Access of Mobile IP Users to Firewall Protected VPNs

Marc Danzeisen and Torsten Braun
Institut für Informatik und Angewandte Mathematik, Universität Bern
Neubrückstrasse 10, CH-3012 Bern
Email: [danzeisen|braun]@iam.unibe.ch

Abstract: *The paper describes an architecture allowing Mobile IP hosts to access to a virtual private network that is protected by a firewall from the public Internet. The implementation based on adaptation of standard protocols (IPSec and Mobile IP) and initial performance results are discussed.*

Keywords: *Mobile IP, IP Security, Virtual Private Networks, Firewall Traversal*

1. Introduction

In general, mobile communication has a strong need for security. A particular problem when using Mobile IP is the firewall traversal problem. In this case, a campus network or a virtual private network (VPN) of an organization such as a university or a company is protected by a firewall from the global Internet. Only authorized users shall get access to that private network.

This paper describes a solution called SecMIP (Secure Mobile IP) to provide mobile IP users secure access to their company's firewall protected virtual private network. While other approaches [2] [3] [4] [7] [8] [9] require either the introduction of new protocols or special nodes within the network, our approach requires a slight adaptation of the end systems communication software in order to adapt Mobile IP and IP Security protocols to each other. It does neither require to introduce new protocols nor does it require to insert or modify network components.

2. Secure Mobile IP

Similar as proposed in [4] a screened-subnet firewall architecture has been chosen. The organization's interior network is isolated from the Internet by a de-militarized zone (DMZ). The firewall between the DMZ and the private interior network is the only entry point to the organization's private network. All Mobile IP devices are outside of the private network (except the home agent), i.e. within the DMZ, and receive their IP addresses from a DHCP server.

Since the mobile nodes that belong to the corporation have to traverse the firewall to access the VPN, they have to authenticate themselves to the firewall. This authentication is realized with IPSec. SecMIP uses an IPSec tunnel to protect the Mobile IP tunnel passing the insecure parts of the Internet (cf. Figure 1). Within the private network, however, the Mobile IP tunnel is sufficient. ISAKMP/Oakley [1] has been chosen for key exchange. Mobile IP is used only in the mobile node de-capsulation mode without using foreign agents as packet relays.

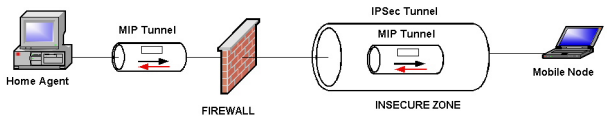

Figure 1 : SecMIP Tunneling

After entering a new network area, a mobile node has to be connected via a wireless access point. Foreign agent advertisements are broadcasted regularly into this demilitarized network (Figure 2). By receiving such an ICMP message, a mobile node learns that it just has entered a new network.

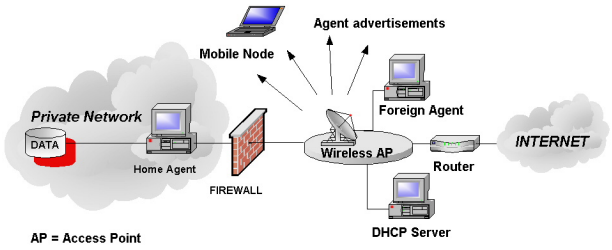

Figure 2 : Network Detection

Then, the mobile node disables the old IPSec tunnel, which was been established from an older location using an old collocated care-of address. The mobile node then needs to acquire a new collocated care-of-address through a DHCP server or from a foreign agent (Figure

3). Retrieving care-of-addresses from DHCP servers avoids the existence of foreign agents like in IPv6. In that case, other mechanisms for network detection have to be deployed.

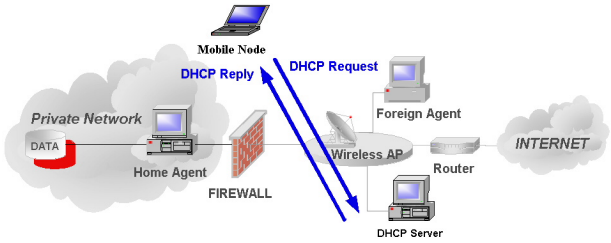

Figure 3 : DHCP

In order to secure data transfer, an IPSec tunnel will then be established between the mobile node's new care-of-address and the home firewall before any Mobile IP messages are exchanged between the mobile node and its home network (Figure 4).

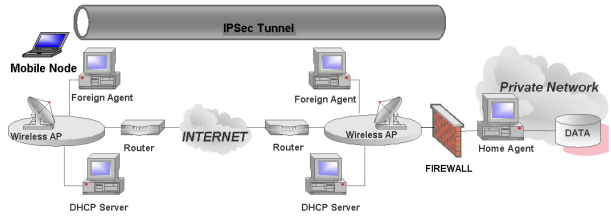

Figure 4 : IPSec Tunnel MN ⇔ Home Firewall

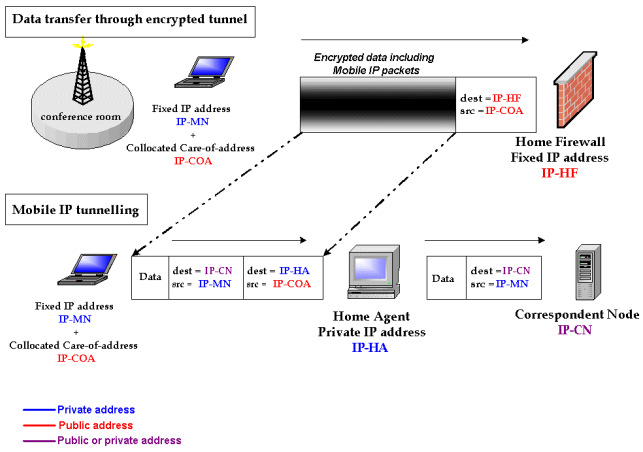

Figure 5 : SecMIP Packets

Until the next movement, the mobile node can communicate with any other correspondent node independent whether this is inside or outside the private network. Any data transfer between the mobile node and any other correspondent node is relayed via the home agent for security reasons. Figure 5 shows the packet format and addresses during data transfer.

It is also possible to communicate directly to correspondent nodes outside of the private network directly using the care-of-address, if that connection does not require to be secured. It can be configured easily by modifying the mobile node's routing table, whether packets have to be relayed via the home agent or not. Figure 6 summarizes the message exchange when a mobile node enters a new foreign network.

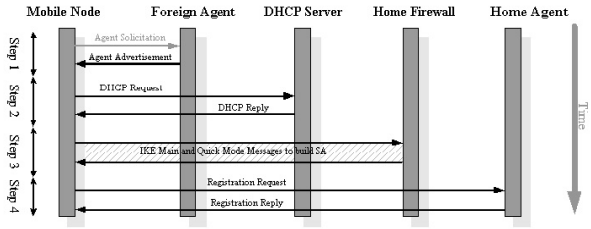

Figure 6 : Message Exchange

3. SecMIP Implementation

SecMIP has been implemented on Linux PCs. It uses two tunnels: a Mobile IP tunnel for supporting mobility and an IPSec tunnel for providing security. The implementation uses two public domain software packages: Dynamics Mobile IP [5] for Mobile IP and FreeS/Wan [6] for IPSec. Both have been chosen because of their source code availability. Source code of Dynamics Mobile IP is required for the adaptation of the implementation described hereafter.

Since these implementations are not thought to be merged, we had to perform many adaptations, before they worked successfully together in our SecMIP implementation. The main part of the implementation work was to achieve interoperability between Dynamics MIP, FreeS/Wan and the operating system. Therefore, the following scripts have been developed. These scripts are running on the mobile node to ensure that Mobile IP uses always a secured network interface to communicate with the home network.

Disconnect executes a Dynamics Mobile IP API call, which sends a deregistration message to the home agent and disconnects the mobile node from the home agent.

Connect executes a Dynamics Mobile IP API call that sends a registration message to the home agent and establishes a direct tunnel between mobile node and home agent.

DhcpSecure sends a DHCP request and updates the network interface configuration and the routing table. Afterwards an IPSec connection to the home firewall is built.

UpdateLocation1 (on a foreign network), ***UpdateLocation2*** (on the home network): By the API call 'update interface' the process dynamics_admin can be forced to read the actual IP configuration of the interface. If this configuration is identical with the home configuration, the mobile node is at home and a deregistration message is sent to the home agent (UpdateLocation2). Otherwise, a new registration procedure is invoked (UpdateLocation1).

UpdateRoute1 updates the routing table of the mobile node when it is connected to a foreign network and when the Mobile IP tunnel between mobile node and home agent is established. When the mobile node arrives at home, the IPSec and Mobile IP tunnels have to be disabled and the routing table must be updated (***UpdateRoute2***).

Firewall.rc: To control the incoming and outgoing network traffic of the mobile node, an IP-Filter is initialized using *ipchains*. The mobile node has a default firewall configuration which protects it against intruders. This protection is always enabled. When not attached to the home network, the mobile node is only allowed to communicate to nodes of the private network through a secured IPSec device. This guarantees data privacy.

Once Dynamics Mobile IP and FreeS/Wan's IPSec has been started, the scripts are executed when moving to a new foreign network or when returning at home as shown in Figure 7.

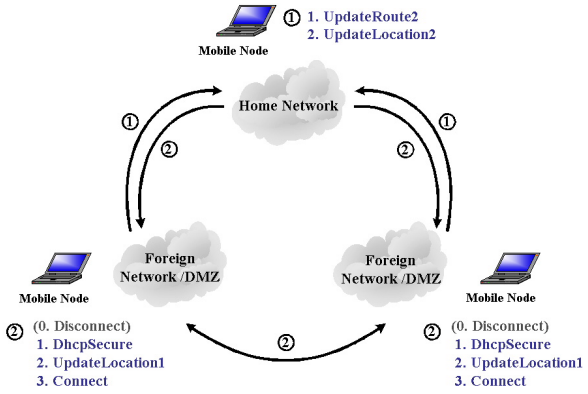

Figure 7 : SecMIP Scripts

All script calls were placed into the source code of Dynamics Mobile IP. No changes were necessary within the FreeS/WAN source code. This allows us to use other IPSec implementations that are more powerful, without the need of code availability.

Since all modifications were done only on to mobile node, it is possible to use any other Home Agent and IPSec gateway in the home network. Especially for performance reasons the use of sophisticated IPSec gateways on the home network is important.

The SecMIP prototype implementation has been successfully tested with Wireless LAN, Ethernet and HSCSD network devices. For further implementation details we refer to [10].

4. Performance Evaluation

The performance of the SecMIP implementation has been evaluated in order to prove the effectiveness of the proposed approach. The tests have been performed with the help of a SMARTBITS 200 network test box. This box has up to four Ethernet interfaces on which traffic can be generated and statistics can be evaluated. In order to lead the test packets through the SecMIP infrastructure, network devices were added to the home agent and the mobile node. All Ethernet devices of the test infrastructure support 100 Mbps in full duplex mode. The traffic generator generated unidirectional flows of IP packets up to 100 Mbps. Two different frame sizes were tested, 64 bytes and 1400 bytes. The smaller packets were transporting UDP/IP as frequently used in streaming applications or Voice over IP, and the bigger ones have been used for TCP/IP data simulating bulk data transfer.

In the different test scenarios, these IP packets were then transported in different manners. In the first scenario, they were just routed by the intermediate routers. In the second scenario, the packets were encapsulated by the Mobile IP tunnel (IP in IP), which extends the frame sizes by an additional IP header (20 bytes). In the third scenario additional IPSec information is carried. Figure 8 describes the three test scenarios and the tunnels established for them.

In the first scenario the performance without any tunneling or additional processing due to Mobile IP or IPSec has been measured. The measurements evaluated the performance of the test infrastructure. The only processing done by the intermediate routers is the routing of the IP packets. It is not surprising that the estimated performance depends strongly on the packet size of the generated traffic. For smaller packets with a

size of 64 bytes the impact on routing performance is much stronger.

The second test scenario was established to estimate the performance impact due to the Mobile IP tunnel between the mobile nodes collocated care-of-address and the home agent. Dynamics Mobile IP agents were started on the mobile node and the home agent. As before, the mobile node is attached on a foreign network and communicating with the acquired collocated care-of-address, which is used as the Mobile IP tunnel endpoint. The IP-in-IP encapsulation and decapsulation is the only additional processing compared to the first scenario. There is nearly no performance impact due to the IP-in-IP tunnel. Again, reducing the packet size reduces the maximum transfer rate dramatically.

In the next scenario SecMIP was enabled. Compared with the previous scenario there is an additional IPSec tunnel between the mobile node and the home firewall. Both computers, i.e. home firewall and mobile node have to encode and decode the Mobile IP tunnel packets and transport them in IP packets. The performance tests have been done after IKE tunnel establishment. The session key life time was set to infinity to avoid IKE message exchange during the test phase.

The traffic stream with large packets begins to break down for transfer rates over 18 Mbps. For small 64 byte packets, the performance is worse, because the IPSec overhead for the stream is much bigger (IPSec has to performs a security association lookup for every packet). The FreeS/WAN IPSec limits the maximum usable bandwidth to approximately 4 Mbps due to encryption and authentication. If the traffic exceeds this value the IPSec module is not fast enough and begins to drop packets.

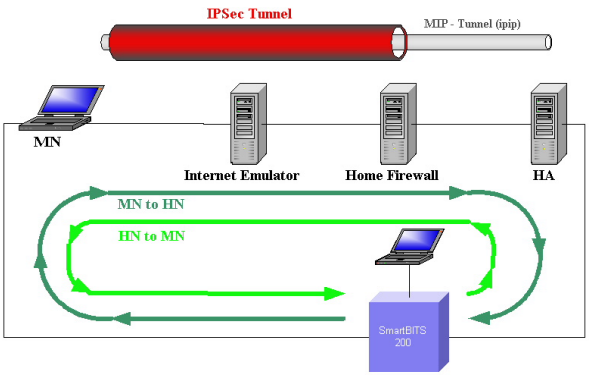

Figure 8 : Test Scenario

Handover from one foreign network to another takes currently up to 7 seconds. The delay has mainly been caused by the FreeS/Wan IPSec module since the generated IPSec device has to be destroyed and rebuilt after receiving a new IP address. This restart of the IPSec module takes about 4 seconds on the test PCs. Using a more dynamic IPSec module could decrease this handover delay up to 3 seconds, since the system just would have to wait for the DHCP procedure to configure the network interface to work in the new network environment. This needs a fast network neighborhood detection.

Another performance improvement can be achieved by establishing two simultaneous IPSec tunnels and two Mobile IP registrations for an overlapping period of time during handovers in order to achieve seamless handovers without service disruption.

However, those performance optimizations are subject for future research. This is in particular important since the TCP congestion control algorithm reacts to this handover interrupt and takes about 20 seconds to increase the transfer rate to its original value. We, therefore, see a strong need to adapt TCP to better cope with wireless environments where packets often get lost without any network congestion but due to handovers.

5. SecMIP for Mobile VPN Access in Heterogeneous Networks

The modularity of this approach makes it possible to integrate different network technologies without the need of changing any application software above the network layer. In combination with a management module that configures all available network devices, the SecMIP concept can be used for mobile VPN access through heterogeneous networks (Figure 9).

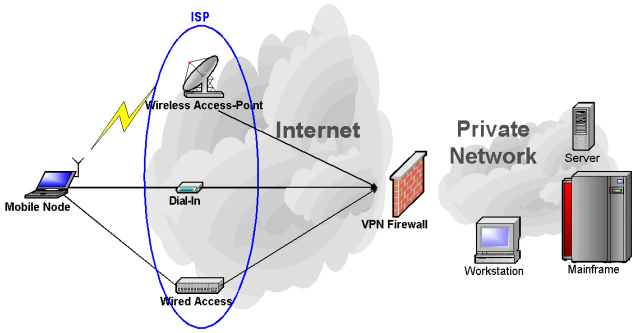

Figure 9 : Mobile VPN Access

The management module was designed, implemented and integrated into the SecMIP prototype to support

different access technologies like Ethernet, Wireless Ethernet, HSCSD, GPRS and conventional Modems (analog or ISDN).

The main advantage of this concept is the fact that there is only a real end-to-end security association needed between the mobile node and the Home Firewall. Once the mobile node is able to use an Internet access, the handover can be done automatically (based on characteristics of the access state as signal-noise-ratio, cost, bandwidth, etc.) or the user can be asked for the preferred network technology.

The used physical network device is hidden to the IP stack by introducing a virtual device between the SecMIP modules and the used physical device. This virtual device is called HadeS (Hardware independent SecMIP device). This HadeS is also needed to hide the temporary absence of any physical device while changing a PCMCIA card.

The management module for the physical network devices (card manager) can also help to reduce handover times by keeping the IP configuration of all available devices up-to-date. If several devices are present, the network detection can be done prior to the handover done by the SecMIP module. Figure 10 shows the modules used for the proposed heterogeneous mobility architecture.

For further information about the HadeS concept and the integration of SecMIP and HadeS we refer to [11].

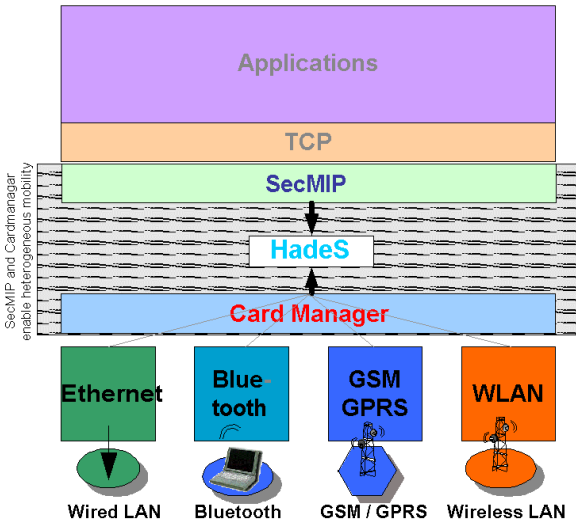

Figure 10: Heterogeneous mobility concept

6. Conclusion and Outlook

In this paper we presented an approach to allow Mobile IP users to access firewall protected VPNs. The solution is based on available standards and required minor modifications of the communication stack in end systems. The prototype implementation has been successfully tested with Wireless LAN, Ethernet and HSCSD network devices. Tests with GPRS and Bluetooth are in progress. Further work is also being planned to minimize the handover delays.

7. Acknowledgements

The work presented in this paper has been funded by the Swiss National Science Foundation (SNSF) and Swisscom AG. The work has been performed in the framework of the SNSF project no. 5003-057753 "Advanced Network and Agent Infrastructure for the Support of Federations of Workflow Trading Systems" (ANAISOFT). Swisscom AG, Bern, provided technical and infrastructure support for the implementation and evaluation of SecMIP.

8. References

[1] *D. Maughan, M. Schneider, M. Schertler, J. Turner „Internet Security Association and Key Management Protocol (ISAKMP)", November 1998, RFC2408*

[2] *John K. Zao, Matt Condell "Use of IPSec in Mobile IP", November 1997*

[3] *Jim Binkley, John Richardson "Security considerations for Mobility and Firewalls, November 1998*

[4] *V. Gupta, G. Montenegro, Secure and mobile Networking, Mobile Networks and Applications 3 (381-390), Baltzer Science Publisher BV, 1998*

[5] *Dynamics Mobile IP documentation, http//www.cs.hut.fi*

[6] *Linux FreeS/Wan documentation, http://www.freeswan.org*

[7] *James R. Binkley, John McHugh, Portland State University "Secure Mobile Networking Final Report", June 1999*

[8] *A. Aziz and M. Patterson, Design and Implementation of SKIP, http://skip.incog.com/inet-95.ps*

[9] *F. Pählke, G. Schäfer, J. Schiller: Paketfilter- und Tunnelkonfiguration zur Firewall-verträglichen Mobilitätsunterstützung in IP-Netzen, Kommunikation in Verteilten Systemen, Hamburg, February 2001.*

[10] *M. Danzeisen: Secure Mobile IP Communication, Diploma Thesis, Institute of Computer Science and Applied Mathematics, University of Bern, May 2001.*

[11] *M. Danzeisen, J. Linder: HadeS, Patent registration, Swisscom AG; June 2001*