Security Aspects of Mobile IP
Dale Conn
December 17, 1921

Background

Just as mobile or cellular phones evolved from the original wireline telephone system, wireless devices offering Internet Protocol (IP) connectivity are likewise developing. This includes devices such as Personal Digital Assistants (PDA) and handheld computers. This mobile computing should not be confused with portable computing, where computing activities are disrupted when the user changes the computer's point of attachment. Mobile computing continues unbroken as the user or node moves from one link to another. It does this without human intervention and noninteractively. The vocabulary normally used to describe this mobile computing is Mobile IP. The original set of Request for Comments (RFC) describing this model is RFCs 2002 through 2006. The purpose of this white paper is to discuss the security aspects of Mobile IP.

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the development of the Internet architecture and the smooth operation of the Internet. RFC 2002[1], proposed by a working group within the IETF, allows the mobile node to use two IP addresses: a permanent home address and a care-of address that changes at each new point of attachment.

Mobile IP Primer

The most important requirement of Mobile IP is to permit a mobile node to communicate using only its home address while varying its point of connectivity to the Internet. Additionally, a mobile node must impart solid authentication when it updates its home agent of its current location.

Mobile IP defines three functional areas. A *mobile node* is a host or router that can vary its location from one link to another without changing its IP address and without disrupting ongoing communications. A *home agent* is a router with an interface on a mobile node's home link which captures packets destined to the mobile node's home address and tunnels them to the mobile node's latest care-of address. The home address is an IP address that is given for an extended period of time to a mobile node. It remains unchanged regardless of where the node is connected to the Internet. The care-of address is the termination point of a tunnel toward a mobile node for datagrams passed on to the mobile node while it is away from home. The protocol can use two different types of care-of addresses. A "foreign agent care-of address" is an address of a foreign agent with which the mobile node is registered, and a "co-located care-of address" is a local address which the mobile node has linked with one of its own network interfaces. A *foreign agent* is a router with an interface on a mobile node's foreign link which helps a mobile node with movement detection and provides routing services on behalf of mobile nodes, including de-tunneling of encapsulated packets when the mobile node uses the foreign agents care-of address.

Home and foreign agents are typically software products that run on traditional routers or in host computers. Mobile nodes are most common in host computers that are portable, such as notebooks or laptops. It is usual for a single node to be a foreign agent for some mobile nodes while concurrently being a home agent for other mobile nodes.

Home and foreign agents advertise their existence on any attached links by periodically multicasting or broadcasting special Mobile IP messages called Agent Advertisements. Mobile nodes receive these advertisements and inspect their contents to determine if they are connected to their home link or a foreign link. A mobile node connected to a foreign link gets a care-of address. A foreign agent care-of address can be read from one of the fields within the foreign agent's Agent Advertisement. The mobile node registers the care-of address with its home agent, using message-exchange defined by Mobile IP. In the registration development, the mobile node requests service from a foreign agent - one is present on the link. The home agent or some other router on the home link advertises reachability to the network-prefix of the mobile node's home address, thus drawing packets that are intended for the mobile node's home address. The home agent captures these packets and tunnels them to the care-of address that the mobile node registered earlier. At the care-of address, the original packet is removed from the tunnel and then sent to the mobile node. In the reverse direction, packets sent by the mobile node are routed directly to their target, without any requirement for tunneling. The foreign agent serves as a router for all packets created by a visiting mobile node.

Security Primer

To protect computer resources and information from unauthorized access, modification, and destruction is the quintessence of security and requires four features. The technology employed to achieve these security features is called cryptography. The following four paraphrased definitions (features) are reproduced from RFC 1825[2].

CONFIDENTIALITY: To transform data such that it can be decoded only by authorized parties.
AUTHENTICATION: To prove or disprove someone's claimed identity.
INTEGRITY CHECKING: To ensure that data cannot be modified without such modification being detectable.
NON-REPUDIATION: To prove that a source of data did in fact send data that might be later denied.

<u>Cryptology</u>
A cryptographic system is composed of two fundamental components: a complex mathematical function, called an algorithm, and at least one secret or public key[3,4,5]. A key is a string of binary digits that is known only to parties who desire to communicate securely. Cryptographic algorithms fall into two general categories: secret-key and public

key. A secret-key algorithm is one in which the same key is used by both the sender and receiver. A public key algorithm is one which uses a duo of related keys, one by the sender and the other one by the receiver. One of the keys in the pair is kept secret or private, while the other is published publicly. Encryption algorithms are universally used to provide confidentiality.

Authentication is imparted via secret-key encryption and public-key encryption[6,7]. Secret-key encryption falls into two categories. The first is built from the same algorithms that are used to execute secret-key encryption as described above. The second uses a entirely separate category of cryptographic algorithms known as message digests. A message-digest algorithm takes an arbitrarily large piece of data and computes from it a fixed-length piece of data called a message digest. Public-key authentication also falls into two categories. The first is similar to the method used to execute secret-key authentication, except that a public-key encryption is used. The second type of public-key authentication uses digital signatures. A digital signature requires simply performing a public-key conversion on some plaintext message, using the private key. This is called signing the message, and the ensuing ciphertext is called a digital signature. Digital signatures also afford non-repudiation since only the sender has the key, and thus there is no refuting who sent the message. To confirm that a message has not been changed in transit, called integrity checking, the sender simply sends a message, a timestamp, and a message digest.

Security Protocols

The security problems introduced by mobility in general, and Mobile IP in particular, is restricted to the IP-layer security and key management protocols. The Security Architecture for the Internet Protocol, RFC 1825[2], describes a framework for security at the IP layer. Two companion documents, RFC 1826[6] and 1827[8], define the exact packet formats of IP-layer authentication and encryption, respectively.

A security association is paramount to the IP-payer security model. It is an contract between two nodes that specifies how the sender will cryptographically change data before transmitting. A security association includes all of the information required for a receiver to realize how to decrypt a message or prove the authentication contained in the message. The Internet Security Association and Key Management Protocol (ISAKMP) grants a framework by which two parties can collaborate security parameters and set up security associations. The Oakley Key Determination Protocol can be used to set up session keys between these parties.

Simple Key-Management For Internet Protocols (SKIP) is another key management protocol for use with IP-layer security. While ISAKMP/Oakley calls for two nodes to swap a number of protocol messages before they can start communicating securely, SKIP supports a model called inline-keying. This model allows a node to launch session keys with another node in the very same packets that are used to exchange data.

The IP Authentication Header, RFC 1826[6], provides authentication, integrity checking, and possibly non-repudiation of the IP header and payload. The authentication header is ordinarily placed between the IP header and the upper-layer header (e.g., TCP) in order to guard the entire packet against being changed in transit and to authenticate the sender. The value of the security provided by this specification depends on the strength of the cryptographic algorithm that has been put into service, the strength of the key being used, and the precision of that algorithm's implementation. It also depends on the security of the key management methodology and its execution, and upon the precision of the IP Authentication Header and IP implementations in all of the contributing systems.

The IP Encapsulating Security Payload, RFC 1827[8], provides encryption, confidentiality, and possibly authentication and integrity examination of the IP payload. It is used similarly to the Authentication Header, being positioned between the IP and upper-layer header or connecting two IP headers in the case of a tunnel. The value of the security provided by this specification depends on the robustness of the encryption algorithm that has been implemented, the accuracy of that algorithm's implementation, and the security of the key management procedure and its execution. It also depends on the strength of the key and the exactness of the ESP and IP performance in all of the contributing systems.

Firewalls
A firewall is a device that separates a trusted, private network from an untrusted, public network such as the Internet. A firewall protects a private network from intrusion, but should not avert people on the inside from exchanging information with others on the public network. Firewalls fall into three basic categories: packet filtering routers, application-layer relays, and secure tunnelers. A packet-filtering router decides whether to forward a certain packet by looking at the packet's header, consistent with a set of rules. Application-layer relays provide a buffer between the host and the public network. The routers do not permit packets to run directly between the host network and the public network. A secure tunneler is a firewall of the application-layer relay type that also supplies a cryptographically secure process for authorized users to access a private network through a public network.

Security Within Mobile IP

This section looks at specific threats to Mobile IP, and discusses protective measures. The threats include denial-of-service attacks, replay attacks, theft of information or passive eavesdropping, and session-stealing (for theft of information) attack. Because of its significance, tunneling is discussed again as a degree of security within mobile IP.

Denial-of-Service Attack
A denial-of-service (DOS) attack is something done to preclude someone from accomplishing useful work. Typically, a DOS attack takes one of two forms: nuisance packets (TCP SYN flooding), or the preclusion of packets from flowing between two nodes. There is little that can be done to prevent this nuisance packet attack, and the sender can always spoof the source address. However, service providers can filter IP packets in their routers to assure the IP source address of a packet is genuine before it is

forwarded. The consequence is that the starting point of the attack may be traced more accurately with this ingress filtering.

To perform the preclusion of packets flowing between two nodes, the attacker must be on the path between two nodes. If the attacker were to create a bogus Registration Request, stipulating his own IP address as the care-of address for a mobile node, all packets would be tunneled by the mobile node's home agent to the attacker. However, if cryptographically resilient authentication is compulsory by a mobile node and its home agent, there would be no difficulty. Mobile IP lets a mobile node to use the authentication algorithm of their preference. However, all must sustain the default algorithm of KEYED MD5. This authentication method draws on RFC 1321[9] to provide secret-key authentication and integrity checking.

Replay Attacks

It is feasible for an attacker to obtain a copy of a legitimate Registration Request, store it, and then replay it later to accomplish a forged care-of address for a mobile node. To avoid this replay attack from occurring, the mobile node produces a unique value for the identification field in each of the successive endeavors for registration. The identification field is made in such a way as to allow the home agent to ascertain what the subsequent value should be. The attacker is hampered because the identification field in his stored Registration Request will be known as being outdated by the home agent.

Theft of Information or Passive Eavesdropping

This type of attack is against the confidentiality of the information. Encryption is the most common means used to protect data from unauthorized persons. There are at least two ways that data can be protected through encryption. End-to-end encryption is the most thorough way to protect the data. This means encrypting and decrypting the data at the source and destination, as opposed to encrypting/decrypting over the first or last link. Some examples of Internet based applications that provide such end-to-end protection include Secure Remote File Copy (SCP), Secure Sockets Layer (SSL), and Secure Remote Shell (SSH). The Encapsulating Security Payload RFC (1827[8]) affords end-to-end encryption for other application programs that do not provide for encryption themselves. Link-layer encryption is classically used between a mobile node and its foreign agent of a wireless link. In this case, the mobile node and the foreign agent encrypt all packets they trade over the foreign link. Link encryption is particularly significant when the foreign link is a wireless LAN. It is easier to snoop a wireless link because no physical connection is required. RFC 1984[10] has more information on this topic.

Session-Stealing (for Theft of Information) Attack

An attacker performs a session stealing attack by waiting for a valid node to authenticate itself and initiate an application session, then captures the session by masquerading as the legitimate node. Typically, this requires the attacker to transmit numerous nuisance packets to thwart the legitimate node from recognizing that the session has been captured. This type of attack is disallowed by the above two methods of encryption; end-to-end, and link-layer.

Secure Tunneling

Secure tunneling[11, 12] uses a firewall of the applications-layer type that also employs a cryptographically secure method for users to gain access to a private network across a public network. Both the IP Authentication Header and the IP Encapsulating Security Payload should be used. Secure Tunnelers can also be used to create Virtual Private Networks (VPN) across a public network such as the Internet. A VPN behaves as a single, secure, logical network while being made up of numerous physical networks of varying levels of trust. The secure tunnel can shield private networks from being accessed by trespassers while providing confidentiality, which keeps a trespasser from eavesdropping on data exchanged between two networks.

References

1. "IP Mobility Support", C. Perkins, ed., Proposed Standard RFC 2002, Oct. 1996, ftp://ftp.isi.edu/in-notes/rfc2002.txt.

2. "Security Architecture for the Internet Protocol", R. Atkinson, RFC 1825 (Obsoleted by: RFC2401), Aug. 1995, ftp://ftp.isi.edu/in-notes/rfc1825.txt.

3. "The PPP Encryption Control Protocol (ECP) ", G. Meyer, Proposed Standard RFC 1968, Jun. 1996, ftp://ftp.isi.edu/in-notes/rfc1968.txt.

4. "Security Architecture for the Internet Protocol", S. Kent, R. Atkinson, Proposed Standard RFC 2401, Nov. 1998, ftp://ftp.isi.edu/in-notes/rfc2401.txt.

5. "IP Encapsulating Security Payload (ESP) ", S. Kent, R. Atkinson, Proposed Standard RFC 2406, Nov. 1998, ftp://ftp.isi.edu/in-notes/rfc2406.txt.

6. "IP Authentication Header, R. Atkinson", RFC 1826 (Obsoleted by: RFC2402), Aug. 1995, ftp://ftp.isi.edu/in-notes/rfc1826.txt.

7. "IP Authentication Header", S. Kent, R. Atkinson, Proposed Standard RFC 2402, Nov. 1998, ftp://ftp.isi.edu/in-notes/rfc2402.txt.

8. "IP Encapsulating Security Payload (ESP) ", R. Atkinson, RFC 1827 (Obsoleted by: RFC2406), Aug. 1995, ftp://ftp.isi.edu/in-notes/rfc1827.txt.

9. "The MD5 Message-Digest Algorithm", R. Rivest, Informational RFC 1321, Apr. 1992, ftp://ftp.isi.edu/in-notes/rfc1321.txt.

10. “IAB and IESG Statement on Cryptographic Technology and the Internet”, IAB, Informational RFC 1984, Aug. 1996, ftp://ftp.isi.edu/in-notes/rfc1984.txt.

11. “Reverse Tunneling for Mobile IP”, G. Montenegro, ed., Standards Track RFC 2344 (Obsoleted by: RFC3024), May 1998, ftp://ftp.isi.edu/in-notes/rfc2344.txt.

12. “Reverse Tunneling for Mobile IP, revised”, G. Montenegro, Proposed Standard RFC 3024, Jan 2001, ftp://ftp.isi.edu/in-notes/rfc3024.txt.