Secure Mobile Networking
Final Report[1]

James R. Binkley and John McHugh
Portland State University

June 1999

[1]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.

Contents

1 Introduction **7**

2 Accomplishments **9**

2.1 Creation of a secure enclave model for wireless mobility that includes both inter and intra-domain Mobile-IP. . . . 9
2.2 Integration of Mobile-IP and IPSEC in terms of routing and security. . . . 9
2.3 Simplified Link-Layer Only Ad Hoc Routing 10
2.4 Multi-hop Multicast Ad Hoc Routing (MADRP) 11
2.5 The Home Agent Redundancy Protocol (HARP) 12
2.6 The Establishment of Two Wireless Campus Infrastructures 12
2.7 Availability of Wavelan drivers for PCCARD and DESKTOP platforms 12
2.8 Use of RSA-based digital signatures to secure the NARP (ad hoc #1) protocol 12
2.9 Use of RSA-based digital signatures to secure the Mobile-IP protocol 13

3 High Points **15**

3.1 Combined Mobile-IP and IPSEC system truly works 15
3.2 The Bjorn-cam 15
3.3 Adoption of wireless systems by IT administrators at OGI and PSU campuses 15

4 Low Points **17**

4.1 Death By Integration 17
4.2 U.S. Export Laws Deemed Not Helpful 17
4.3 Wireless a Moving Target 17

5 Mobile Security Policy Overview **19**

5.1 Secure Enclave approach 19
5.2 Us versus Them 20
5.3 Foreign Agent Considerations 20
5.4 Home Agent Considerations 21
5.5 Mobile Node Considerations 21

6 Suggested Further Work and Other Parting Shots **23**

6.1 Mobile Nodes Abroad 23
6.2 Smarter Foreign Agents 23
6.3 The hard work - integration 24
6.4 Keys as a basis for networking 24
6.5 Wireless Loading 24

7 Acknowledgements **25**

A Ties to the quarterly reports **29**

B Quarterly report – Fall 1995 **31**
B.1 Introduction 31
B.2 The Initial Mobile Network 31
B.2.1 Current Project Status and Operating Assumptions 31
B.2.2 Winter Quarter Results and Plans 31
B.2.3 Spring Quarter Plan 32
B.2.4 Research Notes 32
B.3 International Cryptographic Experiment participation 33
B.4 Report on Wavelan/Link-layer Connectivity in the CS/EE PCAT Building 33
B.4.1 Introduction 33
B.4.2 Equipment 34
B.4.3 Raw Data 34
B.4.4 Interpretation 34
B.4.5 Observations 34
B.4.6 Link-layer Routing and Security Observations 37

C Quarterly report – Winter 1996 **39**
C.1 Project Status Overview 39
C.2 Hardware/Development Environment 39
C.3 Mobile-IP 40
C.4 Mobile-IP Security Analysis 42
C.5 IPSEC 44
C.6 Redundancy and Ad Hoc Routing 45
C.7 Outreach 45
C.8 References 45

D Quarterly report – Spring 1996 **47**
D.1 Project Status Overview 47
D.2 Mobile-IP Status and Planning 47
D.3 IPSEC Status 50
D.4 Towards A Secure Mobile-IP 51
D.5 Mobile Network Authentication 52
D.6 Mobile Network Security 52
D.7 Theory of Mobile-IP Redundancy 53
D.7.1 Ad Hoc Redundancy 53
D.7.2 FA Redundancy 54
D.7.3 HA Redundancy 54
D.8 Outreach 54

E Quarterly report – Summer 1996 **57**
E.1 Project Status Overview 57
E.2 Mobile-IP 58
E.2.1 Considerations Regarding Timestamp Replay In Mobile-IP 58
E.3 Lab and Wavelan Considerations 59
E.4 Authenticated Ad Hoc Routing 59
E.5 Ad Hoc Routing Considerations 61
E.6 X-based User Interface for Mobile Routing Daemon 64
E.7 Mobile IP and IPSEC 66
E.8 Redundancy 69
E.9 Visit to BBN 70
E.10 Plans for Fall Quarter 70

F Quarterly report – Fall 1996 **73**
F.1 Project Status Overview . . . 73
F.2 Accomplishments for Fall 1996 . . . 73
F.3 Winter 97 Plan . . . 74
F.3.1 Winter goals . . . 74
F.3.2 Optional goals . . . 75
F.4 Personnel . . . 75
F.5 Fortezza-note . . . 76
F.6 IPSEC && Mobile-IP . . . 76
F.7 IPSEC-Mobile-IP architecture . . . 77
F.8 BSD(4.4) IPSEC/routing API . . . 77
F.9 BSD route types and the IPSEC route binding . . . 79
F.10 Static Routing Topologies . . . 80
F.11 Tunnel Driver . . . 81
F.12 Firewalls and Tunnel Considerations . . . 82
F.13 IPSEC/Mobile-IP Security Considerations . . . 84
F.14 Redundancy . . . 84
F.14.1 Home Agent Redundancy . . . 85
F.14.2 Foreign Agent Redundancy . . . 85
F.15 Rough Measurements of IPSEC and Finnish ssh over WaveLAN . . . 86
F.16 Actual Measurements . . . 87
F.16.1 Using WaveLAN between the two hosts: . . . 87
F.16.2 Localhost testing on bridgeport: . . . 88
F.16.3 scp testing over Ethernet . . . 88
F.16.4 ncftp testing over Ethernet - plaintext only . . . 88
F.16.5 Benchmark Conclusions . . . 88
F.17 Outreach . . . 89

G Quarterly report – Winter 1997 **91**
G.1 Project Status Overview . . . 91
G.1.1 Specific Accomplishments for Winter 1997 . . . 91
G.1.2 Spring and Summer 1997 projects: . . . 92
G.1.3 Personnel and sub–projects: . . . 93
G.2 IPSEC and Mobile–IP . . . 93
G.2.1 Keys In Our Current Software System . . . 93
G.2.2 IPSEC/MIP status and issues . . . 94
G.2.3 IPSEC and MIP - Firewalls and Tunnel Considerations . . . 95
G.2.4 Fortezza under FreeBSD . . . 96
G.3 Redundancy . . . 96
G.3.1 Redundancy - Mobile Routers (Mobile FAs) . . . 97
G.3.2 Redundancy – Multi–Hop Ad Hoc Routing . . . 98
G.4 Protocol Overview . . . 98
G.4.1 Implementation Details . . . 99
G.4.2 Experimental Goals . . . 100
G.5 Home Agent Redundancy . . . 101
G.5.1 The basic HARP topology . . . 102
G.6 Outreach . . . 103
G.7 Appendix - IPSEC, Mobile–IP and Policy . . . 103
G.7.1 MNs/HAs . . . 104
G.7.2 MNs/FAs . . . 105
G.7.3 MNs/COAs . . . 106
G.7.4 HAs/FAs . . . 106
G.7.5 ad hoc MNs . . . 106

G.7.6 Route Optimization 107
G.7.7 Summary 107

H Quarterly report – Spring 1997 **109**
H.1 Project Status Overview 109
H.2 Accomplishments for Spring 1997 109
H.3 Current Personnel and Projects 110
H.4 Future Release Deliverables 111
H.5 Public–Key Cryptographic Work 112
H.6 ISAKMP (Bill Trost) 113
H.7 Considerations on the Mobile–IP Firewall Problem 114
H.8 COA acquisition 115
H.9 IPIP security issues 116
H.10 Formal Methods for Protocol Analysis 116

I Quarterly report – Summer 1997 **119**
I.1 Project Status Overview 119
I.2 Summer Accomplishments 119
I.3 Ad Hoc Routing 120
I.4 Home Agent Redundancy Work 121
I.5 ISAKMP Progress 123
I.6 Distance Mobility 124
I.7 Signed MN Registration 125
I.7.1 Mobile Node Considerations about FA Signatures 127

J Quarterly report – Fall 1997 **129**
J.1 Project Status Overview 129
J.2 Next quarter plan 130
J.3 Outreach 131
J.4 Equipment 131
J.5 Appendix - The HARP Draft 132

K Quarterly report – Winter 1998 **149**
K.1 Project Status Overview 149
K.2 Use of DHCP in Mobile IP – Zhong Chen 149
K.2.1 Architecture Overview 149
K.2.2 Address Binding 150
K.2.3 Routing Table Configuration 150
K.2.4 An example: 151
K.2.5 Configuration and Usage 151
K.2.6 IPSEC 152
K.2.7 Conclusion 152
K.2.8 References: 152
K.3 Security Considerations for Mobility and Firewalls 153

L Quarterly report – Spring 1998 **163**
L.1 Project Status Overview 163
L.2 HARP – Bjorn Chambless 163

M Quarterly report – Summer 1998 **165**
M.1 Project Status Overview 165
M.2 Status Items 165
M.2.1 Wireless Network Real-Time Monitoring 165
M.2.2 Linux Port 166

M.2.3 Policy Work 166
M.2.4 Just For Fun 166
M.3 Summer Release Information 167
M.4 Security Considerations for Mobility and Firewalls 177

Chapter 1

Introduction

This document is the final report for the Portland State University Computer Science Secure Mobile Network project. In this paper, we will summarize our accomplishments, discuss high and low points of the project, and suggest further work that might be done to further mobile/wireless security research. We will also present a final overview discussion of Mobile Security Policy.

We would like to point out that a recent IETF draft authored by Jim Binkley while at Oregon Graduate Institute and John Richardson of Intel [2] presents a number of thoughts on the subject of how cross-domain (inter-site) Mobile-IP might be made secure. We regard that document as part of this final report and urge any interested readers to obtain it.

Interested readers should note that source code releases and related papers may be found at the PSU Secure Mobile Network site: http://www.cs.pdx.edu/research/SMN. Although our DARPA funding period is over, we intend to pursue more modest secure wireless research, and will use this site to post any future results in software or technical reports. We would like to thank DARPA for giving us the opportunity to get started in this research arena.

Chapter 2

Accomplishments

In this section, we will briefly present our accomplishments (non-accomplishments will be relegated to the low points section below). We will minimize details and provide only bare bones summary text.

Please note that Appendix A below serves to tie these accomplishments to our quarterly reports. We hope that the appendix may serve as a bibliographic guide to content in previous reports.

Our accomplishments are discussed in the following subsections.

2.1 Creation of a secure enclave model for wireless mobility that includes both inter and intra-domain Mobile-IP.

We constructed an integrated Mobile-IP/IPSEC system in which Mobile Nodes abroad can use 2-way tunnels to securely tunnel all their packets to and from their Home Agent (assumed to be at home in the secure enclave, of course). This solution only addresses one possible facet of a many-sided security problem. We also invented two forms of ad hoc routing (including multi-hop) and tied them to end to end (but network-layer) IPSEC-based routing. Thus hosts that a priori belong to the same security enclave may choose to securely talk to their security peers. Further our Home Agent and Foreign Agents use one-way tunnels authenticated with AH. This allows all agents to reject any arriving (tunnel) packets that do not have an IPSEC binding using agent IP addresses.

Our 2-way tunnels deal with the problem of what to do about "our" mobile nodes, but neglect dealing with non-local mobile nodes. Issues here are complicated and we cannot claim to have the last word. However we have addressed many security issues in this area in our Internet draft [2] and refer interested readers to that document. In brief, we suggest that foreign nodes simply be logically treated as being "outside" the enclave and their packets need only be tunneled across the enclave to a firewall access point.

2.2 Integration of Mobile-IP and IPSEC in terms of routing and security.

A key focus of our work was to tie Mobile-IP and IPSEC directly together. At this point in time, Cisco (for example) has made both Mobile-IP and IPSEC available in their routing devices in IOS version 12.0 [5]. However there is no evidence that the two have been integrated. We believe that the combination of IPSEC and Mobile-IP is far superior to virtual link-layer tunneling schemes a la L2TP [6] or Microsoft PPTP [7] simply because IPSEC has wide-spread architectural utility, generality, and is liable to be more supported than more proprietary schemes. For example, IPSEC can cover both the link layer (by being at the network layer) or the transport layer OR run router to end system, router to router, etc. There is also no point in separate security mechanisms for the latest virtual link tunneling scheme when IPSEC can be used in all places. Mobile-IP needs IPSEC by definition as all packets between a remote Mobile Node (or Mobile Node on a wireless link) to/from home should be made secure.

In our system, we tied IPSEC to routes. For example, when a Mobile Node installs a default route, it is aiming that route at an agent. A route binding that included an indirection mechanism (tunnel IPSEC to the Home Agent) was part of the picture. When we did non Mobile-IP work (say using our multi-hop ad hoc routing protocol) to tie two Mobile Nodes together, we also naturally tied IPSEC to the host routes installed in each Mobile Node. All other IPSEC implementations we have seen so far tie IPSEC to some sort of additional packet-filter like access list mechanism. Our mechanism seems more powerful and in some ways simpler, but to be fair we cannot make a compelling case for its superiority over access list mechanisms (other than one less lookup in the IP layer, but even that is not terribly important given the relatively blinding speed of processors these days). Our IPSEC route binding mechanism can however easily be used to setup manual Virtual Private Networks between two routes simply by installing symmetric keys in a key file, and using the route(8) administrative command to install a route (to a network, subnet, or host). Our mechanism also applies to ARP/link-layer bindings. Our architecture seems to have general utility.

2.3 Simplified Link-Layer Only Ad Hoc Routing

In this protocol, we do not use ARP on a link. We instead use a protocol (like the ISO ES-IS) in which all nodes, agents, and Mobile Nodes send authenticated beacons. This "not" ARP mechanism is intended to serve a number of purposes. First, it tries to mitigate possible ARP spoofing by insisting that the (IP address, MAC address) binding be authenticated. Note that we have implemented this mechanism with both symmetric and asymmetric key systems (in the former case, we have a network-wide key; in the latter, a per host signature). Secondly, the mechanism serves to tie networks together by key possession. It is not important if two laptops do or do not share a subnet. All systems beacon. Therefore if you share a key, you can talk. The low-level IP subnet semantic that requires a router for communication between two hosts from different subnets is obviated. The mechanism also serves a gateway function so that systems who do not possess the secret cannot penetrate into a secure enclave through a "firewall-like" mobility agent. Lastly the mechanism serves a very important purpose in that we assume that if we can hear your beacon, we can talk to you. Beaconing (unlike ARP) is done at a relatively high rate of speed. If a system disappears, we will use other routing mechanisms to try and find it (and not believe an ARP cache entry that is going to hang around for twenty minutes).

The only toothless worn-out criticism that can be made of this system is that if everyone beacons the link itself may be less scalable/useable in terms of throughput.

Given that current wireless links cannot support many simultaneous hosts anyway, it is hard to understand how this criticism can be valid. ES-IS originally was criticized along these terms, but the critics apparently did not notice that beacon rates were extremely slow (once per minute for fixed ethernet systems). (See our criticism of wireless loading in the Suggested Future Work section below for more discussion on this topic). Slow beacon rates for Mobile Nodes along with a combined unicast ACK "reply" to agent beacons make the mechanism more scalable. Agents can beacon and Mobile Nodes can simply append their MAC address under Mobile-IP authentication when they use Mobile-IP to register. This takes care of Mobile Nodes that only desire to talk to the wired infrastructure and do not want ad hoc service. Non-motile Mobile Nodes do not need to beacon very often and can probably slow down their beacon rates (as long as agents do not remove them from the routing state in the agent). Highly Mobile Mobile Nodes need to beacon at higher rates in order to talk to each other.

We suspect the real problem here is wireless loading. If the link itself should be able to tolerate 100 FTP transfers at the same time – one should not worry overly much about 100 nodes sending out 100 byte beacons, even if the beacon rate for all nodes is 1 per second. Of course, this would be too much for WAN wireless systems with small overall bandwidth, but in such cases an IEEE 802.11 [8] style link-layer registration protocol only between agent and Mobile Node can make sense; i.e., one could well neglect the ad hoc function when there are too many nodes in a cell, or one simply doesn't care to talk to anything other the agent (highly likely in many usage scenarios).

2.4 Multi-hop Multicast Ad Hoc Routing (MADRP)

Our multicast ad hoc routing protocol was based on ideas freely borrowed from early suggestions by Dave Johnson [3] of CMU and Scott Corson of the University of Maryland. Our system differs from others in that

1. We did not neglect security between the systems.,

2. We considered redundant communication paths as possibly important., and

3. We integrated our system with Mobile IP so that it allowed systems more than one hop away from an agent on a wireless link to still communicate with the Internet.

The basic idea is that a source Mobile Node would use a multicast discovery packet to do an expanding ring search for another destination ad hoc host across any number of participating mobile hosts acting as routers. A multicast discovery packet would be sent out and "flooded" or forwarded until it reached either the desired Mobile Node or any Agent. Note that the flooding occurs across systems with only one interface, which is unlike how conventional routing protocols work, as in general, they will take a control packet in one interface and flood it out other interfaces; i.e., Mobile Nodes are assumed to have only one wireless interface. Intermediate systems and the final system would setup host routes pointing back towards the sender. A discovery ACK would be returned to the sender by the receiver which could either be multicast or unicast. The return trip packet would also cause routes to be set up (the send/receive discovery packets always cause routes in the opposite direction to be set up). Thus two-way communication would be enabled. Ordinarily the returned ACK might be unicast back across the "best" path. However if redundancy was desired, one could choose to multicast that packet back, thus informing the source of possible multiple paths to the target.

We also improved redundancy by considering agents as possible potential default routes; i.e., agents would always claim that they knew the way (even if they didn't). Thus a Mobile Node might get at least two path answers back:

1. from the true Mobile Node target if available., and

2. from a default agent.

The latter would be used only if the former was not available.

We made Mobile IP work in the multi-hop case by considering the Home Agent one more remote ad hoc node, and we would search for it. This would produce a host route (through a nearby agent) that would allow Mobile IP to work. We submit this is a rather elegant recursive architectural idea. End to end Mobile Node security was implemented by setting IPSEC route bindings up to the source and destination host routes respectively. Thus end path (from source to destination or destination to source) used IPSEC. Note that this mechanism is end to end, not end to router. It does not suffer from the possibility of a proposed plaintext attack. Intermediate systems are presumed to usually NOT impose additional IPSEC bindings. MADRP routing security itself is similar to Mobile-IP authentication. The protocol itself was implemented in the summer of 1997 and designed in 1996.

We submit that the routing metric system we developed was interesting but we never fully tested it. The basic idea was that each participating node would have the same function for metric computation based on a network-wide settable weight function consisting of

$m = f(\mathrm{hopcount}, \mathrm{power} - \mathrm{remaining}, \mathrm{signal} - \mathrm{strength})$.

Thus there were three possible variables in the metric, and weights could be set by the administrator to determine which of the three or combinations therein would be used. For example, one could decide that power at Routes with better power and signal-strength would be chosen. Hop count would be ignored. Or one might setup a link based singly only on power, hop count, or signal-strength. We felt that a combination of signal strength, and power would make the most sense.

We should point out that our protocol name "MADRP" stands for Multicast Ad hoc Demand Routing Protocol. Other possible expansions for the acronym never crossed our mind.

2.5 The Home Agent Redundancy Protocol (HARP)

HARP is documented elsewhere (for example, see [4]). Briefly we developed a protocol that is used between two or more Home Agents to share Mobile registration state (including IPSEC bindings). The agents essentially tunnel in parallel to Mobile Nodes. This mechanism is opaque to Mobile-IP as a whole. Mobile Nodes and Foreign Agents are not affected. HARP is an Interior Gateway Protocol. We assume that a protocol like OSPF is in use, and that a partitioned subnet scheme will be used. As a result packets sent to HARP agents may be evenly distributed by OSPF due to equal multi-path routing. We suggest that Home Agents not be on the same subnet, so that local power or routing failures cannot take out both Home Agents simultaneously.

The downside of HARP is that one must manually administer at least two sets of tables including Mobile-IP registration and IPSEC keys. One might attempt to cleverly "simplify" here by introducing yet another single point of failure. Beware.

We have experimentally developed a version of routed under FreeBSD that can live with our Mobile-IP daemon ("mipd"). We did this so that HARP Mobile-IP subnet availability can be dynamically advertised. However, we never made a production release of this code.

We have demonstrated the extreme usefulness of HARP on several occasions. Last Christmas, we shut down the main Home Agent in order to improve the ethernet wiring in its building area. We had a priori switched a static route in local Ciscos (which is advertised into our OSPF mesh) to the backup agent only. Mobile-IP use was unaffected. No one even noticed that the traditional Home Agent had disappeared and no one noticed when it came back two weeks later.

2.6 The Establishment of Two Wireless Campus Infrastructures

We established a wireless network that has a few users (mostly IT staff, faculty, and a few graduate students) within the School of Engineering at PSU [21]. We intend to maintain this network and extend it where possible. A more limited three-node network was established at OGI last year and is still in use by OGI IT staff and a few researchers.

2.7 Availability of Wavelan drivers for PCCARD and DESKTOP platforms

We have made our Wavelan drivers available to the FreeBSD community. The ISA driver is currently in FreeBSD. The fate of the PCCARD driver has been more complex, but is at least available in the so-called Hosokawa FreeBSD PAO (PCCARD package), although we still make it available on our SMN site as well. It has become obvious over the years that a small but hardy bunch of radio researchers who use point to point directional antennae have adopted Wavelan for long-haul WAN links. We are pleased that our efforts have aided them.

2.8 Use of RSA-based digital signatures to secure the NARP (ad hoc #1) protocol

Given that ad hoc #1 [1] was originally implemented with a symmetric key system (two symmetric keys, one for our side, and one for limited use by visitors), it could be claimed that it was challenged in terms of key scalability. As an experiment, we re-implemented beacons using signatures as authentication and tied our signature schemes to a DNSSEC server (this was lookup by IP address to get a public key). Thus agents could either use a flat file to obtain address/key bindings or could dynamically look up key bindings via DNS. The chicken and egg problem of how a Mobile Node "verifies" a Foreign Agent remains of course. But it is simply a matter of policy. One either brings needed certificates with you, you can choose to "not care", based on the observable notion that communication is proceeding with systems elsewhere, or you ask the Home Agent how it feels about a particular Foreign Agent. Agents, of course, are configured to care, and will not allow Mobile Nodes access unless certificate verification can occur. DNS at least offers relief from yet another single point of failure due to its master/slave setup. Our experiences with DNSSEC (even in a rather limited way) were positive.

Note that ad hoc relationships with pairs of Mobile Nodes are exactly like possible relationships between Foreign Agents and Mobile Nodes; i.e., you may decide a priori that you must somehow have the other sides certificate installed "manually" before communication can proceed. Face to face floppy transfers remain a distinct possibility (of course). Please show two forms of ID.

2.9 Use of RSA-based digital signatures to secure the Mobile-IP protocol

Signatures were also used to replace Mobile-IP's own authentication system. The symmetric authentication system used in Mobile-IP applies to all three possible relationships, 1. MN/HA., 2., MN/FA., and 3. FA/HA. The former is scalable but the latter two are subject to many to many explosions. Thus one of the obvious virtues of a asymmetric key system based on DNS is that one secure enclave with possibly many HAs, FAs (belonging to our side), and MNs (belonging to our side) might centralize its keys with DNS. We did not have the administrative time or manpower to make this so. It seems like a very good idea.

One of the interesting aspects of our implementation was that we decided to solve the MN/FA chicken and egg problem by allowing the MN to ask the Home Agent how it felt about a particular FA. The HA had an access control list for "approved" Foreign Agents and could act as the MN's proxy in terms of any possible DNS lookups and key verification activities where the MN/FA relationship was concerned. In general, it is extremely useful for security (and possibly other systems) to take advantage of the notion that the MN has a proxy partner at home, able and willing to act on its behalf. We believe this is a very important and key concept for trusted mobility.

Chapter 3

High Points

Our accomplishments as listed above are "high points". However we thought we would briefly mention a few positive tangential aspects that we feel are of interest.

3.1 Combined Mobile-IP and IPSEC system truly works

Given the complexity of many of the sub-systems, we are pleased that our system is in use at the PSU campus by small numbers and that the combined IPSEC/Mobile-IP system itself is also in use. Given our UNIX basis, it is not unknown for people to use slogin and scp on top of IPSEC, with the additional ad hoc #1 defence mechanism, thus giving us an in-depth set of security mechanisms, roughly at application (ssh), network (IPSEC), and link-layers (NARP).

3.2 The Bjorn-cam

As we had ported our mobile node daemon to linux/Redhat, we decided that a natural application would be to meld a wireless laptop with a color quickcam, thus producing a mobile camera (mobile within the wireless infrastructure of course) that takes periodic snapshots and puts them on the web. This is known as the "bjorn-cam", as Bjorn Chambless, a graduate student who has been with us for quite some time, developed the system. The bjorn-cam has evolved into a minor sociological phenomenon. Typically one person will take it and put it in his or her office for a week or two, and then send email or call friends and relatives and invite them to observe daily office activities on the web.

3.3 Adoption of wireless systems by IT administrators at OGI and PSU campuses

School of Engineering staff and IT administators at OGI have seemingly become very fond of our mobile system (especially network engineers). From the network engineering point of view, wireless is a natural out of band access system to the network, and represents a secondary path for troubleshooting. An IT staff person may typically be called to service a "broken" computer, that may simply be broken due to network setup problems. It is extremely useful to be able to bring along a working mobile computer that can then be deployed to troubleshoot the fixed wired computer's problem.

Chapter 4

Low Points

All efforts of this scope have their share of frustration and other low points. We are no exception. This section discusses some of the things that did not go as well as we would have liked.

4.1 Death By Integration

Our system involved kernel drivers, kernel security code, modifications to routing table code, complex application routing daemons, symmetric and asymmetric key-based systems, including an experimental version of DNS. The integration work included at least one kernel port (a new release) in the middle of the project. We ended up with roughly twenty systems that needed software replacements or upgrades. Certainly, in general, security code is complex, and requires complex skills especially when combined with fundamental operating system level system's programming. The complexity of our system required ever increasing release testing and integration testing. The worst aspect of the problem was probably the number of moving targets including frequent "upgrades" by FreeBSD itself. We cannot blame them for that, of course, but it seemed like everytime we tried to catch up, before we could make a release, a new FreeBSD release would appear. During the last year, when graduate student code was finally released, we did not have the resources to test the more complex parts and fully integrate them. We did however make a last gasp attempt to capture our kernel modifications in a set of patches. This was released in the fall of 1998 (this school year). Our hope is that the patch release may aid in future ports. Our belief is that complex security systems require long term commitment and serious test and integration phases.

4.2 U.S. Export Laws Deemed Not Helpful

We chose to use NRL's IPSEC work inside FreeBSD. FreeBSD has chosen to not implement our work. One of the reasons is that FreeBSD wants an IPSEC solution that is exportable and as a result is considering the Japanese Kame work which is an IPv6/IPSEC solution for FreeBSD.

Nevertheless, we wish to publicly thank MIT for helping to make our system available.

4.3 Wireless a Moving Target

802.11 as an IEEE project started in the early 1990's (we believe), which was before our project started. Ironically, the 802.11 standard only became available when our project was winding down. In the last few months, IEEE 802.11 wireless hardware has begun to be available. Unfortunately all of our Wavelan hardware was pre-IEEE. Lucent is in the process of making the previous Wavelan hardware unobtainable. The old Wavelan (naturally) does not interoperate with the 802.11 hardware as the fundamental link-layer mechanisms (and encapsulation) are different. When Wavelan (original) was available, Lucent advertised third-party drivers on its web pages. When they released the IEEE code, they expunged all mention of third-party drivers and only provided a limited number of PC OS-centric drivers for the IEEE systems, thus making things difficult for the UNIX-based research community. Only recently has a linux driver (which still has limited features) been made available [9]. We have already purchased a limited amount of IEEE hardware and intend to begin to move our test systems and wireless infrastructure in that direction. (We may simply transition to linux as well from FreeBSD).

The good news is that prices per NIC card have fallen approximately to 1/2 or 1/4 of the prices when the project started. (From $1000 per unit when we started to $250 for some (non-Lucent) IEEE cards).

Chapter 5

Mobile Security Policy Overview

In this section, we will briefly review our overall thoughts on mobile security policy. We will first look at the situation from the point of view of a given secure enclave trying to implement mobility, and then we will review the situation from the point of view of the traditional Mobile-IP architectural elements (Mobile Node, Home Agent, Foreign Agent).

5.1 Secure Enclave approach

By "secure enclave" we mean one set of hosts under a single security administration that is protected by some sort of a priori security mechanisms. For example, the secure enclave may be hooked up to the Internet but is protected by one or more firewall systems which might either be of the packet filter or bastion host variety. We do not rule out "defense in depth" for interior hosts. We do however assume that some hosts are exposed to the Internet and others are not. We are interested in hosts that are exposed to the Internet. We are also interested in hosts with wireless link layers, which for the sake of argument, we will assume are more susceptible to attacks like promiscuous mode sniffing.

In combining Mobile-IP and IPSEC in Mobile Nodes, we first of all made a number of simplifying assumptions. We assumed that a Mobile Node when at home could maintain a two-way IPSEC tunnel connection between it and its Home Agent. We assumed that a Mobile Node when abroad at either a DHCP link or Foreign Agent link could use two-way IPSEC to tunnel home to the Home Agent. The mobile node would dynamically discover these situations and setup tunnels with appropriate security mechanisms. The Home Agent was thus always a bastion host or security gateway to the secure enclave, via any link on it (wireless or wired). Foreign Agents in our first-cut model only serve as link-layer wireless gateways to a secure enclave and may or may not serve external visitors (but must serve internal wireless users, else they are not of interest). IPSEC associations between Mobile Nodes and Foreign Agents did not exist. A Mobile Node abroad might thus be viewed as an extension of the home secure enclave. The two-way tunnel to and from home would serve as an umbilical code to extend the umbrella of the secure enclave to the Mobile Node.

In more detail, let us look at the relationship between a Mobile Node and Home Agent with the Mobile Node at home. If the Mobile Node is a wireless node, our IPSEC system gives it a functional equivalent for link-layer security. (If it was wired, the user (or the local security authorities) might disable this function). What is important is that all packets barring ARP or Mobile-IP itself would be subject to network-layer IPSEC security, which might be more or less good depending on the specific IPSEC implementation and security transforms in use. We replaced ARP with a more secure ad hoc mechanism that simply made traditional ARP spoofing more difficult and made two-way exchanges into the secure enclave (via any agent) difficult as well. Mobile-IP had its own authentication mechanism (and we developed a digital signature replacement scheme for its authentication). There is nothing here to prevent the use of additional security at non-network layers including IPSEC at the transport layer, or transport-equivalent security mechanisms like the Finnish ssh (which we use all the time).

This mechanism is very general. The Mobile Node at home is simply equivalent to any current system using its default router. What is curious is that one still finds weak mechanisms such as the 802.11 WEP

(Wired Equivalent Privacy) in which an algorithm like RC4 may be used for confidentiality between Mobile Node and "bridge" (access point), but is unlikely to be sufficiently strong both because the key length will be restricted due to export reasons, and there is no provision for a key management protocol with the power of protocols in IPSEC. Ironically our ad hoc #1 system seems to be in competition with 802.11 and we believe our overall integrated system is far superior in many ways.

5.2 Us versus Them

When one thinks about a secure enclave, one must consider the enclave from two possible points of view. First one must consider mobile systems that belong to "our side". One must then consider mobile systems that may belong to less trusted visitors. Obviousally different security policies might exist for wireless (or wired) mobile systems that belong to the home team as opposed to possible potential visitors (or "evil" crackers trying to gain access via a wireless link available via a passing motor vehicle). For example, one might choose to allow local wireless nodes access to the secure enclave and might disallow visitor nodes. Or one might allow visitors access to the wireless network, but disallow access to key internal secure enclave areas. Certainly any number of policies might exist. It seems that flexibility in this area could be useful. On the other hand, rich security policy implementations could easily be confusing and hard to get correct.

We did some policy work here, and probably could have done more (see below under foreign agents for some discussion of one possible interesting security extension). Our work can be summarized in two ways:

1. We made it possible to limit access via "mobile" link-layer interfaces into the secure enclave. Visitors might be totally disabled or allowed access on a case by case basis. This was done via the ad hoc #1 authentication mechanism. A mobile node was required to know a shared secret (or present a signed beacon) to a agent. If the agent recognized the beacon, it would install a route to give the mobile node access. If the route was not installed, the mobile node might be able to initiate one-way attacks on the enclave, but it would lack the means for two-way communication. Visitors could be given a temporary key to allow them temporary access into the enclave. We implemented ad hoc #1 with symmetric keys to start with, but experimented with a DNS-based database system for asymmetric keys which would give more key scalability. The critical idea here is that agents act as routers and do not bridge packets naively into the interior infrastructure.

2. We suggested that network design might be employed to deal with the problem of remote visitors (or local wireless systems) by simply rerouting the internal pipes. For example, any packets coming in on an external unsecured link might simply be tunneled to come back in via an outside external firewall interface. Thus one can easily enable visitors (or local untrusted wireless access) by designing them "outside" the firewall. Packets from trusted external hosts might be allowed direct interior access as long as IPSEC is used (and this risk is deemed worth taking). Mechanisms used here might include known tunnel technologies like CISCO's GRE or IPIP, or even IEEE virtual lans at the link-layer. The tunnel endpoint (from agent to firewall) must tie to the same sort of input packet filter checks imposed on ordinary Internet packets coming back into the enclave through firewall systems.

5.3 Foreign Agent Considerations

Security policy for foreign agents in our original system was simplified and very natural. We class foreign agents as either trusted or non-trusted and implemented mechanisms to allow foreign agents to both exclude Mobile Nodes at the link-layer (ad hoc #1) and securely accept tunnel packets from the Home Agent (basically with IPAHIP). Confidentiality was left to the Mobile Node; i.e., the Mobile Node is responsibile for making sure that its own packets are secure to/from the Home Agent as it might be using an untrusted Foreign Agent. The reason for using IPSEC authentication in tunnels is to exclude tunnel spoofing possibilities; i.e., the possibility that an attacker might use barebones IPIP to send packets into an infrastructure at an agent, have them decapsulated, and thus appear to be local with a local IP source address. This is not possible if "our" Foreign Agents only accept IPAHIP packets from Home Agents that they trust and throw away IPIP packets.

We will discuss a more complex security policy system (and implementation) below that we did not implement, but could serve to allow even more complex policies vis-a-vis Mobile Nodes and Foreign Agents.

5.4 Home Agent Considerations

Home Agents serve as a bastion-host for mobile systems. Two-way tunnels terminate (or originate) at the Home Agents. It is assumed that barebones (HA to FA) IPIP tunnels are not used with Mobile-IP. Instead one ties IPSEC into the tunnel mechanism. We have already discussed how Foreign Agents could insist that all tunneled packets must a priori have some sort of IPSEC association between the Foreign and Home Agent. The Home Agent also serves as the tunnel destination for Mobile Node packets coming back to the enclave. It can enforce a similar semantic; i.e., insist that all inbound IPIP packets must have a Mobile Node/Home Agent (or "our-side" Foreign Agent/Home Agent) security relationship. Barebones unsecured IPIP packets would be tossed. Thus the Home Agent can defend the security enclave. One downside here is that Home Agents in this system are not end systems; they are intermediate systems (routers). Thus IPSEC packets may be subject to proposed plaintext attacks, as a "man in the middle" attacker might send packets to the Mobile Node to the Home Agent, and then observe the encrypted packets arriving at the Mobile Node. Defenses against this problem can include session key mechanisms that limit the exposure of keys and/or firewall mechanisms that do not allow Mobile Nodes abroad to talk to systems that are not in the secure enclave.

As a matter of policy, it would be reasonable to assume that Home Agents cannot suffer from a single point of failure scenario. We implemented the Home Agent Redundancy Protocol (HARP) so that Home Agents could act in parallel. We did this in such a way that IPSEC associations were shared and that in general, Mobile Nodes had no knowledge of HARP.

5.5 Mobile Node Considerations

In summary, we suggest that Mobile Nodes at home might use two-way IPSEC to talk to the Home Agent when an unsecure link is in use. (Note that this implies that a Home Agent should have an exterior and interior secure enclave interface). When abroad, they should use two-way IPSEC tunnels to both defend against malign influences on less secure links, and/or possible interception across the Internet. We regard concerns about "triangle routing" as irrelevant to security concerns. In general, security between parties who have no trust relationship is an oxymoron. The real security policy considerations for systems outside the secure enclave are two:

1. Should that system be allowed to talk to home? If the answer, is yes, mechanisms such as two-way IPSEC tunnels could be employed.

2. Should systems that are away be allowed to talk to untrusted systems outside of the secure enclave? If the answer is no, this would obviate such notions as routing redirection targeted to fix "triangle routing".

We also want to point out that our integrated solution includes the possibility of so-called "ad hoc" Mobile Nodes engaged in secure communication. With both our ad hoc systems, Mobile Nodes with a priori trust relationship could setup end to end IPSEC tunnels and thus securely communicate using legacy protocols like telnet and ftp. These tunnels were at the network layer, but unlike the Mobile Node to Home Agent relationship, they were end to end. Thus it is not possible for any attacker to forward packets through a Mobile Node and create a proposed plaintext attack.

Another key idea (pun intended we fear) was the notion in the first ad hoc protocol that an ad hoc network could be based on shared trust. In this case shared trust was blatant as ad hoc #1 uses two shared symmetric keys network-wide. One key was intended for our side and one key was intended to be temporarily created and shared with strangers deemed temporarily trustworthy (and then revoked). However our digital signature experiment assumed that there was one asymmetric key-pair per Mobile Node. We used a digital signature scheme for all beacons (Mobile Node and Agent), and also used digital signature with Mobile-IP authentication itself. This offered a very novel policy mechanism that as far as we know has not been considered before. In our signature scheme, we solved the chicken and egg problem of how Mobile-IP nodes can trust Foreign Agents, by simply asserting that the Foreign Agent's trust statement had to be "mailed" home (sent in the Mobile IP registration) from the Mobile Node to the Home Agent. Thus the Home Agent could use trusted infrastructure to both decide if the FA was trustable and also implement a possible access list control mechanism on non-acceptable Foreign stations. We suggest that the tie between the Mobile Node and Home Agent (as a basic trust duo) is important and can be used to solve many mobility problems. Yes, the Mobile Node is mobile, but it has a fixed surrogate at home that it can interrogate about possibly sticky situations.

Chapter 6

Suggested Further Work and Other Parting Shots

In this section we are going to present a few ideas that we would like to have pursued but lacked the means or time.

6.1 Mobile Nodes Abroad

It is important to note that Mobile-IP may be viewed as either an Interior Gateway Protocol or Exterior Gateway Protocol (or neither), simply based on security policies. Put another way, it is a reasonable security policy to claim that one is not going to allow foreign Mobile visitors using Mobile-IP (or simpler DHCP loaned addresses) to appear "inside" ones secure enclave. In [2] we noted that anti-spoofing measures currently used in the Internet make cross-domain Mobile-IP problematic. We implemeneted DHCP-based IPSEC tunnels to show that Mobile Nodes abroad could securely tunnel home and not have any problems with Mobile-IP source address spoofing (the Mobile Node source address is inside the external IPIP encapsulation and will not be seen until the packet arrives home). However we did not implement any mechanisms that would allow an agent to automatically setup tunnels to tunnel non-trusted Mobile Node packets outside the realm of the secure enclave. This is one mechanism for making smarter security agents that could make cross-domain Mobility more feasible.

With such work, the implementors should pay attention to both verification of the security mechanism and should consider risk assessment for what might happen if such mechanisms are breached. One of the problems with "dynamically poking holes in firewalls" is that one may get unintended holes. One of the problems with the notion of "active networks" is that they may be more active than you anticipated.

6.2 Smarter Foreign Agents

As another possible mechanism for dealing with both trusted and untrusted Mobile Nodes, Foreign Agents could be made smarter. We suggest two possible optimizations: 1., our ad hoc #1 protocol, served as a very primitive (but brutally effective) mechanism for disallowing cross enclave traffic by Mobile Nodes lacking beacon keys simply because the Foreign Agent would not install a local route for unwanted Mobile Nodes. The result (again) is that the Mobile Node could send packets but could not receive them through the Foreign Agent. One could improve this mechanism by tying a packet filter access control list to the registration process (802.11 can do this, but at the MAC level). A Mobile Node could present a certificate to a Foreign Agent, and upon verification, the Foreign Agent would then install an ACL that would permit two-way traffic for the Mobile Node. Note that this mechanism should not stand alone (as it is still spoofable) from IPSEC measures. For example, a Foreign Agent might also then insist that all forwarded packets must first be send directly to the FA itself using a MN/FA IPSEC association. Packets lacking that relationship would be thrown out or unceremoniously tunneled outside the secure enclave. Flexible policy for Foreign Agents may be useful, but appears complex. Of course, the risks inherent in such systems should be considered as well.

6.3 The hard work - integration

To make a long story short, security software is complex and integration although unloved is extremely important. Any key management system seems to have inherent and possibly untoward complexity that informally appears non-linear in nature. This should be recognized and time should be given to security and redundany oriented research projects that takes these problems into account. Given that we tried to combine Mobile-IP, IPSEC (including ISAKMP), digital signatures, redundancy in many forms, ad hoc routing, various versions of various operating systems, DNSSEC, etc., it is no wonder that we have had a nightmare integration problem. Our entire software system could stand thorough review and slow and patient replacement of key sub-systems with better quality code. We respectfully suggest that programs oriented towards security and redundancy need to be carefully nurtured and managed in terms of time and budget.

6.4 Keys as a basis for networking

Lastly, our integrated system seems to contain a rather curious notion. In ad hoc #1, we suggested that IP subnets were not the basis of networks. Instead shared trust (keys ...) should be the basis of networking. Our ad hoc #1 and ad hoc #2 systems could be viewed as small groups of Mobile Nodes that formed a network based on individual atomic key knowledge of members. Routing in truth may present a chicken and egg problem as you cannot speak ordinary data before you setup routing as control. But routing protocol security is usually solved by an a priori assumption that a set of routers share a shared secret. We suggest it is not unreasonable to assume that all packets might have a trust relationship and that networking might be done from the ground up (even ARP ...) on that basis.

6.5 Wireless Loading

In the course of the project we discovered that in general Wavelan did not "load" very well. What we mean is that the number of simultaneous transfers between N laptops and 1 agent is strictly limited and certainly does not scale to the level of ethernet. For example, at the height of our project in terms of group numbers, we had a meeting with seven people present all using a Wavelan equipped laptop. All members attempted to simultaneously do an ftp download of a large file. About only four succeeded in simultaneous download. In fact, several of the ftp transfers totally failed, while others would simply wait. This was an informal experiment but we believe it is truly illustrative of the problem. This has never really been a problem for us due to limited numbers of users, lots of cells (10), and a wide distribution of users on campus (in two different buildings). However we expect that anyone who widely adopts a wireless lan link and then faces > 5 users in the same cell will experience difficulties when simultaneous bulk transfers are attempted. We expect this problem is due to a number of factors including the limited spreading inherent in current spread spectrum techniques (currently limited by FCC regulations), the smaller overall bandwidth (1-2 megabits), and the fact that such a technology is only capable of "listen while send"; i.e., there is no out of band channel mechanism for true collision detection.

Solutions might lie with techniques borrowed from DARPA "Software Radio" techniques; i.e., a very wide spectrum spreading in terms of frequency. More narrowly based devices might use techniques for sampling limited ranges and then switch to another range that does not show so much current use. An agent could easily include the number of current users in its beacon. More research in this area is necessary.

Chapter 7

Acknowledgements

We would like to thank the following PSU students and staff for their participation in the project: David Reeder, Bill Trost, Bjorn Chambless, Radheka Godse, Jennifer Ye, Zhong Chen, Xu Hao, Eric Bergren, and David Burns. We would like to also thank Don Westlight of OGI for his support and interest. We wish also to thank Robert T. Morris Junior of Harvard for supplying us with the original set of Wavelan drivers, Jon Inouye (then of OGI) of Intel for his freebsd/pccard infrastructure support, and Ted Tso of MIT for making our security bits available.

Bibliography

[1] Jim Binkley. Authenticated ad hoc routing at the link layer for mobile systems. Technical Report 96-3, Portland State University, Computer Science, 1996.

[2] Jim Binkley and John Richardson. Security considerations for mobility and firewalls. Internet-Draft, November 1998.

[3] Josh Broch, David Johnson, and David Maltz. “the dynamic source routing protocol for mobile ad hoc networks”. MANET IETF draft, draft-ietf-manet-dsr-01.txt, December 1998.

[4] Bjorn Chambless and Jim Binkley. Harp - “home agent redundancy protocol”. Internet Draft, October 1997.

[5] http://www.cisco.com. Internet web site. Search on IPSEC and Mobile-IP.

[6] http://www.cisco.com. Internet web site. Search on L2TP.

[7] Counterpane systems announces crack of microsoft’s point-to-point tunneling protocol. http://www.counterpane.com/pptp.html. Bruce Schneier’s Cryptanalysis paper should be read first. More information can be found at http://www.microsoft.com.

[8] Wireless lan medium access control (mac) and physical layer (phy) specifications. IEEE Std. 802.11-1997, November 1997.

[9] linux ieee wavelan driver. http://www.fast.fh-dortmund.e/users/andy/wvlan.

[10] John McHugh and Jim Binkley. Secure mobile networking, fourth quarterly report. http://www.cs.pdx.edu/research/SMN/3q96.ps, Oct. 1996.

[11] John McHugh and Jim Binkley. Secure mobile networking, second quarterly report. http://www.cs.pdx.edu/research/SMN/1q96.ps, April. 1996.

[12] John McHugh and Jim Binkley. Secure mobile networking, third quarterly report. http://www.cs.pdx.edu/research/SMN/2q96.ps, July. 1996.

[13] John McHugh and Jim Binkley. Secure mobile networking, eighth quarterly report. http://www.cs.pdx.edu/research/SMN/3q97.ps, Oct. 1997.

[14] John McHugh and Jim Binkley. Secure mobile networking, fifth quarterly report. http://www.cs.pdx.edu/research/SMN/4q96.ps, Jan. 1997.

[15] John McHugh and Jim Binkley. Secure mobile networking, seventh quarterly report. http://www.cs.pdx.edu/research/SMN/2q97.ps, July. 1997.

[16] John McHugh and Jim Binkley. Secure mobile networking, sixth quarterly report. http://www.cs.pdx.edu/research/SMN/1q97.ps, April. 1997.

[17] John McHugh and Jim Binkley. Secure mobile networking, 11th quarterly report. http://www.cs.pdx.edu/research/SMN/2q98.ps, July 1998.

[18] John McHugh and Jim Binkley. Secure mobile networking, 12th quarterly report. http://www.cs.pdx.edu/research/SMN/3q98.ps, December 1998.

[19] John McHugh and Jim Binkley. Secure mobile networking, ninth quarterly report. http://www.cs.pdx.edu/research/SMN/4q97.ps, Feb. 1998.

[20] John McHugh and Jim Binkley. Secure mobile networking, tenth quarterly report. http://www.cs.pdx.edu/research/SMN/1q98.ps, May 1998.

[21] Seas wireless network. http://guinness.cs.pdx.edu.

Appendix A

Ties to the quarterly reports

In this appendix, we tie our accomplishments to the quarterly reports which give mode details. For completeness, the the individual reports are included (in slightly modified form) as appendices to this report. The references are to the appropriate pages in this volume. Also given are references to the URLs where the individual reports may be found and the section titles that may be used to locate the reference.

1. Creation of a secure enclave model for wireless mobility that includes both inter and intra-domain Mobile-IP.
   - Mobile-IP Security Analysis, (section C.4, p. 42. See also [11, p. 6])
   - Appendix - IPSEC, Mobile-IP, and Policy, (section G.7 p. 103. See also [16, p. 19])
   - Security Considerations for Mobile and Firewalls, (section M.4 p. 177. See also [18, p. 16])
2. Integration of Mobile-IP and IPSEC in terms of routing and security.
   - Mobile-IP, (section C.3 on p. 40. See also [11, p2].)
   - Mobile-IP Status and Planning, (section D.2 on p. 47. See also [12, p. 2])
   - IPSEC status, (section D.3 on p. 50. See also [12, p. 6])
   - Towards A Secure Mobile-IP, (section D.4 on p. 51. See also [12, p. 7])
   - Mobile-IP, (section E.2 on p. 58. See also [10, p. 2])
   - Mobile IP and IPSEC, (section E.7 on p. 66. See also [10, p. 15])
   - IPSEC && Mobile-IP, (section F.6 on p. 76. See also [14, p. 5])
   - IPSEC/Mobile-IP Security Considerations, (section F.13 on p. 84. See also [14, p. 15])
   - IPSEC and Mobile-IP, (section G.2 on p. 93. See also [16, p. 4])
   - ISAKMP, (section H.6 on p. 113. See also [15, p. 7])
   - Use of DHCP in Mobile IP - Zhong Chen (section K.2 on p. 149. See also [20, p. 2])
3. simplified link-layer only ad hoc routing
   - Authenticated Ad Hoc Routing, (section E.4 on page 59. See also [10, P. 5].)
4. multi-hop ad hoc routing (MADRP).
   - Multi-Hop Ad Hoc Routing, (section G.3.2 on p. 98. See also [16, p. 11])
   - Ad Hoc Routing, (section I.3 on p. 120. See also [13, p. 3])
5. the Home Agent Redundancy Protocol (HARP).

- Home Agent Redundancy, (section F.14.1 on p. 85. See also [14, p. 17])
- Home Agent Redundancy, (section G.5 on p. 101. See also [16, p. 16])
- Home Agent Redundancy Work, (section I.4 on p. 121. See also [13, p. 5])
- HARP Internet Draft, (section J.5 on p. 132. See also [19, p. 5])
- HARP, (section L.2 on p. 163. See also [17, p. 1])

6. the establishment of two wireless campus infrastructures.
   - See http://guinness.cs.pdx.edu.
7. availability of Wavelan drivers for both PCCARD and DESKTOP platforms.
   - See http://www.cs.pdx.edu/research/SMN
8. use of RSA-based digital signatures to secure the Mobile-IP protocol itself.
   - Public-Key Cryptographic Work, (section H.5 on p. 112. See also [15, p. 6])
   - Signed MN Registration, (section I.7 on p. 125. See also [13, p. 10])
9. use of RSA-based digital signatures to secure the NARP (ad hoc #1) protocol.
   - Signed MN Registration, (section I.7 on p. 125. See also [13, p. 10])