. Andrews, Ronan J. Skehill, Michael Barry, Sean McGrath
University of Limerick, Limerick, Ireland

Keywords: Mobility, Transparent, Mobile IP, Virtual Private Networks, IP Security, Internet Protocol, Internet Key Exchange, Agent.

Abstract: Mobility has become an integral part of modern computing. It increases user flexibility by releasing the potential of fixed data. Reliance on a static computing platform is not sufficient for the future needs of nomadic users. Portable e-mail devices have become popular in recent years due to their simplicity and functionality. These devices give the average user transparent access to their e-mail from any location. Similar transparent access does not exist for general notebook or Personal Digital Assistant (PDA) computing environments. This paper addresses such access, and details a secure mobility architecture from which users can extract greater value. It utilises Mobile IP, IP Security, Internet Key Exchange and Firewalls to provide a comprehensive mobility solution. It evaluates a test-bed in which this secure mobility solution was deployed, and discusses the viability of a secure, transparent architecture which supports mobility.

1 INTRODUCTION

Mobile computing is set to be the new growth driver for overall PC sales worldwide. In 2004 worldwide notebook sales grew 22.1% compared to 10.6% in desktop computer growth (THG, 2005). This rapid increase in demand for mobile hardware has problems associated with data mobility. By its very nature TCP/IP was designed for a fixed network architecture where each computer is assigned a static IP address. If a computer is moved to a different network or subnet (i.e. if it changes location), the computers IP address must be changed to reflect the new location (Redi, 1998).

The 'mobile nature' of computing hardware like notebooks and PDAs does not integrate in a satisfactory manner with the static TCP/IP platform. Accessing information is made more difficult due to the fact that Mobile Nodes may be constantly changing network location.

In 1996 C. Perkins published a protocol called 'Mobile IP' in Request For Comments (RFC) 2002. This laid the foundations for mobility support in IP networks – RFC 2002 has since been updated in RFC 3344. Mobile IP provides a method for transparent connectivity between the 'home network' and Mobile Nodes connected to 'foreign networks'. However, it was never adopted in any significant proportion by the computer industry. Mobile IP's lack of data encryption and Firewall support functionality make it untenable for deployment in most networking environments. Both Firewalls and data encryption are critical for the security of users, their 'home networks' and their transmitted data.

This paper details a secure mobility architecture, in which Mobile IP is adapted to support firewalls, authentication and data encryption. The resulting architecture allows individuals to roam between different foreign networks in a secure, managed fashion. The paper is presented in the following manner; Section 2 describes network security, and the elements of network security which complement the secure mobility model presented later in the paper. Section 3 highlights the Mobile IP protocol, its operation and the effect Mobile IP has on network security. Section 4 details the network topology of the secure mobility model. Section 5 demonstrates the functional aspect of the solution, in terms of the protocol interaction and configuration. Section 6, analyses the solution in terms of its operation and performance. Section 7 concludes the paper by summarising the main points, and the practical application of this secure transparent mobility solution.

W. Andrews M., J. Skehill R., Barry M. and McGrath S. (2005).
SECURE TRANSPARENT MOBILITY - Secure Mobility Infrastructure using Mobile IP.
In *Proceedings of the Second International Conference on e-Business and Telecommunication Networks*, pages 41-48
DOI: 10.5220/0001410300410048

2 NETWORK SECURITY

Data security is a pressing concern of users around the world. CERT recorded 137,529 computer security incident reports in 2003, compared to 1,334 in 1993. Protection of data is of serious importance to users, as the increasing number of threats grows significantly on a yearly basis (CERT, 2004).

The network security elements discussed in this section are necessary for the successful implementation of a secure mobility solution. Computer network security is the process of preventing and detecting unauthorised use of your computer network resources. Prevention measures help to avert unauthorised users from accessing any part of your computer system or network. Detection helps determine whether or not someone attempted to break into a computer network, if they were successful, and what they may have done to compromise that system (Valenita, 2005).

Firewalls, Virtual Private Networks, IP Security and Internet Key Exchange (IKE) are important security protocols and technologies. A brief overview of each is given in the following subsections.

2.1 Firewalls

Firewalls are the principal way a private network is protected from intrusion by external nodes. A Firewall is a system or group of systems that enforces an access control policy between two networks (CERT, 2001). In simple terms, a Firewall is a security device that separates an internal network from and external network. All traffic passing between the two networks must traverse the Firewall by virtue of the network topology. The Firewall enforces security and access control policies and protects the internal network from malicious users. The majority of Firewalls today use stateful inspection, whereby the Firewall tracks the state of each traffic flow and then determines whether a packet or connection should be allowed or dropped. A Firewall monitors traffic from an external host to a host in a Firewall-protected network and conversely, monitors traffic from internal hosts to external ones. Typically, connections initiated from outside hosts to hosts on the internal network are severely restricted (Kopparapu, 2002).

2.2 Virtual Private Networks

A Virtual Private Network (VPN) is a network that is constructed by using a public network infrastructure to connect nodes. VPN's use encryption and other security mechanisms to ensure that only authorised users can access the network, and that the data cannot be intercepted (Webopedia, 2005).

Characteristically VPN's are used to provide an encrypted connection between a user's distributed sites over the Internet. By contrast, a private network uses dedicated circuits (via leased lines or otherwise) and possibly encryption. The encrypted tunnel a VPN provides, is a secure path for network applications to transmit data and requires no changes to those applications.

A VPN generally uses Firewalls, encryption and authentication to keep data and the connection secure. The most common protocols that facilitate a secure VPN connection will now be discussed (Dunigan, 2004).

2.3 IP Security

The Internet Engineering Task Force (IETF) defined IP Security (IPSec). It is a standard that provides a common means of authentication, integrity and IP encryption. It offers two modes of operation, tunnel mode and transport mode.

IPSec packets can be routed and switched on any network that supports IP traffic. No additional support capabilities are required on the carrier network. One of the benefits of this protocol is that it is transparent to the application layer. Therefore, it can be used in conjunction with existing application layer security software. In addition, VPN solutions using IPSec as the basis for a common protocol can interoperate, opening up new possibilities for securely sharing data (Atkinson, 1995).

IPSec uses two principal elements to protect network communications:

- Authentication Header (AH), this provides source authentication and data integrity. This ensures the data cannot be altered without the recipient's knowledge and verifies the identity of the sending node.
- Encapsulated Security Payload (ESP), this provides confidentiality, ensuring that data will not be intercepted, read or copied. This security is provided through encryption.

2.3.1 IPSec Authentication Header

In Authentication Header (AH) transport mode, an AH header is inserted between the IP header and the

payload. This provides the Security Parameter Index (SPI), sequence number and other authentication data required (RFC1826).

2.3.2 IPSec Encapsulated Security Payload

In IPSec Encapsulated Security Payload (ESP) transport mode, an ESP header is inserted between the IP header and IP payload. An ESP trailer and authentication MAC are added to the end of the packet. In tunnel mode ESP, the entire packet is encrypted and appended to a new ESP header and IP header, with an authentication trailer added (Intel Networking, 1999).

2.4 Internet Key Exchange

Internet Key Exchange (IKE) is defined as an IPSec (IP Security) standard protocol used to ensure security for Virtual Private Network (VPN) negotiation. IKE defines an automatic means of negotiation and authentication for IPSec SAs (Security Associations). Security Associations are security policies defined for communication between two or more entities (Harkins, 1998). A key represents the relationship between the entities. IKE in essence, enables the establishment of a symmetric key between two entities using a cryptographically secure key exchange mechanism. This exchange is called *Diffie Hellman,* and a key is established in the following manner:

1. Alice and Bob select a prime number p and calculate p's generator g. These two calculated values are public
2. Alice chooses a large private number, such that $x < p$ and transmits Bob the remainder x from the equation:

$$x = g^x \bmod p$$

3. Similarly Bob chooses a large private number, such that $y < p$ and transmits Alice the remainder y from the equation:

$$y = g^y \bmod p$$

4. Alice calculates the remainder:

$$s = y^x \bmod p$$

5. Bob calculates the remainder:

$$s` = x^y \bmod p$$

6. The remainders s and s` are equal because:

$$s = s` = g^{xy} \bmod p$$

7. Thus Alice and Bob now share a symmetric key s, which can be used for fast encryption by both parties.
8. It is not possible to obtain the value s from the two public keys passed over the Internet, since the final value s also depends on the two private values, which remain secret (Diffe Hellman, 2004).

IKE also grants the ability to change encryption keys during an IP Security session. This is useful in situations where the lifetime of the key should be changed frequently for security purposes.

2.5 General Comment

The security components discussed are necessary in order to provide confidentiality, integrity, authorisation and non-repudiation for the secure mobility architecture. The final component, Mobile IP, enables the transparent network connectivity between mobile nodes and the 'home network'. Mobile IP, while not a viable solution by itself, can be used in conjunction with other protocols such as those already discussed, to provide a secure cryptosystem that completes the overall architecture.

3 MOBILE IP

The fundamental need for Mobile IP arises when a node connected to the Internet changes its point of attachment (Redi, 1998). This means, when a mobile node moves from its home network to a foreign network, such as a public wireless hotspot, there will be transparent network connectivity to the home network from the new location.

TCP/IP was not designed to support this type of connectivity. However, with the use of Mobile IP, the mobile node can configure itself with the aid of devices called 'agents' for such connectivity. This process is transparent to users, allowing them to maintain contact with the 'home network' at all times by any network media.

Each agent device in Mobile IP carries out a specific function. The 'Home Agent' resides on the users 'home network'. This device acts as a packet forwarder. If the Mobile Node is attached to a 'foreign network', any packets destined for the Mobile Node will be intercepted by the Home Agent using proxy ARP (Address Resolution Protocol), and forwarded using IP-in-IP encapsulation to the 'foreign network' using the mobile nodes Care-Of Address (Perkins, 2002). Hence, the Home Agent acts as the Mobile Nodes point of attachment to the Internet when it is located on a 'foreign network'. Once the tunnelled packet reaches the 'foreign network', a Foreign Agent decapsulates the data and forwards it to the Mobile Node residing on its network. Figure 2, illustrates the triangular route the Mobile IP protocol typically uses between the

mobility nodes, Home Agent, Mobile Node and Corresponding Node.

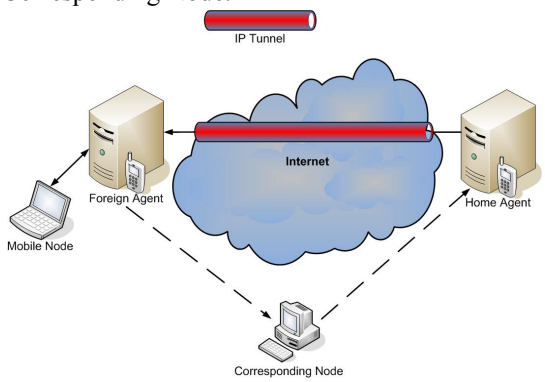

Figure 1: Mobile IP Triangular Routing

3.1 Mobile IP and Network Security

3.1.1 Mobile IP & Firewalls

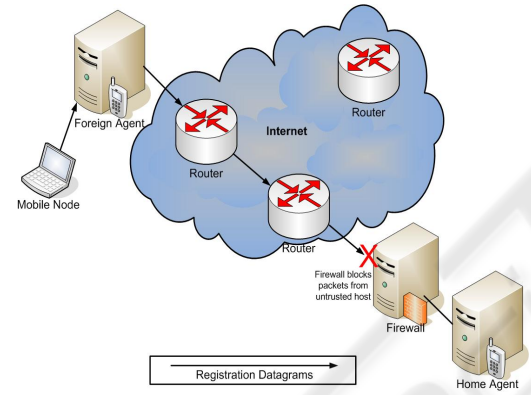

Figure 2: Firewall Blocking Mobile IP Registration Process

Mobile IP does not interoperate with Firewalls.Typically, a Firewall severely restricts the type of connections initiated from outside hosts to hosts on the internal network. This restriction prevents a Mobile Node running Mobile IP to register with the Home Agent, Figure 3 illustrates this.

The Foreign Agent will be seen as an unauthorised host on the Internet, and thus will be considered untrustworthy. The registration datagrams cannot negotiate with the Home Agent, which sits on the 'home network' and the mobile process cannot be initiated.

3.1.2 Mobile IP & Data Security

Data protection has become a high growth market in the computer systems environment (IT Facts, 2003). Unprotected data routed around the Internet is no longer considered safe practice, especially when that data is of a sensitive nature. Vanilla Mobile IP transmits data between nodes in plaintext, thus the data can be intercepted when being routed around the Internet. This data can then be easily deciphered and used against the sender and receiver. These issues make vanilla Mobile IP an unviable protocol, due to its inadequate data payload security protection.

3.1.3 Solution

The solution is to use the transparent mobility functionality of the Mobile IP protocol, coupled with the authorisation and encryption protocols IKE and IPSec. In addition, the Firewall must complement the overall solution to fulfil the security requirements. Minor alterations can be made which will support the mobility aspect of the solution, while limiting the security impact on the private network. The network design element will now be discussed.

4 MOBILITY NETWORK TOPOLOGY DESIGN

The most secure network topology for secure mobility is for the agent device to be integrated with the Firewall. This ensures that an optimal security policy can be enforced at the boundary between the public and private networks. The Firewall is the best security device for maintaining perimeter security. It would be unsafe to place the Home Agent outside the protection of the Firewall and into the De-Militarised Zone (DMZ). A knowledgeable attacker would compromise the Home Agent and gain access to the home network via this path, thus bypassing the Firewall.

Figure 3, illustrates the proposed secure configuration arrangement for the secure Mobile IP implementation.

4.1 Firewall Design

The Home Agent functionality will be incorporated within the Firewall design. The overall security policy can be implemented in a more integrated manner when one security perimeter device

monitors and controls access and security levels between the private network and the Internet.

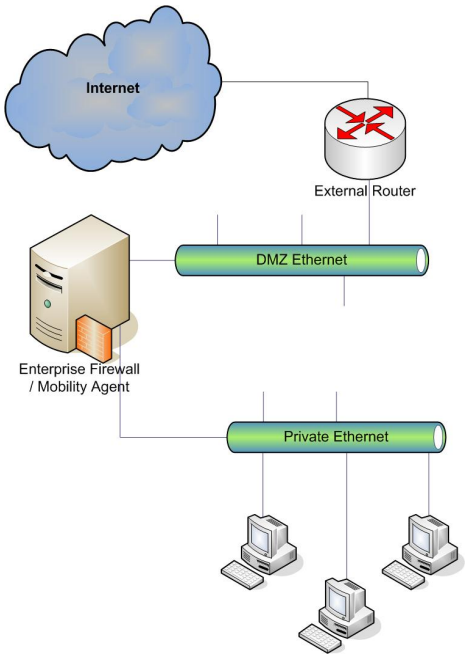

Figure 3: Proposed Home Network Device Architecture

The design of the Firewall must not impact on the level of security it is designed to provide. It must not interfere with the operation of the Mobile IP protocol; it must work in conjunction with it to provide the best functionality.

Reverse tunnelling is a prerequisite for security purposes (Montenegro, 2001). Tunnelling back to the Firewall gives guaranteed secure flow of data in both directions. Thus the Firewall can enforce a strict data flow policy, thereby protecting the 'home network'.

5 SECURE MOBILITY MODEL

The Firewall stands as the primary defence for the security of the 'home network'. However, it is also critical that the Mobile Node maintain a high level of security, otherwise this could become the conduit through which an attack is mounted against the 'home network'. A software based stateful inspection Firewall will be installed on the Mobile Node. This adds the final layer of security into the integrated network architecture.

5.1 Test-bed

Utilising the various technologies described, comprising of: Mobile IP, IP Security, IKE and Firewalls, a working model of these components was implemented in a test-bed. The test-bed provided an environment in which the solution could be analysed. It also provided a data analysis platform from which real network performance statistics were obtained.

The test-bed consisted of a Home Agent/Firewall, Foreign Agent, Corresponding Node, Mobile Node and a Router. The Linux Open Source environment was used as the Operating System platform due to the availability of source code. The protocols were adapted slightly, without alteration of their design parameters, to work in conjunction with each other. In addition, the Linux IPtables Firewall was adjusted to authenticate Mobile IP datagrams. Details of the protocol interaction will now be highlighted.

5.2 Protocol Interaction

The Message Sequence Chart (MSC) in figure 5, illustrates the protocol interaction process. Firstly, the Mobile node sends a Registration Request in response to an Agent Advertisement, or as a result of an Agent Solicitation. The Foreign Agent forwards the Registration Request to the Firewall/Home Agent. Once the Firewall detects a UDP transmission to port 434 (the port Mobile IP uses for registration), it allows that packet to negotiate with the Firewall/Home Agent. If the request is accepted (through authentication HMAC Message Digest 5 (MD5)) the Firewall/Home Agent sends a Registration Reply, which the Firewall policy allows. A reverse tunnel is then permitted between the Care-of Address and the Firewall/Home Agent. The Firewall restricts traffic in this reverse tunnel. It only permits UDP traffic (from OpenVPN) to port 5000. Further, OpenVPN only allows this traffic passage to the private network once the data flow has been further authenticated and authorised. This provides security against individuals inserting unauthorised data into the reverse tunnel payload, outside the VPN tunnel. Even if this data does enter the tunnel, the Firewall will immediately disregard without inspection. Once a location update is received (i.e. a new Registration Request) the Firewall closes access to the previous Care-of Address – thus enforcing the security of the system.

The reverse tunnel acts as the primary data conduit between the Firewall/Home Agent and the Foreign Agent. Within this tunnel the VPN is established.

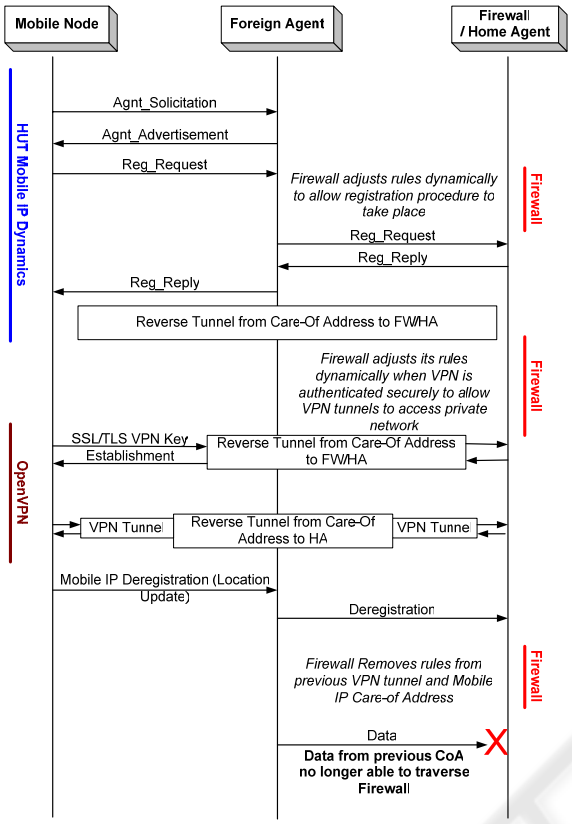

Figure 5: Protocol Interaction Message Sequence Chart

The VPN extends from the Firewall/Home Agent, through the Foreign Agent and terminates at the Mobile Node. This prevents nodes on the 'foreign network' from being able to decipher data transmitted between the Mobile Node and the 'home network'. The VPN utilises the technologies IKE and IPSec to function as a secure extension of the 'home network'. IKE and IPSec provide:

- Authentication – The sending entity is verified as the actual sending entity.
- Integrity – Data cannot be intercepted and changed without the receiving entity detecting the change.
- Confidentiality – The data transmitted cannot be deciphered if it is intercepted. This is achieved through the cryptographic process of IPSec.
- Non-repudiation – The sending node cannot deny sending a transmission, when in fact it did send that transmission. This is useful in scenarios where auditing is necessary, for example, in legal or financial transactions.

When all the technologies are coupled together, an overall picture of how each of the components interacts is established; figure 6, illustrates this in schematic form.

The net result is a cryptographically secure, transparent, network connectivity solution from the Mobile Node to hosts on the 'home network'.

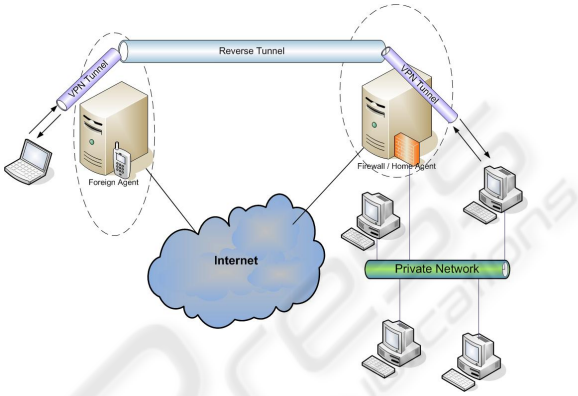

Figure 6: Solution Schematic

6 ANALYSIS

When moving the Mobile Node between the 'home network' and the 'foreign network' the protocol interaction configures the Mobile Node transparently. The net result is a Mobile Node that has connectivity to the 'home network' without user alteration of any protocol, or configuration of any network parameters. In addition, if TCP sessions were established, when the node moves between networks, that nodes TCP sessions would be re-established without loss of the session. In situations where a Database Management System, for example, had a TCP connection to the Mobile Node for update purposes, this feature of the Mobile IP protocol maintains the connection without the need to reinitialise it. This is one of the benefits of Mobile IP. Even though the IP address changes, the Mobile Node is always reachable, and it is able to maintain its session connectivity.

6.1 Connection Oriented & Connectionless Tests

The test-bed was used to evaluate the transparent mobility functionality Mobile IP provides. This was achieved through testing connectionless and connection-oriented network traffic with the

solution. A more detailed network analysis is undertaken in subsection 6.2.

Firstly, connectionless network traffic was evaluated via media streaming. A media stream was initiated and the Mobile Node was transitioned between different networks. While the data throughput was not as high as general network routing, or vanilla Mobile IP; the test effectively demonstrated that UDP streaming traffic works with the secure solution.

TCP (connection-oriented) session traffic was demonstrated using Secure Copy (SCP). Large files were transmitted between a host on the 'home network' and the Mobile Node. When the mobile node migrated to the foreign network the SCP file transfer session was re-established after a short delay.

In summation, both reliable and unreliable network traffic effectively worked with the secure mobility solution. This was critical, since the transparent aspect of Mobile IP grants users seamless connectivity to static 'home network' resources without configuration. It was important that the enhanced security and functionality did not affect Mobile IP's capabilities. Following the successful testing of TCP and UDP traffic, network performance statistics were evaluated.

6.2 Network Performance

Network latency was tested between the Mobile Node and a host on the 'home network'. This test was carried out with normal routing, using vanilla Mobile IP and with the new secure mobility solution. The results are illustrated in Figure 7. The secure mobility solution did introduce a small amount of lag in comparison to vanilla Mobile IP. This indicates that the cryptosystem does not introduce a network latency that would be undesirable for real-time applications. In addition, the media streaming test worked effectively and there was no noticeable delay incurred.

Network throughput was calculated by transferring various file sizes and data types across the network. An aggregate throughput was calculated over all the tests. This gives the average performance level for general network traffic, and is a more realistic estimation of actual network performance, than a specific data transfer test. Figure 8 illustrates the network throughput results obtained from the test-bed.

When analysing the test-bed performance it is clear that the increased authentication and cryptography overhead impacts the maximum transfer rate of the secure Mobile IP system. While the bandwidth of Secure Mobile IP is not as fast as standard network transfer rates, it is more than sufficient for most applications. Ultimately, the enhanced security of the solution was more critical than its performance. The result is a transparent secure mobility solution, which offers real benefits to the end user.

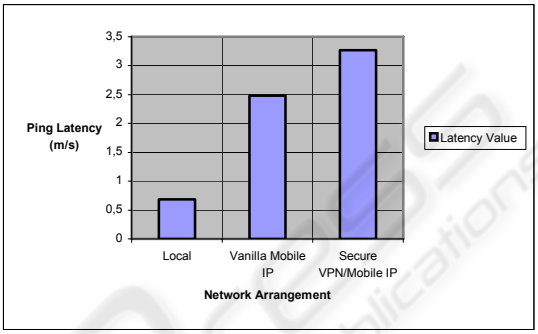

Figure 7: Network Latency

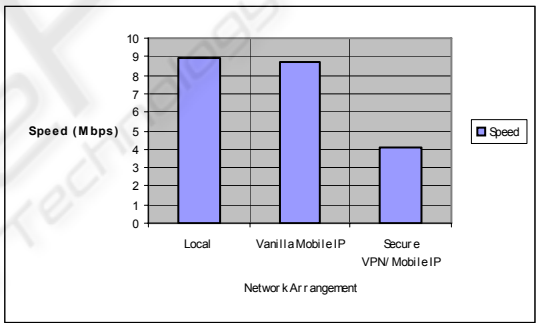

Figure 8: Network Throughput

7 CONCLUSION

The applicability of the secure Mobile IP solution spans across all areas of mobile computing. Connectivity to Mobile Nodes throughout the Internet despite the continuous change of IP address brings an element of convergence to mobility hardware and static computing platforms. The secure element of this solution also brings a feasible solution to businesses and individuals alike. It provides transparent connectivity in a secure manner.

Technology that provides security, functionality and ease of use, can be adopted by the mass market. The result is a solution that is user-friendly because the users do not have to configure it, and secure, so

those users can rest assured that their data is safe from competitors or eavesdroppers. These critical elements have been addressed with the secure mobility model presented.

The result of this research, is a solution which is based on established standards. Figure 9, illustrates (in a basic manner) the relationship each component has with each other.

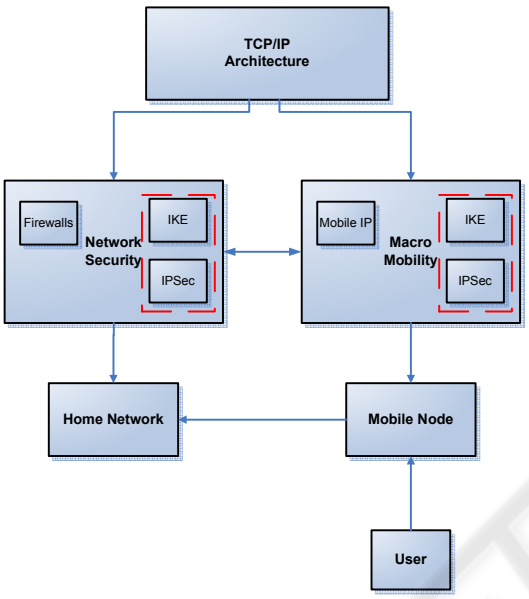

Figure 9: Solution Component Relationships

Further research will be conducted by enhancing the performance of this solution by utilising VPN accelerators. This technology should increase the throughput of the cryptographic process by removing some of the encryption and decryption processes from Mobile Nodes, and Firewall/Home Agents CPU. In addition, Mobile IP can be adapted to simply use a single VPN tunnel, as opposed to an unsecured bi-directional tunnel which encapsulates a VPN tunnel. This will also have a positive effect on the performance of the solution by decreasing the encapsulation overhead.

The aim of this research is to evaluate a secure mobility technology that is useful to the consumer, and can enhance productivity while providing a safe environment in which they can conduct their business.

REFERENCES

Atkinson, R., 1995. RFC 1825. *IP Security (IPSec).*

Atkinson, R., 1995. RFC 1826. *IP Authentication Header*

CERT, 2005. *CERT Coordination Centre Statistics 1988-2004.* http://www.cert.org/stats/cert_stats.html

CERT, 2001. *CERT Coordination Centre Home Network Security.* http://www.cert.org/tech_tips/home_networks.html#I-A

Chandra Kopparapu, 2002. *Load Balancing Servers, Firewalls and Caches. WILEY.*

Group 1 Internet, 2004. *Firewall Technologies.* http://www.group1ifw.com/fw_tech.html

Harkins. D & Carrel. D, 1998. RFC2409. *The Internet Key Exchange (IKE).*

Intel Networking, *White Paper IP Security,* 1999. http://www.intel.com/network/connectivity/resources/doc_library/white_papers/products/ipsecurity/

ITFacts.biz, 2003. *Network Security Applicances Sales Surge.* http://www.itfacts.biz/index.php?id=P476

Montenegro, G., 2001. RFC3024. *Reverse Tunneling for Mobile IP.*

Perkins, C., 2002. RFC3344. *IP Mobility Support for Ipv4.*

Redi, J. & Bahl, P. 1998. *Mobile IP: A solution for transparent, seamless mobile computer communications.*

RocSearch, 2004-2005, *Worldwide Market Potential and Acceptability*, RocSearch.

RSA Laboratories, 2004. *Diffe Hellman.* http://www.rsasecurity.com/rsalabs/faq/3-6-1.html

Toms Hardware Guide. February 2005. *Notebook shipments at all time high.* http://news.com.com/Notebooks+continue+shipment+gains/2100-1044_3-5070313.html

Tom Dunigan, 2004. *Virtual Private Networks.* http://www.csm.ornl.gov/~dunigan/vpn.html

Valentia Community College, 2005. *Network Security,* http://valencia.cc.fl.us/oit/network_security.cfm

Webopedia, 2005. *VPN Definition.* http://www.webopedia.com/TERM/V/VPN.html