# Secure Mobile Networking
# 10th Quarterly Report*

James R. Binkley and John McHugh
Portland State University

1 May 1998

## Project Status Overview

We began this quarter under the assumption that there might be no additional funds forthcoming for FY 98. Under this assumption, we would have had barely enough funding to continue support of our existing students through their scheduled graduation dates. In early January, we received an additional $75,000 (including overheads) which will allow completion of work currently under way and at least two additional releases of our system. It will also allow modest improvements in our equipment base and support for the one student remaining for the spring and summer.

In summary, we have slowed down quite a bit due to the programmers departing at the beginning of the quarter. We have three M.S. graduate students working on certain aspects of the mobile project at this point. Two of them will graduate at the end of the winter quarter and one will remain until the end of the spring quarter. It should be pointed out again that we made a combined release of Mobile-IP/IPSEC last summer and those files remain available at PSU and MIT.

Graduate students Jennifer Ye and Zheng Chen graduated at the end of the winter quarter. Bjorn Chambless will stay on for the spring and probably the summer. Jim Binkley has accepted a full time, non faculty, position at PSU effective in September and will remain associated with the project through its end.

Zheng Chen has completed work on supporting DHCP (Dynamic Host Configuration Protocol) in Mobile IP. This work is reported more fully in the following section. Mobile Hosts use the protocol to obtain temporary addresses at foreign networks for routing purposes but still maintain "permanent" home addresses for identity purposes and keep continuous transport layer connectivity while moving. This way, the Mobile Node can acquired a "co-located-care-of-address" at the foreign network and can detunnel packets itself.

Jim Binkley has completed an internet draft on mobility and security which appears below.

*Supported by th U.S. Department of Defense Advanced Research Projects Agency and the U.S. Air Force Rome Laboratory under contract F30602-95-1-0046.

## Use of DHCP in Mobile IP – Zhong Chen

### Architecture Overview

In addition to registering via a Foreign Agent, the Mobile Node can also register directly by obtaining a temporary IP address at the Foreign Agent. The temporary IP address is called a "co-located-care-of-address" in this situation. The "co-located-care-of-address" is the end point of tunnel and the Mobile Node detunnels data packets itself.

We decide to use the Dynamic Host Configuration Protocol (DHCP) for the purpose of address acquisition in our project. DHCP is a well deployed protocol for address allocation and host configuration. We use Internet Software Consortium's implementation of DHCP server and choose to write DHCP client code ourselves.

Although potentially in-efficient, we use DHCP itself as a mechanism of movement detection. If the Mobile Node DHCP client receives a DHCPNAK in response to DHCPREQUEST or no responses when renewing lease, the Mobile Node assumes itself has moved and tries to initialize a new round of DHCP session. The time interval in which the Mobile Node client renews leases is user configurable. The client tries to suggest a short lease time according to the time interval value with the DHCP server each time it sends a DHCPREQUEST.

We believe registering through Foreign Agent is preferable to registering directly using a "co-located-care-of-address". Thus, if the Mobile Node is configured to switch between modes automatically, the Mobile Node abides to the following rules:

- If the Mobile Node is in "NOWHERE" state and is not hearing from agents, switch to DHCP_MODE automatically
- If agent beacons are heard when the Mobile Node is in DHCP_MODE, switch to AGENT_MODE automatically

The Mobile Node can also be forced to work only in AGENT_MODE or DHCP_MODE.

A new state is defined for the Mobile Node: CO_LOCATED state. The Mobile Node is in this state after it has successfully obtained an IP address from the DHCP server.

In Foreign Agent mode, the reverse tunnel from Mobile Node to Home Agent is optional. In DHCP mode, this is required, because the existence of a new IP address makes outgoing packets carrying this new IP address as source address if not otherwise tunneled.

Security between DHCP client and server is not considered and left for future study.

### Address Binding

Now the Mobile Node has two IP addresses, one home IP address and one temporary IP address, but only one physical interface (assumed), how can these two IP addresses be bound? Fortunately, we have a mvif virtual interface. We bind the addresses in this way:

- bind temporary address to physical interface
- bind home address to virtual interface

The binding of temporary address to physical interface is essential to the functioning of network services. DHCP servers rely on ARP (Address Resolution Protocol) to verify that an address is not occupied before it assigns the address to the client. IP routers sitting at the Foreign Network which will route packets for the Mobile Node also rely on ARP to resolve host IP address to link layer address.

### Routing Table Configuration

As explained earlier, in order for the mobile host to appear to the outside world as if it communicates with its home address, we use reverse-tunneling technique. To achieve this goal, the routing table is configured this way:

- Default route is a tunneled route to Home Agent
  - inner source address is set to home address
  - outer source address is set to temporary address
  - inner destination address is the IP address of corresponding host
  - outer destination address is home agent
- An additional route is setup to redirect packets destined for Home Agent being routed through the IP router at the Foreign Network (this information is also given by DHCP server)

### An example:

Suppose the name of physical interface is wlp0, virtual interface is mvif0, home address is 131.252.222.80/26, temporary address is 131.252.210.174/26, home agent is 131.252.222.65, IP router of the Foreign Network is 131.252.210.129, then the following is true when the Mobile Node works in DHCP_MODE:

- Address Binding:
  - mvif0 ¡- 131.252.222.80/26
  - wlp0 ¡- 131.252.210.174/26
- Tunnel Setting:
  - inner source address = 131.252.222.80
  - outer source address = 131.252.210.174
- Routing Table:
  - to default, next hop 131.252.222.65, tunneled, interface mvif0
  - to 131.252.222.65, next hop 131.252.210.129, interface wlp0

### Configuration and Usage

In order to configure the Mobile Node to use DHCP, a new configuration directive is added. Here is the syntax and semantics:

`dhcp [mvif] [period]`

If this line is defined, the Mobile Node is DHCP capable. "mvif" is the name of the mobile virtual interface. "period" is the time interval in which the Mobile Node tries to renew lease with DHCP server. If this value is 0, then, the Mobile Node will not suggest lease time with DHCP server and will use whatever given by server (typically long, for example, 10 minutes). If this value is non-zero, the Mobile Node suggests a lease time which equals to 2 * period with DHCP server. The value defaults to 10 seconds and the minimum value is 5 seconds.

The Mobile Node switches between DHCP_MODE and AGENT_MODE automatically by default. However, this behavior can be changed by using "mnstat". The syntax is:

`mnstat -m auto|agent|dhcp`

where:

**auto** – automatic

**agent** – AGENT_MODE, manual

**dhcp** – DHCP_MODE, manual

The state information given by "mnstat -S" could be:
CO_LOCATED-ACKED
CO_LOCATED-PENDING
CO_LOCATED-DISCONNECTED?

### IPSEC

Efforts are made to make IPSEC still functional in DHCP_MODE. We can setup an IPSEC tunnel from the Mobile Node to Home Agent. To do so, the default route via home agent is set to be secure using kernel IPSEC functions.

Registration messages themselves are not protected by IPSEC (because of the auxiliary route to home agent). Fortunately, they are protected by Mobile IP authentication extensions. For data communication, the IP packet has the following structure if IPSEC is turned on and ESP is used:

```
+--------+--------+--------+--------+---------+
| Outer  | IPSEC  |  ESP   | Inner  |         |
|   IP   |   IP   |        |   IP   | payload |
| header | header | header | header |         |
+--------+--------+--------+--------+---------+
                           |                  |
                           |<--- encrypted -->|
```

Note that now we have two tunnels (IPSEC tunnel and Mobile IP tunnel) and three IP headers. The addresses in these IP headers are:

- outer IP header: src = temporary address, dst = home agent
- IPSEC IP header: src = home address, dst = home agent
- Inner IP header: src = home address, dst = correspondent host

The outer IP header makes packets easily penetrate firewalls; the IPSEC IP header makes IPSEC security relationship (Mobile Node - Home Agent) work; the inner IP makes Mobile IP work (Mobile Node location transparent to correspondent host).

Use `mnstat -r on|off` to turn IPSEC on or off.

### Conclusion

Using DHCP in Mobile IP is challenging because we have more network configurations to do. For example, we have two IP addresses instead of one; routing table could be more complex and reverse tunneling has to be used. When IPSEC is considered, we have to make sure that placement of protocol headers inside an IP packet is reasonable. Security problems of DHCP itself need to be future studied. Under any circumstance, the only purpose of DHCP is to obtaining temporary addresses. It should not be confused with Mobile IP, although the use of it can be integrated with Mobile IP, as in our implementation.

### References:


1. C. Perkins, "IP Mobility Support", RFC 2002, Oct. 96
2. R. Droms, "Dynamic Host Configuration Protocol", RFC 2131, Mar. 97
3. S. Alexander and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, Mar. 97
4. R. Atkinson, "Security Architecture for the Internet Protocol", RFC 1825, Aug. 95
5. R. Atkinson, "IP Authentication Header", RFC 1826, Aug. 95
6. R. Atkinson, "IP Encapsulating Security Payload", RFC 1827, Aug. 95


## Security Considerations for Mobility and Firewalls[1]


```
Abstract

In this paper we discuss various issues concerning Mobile Hosts using
Mobile-IP or other mobility systems (DHCP) and firewalls.  We first
discuss some recent attacks on the Internet and what they might mean
for such systems as Mobile-IP.  We then consider tunnels as used in
Mobile-IP (and elsewhere) as a security threat.  We suggest how mobile
systems may be made "less insecure" with current firewall technology
and near-term packet firewall technology that will use Virtual Private
Networks and IP layer security (IPSEC).  The goal is to describe a
```


[1] Internet-Rough-Draft by Jim Binkley (jrb@cse.ogi.edu)

security model wherein mobile systems can work across the I and not just as a interior routing protocol within one security and/or interior routing domain.

## Introduction and Assumptions

The focus of this document is on how a secure enclave (firewall protected area) may tolerate Mobile-IP and remain secure. By secure enclave in the simplest sense we mean a conventional IP site with one management domain and centralized security administration typically behind one IP packet firewall [Cheswick]. Our focus here is on how a secure enclave can protect itself from foreign (non-local) Mobile Nodes. We also deal with IP spoofing issues.

The discussion here is focused on the network layer. We are not considering higher-level authentication or confidentiality services that might be part of an application-level system. When we talk about firewalls, we are mostly talking about network layer access, and such mechanisms as packet-level firewalls with access control, Virtual Private Networks implemented as IP tunnels, and IP layer security (IPSEC) [ipsec].

When we cite IP addresses in the text, we will use private IP addresses[cite]. These should be viewed as place holders for public ("real") IP addresses associated with an interior routing domain. They are not meant to be private as used "out there" and merely provide address anonymity for the sake of discussion.

## The Problem

According to the BUGTRAQ list [cite] and recent CERT [cite] advisories the Internet has seen a set of attacks whereby attackers use various forms of address spoofing at the IP level. Some of the attacks are denial of service oriented. Some seek to cause the attacked system to crash or hang. Many of the attacks can be characterized as single packets wherein the IP source and destination addresses in the IP header appear to originate within the attacked systems site. We will mention three such attacks, TCP SYNC [CERT cite], smurf [CERT cite], and land [CERT cite].

In TCP SYN attacks, the attacker sends TCP initialization packets to a given site. The attacker system is tied up simply due to opening TCP control blocks, hence allocating internal memory. The attacker need only send one TCP SYNC packet. The attacker may choose to use a spoofed IP source address so that tracing the attack back to its originating system is difficult.

In smurf attacks, the attacker sends one or many ping packets to an IP directed-broadcast address with an IP source address that may also be in the site. For example, if a site had a site specific class C address along the lines of 192.168.1.0, the attacking IP destination might be 192.168.1.255 or 192.168.1.0 (0 broadcast addresses may be used as well). The IP source address may be external or internal. The result is that two systems (at least) may be attacked. The IP source itself is bombarded with ping reflections from all the systems at the directed broadcast address. Further the smurf vehicle may also be used for single packet "ping of death" attacks.

Land attacks involve one TCP packet in which the IP src is set to be the same as the IP destination. The attack may cause the victim to hang.

In general, note these attacks do not involve packets being returned, unless the packets are returned to another system that is being indirectly attacked itself (smurf). They may serve a denial of service function either by tying up network resources or causing systems to reboot. One general technique that can be used against them is to disallow IP spoofing for internal source addresses [cite]. Packets entering a network may not possess an IP source address internal to the network. Packets leaving the network must possess an internal IP source address.

We will briefly look at how this may be done with a Cisco router which we assume is the interface between a site having 172.16.*.* as its address space and the Internet at large. Note that the access list entries shown here may be part of a more complex firewall policy and/or access list, but we only show the part relevant to IP spoofing.

We apply the following access list to packets headed out on the external interface:

```
access-list 111 ...
access-list permit ip 172.16.0.0 0.0.255.255. any
access-list deny ip any any log
```

This blocks packets headed out that do not have IP src addresses in the 172.16.*.* range and logs any internal attempts at spoofing. Thus spoofing attacks cannot originate in this site.

The following access list entry may be bound to an external router interface and would be applied to packets entering the site.

```
access-list 101 ...

access-list 101 172.16.0.0 0.0.255.255 any
```

The result is that a site firewall or border router will neither send or receive packets over an interface when the packets do not belong to the source IP routing domain. In addition, it has been suggested that firewalls might not accept unicast packets over a given interface when their IP source address would not be the unicast routing interface. [see cisco/firewall rfc].

The result of such anti-spoofing measures is that Mobile-IP packets headed in to "foreign" Mobile Nodes; i.e., Mobile-Nodes from some other site than 172.16..*.* will not be permitted to enter. Packets trying to leave from systems from another site, say 192.168.1.0, will not be permitted to leave. Mobile-IP within the same routing domain, which we might call "interior Mobile-IP" would be permitted. Mobile-IP between two interior routing domains would not be permitted.

There are a couple of considerations that should be pointed out at this stage. First the Mobile-IP registration protocol would still work, unless blocked (see below). Hence a foreign visitor at the 172.16.*.* site could run the Mobile-IP registration protocol to its Home Agent at say 192.168.1.1. This is because the Mobile-IP protocol may be viewed as an application level entity (UDP port 434) and a "Care Of Address" (a local non-mobile IP address) could be used as the IP source address for the registration packet itself. Hence it will reach the Home Agent across the firewall and not be blocked by the IP spoofing measures given above. See the figure below:

```
                                                    172.16.1.1
Home Agent: <-- MIP registration --> Firewall <---> Foreign Agent
192.168.1.1                                           |
                                                      |
                                                      |
                                                   Mobile Node
                                                   192.168.1.2
```

The Mobile Node would acquire the COA 172.16.1.1 from the Foreign Agent and use that to get its Mobile-IP UDP registration packet to/from the Home Agent. In the picture above, in security terms, the Foreign Agent is basically a application-level bastion host for Mobile IP.

The irony is that Mobile-IP will still work, but the Mobile Node will not be allowed to talk to home with ordinary data packets. Data packets tunneled from the Home Agent to the Foreign Agent will be allowed through. The Mobile Node may still engage in full 2-way traffic with nodes in the 172.16.*.* domain. It might also (if not blocked) attack systems behind the firewall itself with the one way attacks previously described.

Tunnels Considered Harmful

One mechanism that is part of Mobile-IP and in point of fact many other routing protocols are IP tunnels which might be implemented with IPIP[cite] or Cisco's [GRE]. It should be pointed out that IPIP tunnels are not peculiar to Mobile-IP. They are used in many routing protocols for many purposes including tunneling non-IETF protocols (e.g., Appletalk) or building virtual networks on top of the current Internet (MBONE, 6BONE).

Tunnels may mean encapsulated packets where one has one IP datagram inside another IP datagram and we will use IPIP (IP protocol 4) as our example here. Mobile-IP contains at least 3 forms of tunnels, IPIP, GRE, and so-called {TBD} direct encapsulation tunnels.

Mobile-IP uses tunnel mechanisms like IPIP to forward packets from the Home Agent to a remote "Care Of Address". The COA is a local site address that may represent a Mobile Node that has acquired a local IP address itself directly via DHCP or a router system that speaks Mobile-IP called a Foreign Agent. Any Mobile-IP system, including Mobile Nodes, Home Agents, or Foreign Agents, may source or sink tunnel packets. When a Home Agent forwards packets to a Mobile Node that is at a Foreign Agent, the use of IPIP may appear as follows:

```
IP outer                      IP inner                 IP datagram
ip src= Home Agent            ip src = peer end host
ip dst= Foreign Agent         ip dst = Mobile Node

|
| packets to MN
v
Home Agent ========= IPIP tunnel to COA ===>   FA/MN
```

One might ask if it is enough to simply use IPIP tunneling and tunnel somehow either from the Foreign Agent or Mobile Node back to the Home Agent and thus evade the anti-spoofing measures at a firewall? This is an insecure approach.

In the first place, it is not enough to simply tunnel over the IP spoofing firewall. This is simply "IPIP spoofing". The problem is that if one has a tunnel sink (be it any kind of agent or Mobile Node) that decapsulates packets and then forwards them, others can launch their spoofing attacks with IPIP too and thus have the spoofing emerge "inside" the firewall. For example, smurfing might simply be redirected through a tunnel. The inner IP header might be directed broadcast with an interior IP source named as a target.

Solutions here may involve secure network design, which is not a new idea where firewalls are concerned. We will suggest that one can in general block tunnels with current access list mechanisms and thus control tunnels so that tunneling from the outside can only be done to certain hosts that will be considered as bastion hosts. For example, with Cisco IOS one can add the following statements to access list 101:

```
        access-list 101 deny ipinip any any
        access-list 101 deny gre any any
```

and thus block any IPIP or GRE packets coming in over the router. One can further add a permit statement to force any IPIP coming in to land at a certain host and then treat that host as a bastion host; i.e., a nexus of security focus.

For example,

```
...
access-list 101 permit ipinip any host 172.16.1.3
access-list 101 deny ipinip any any
access-list 101 deny gre any any
...
```

in an input access list, means ipip will only be allowed to the host 172.16.1.3, which we will assume is a tunnel sink agent.

We have focused internal trust for IPIP on that one system. We next need to explore how to make sure that packets arriving at the Home Agent are *not* attacks that can be made on a tunnel sink. This can be done with IPSEC (site) tied to Virtual Private Network (secure tunnel) technology. We will explore this idea further in the next section.

Mobile Nodes Abroad

In this section we will consider the problems for a secure enclave if Mobile Nodes in that secure enclave go abroad; i.e., out to the Internet beyond the firewall. In essence, we are considering the problems for "our side". There are two sets of problems here. We must ask how the Mobile Node can secure its own traffic and in effect, take its security enclave with it. We must also ask how the enclave can secure traffic coming from that Mobile Node back inside, which will extend the thinking in the previous section.

We must point out that the security problems here are not terribly different from those encountered by current dialup clients into a secure enclave that have access to the enclave via a internal terminal multiplexor. One crucial difference is that data in our case will be assumed to be sent across the Internet, and not a telephone switching system. Thus some think that the data itself need not have authentication and/or confidentiality measures applied to it. All that is needed is a system along the lines of PPP with CHAP[cite] and RADIUS[cite] for one-time authentication. However commercial products are available from Cisco and Microsoft [cite] that at a high level are very similar to what we propose here. The exterior host tunnels into a secure enclave and an agent in the secure enclave applies crytographic measures to packets that have came in from the outside.

Glass and Gupta[cite] suggest that Mobile-IP Mobile Nodes abroad may use DHCP to acquire "local" IP addresses, thus they can get by the anti-spoofing measures in the firewall router. Further, the Mobile Nodes can use IPSEC with two-way tunnels between the Home Agent as a classic bastion host and the Mobile Node. (See [http://www.cs.pdx.edu/research/SMN for a combined Mobile-IP IPSEC system in which Mobile Nodes can do two-way MN/HA ESP tunnels). Please see the figure below:

```
                               Internet           172.16.1.1
Home Agent: <----> Firewall <-----------------> router/DHCP server
192.168.1.1                                           |
                                                      |
                                                      |
                                                  Mobile Node
                                                  172.16.1.2/
                                                  192.168.1.2
```

Packets sent from the Mobile Node to the Home Agent might have the structure:

```
IP(1) | IP(2) | <IPSEC> | IP(3)
```

Each IP header has its own purpose. The most external header, IP(1) exists to get the packets to the Home Agent with an IP source address == 172.16.1.2 acquired from a local DHCP server. The IP destination would be 192.168.1.1. Thus this header allows transit of the Internet and any firewalls. When the packet arrives at the Home Agent, that header is discarded and the IP(2) | <IPSEC> IPSEC tunnel portion is processed. Here we assume that the Mobile-IP address 192.168.1.2 is used for the source address and the Home Agent is again the destination. The fixed Mobile-IP address may be needed here as it allows a priori manual IPSEC keys to exist between the Mobile Node and the Home Agent. In effect, this is an IPSEC tunnel. The interior header would contain the Mobile Nodes fixed address (192.168.1.2) and the address of any destination to which it is allowed to send packets.

The above triple-header system may possibly be optimized by a higher-level protocol that could produce a dynamic binding between the local DHCP-acquired COA and the Home Agent's destination address. This would allow one header to be deleted. Such a system could be used by Mobile Nodes abroad that are not using Mobile-IP and are simply using DHCP for a simpler form of mobility.

We must also consider the threat to the secure enclave itself. The tunnel-sink agent must guarantee that all packets sent to it via tunnel are cryptographically verified; i.e., shared secret keys exist between it and the Mobile Node abroad and no packets that are leaked to it by the firewall will be internally forwarded until they have been verified. This might be done with an access list mechanism tied to IPSEC or by simpler means. For example, the PSU system mentioned above has a BSD sysctl(8) switch

```
sysctl -w net.inet.ip.mvifipsecinput=1
```

that if set forces the IPIP driver to only forward packets if and only if IPSEC authentication or decryption has successfully occured between the remote system and this system. This allows a Home Agent to only internally route packets post successful IPSEC processing.

If a system abroad can send a simpler tunneled packet into our enclave, it might take the form:

IP(1) | IPSEC | IP(3)

The local firewall might then permit only ESP (ip proto 50) or AH (51) to the Home Agent depending on local security policies:

```
        ...
        access-list 101 permit 50 any host 172.16.1.3
        access-list 101 permit 51 any host 172.16.1.3
        access-list 101 deny ipinip any any
        ...
```

Hosting Visitors From Abroad

Paranoia in the defence of internal security is no vice. Thus we could start from a position of not allowing visitors. However we wish to construct a system that will allow external visitors to visit our site securely. We suggest than an approach that can be made with current (or near-current) technology involves secure network design. A basic principle is: "design the network so that visitor packets are not allowed inside". We may observe that whatever is done will probably be similar to current systems that have two-level security enclaves.

For example, one might have a network designed as follows:

```
                          ^
                          |
                      Router(1)
                          |
                -------------------------- internal less secure DMZ
                |         |             |
              Firewall(2) term mux      DHCP/router for Mobile Visitors
                |
             ------------------------
             | bastion hosts        | Firewall(3) (secure enclave)
```

The above may be viewed as a logical (not necessarily physical) structure that may be optimized by careful design. We have a Router that simply serves to allow access (possibly serial) to the Internet. Inside the external router we have a less secure network that may serve to allow unfiltered access to the Internet. This network might include terminal multiplexors and local mobility servers. Behind it we would have at least one level of firewalls with bastion hosts (which might e on the less secure network as well).

The above may be viewed first as a physical system that would tolerate visitors. However it can probably be optimized with a number of techniques. Let us consider two methods that may be used to logically separate networks and thus remove the difficulties that may be imposed on a site by physical construction. Note that these techniques *require* careful network security design. The security onus here is certainly on the designer, who must be careful and have confidence in these techniques.

One might use Virtual Lans (VLANS) [cite CISCO] to isolate visitors to a particular subnet and then make sure there are no unintended local link systems that are accessible to a visiting Mobile Node. VLANS can be used 1-1 with IP subnets, hence packets sent from the visitor will have to visit a router and access lists can be applied to interior interfaces. In the above system, Router(1) or Firewall(2) (which might be the same system), could apply an access list on interior secure interfaces to prevent access to interior systems by the less secure network. Please see the following picture:

```
^
| Internet  (vlan 2)
Router --------------------- DHCP/server (insecure net)
| (vlan 1)                    192.168.2.0
secure net 192.168.1.0
```

Packets from 192.168.2.0 might not be permitted to access the secure network and could only go outside. Note that access lists on the Router above must be applied to the vlan 1 interface.

One might also use Virtual Private Networks in the guise say of tunnels between interior routers that disallow foreign packets from internal access. As a very simple possibility consider a combination DHCP server/router that would simply construct a 2-way IPSEC VPN between itself and a network that was "outside" the secure enclave:

```
  | ----------------------------------- Internet accessible network
 Firewall(1)           VPN tunnel /router(2)
  |                            ^
  |                            |
  v                            |  VPN tunnel
secure enclave                 |
                               v
                       DHCP/server router (3)
```

In this case the VPN would make sure that any packets sent by visitors on a visitor link would be securely tunneled outside. We suggest that careful combination of access lists with VPN technology should allow the above picture to be collapsed in various ways. For example the Firewall(1) and router(2) systems might be the same.

## Miscellaneous Considerations

### Firewall Discovery

(This section might be burned if a reasonable citation cannot be found).

It has been suggested by some (cite) that some sort of Firewall Discovery system might allow Mobile Nodes to dynamically tunnel to and from firewalls. There are several problems with this notion:

1. It is complicated and probably unnecessary since our solution here will work with current firewall technology.

2. It is not very likely from a security point of view. Security people may not care for notions that poke holes through firewalls in the first place even when done dynamically. Complexities involved in cross-security domain certification are likely beyond near-term scope. The security folks "at-home" may not care for the notion of a Mobile Node somehow securing its packets between itself and a foreign Firewall. After all, that firewall might choose to store all data traffic, and enable a classic "man-in-the-middle" attack.

3. Traditional notions of IP Fate Sharing (considered bad) may apply here. Mobile-IP systems are already tied to the fate of their Home Agent. Additional tunnel ties between systems that are not related from interal routing or security enclave considerations may be complex. After all, it is hard to predict how many firewalls that rule out IP spoofing to/from a given cite may exist.

### The Role of a Mobile-IP Foreign Agent

It would seem that there is little role for a Mobile-IP Foreign Agent in the system we have outlined above. However this is not necessarily the case. There is in general, no reason, why DHCP and Foreign Agents cannot be combined. Local nodes may perform some sort of security handshake with a local Foreign Agent [cite MOIPS] and avoid using DHCP for a local IP address. Once a Mobile Node has identified itself to a Foreign Agent as belonging to the agent's secure enclave, it could use a IPSEC VPN between itself and the agent. Any packets verified by the Foreign Agent as local could thus be delivered locally and not sent over the VPN from the Foreign Agent outside the secure enclave. Thus locals and visitors could both be tolerated at the same agent link. Of course a local enclave might choose for policy reasons to force all visitors to be "local" or "foreign". "Locals" could be always treated as remote visitors and tunneled outside, thus having to use secure means to come back inside. Or foreigners might simply not be permitted entrance at a given agent. Both policy considerations are possible and should be considered in implementations.

## Conclusions

In this document we have presented secure network proposals that will enable Mobile Nodes from abroad (or nearby) to securely access the Internet. We point out that such systems are not dissimilar from current dialup systems that involve a remote PPP-based dialup client and a local terminal multiplexor. VPN mechanisms may be used between the Mobile Node system and its home security companion. Very simply put, the Mobile Node is an extension of the local security domain. In addition, one must also consider how to make that security enclave secure in the face of foreign visitors.

In summary, we will make the following suggestions:

1. DHCP to acquire a local COA solves IP spoofing problems and may or maynot be combined with Mobile-IP.

2. Suitable two-way crytographic tunnels between a system abroad and a routing system at home will allow the Mobile Node's own traffic to be securely tunneled over the Internet.

3. IPIP tunnels sans cryptographic safeguards should be viewed with caution. If an IPIP tunnel sink does not guarantee cryptographically controlled access, an attacker may tunnel various attacks (land, etc.) into an enclave.

4. Flexibility in routing, access list mechanisms, and VPNs should be considered by implementors with the goal of allowing mobility.

5. security considerations must apply both to Mobile Nodes abroad, their implact on the home enclave, and also how an enclave itself might be designed to tolerate visitors.

biblio

mip rfc
ipsec
cert
bugtraq
cisco firewall design
TIS vpn document
firewall book
PSU web site