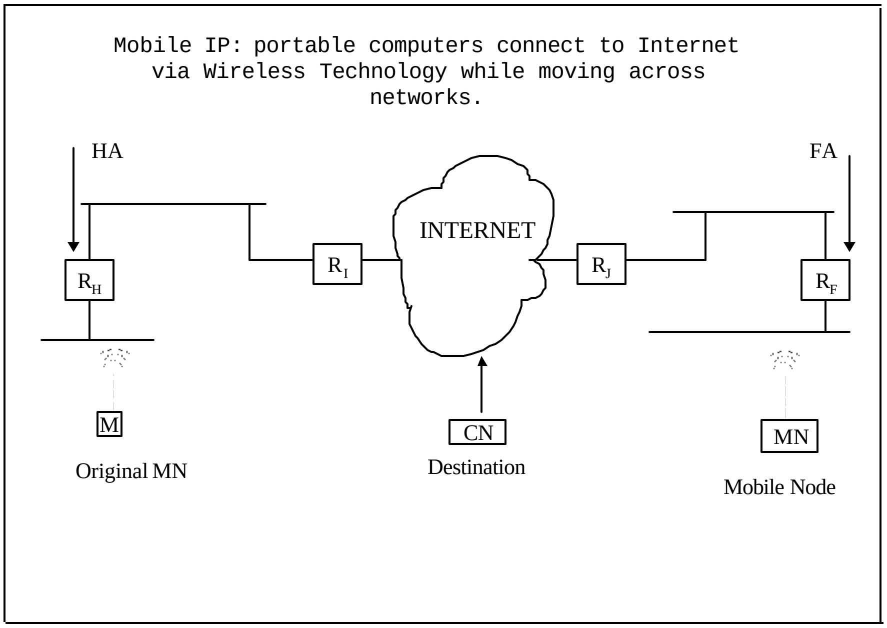
Mobile IP Security

Shihe Wang

1. What is Mobile IP?

Mobile IP (or IP mobility support): Portable computers connect to Internet using wireless technology while moving across one network to another.



Mobile IP: portable computers connect to Internet via Wireless Technology while moving across networks.

Among the Figure:

MN: Mobile Node. Such as portable computers in the link are called Mobile Nodes, which may be reached by their home link.
HA: Home agent. MN’s home link with which MN registers a primary or permanent address.
FA: Foreign Agent. An agent on a foreign network with which MN connects.
CN: Correspondent Node. A node on either foreign network or home network or other network with which MN communicates.

2. How does mobile IP work?

Mobile IP works in this way: a MN is allowed to have two addresses simultaneously. Primary one obtained at home network is fixed and permanent, just as a stationary node’s IP address. The second

obtained from a foreign agent is temporary one, which is called care-of address. It changes as the MN moves.
While attached to some foreign link away from home, a MN works associated with its home address and care-of address:

- Receives packets from the correspondent node addressed either to the care-of address or to its home address routed to its location away from home.
- Sends a packet, generally using its home address as the source of the packet for most packets, since Mobile IP is designed to make mobility transparent to such software.

While at home, it acts as same as a stationary host does.

Mobile IP working processes:

- Agent Discovery: To find agents

Home agents and foreign agents advertise periodically on network layer and optionally on datalink, so an MN can detects new routers with the primary movement detection mechanism. After detecting that it has moved from one link to another (i.e., its current default router has become unreachable and it has discovered a new default router), forms a new primary care-of address using one of the on-link subnet prefixes advertised by the new router.

- Registration

MN registers its care-of address with home agent either directly or through foreign agent in order to make this its primary care-of address.
Home agent sends a reply it via FA.
A Binding Update Request message sent to MN from HA, or FA or CN. MN sends a Binding Update to at any time to HA, CN and FA to allow them to cache its current care-of address. And then MN will receive Binding Acknowledgment from them.

- Return to Home: deregisteration

MN deregisters with home agent sets care-of-address to its permanent IP address. Deregistration with foreign agents is not required because the care-of address expires automatically. Simultaneous registrations with more than one COA are allowed (for handoff).

3. Security Issues

Since the environment of mobile computing is quite different from the ordinary computing environment, mobile IP has more security problems. Because wireless link and moving, MIP is particularly vulnerable to:

- passive eavesdropping,

- active attacks, and
- More susceptible to loss or theft.

4. Protection Measurements

Mobile IPv6 worked out by an IETF group requires: all IPv6 nodes implement strong authentication and encryption features to improve Internet security. Mobile IPv6 follows the design for Mobile IPv4, using encapsulation to deliver packets from the home network to the mobile point of attachment.

Any packet that includes a Binding Update or Binding Acknowledgment option MUST be protected by IPsec to guard against malicious Binding Updates or Acknowledgment. Specifically, any packet that includes a Binding Update or Binding Acknowledgment option MUST utilize IPsec sender authentication, data integrity protection, and replay protection.

objects	contents	Methods
Binding Updates, Binding Acknowledgment	sender authentication, data integrity protection, reply protection	AH, ESP, AH + ESP

AH: *(*Authentication Header) provides source authentication, and allows the receiver to verify the identity of the sender prevents IP Spoofing.
ESP: (Encapsulated Security Payload) provides data encryption and ensures that data has not been read by anyone except for the intended recipient, prevents Packet Sniffing.

5. My Suggestion

Binding update request is one of the three important messages. MIPv6 does not assign protection to it.

- **It should take Binding update request message into consideration to be protected using AH *(*Authentication Header).**

Necessary? Yes, because packets with Binding Request option opens some issues with binding privacy.
Benefit? Packets with Binding Update Request be authenticated can reduce the vulnerability to be tricked by malicious guys.

Conclusion

Mobile IPv6 designed by IETF has been studied. Based on understanding Mobile IP security, an improvement is suggested:

taking measurement to protect Binding update request message.

References

1. John McHugh, Jim Binkley, the Computer Science Department at Portland State University http://www.cs.pdx.edu/~mchugh
2. Mobile IP Working Group Chairs Phil Roberts <phil.roberts@motorola.com> and Basavaraj Patil <basavaraj.patil@nokia.com>
3. Douglas E. Comer, Internetworking with TCP/IP Vol I: Principle, Protocols, and Architecture, Fourth Edition, Chapter 19
4. Marcos Rogério Salvador, Ron Sprenkels, Gloria Tuquerres (1999) e-mails: {salvador, sprenkels, tuquerre}@cs.utwente.nl , Telematics Graduate School (TGS), Telematics Systems and Services (TSS) Group.