G. Montenegro
Sun Microsystems, Inc.

August 25, 1997

Tunnel Set-up Protocol (TSP)

draft-montenegro-tsp-00.txt

Status of This Memo

Abstract

Remote access over the internet and IP mobility are currently being addressed as two separate problems. The L2TP specification is defining a protocol, or rather a tunnel control mechanism to solve the remote access problem. On the other hand, the Mobile IP working group has been solving the mobility problem. Nevertheless, the same solution applies to both problems, namely, tunneling.

This document defines a Tunnel Set-up Protocol (TSP) that solves both problems using a common approach. TSP is heavily based on the control messages defined by Mobile IP.

Table of Contents

1. Introduction

1.1. Motivation

The Mobile IP protocol has great provisions for dynamic tunnel set up to effect Layer 3 forwarding (IP packet forwarding). The purpose is to dynamically and securely set up an IP packet forwarder (the "home agent" functionality) toward a current point of attachment (the "care-of address") of a roaming system.

Notice that if the packet forwarder happens to be the home agent of the device, then we are dealing with Mobile IP. However, there are very good reasons to use the same protocol to establish a packet forwarder at, for example, the border of a private net. This allows a remote device to appear to be within the confines of the private network, albeit at its periphery. Doing so, and using IP security to authenticate and encrypt the data traffic, presents a homogeneous and simple solution to two fundamental problems in the internet:

- mobility

- secure remote access over the internet.

Another characteristic of Mobile IP that plays perfectly in the remote access arena is the foreign agent. Many service providers need exactly this as a point of control for billing purposes.

However, there are certain limitations that must be addressed in order to achieve a homogeneous solution to the problems listed above.

Current Mobile IP lacks flexibility in how registrations are accomplished in that it assumes that the endpoints of the tunnel are mutually trusting entities that are able to and willing to exchange registration protocol packets.

Furthermore, it assumes that the mobile node creates the Registration Request. TSP addresses these issues by allowing the creation of compound tunnels. TSP recognizes that in addition to tunnel endpoints, there may be tunnel intermediate points. Registrations are exchanged only between intermediate points. The result is a composite tunnel with some very desireable security and scalability characteristics:

- Different security domains interface at an intermediate point, which provides a clean separation between segments.

- Movement beyond a certain intermediate point only implies re-registrations from that point onward.

1.2. Terminology

This discussion uses terms defined by Mobile IP [Perkins96a]. Additionally, it uses the following terms:

Chained Registration

A registration in which the home agent and the mobile node do not directly exchange a Registration Request and Reply. Rather, the request/reply is carried out between endoints of tunnel segments. The composition of tunnel segments represents the compound tunnel from home agent to mobile node.

Surrogate Registrations

These are registrations that are not created by the mobile node. Rather, they are created on its behalf by another entity (a foreign agent). This is not a new concept and is in use in commercial implementations. Nevertheless, with its introduction of chained registrations and compound tunnels, this document allows for registrations that neither originate at the mobile node (i.e. they are surrogate registrations), nor do they terminate at the home agent (i.e. they terminate at an intermediate point at least one tunnel away from the home agent).

Upstream Agent

The endpoint of a tunnel segment that is closest to the home agent. The last upstream agent is the home agent itself.

Downstream Agent

The endpoint of a tunnel segment that is closest to the mobile node. The last downstream agent is the mobile node itself.

1.3. Related Work

VTP (Virtual Tunneling Protocol) [Calhoun96] also uses Mobile IP as a basis for a tunnel set-up protocol. The registrations composed by VTP's "proxy mobile nodes" are essentially surrogate registrations.

Chained registrations add the flexibility that the registration request need not end at the home agent, but at an intermediate system (an upstream agent).

There has been some work on enabling secure mobile remote access using SKIP [MoGu97]. Subsequently, the Mobile IP Working Group is extending these efforts and defining a solution based on ISAKMP/OAKLEY [GuGl97a, GuGl97b]. However, these documents still assume that the mobile node and the home agent exchange Registration Protocol packets directly. True, they may tunnel or relay them through participating firewalls, but the latter are merely IP Security aware devices, unaware of Mobile IP. TSP allows for firewalls to be Mobile IP aware so they can serve as endpoints of tunnel segments.

However, TSP does not require the use compound tunnels, as this is a policy issue. When they are not required, secure remote mobile access may be accomplished along the lines proposed by the documents in the previous paragraph.

1.4. Design Goals

One of the main objectives in defining TSP is to support Mobile Network Computers [MNCRS]. Given that these devices are meant to be very lightweight and to keep as little state as possible, TSP's design goals are:

- Simplicity.

  TSP only defines the minimum required to support the additional applications and target devices. Surprisingly little needs to be specified in order to adapt Mobile IP to serve as a remote access mechanism based on layer 3 forwarding.

- Reusability.

  Unless otherwise specified, TSP adopts packet formats and protocol behavior as specified by Mobile IP. This results in one protocol that solves mobility and remote access.

- Security.

  Given the nature of remote access, security associations are required of entities exchanging Registration Protocol packets over public sectors of the internet. Privacy of data transfer is also a requirement in these conditions, and is accomplished by using ESP [Kent97a] and AH [Kent97b].

2. Overview

2.1. Base Mobile IP

Mobile IP [Perkins96a] defines 3 entities: mobile node (MN), foreign agent (FA) and home agent (HA).

The idea is that a mobile node is always able to use its permanent IP address ("home address"), even if it is not "home" (the logical location of its IP address). When the mobile node moves to another region of the internet, it's home address is no longer usable, as the routing fabric still delivers packets to its home location. In a manner similar to how one leaves forwarding indications at the post office when out of town, the mobile node engages in a secure "registration" with the home agent. Once this forwarding indicator or "binding" is in place, the home agent intercepts all packets destined for the mobile node and forwards them to the foreign agent currently being visited by the mobile node. In essence, the foreign agent lends the mobile node its topologically correct address ("care-of address").

The home agent forwards packets destined for the mobile node by adding another IP header so the routing fabric sees the home agent's address as source and the care-of address as destination. Once at the care-of address, the original packet meant for the mobile node is recovered and delivered without recourse to regular routing. Notice that the mobile node may possibly acquire the care-of address necessary for tunneling. In this case, there is no separate foreign agent, rather, the mobile node serves as its own tunnel endoint.

This "local" delivery from the foreign agent to the mobile node is possible because it does not rely on traditional network layer routing.

2.2. Chained Registrations

Base Mobile IP assumes that the foreign agent is directly reachable from the home agent. In many situations this is not possible or desirable. For example, if the foreign agent belongs to an ISP, or a wireless carrier, it is not desirable to allow it direct reachability to a system (the HA) that "lives" within the private network.

A much more secure configuration is to allow the ISP's system to directly reach only as far as the private network's gateway or firewall. These two systems need to share some mutual trust,

particularly if using surrogate registrations.

Another separate trust relationship is then built between the gateway or firewall system, and the home agent inside the private network. Notice that by introducing this intermediate system there is a very clean separation between external and internal systems security domains.

This configuration is possible because of the use of chained registrations, whereas usual registration requests flow directly from the mobile node to the home agent.

2.3. Surrogate Registrations

Surrogate registrations are composed on behalf of a given node by another node. Consider the following network:

```
MN@COA  ---------------------- GFA ----- HA
```

where the mobile node has acquired a co-located address (COA). Assume that the mobile node is not allowed to exchange packets directly with its home agent within the private network. Instead, it sends a Registration Request to the gateway foreign agent (GFA) as follows:

```
MN@COA, home agent = GFA.
```

The gateway foreign agent is not, of course, the mobile node's home agent. Nevertheless, it has knowledge or can obtain knowledge (perhaps after consulting a RADIUS database) of the mobile node's home agent. It then composes a Registration Request aimed at establishing a tunnel with the home agent:

```
MN@GFA, home agent = HA.
```

From the home agent's point of view, this registration request is almost indistinguishable from what it would have received from the MN directly. Notice that when the mobile node roams within the private network, mobility is probably accomplished without surrogate registrations. Hence, Registration Requests like the above are sometimes sent directly by the mobile node to the home agent.

The target system can always tell the identity of the system that composes a Registration Request by the value of the SPI. If the target system is the home agent, a security association is already required by Mobile IP. However, intermediate nodes may set up tunnel segments with other intermediate nodes.

Because the SPI is the only way to identify the creator of a Registration, TSP requires that entities setting up tunnel segments MUST share a security association. Since surrogate registrations have exactly the same format as registrations issued by the mobile node itself, they MUST use the Mobile-Home Authentication Extension as dictated by Mobile IP.

3. Dynamic Home Address Discovery

It is possible for a mobile node to not have a permanently assigned IP address. This is the default operating condition for a Mobile Network Computer.

3.1. Registering over the Internet

When a Mobile Network Computer tries to register over the internet, it may not have a valid IP address (because it is booting instead of resuming, or because its lease ran out). TSP defines a home address discovery mechanism akin to the home agent discovery mechanism defined by Mobile IP. In both cases, a registration denial carries the necessary information (see Section 5).

3.2. Registering within the Corporation

In this case, the Mobile Network Computer boots using the Network Computer model of obtaining its operating parameters from a DHCP server. One of the parameters received is the IP address to be used. The Mobile Network Computer must make sure that it receives an IP address valid for roaming as a Mobile IP node, i.e. it must be an address that a home agent is willing to provide forwarding service to [Alex97]. The home agent could also be communicated using DHCP, or it could be discovered using the home agent discovery mechanism in [Perkins96a].

4. New Packet Formats

This section specifies packets formats that are different or new as compared to those defined by Mobile IP [Perkins96a] and Reverse Tunneling [Monten97].

4.1. Mobile Node Identifier Extension

If the mobile node is using a co-located care-of address, the

Registration Reply is delivered directly to it.

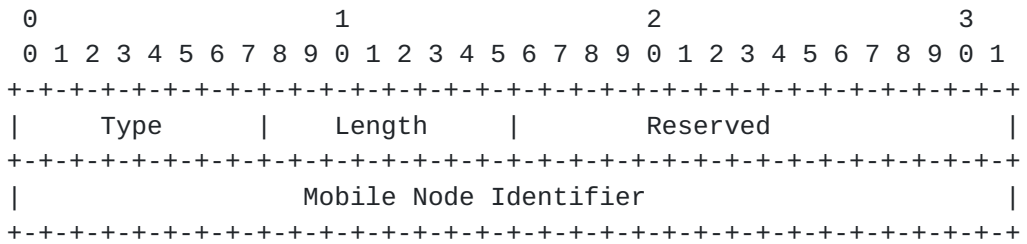
On the other hand, if the care-of address belongs to a foreign agent, it uses the mobile node's home address and the ID field in the Registration Reply to determine which link-layer address to relay it to. However, if the mobile node is carrying out dynamic home address discovery, then the foreign agent can only rely on the ID field, which is not guaranteed to be unique. The foreign agent (or downstream agent) MUST add some extra information to Registration Requests to uniquely identify the mobile node. The home agent (or upstream agent) MUST return this identifier for the foreign agent to be able to resolve which mobile node it is intended for.

The Mobile Node Identifier Extension defined below serves this purpose.

The Mobile Node Identifier Extension MUST appear before the TSP-required Foreign-Home Authentication Extension. It SHOULD appear immediately before it.

As per section 1.9 of [Perkins96a], the type value of 130 implies that if a node encounters a Mobile Node Identifier Extension in a Registration Request or Reply, it MAY silently ignore it. This implies that home agents that comply with Mobile IP, but are unaware of the TSP extension MAY still be used, as long as the mobile node does not attempt home address discovery.

TSP home agents that support Mobile Network Computers MUST understand the Mobile Node Identifier Extension and return it in its replies. The reason is that Mobile Network Computers may attempt to register using a certain home address whose DHCP lease may have expired. Furthermore, two or more Mobile Network Computers may attempt to use the same home address. Without the Mobile Node Identifier Extension the foreign agent (or downstream agent) may be unable to resolve the conflict.



Type

130

Length

6

Reserved

0

Mobile Node Identifier

A pseudo-random number created by the tunnel initiator (e.g. foreign agent) as a unique identifier of the mobile node.

NOTE: This is not optimized for the usual case. Should try to do so, perhaps by claiming the last unused bit in the "rsvd" field of the Registration Request to mean "it is ok to assign me a new home address". Only if this bit were on would the Mobile Node Identifier Extension be needed.

4.2. "Invalid Home Address" Error Code

In order to support dynamic home address discovery, we define a new error code:

Service denied by the home agent:

140 invalid home address

Notice that "invalid" home address includes two cases:

1. mobile node requires an address assignment,

2. mobile node's lease on its previous address has expired.

An "invalid home address" denial carries the assigned home address in the home address field of the registration reply.

5. Protocol Behavior

Unless otherwise specified, TSP assumes the behavior defined by Mobile IP [Perkins96a]. TSP operates in two different modes:

1. When operating within a private network, TSP MAY adopt the same protocol behavior as Mobile IP, that is, there are no surrogate registrations, compound tunnels or home address assignment.

2. However, when setting up a compound tunnel, or when a tunnel traverses a public sector of the internet, bi-directional tunnels MUST be used. This MAY be accomplished by using either reverse tunneling [Monten97] or GRE [Hanks94]. In this case, all Registration Requests and Replies MUST include the proper Authentication Extension. Also, dynamic home address discovery while using the services of a separate foreign agent implies the use of the Mobile Node Identifier Extension.

[gab: must add more detail]

6. Data Transfer: Tunneling Modes

The Registration Protocol defined in [Perkins96a] and the extensions specified in this document enable tunnels to be set up in an authenticated fashion. However, there is still the separate matter of sending data through the tunnels.

Mobile Network Computers MUST use IP in IP encapsulation [Perkins96b] preferrably using reverse tunneling [Monten97]. Other types of mobile nodes MAY specify GRE [Hanks94].

However, one of the main applications of TSP is remote access. Accordingly, tunnels that traverse public sectors of the internet MUST be protected by using ESP [Kent97a] and AH [Kent97b]. Manual keying MUST be supported. Key management MUST use either SKIP [Aziz95] or ISAKMP/OAKLEY [ISAKMP, OAKLEY, ISAOAK]. The exact mechanism is not determined via Registration Protocol exchanges.

Tunnels that traverse private sectors of the network MAY optionally protect their traffic in similar fashion.

7. Example Scenarios

7.1 TSP as a Mobile Remote Access Solution

Chained registrations flow in separate steps which together build one compound tunnel. For example, assuming there is only one intermediate point (or "traversal point"), labelled GFA ("gateway foreign agent"), this is how the chained registration would work:

EXAMPLE: TSP for Mobility and Remote Access

MN -- FA ---------------------- GFA ----- HA

a. The MN sends a registration request to the FA with the following information:

   name: MN
   care-of address: FA
   home agent: GFA

b. The FA then forwards this registration to the "home agent", i.e. to GFA. Notice that GFA is not a home agent in the traditional sense, because it's address and MN's do not belong to the same subnet. Also notice that the FA could have composed the above registration on behalf of the MN (the so-called "surrogate registration"). At any rate, whoever composes the registration request must share a secret with GFA, as this is needed to fill correctly the authenticator field of the registration request (not shown above).

c. GFA verifies the authentication for this registration and fetches the information contained therein. It notices that it is listed as the home agent for the MN, which is not really true. However, it checks its database, and obtains information that MN's real home agent is HA, with which it can engage in yet another authenticated registration protocol exchange ("chained registration").

   GFA sends the following registration to HA:

   name: MN
   care-of address: GFA
   home agent: HA

   Notice two things:

   1. This registration is composed by the GFA on behalf of the MN, so it is a surrogate registration.

   2. If GFA is indeed the home agent for the mobile node at this point Remote Access has been accomplished.

d. HA verifies the authentication for this registration and notices that it is indeed valid (it is possible for HA and GFW to use a shared secret different from the one used by HA and MN). It then establishes a "tunnel" (i.e an IP forwarder) of MN's packets to GFA.

Once this chained registration is in place, this is how data transfer may occur:

a. A correspondent node, CN, sends a packet to the MN with the following IP header:

```
IP source:              CN
IP destination:         MN
```

b. The packet arrives in the vicinity of HA, which intercepts and forwards it to GFA by prepending a new IP header like this:

```
New IP source:          HA
New IP destination:     GFA
```

c. GFA receives the packet, recovers the original packet:

```
IP source:              CN
IP destination:         MN
```

and notices that it has a binding or registration for MN. This prompts GFA to forward the packet, this time with the following new IP header prepended to it:

```
New IP source:          GFA
New IP destination:     FA
```

d. FA obtains the packet, recovers the inner, original packet:

```
IP source:              CN
IP destination:         MN
```

and notices that is has a binding or registration for MN. This time, it just forwards without any additional headers because MN is directly reachable.

e. MN receives the packet:

```
IP source:              CN
IP destination:         MN
```

which from the point of view of its applications is exactly the same packet they would have received if MN had been in its office. Thus mobility is transparent.

7.2 Registering Without a Permanent Home Address

Assume that the mobile node is a Mobile Network Computer, and as such, does not have a permanent home address. If at home, it

typically acquires an address via DHCP for use during that session. The notion of session, however, does not necessarily imply a certain time limit. As long as the Mobile Network Computer renews its DHCP lease, it can continue to use the assigned address. If it reboots again, it will need a new address, but this is probably a very rare ocurrence. Instead of rebooting, what is customary is for a Mobile Network Computer to suspend its state and resume it at a later time. At that time, it will attempt to use the same address as it was using when it suspended its state. It's DHCP lease may have expired, or it may even ignore what to use as a home address. At this point, it establishes a presence on the public internet, perhaps by starting a PPP session with an ISP. It needs to obtain a new home address.

This is what it knows:

*1. the home prefix is known
2. HA is known
3. secret is known
4. care-of address is known
*5. care-of address is co-located

This is what it wishes to find out:

1. MN home address

The mobile node issues this Registration Request:

IP fields:
Source Address = co-located care-of address
Destination Address = IP address of home agent
Time to Live = 64
UDP fields:
Source Port = <any>
Destination Port = 434
Registration Request fields:
Type = 1
S=0,B=x,D=1,M=x,G=x
Lifetime = 1800 (seconds)
Home Address = the mobile node's home prefix
Home Agent = IP address of mobile node's home agent
Care-of Address = co-located care-of address
Identification = timestamp
Extensions:
The Mobile-Home Authentication Extension

The home agent sees that the home address field is not completely

filled out, obtains a new address within the indicated prefix and returns it to the mobile node using this reply:

Upon return:

IP fields:
Source Address = IP address of home agent
Destination Address = co-located care-of address
Time to Live = 64
UDP fields:
Source Port = <any>
Destination Port = copied from src port or reg req
Registration Reply fields:
Type = 3
Code = 140 (invalid home address)
Lifetime = 1800 (seconds)
Home Address = the mobile node's newly assigned home address
Home Agent = IP address of mobile node's home agent
Identification = timestamp
Extensions:
The Mobile-Home Authentication Extension

Notice that it is possible to discover both the home agent and the mobile node addresses:

Now, this is what the Mobile Network Computer knows:

*1. the home prefix is known
*2. HA prefix is known
3. secret is known
4. care-of address is known
*5. care-of address is co-located

And this is what it wishes to find out:

1. HA address
2. MN home address

It issues this Registration Request:

Registration Request fields:
Type = 1
S=0,B=x,D=1,M=x,G=x
Lifetime = 1800 (seconds)
Home Address = the mobile node's home prefix
Home Agent = directed broadcast to HA's prefix
Care-of Address = co-located care-of address
Identification = timestamp

Extensions:
The Mobile-Home Authentication Extension

An initial reply with code 136 (unknown home agent address) tells the mobile node which home agent to use. Subsequently, the mobile node may discover its own home address. It must first discover the home agent address because the latter must be willing to provide some address allocation services on the mobile node's behalf.

We could also use a separate foreign agent:

In this case, these are the known quantities:

*1. the home prefix is known
*2. HA prefix is known
3. secret is known
4. care-of address is known

In this case, the foreign agent uses a Mobile Node Identifier Extension (Section 4.1.2) to determine which mobile node to send replies to. Notice that it is presumed that an foreign agent learn the mobile node MAC address from snooping the Registration Request.

8. Security Considerations

This document is very heavily based on Mobile IP. Tunnel Set-up Protocol focuses on additional applications, namely, remote access. Because of this, items which may be optional in basic Mobile IP become absolute requirements for TSP. The registration protocol messages MUST always be authenticated. This means that there MUST always be a security association between both endpoints of any given tunnel segment.

References

[Aziz95] A. Aziz and M. Patterson, Design and Implementation of SKIP, available on-line at http://skip.incog.com/inet-95.ps. A previous version of the paper was presented at INET '95 under the title Simple Key Management for Internet Protocols (SKIP), and appears in the conference proceedings under that title.

[Calhoun96] P. Calhoun, E. Wong. Virtual Tunneling Protocol -- work in progress, draft-calhoun-vtp-protocol-00.txt,

July 1996.

[GuGl97a] V. Gupta and S. Glass, "Firewall traversal for Mobile IP: Goals and Requirements". -- work in progress, draft-ietf-mobileip-ft-req-00.txt> -- work in progress, January 1997.

[GuGl97b] V. Gupta and S. Glass, "Firewall traversal for Mobile IP: Guidelines for Firewalls and Mobile IP entities" -- work in progress, draft-ietf-mobileip-firewall-trav-00.txt, March 1997.

[Hanks94] Hanks, S., Li, R., Farinacci, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 1701, October 1994.

[ISAKMP] Maughhan, D., Schertler, M., Schneider, M., and Turner, J., "Internet Security Association and Key Management Protocol (ISAKMP)", draft-ietf-ipsec-isakmp-08.{ps,txt}, July 1997.

[ISAOAK] Harkins, D., Carrel, D., "The resolution of ISAKMP with Oakley", draft-ietf-ipsec-isakmp-oakley-04.txt, July 1997.

[Kent97a] S. Kent, R. Atkinson. IP Encapsulating Payload -- work in progress, draft-ietf-ipsec-esp-v2-00.txt, July 1997 (obsoletes RFC 1827, August 1995).

[Kent97b] S. Kent, R. Atkinson. IP Authentication Header -- work in progress, draft-ietf-ipsec-auth-header-01.txt, July 1997 (obsoletes RFC 1826, August 1995).

[MNCRS] Mobile Network Computer Reference Specification, June 1997. http://www.internet.ibm.com/computers/networkstation/os/mncrs.html

[Monten97] G. Montenegro, "Reverse Tunneling for Mobile IP" -- work in progress, draft-ietf-mobileip-tunnel-reverse-04.txt, August 1997.

[MoGu97] G. Montenegro and V. Gupta, "Firewall Support for Mobile IP". -- work in progress, draft-montenegro-firewall-sup-01.txt, July 1997.

[OAKLEY] Orman, H., "The Oakley Key Determination Protocol", draft-ietf-ipsec-oakley-02.txt, July 1997.

[Perkins96a] C. Perkins, Editor. IP Mobility Support. RFC 2002.

[Perkins96b] C. Perkins, Editor. IP Encapsulation within IP. RFC 2003.

[Alex97] S. Alexander, R. Droms. DHCP Options and BOOTP Vendor Extensions. RFC 2132.

Author and Chair Addresses

Questions about this document may be directed at:

Gabriel E. Montenegro
Sun Microsystems, Inc.
an Antonio Road
Mailstop UMPK 15-214
Mountain View, California 94303

Voice: +1-415-786-6288
Fax: +1-415-786-6445

E-Mail: gabriel.montenegro@eng.sun.com

The working group can be contacted via the current chairs:

Jim Solomon
Motorola, Inc.
1301 E. Algonquin Rd. - Rm 2240
Schaumburg, IL 60196

Voice: +1-847-576-2753
Fax: +1-847-576-3240
E-Mail: solomon@comm.mot.com

Erik Nordmark
Sun Microsystems, Inc.
901 San Antonio Road
Mailstop UMPK17-202
Mountain View, California 94303

Voice: +1-415-786-5166
E-Mail: erik.nordmark@eng.sun.com