Secure Mobile Networking
Second Quarterly Report

James R. Binkley and John McHugh
Portland State University

14 April 1996

Project Status Overview

We have gotten our project up and going this quarter and feel that we are making progress. We are about on track with what we predicted last quarter. We have built a small lab, and put together a development environment. A few laptops equipped with Wavelan radio pcmcia devices are being given out to project team members. We are in the process of building and deploying the mobile routers that are needed to implement Mobile-IP in our CS/EE building. We have made an informal security analysis and design of Mobile-IP. The security analysis is presented in more detail below. The implementation of Mobile-IP is underway. We include a short discussion of Mobile-IP issues below. We think we have some interesting results in terms of routing design in that area. We are at least engaged with IPSEC issues. Our analysis team is looking at both the cryptographic issues involved with the authentication algorithms (how MD5 is to be used) and is planning on reviewing the current set of session key management papers. We are also investigating the architectural issues where IPSEC is concerned. We hope to be able to "reuse" an existing UNIX based IPSEC implementation and integrate it with our version of Mobile-IP. We expect to make that determination in spring quarter. We believe that we should have a functioning Mobile-IP by the end of next quarter and that IPSEC should be started and integrated with Mobile-IP (and hopefully finished by the end of summer, although it may drag on into fall). For next quarter, we are starting up our mobile security reading group again and plan to read a number of papers on both mobility and related network security issues. We hope to encourage student involvement from both our department, Electrical Engineering, and also from the Oregon Graduate Institute, with whom we have ties.

We have made contact with our counterparts at BBN during the March PIs meeting and hope to exchange visits with them during the early summer.

Hardware/Development Environment

We have purchased a number of laptop computers, Wavelan ISA and PCMCIA cards, and desktop pentium systems to use as mobile routers. We had already ascertained that around 4 mobile routers would cover our CS/EE building. We have gotten 2 mobile routers deployed at this point, and are working on getting the other 2 out. We have ported Wavelan drivers from BSDI for both ISA and pcmcia cards to FreeBSD UNIX, which we have settled on as a development system. The laptops in question are IBM thinkpads, 701c, and 755cx. Buying laptops and running UNIX on them is problematic. There is a danger that hardware might not be compatible, especially the pcmcia controller and display graphics chipset. The Wavelan pcmcia driver assumes an Intel pcmcia controller. Where graphics cards are concerned, probably the hardest thing with putting UNIX on a laptop is making sure that X works, since after all, given the popularity of the World Wide Web, we need to be able to run netscape. (By the way, we have successfully run the Mbone nv app over Wavelan). IBM has complicated things by discontinuing the 755cx (we managed to purchase one) and apparently the 701c is headed down that path too. However the FreeBSD, 2.1 release seems to work well on the laptops so far. We have managed to save money by avoiding the purchase of ATT's Wavelan access points ($2k list). Instead we ported the ISA Wavelan driver and are simply integrating it into the mobile routers (Pentium-90s) as the Mobile Agents in question would have to exist on subnets in our building and elsewhere anyway. The ISA cards list at $600.

Our entire building will be covered with wireless access by the end of April. This will give us a Mobile-IP test bed as most if not all of the mobile routers just happen to be on different IP subnets. Our current building is essentially a square with a central courtyard and halls with offices around the edge. It covers one (small) city block. Offices exist with doors, walls, and a fair number of metal cabinets; i.e., there is not much line of sight access. We find that by putting a router in each of the corners, we should be able to ensure reachability for the entire building. Penetration in one corner through walls is not a problem. Wavelan actually is mostly reachable down any given hall from one corner to another. However, there are a few spots where end to end reachability doesn't exist (too many walls).

Mobile-IP

Having followed Mobile-IP since almost the inception (1992-1993), we would like to point out that it is a classic case of "design by committee". Mobile-IP has many, many feature points (too many), and we feel we would not be able to get anywhere by trying to implement them all. As a result, we are going to produce a Mobile-IP that is more limited in terms of features, but includes all security features, plus features that we deem essential in terms of security (two-way tunnels). For example, Mobile-IP allows authentication between all FA/HA/MN pairs and we intend to implement and use that capability. There are two forms of replay protection permitted and we intend to implement both forms and experiment with them.

Here are a few examples of the overdone Mobile-IP semantic set and what we plan to do about it:

1. Mobile-IP somewhat unclearly assumes that you will use ICMP router advertisements and solicitations (RFC 1256). We have already implemented a simple form of Mobile-IP router advertisments and do not plan on using solications at this point. Agents (FAs/HAs) will solicit and we regard the ICMP router advertisements as network-layer beacons, analogous to the HELLO messages used in the ISO/OSI ES-IS protocol. Our infrastructure will rely on Foreign Agents anyway as the odds of our having enough administrative control to get other people to deploy DHCP (or bootp) are slim to none. Further, beacons from agents can provide link-layer signal strength status. This information can be used to improve how and when Mobile Nodes switch between Agents.

2. Mobile-IP permits 3 different kinds of encapsulation, the basic required IPIP form, Cisco's GRE, and so-called minimal encapsulation. We plan on implementing only the basic unicast IPIP form to start with. The Mobile-IP draft states that the basic form of IPIP should have a so-called "soft state" mechanism that basically allows a HA to keep track of tunnel state and do something more intelligent with certain ICMP messages returned regarding encapsulated packets. Further, the tunnel mechanism should use the PATH MTU mechanism. We are in sympathy with these ideas but we do not intend to implement soft state at this time. We only want bare unicast tunnels between Mobile Nodes and Agents as appropriate. The required tunnel mechanism is complex, given PATH MTU, soft state, etc. Possibly it is too complex. There does not seem to be any implementation experience here. The draft doesn't note that unicast tunnels are also the exact same transport protocol as used with the current Mbone IPIP tunnels. These tunnel mechanisms are going to have to coexist in an operating system that supports mrouted. We are implementing a simple form of IPIP tunnel that will be accessable as a route to a virtual device in the routing table. Our bare bones IPIP should at least interoperate with other implementations.

3. Mobile-IP systems may choose to use one of two forms of protection against replay attacks. A timestamp mechanism based on NTP timestamps may be used or a nonce mechanism may be used. For timestamps, the bottom line here is that NTP must be used and presumably authenticated possibly from source to mobile node.

4. Mobile-IP optionally permits forwarding of broadcast and multicasts (via a bizarre unicast encapsulation scheme) to a remote Mobile Node. We do not intend to implement these mechanisms.

The above are just examples. Consider that Mobile-IP as it stands MAY contain semantics involving NTP, ICMP router solicitation, PATH MTU, DHCP, multicast routing, and it comes in two basic modes (FA-based and MN sans FA). Mobile-IP routing daemons may have to live alongside of mrouted, gated, routed, xntpd, and rdisc (routing discovery). Although the protocol itself is simple, the resulting architectural and test considerations are not.

One problem with IETF output is that in general, a working group might produce a protocol, but there is no guarantee that resulting application/operating system implementations and architecture will make sense. We feel that both IPSEC and Mobile-IP seem to suffer from some problems in that regard.

In the case of IPSEC, it is not clear at what layer security associations should be made in the operating system. If we use FreeBSD as our reference, we might tie IPSEC security associations (key binds to X) to sockets (application/transport), protocol control blocks (transport), or to routes (network layer). The choice ultimately will profoundly affect the ease of use of a system. It is also important for system security of course and in fact there may be no right choice. For example, both sockets and routes may need security associations.

With Mobile-IP, one problem is that the current IP subnet model has to be violated. For example, Foreign Agents must be able to talk to any Mobile Node from any subnet and not pay attention to the MN's subnet home ip address. This is contrary to the way current kernels work as they determine the subnets they are on from looking at the IP addresses associated with their interfaces. The BSD stack has another problem which is that in general it is not possible for an application to determine the input interface for an incoming packet. It is difficult (but not impossible) for applications to direct packets out a given interface. In general, the latter mechanism exists in a crude form and is called a "route to interface". Typically a routing daemon (that only talks to the local links anyway) may send a UDP packet to the directed broadcast address (e.g., via subnet.255) and the subnet address can be used to route the packet out the desired interface. Routing daemons that receive packets determine the interface by matching the incoming broadcast subnet with their own set of interfaces.

Without going into great detail, we have broken the design of Mobile-IP down into state machines based on the FA, HA, and/or MN role. There is a state machine model for each. Inputs are timer timeouts or ICMP or UDP packets. Outputs are actions like inserting or deleting routes, dropping a node from a visitor list, and/or sending control packets. The outcome of this decomposition is that we feel that we have successfully separated the functionality between application/routing daemons that will implement policy and a few bare-bones kernel mechanisms. It is obviousally desireable that as much functionality as possible should be put in the application layer and as little mechanism as possible in the kernel. Our design is complete and our implementation is under way. We are finishing the kernel implementation and beginning to focus on the routing daemons (applications).

One interesting aspect of our design is the routing table mechanisms we have added to the FreeBSD kernel. These mechanisms are necessary to make Mobile-IP work and also to make it secure. To implement Mobile-IP, we have added 3 types of routes to the kernel. This mechanism is important because Agents (FAs/HAs) need to maintain "visitor lists"; i.e., what MNs are registered at any given time. We want these visitor lists to be maintained by the application layer daemons. However the daemons have to be able to insert or remove routes in correspondence with the MNs in the visitor lists. As a result, new routing semantics are probably the most important kernel mechanism needed to enable Mobile-IP. Where FreeBSD is concerned, the routing table is the central focus at the network layer and it is a very efficient and useful mechanism. Even ARP is integrated with the routing table.

Our new routes take the following forms:

1. for unicast tunnels, we have implemented a virtual tunnel driver. A tunnel route can be added to the kernel as follows:

   ```
   # route add -tunnel <to Mobile Node> <via Care Of Address>
   ```

   The routing mechanism will direct an outgoing packet to the MN through the tunnel driver. The COA is used as the destination IP address in the outer IPIP packet. This mechanism is two-way and can be used by MNs to tunnel packets back to the HA or to the home network. We may want to implement a socket option mechanism that will cause a MN to switch ALL routes (except for the default or local link routes) to the tunnel back to the HA.

2. the MN itself needs to be able to setup a default route to the Foreign Agent. The problem here is that the FA's subnet address may not be the same as the MN's home subnet. We have introduced a default route mechanism that allows a default route to be inserted according to a predefined mobile interface (an ip-layer socket option). The route is of the form:

   ```
   # route add -foreign <to default> <Foreign Agent IP>
   ```

   The foreign switch coupled with the default destination tells the kernel that it had better use the mobile interface and avoid looking up the gateway in terms of its own set of subnet addresses.

3. the FA needs to be able to insert host routes to MNs that are present. It will do this (and hence enable routing for the MNs) once a successful HA UDP request is returned to it subsequent to an initial MN request. The result is that routing will not occur until the MN is cleanly registered with the FA. The route here takes sly advantage of the kernel's mechanism for determining an interface binding as we pass in the interface IP address that we desire to use as the Gateway portion of the route. This will allow the FA to be multi-homed, which would be useful for a FA system that wants to allow mobility on say ethernet or other wired links. The route is of the form:

```
# route add -foreign <to MN> <local interface ip address>
```

The kernel mechanism here basically only adds an ARP stub route (sans MAC address) and as a result we actually have optimized the number of routing table entries. More important, there is a very interesting and potentially useful result associated with this form of "foreign" route (foreign implies one or more IP addresses in the route that are not local to the system). This form of foreign route enables an initial and simple form of Ad Hoc routing between MNs. MNs can insert this form of route and talk directly sans agents even when their subnets do not match. It is important to note that they will not be able to talk to each other unless an explicit policy decision is made by a human or routing daemon to permit them to talk; i.e., local host routes must be inserted. Once the routes are inserted, ARP will work. Without them, ARP requests are ignored. We plan on constructing a simple UDP based form of host beaconing that when coupled with authentication will at least allow a primitive and simple form of Ad Hoc routing.

The upshot of the above routes is that they allow clean separation of policy and mechanism between the mobile routing daemons and the kernel.

Mobile-IP Security Analysis

John McHugh and Jim Binkley made an analysis of what we feel are potential security problems with Mobile-IP. (We are not entirely ignoring the issue of MAC authentication algorithms, but are deferring the analysis of those issues to both our cryptographer, Sarah Mocas, and to cryptographers working with the IPSEC working group). We present a discussion below of potential problems and solutions, where solutions exist.

Some potential issues/and solutions:

- Mobile-IP naively relies on ip address authentication; i.e., when a packet is coming into a Home Agent from somewhere remote; it will appear that Mobile Node ip addresses that should be originating inside the domain, are coming from outside the domain. Put bluntly, Mobile IP cannot be distinguished from a remote spoofing attack. Of course, this has long been recognized as a security issue [Bellovin 89]. The solution is that all packets between home networks and a MN should be at a minimum be authenticated using IPSEC AH (with static keys to start with). Better security may be obtained by combining authentication with encryption and tunnels for privacy (more below). An issue has been raised in the IETF as to whether or not it makes sense for Mobile-IP packets to authenticate their Mobile Node to HA registration packets. The point was that IPSEC should be used. We agree in part, but we do not know that it hurts to also authenticate the UDP registration packet. In effect, it is a request to the

HA to install a route and extra authentication there may add a small amount of utility and security redundancy as long as different keys are used. Certainly it makes logging easier.

- There is lack of encryption and or authentication for normal (non-control) packets. We presume that IPSEC AH combined with encryption (ESP) is a first cut here. One point to make is that encryption without authentication should not be used. This of course does not preclude the use of application layer security mechanisms.

- The Mobile-IP implementation on the HA/FA should be careful about denial of service attacks based on spurious registration attempts. For example, Mobile Agents (HA/FA) are supposed to maintain a visitor list (in effect a routing table) for registered MNs. In order to register with the HA, a MN must first have its UDP registration packet authenticated. If a bogus registration packet for the MN appeared with an invalid authentication, and the HA dropped the MN as a result, routing service to the MN could be disrupted. The implementation should ignore invalid authentication requests (except for logging) and allow currently valid registrations to timeout.

- There is the issue of MN location secrecy. How do we minimize information about our current location to the outside world? We combine the discussion here with the next item.

- There is a question about what circumstances make use of a FA a good idea, since the FA by definition has easy access to packets sent from a MN. In general, passive or active attacks could come from an arbitrary point between an MN and its HA, but they are most likely either on the MN's current link or via the FA. The FA is a good candidate for passive snooping attacks. For maximum security, the HA-FA and FA-MN relationships should be authenticated as Mobile IP permits. Of course, this means that the FA in question is effectively under the control of a given authority. There needs to be terminology to distinguish between Foreign Agents that are controlled by a given organization seeking security and FAs that are truly foreign to that organization. We will call the latter "untrusted FAs". The more interesting question is what if anything can be done with untrusted FAs? We believe that the principle here should be: "do everything possible to minimize knowledge about network traffic between the MN and HA". All packets should be authenticated and encrypted, and an MN to HA tunnel should be used (we will consider the HA function to be colocated with a firewall) for any "home" traffic and/or all traffic. The tunnel will minimize the exposure to a FA, since we presume that the only IP source and destination addresses exposed (not encrypted) will be those of the FA and HA. Packets will have the following encapsulation, outer IP (FA/HA), Authentication, Encryption (authenticated), inner IP, etc. A FA could attempt to disrupt and or slow down traffic, but it certainly could not decode it or fake authenticated packets (i.e., denial of service is a possibility of course). There is an question here about how much if any security might be added by an MN obtaining its own COA (Care Of Address) and not using FA services. This would simply hide the MN's own home IP address from the foreign network and is a small but potentially useful service.

- Link layer access to packets in the clear is of course a consideration. The arguments from the previous discussion hold. We assume at least network layer security and do not rule out application layer security as desired or appropriate.

- UDP registration packets and IPSEC presents an interesting problem where untrusted Foreign Agents are concerned. The problem is that the UDP registration packet itself cannot be encrypted or the FA will not be able to use it. The obvious solution is that the registration packet should not be encrypted. However it is not yet obvious as to whether any elegant architectural solution exists to make that happen. The operating sytsem will be responsible for IPSEC crypto mechanisms and an application routing daemon will be responsible for sending and receiving the UDP registration packets. Hence we have a disconnect. This is in fact a generic problem with IPSEC as we mention below.

- There may be potential pitfalls with the use of simultaneous registration with ¿ 1 Foreign Agents. Simultaneous registration in Mobile-IP is currently specified as meaning that packets outbound from HA to MN should be duplicated for as many FAs as the MN is registered with. This may certainly be useful from a redundancy point of view. However it offers an untrusted FA a distinct opportunity to keep the MN's registration a little longer (or forever) if the MN moves on. We will keep this problem in mind during our second year research on redundancy.

- One of the replay protection mechanisms is based on NTP timestamps. Presumably an active attack might be started by spoofing NTP packets, adjusting time appropriately, and then launching a replay. NTP has an authentication mechanism, but if you are hoping for total source to end system authentication, that may be unlikely. The NTP deployment situation here is complex and we do not know what capabilities may really be available. Certainly a Mobile Node can get NTP packets from home. We may be able to use IPSEC to guarantee that those packets are authenticated in lieu of cradle to grave NTP authentication mechanisms. We will look into this. NTP is deployed on our routers on campus, but it is not authenticated.

IPSEC

We are tracking developments in IPSEC and attended the recent L.A. meetings. We feel that we at least are beginning to grapple with the issues. At this point, one might feel that IPSEC is coming somewhat unglued. The fundamental authentication and encryption "transforms" (algorithms + mechanisms to secure various network headers) are undergoing change. IPSEC has a tension between cryptopgraphers who always feel that more analysis is needed and engineers who want to do something and throw it over the wall. Lately the cryptographers are winning. The AH MD5 transform is probably going to be replaced by a better transform in terms of cryptography (HMAC from Hugo Krawcyzk et. al. of IBM). Our cryptographer Sarah Mocas has investigated Hugo's work and feels that his reasoning is sound. Basically his HMAC algorithm will offer much more authentication security for a small amount of computational overhead. The ESP (encryption) packet was originally assumed to be "standalone"; although many thought that it would of course be combined with an AH authentication packet. This was a point of confusion. As a result, a new ESP transform is under way and the original will be replaced with one that subsumes authentication inside the transform; i.e., it will not be possible to produce encrypted packets sans authentication. Our analysis folks also intend to look at the proposed session key protocols (Oakley, SKIP, ISAKMP, Photuris). Although this is preliminary, we rather like the NSA ISAKMP protocol.

It has been pointed out by the IETF community that IPSEC has some built-in difficulties where encryption is concerned. Both RSVP and DHCP may need information that is present in higher-level headers in order to function. (Anyone who believes in strict layering separation may be in for a rude shock). This problem applies to Mobile-IP's UDP registration header too.

In terms of implementation, we are currently investigating the kernel architecture of the Naval Research Labs initial IPSEC kernel. This kernel is of BSD 4.4 vintage and includes IP next generation code. If possible, we would like to borrow as much (or all) of an existing implementation and combine it with our version of Mobile-IP. The NRL implementation by this point is somewhat flawed since the security mechanisms for AH and ESP are changing. On the positive side, it has a key socket mechanism that is certainly something we would want to use. It curiously binds security associations with sockets as opposed to protocol control blocks or routes. We are not sure that is the right choice (although it may be a valid choice) and we need to think about this issue more.

It was announced recently on the IPSEC mailing list that Cisco would be releasing a version of ISAKMP including fundamental IPSEC headers as a UNIX reference implementation sometime in April. FreeBSD in particular was mentioned. From what we understand of ISAKMP at this point, we think that the architectural aspects are important and useful. ISAKMP offers a model where security associations may be exchanged and policy is negotiated and decided on by application-layer daemons. Of course it also includes session-key management. We hope that this code is released soon, as it may be a better choice for us.

It should be pointed out that until we have IPSEC, we are naked at the link layer when it comes to sending telnet/ftp passwords in the clear. As a result, we are installing the Finnish "secure shell" that is a drop-in replacement for rlogin/rsh, etc. on our laptops and mobile routers. Secure shell uses static RSA keys for authentication and IDEA for encryption. We can use slogin as a replacement for telnet, and you can run ftp over a secure shell tcp link to hide passwords (and data). We have managed to get ssh deployed on local CS/EE systems by systems staff. It will be interesting to informally compare the two mechanisms (ssh versus IPSEC) once we have IPSEC implemented.

Redundancy and Ad Hoc Routing

Although this is work for next year, we have done a little research on redundancy mechanisms and have some initial ideas. We have already mentioned an initial form of Ad Hoc routing that will at least allow direct but authenticated contact between "consenting" Mobile Nodes. Our review of papers in this area and our own ideas lead us to believe that this protocol can be enhanced to allow more indirect communication between Mobile Nodes by developing a limited flooding source routing protocol based on multicast, and sequence numbers. We also think that we might investigate pairing the use of multiple Foreign Agents (allowed by Mobile-IP) with packets multicast to the "default" FA. This would give two-way redundancy between MNs and FAs. Multicast looms important here and we need to test and make sure that our Wavelan drivers support it.

Outreach

It is ironical that we teach Computer Science in places where computers and networks do not (and sometimes cannot) exist. We hope to eventually deploy a number of mobile routers elsewhere, as for example, we have labs and offices in another building across the street. We also want to cooperate with central PSU computer management who manage access to classrooms elsewhere that we use. We have demoed Wavelan to them and they are quite interested in using it to address certain wiring problems in PSU buildings that are not capable of being wired. (By coincidence there are classrooms that we use in one such building). Naturally they brought up link-layer security as a concern. Of course, that is the focus of our project. As a result, it appears that we may be able to do outreach within our own campus in the next year, at least to extend coverage to a few remote classrooms where we teach. Our initial goal here is to enable the use of mobile systems via some of our faculty. Ideally, we may be able to interest the university in some scheme to allow students (at least engineering students) access to mobile systems as well.

There is Ph.D research on-going at Oregon Graduate Institute that is focused on mobile concerns. One issue being investigated there is how to do dynamic switching of network pcmcia cards. One of our PIs is on the Ph.D committee and OGI is going to buy and deploy a small Wavelan network.

References

These are informal and are all available on the Internet.

Randall Atkinson. IP Authentication Header. RFC 1826, August 1995.

Randall Atkinson. IP Encapsulating Security Payload. RFC 1827, August 1995.

S. M. Bellovin. Security Problems in the TCP/IP Protocol Suite. ACM Computer Communications Review, 19(2), March 1989.

S. M. Bellovin. Problem Areas for the IP Security Protocols. draft. March 1996.

Mihir Bellare, Ran Canneti, Hugo Krawczyk. Keying Hash Functions for Message Authentication. preliminary version. January 1996.

Charles Perkins, editor. Mobile-IP. Internet Draft 15 – work in progress.

Secure shell URL - http://www.cs.hut.fi/ssh