MIF Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 30, 2012

D. Migault
Francetelecom - Orange
C. Williams
MCSR Labs
March 29, 2012

Multiple Interfaces IPsec Security Requirements
draft-mglt-mif-security-requirements-01.txt

Abstract

ISPs wants to take advantage of MIF Transport protocols like SCTP, MPTCP to enhance their End User's experience when the End User has been offloaded on WLAN. In addition, WLAN are untrusted so ISPs MUST Secure at least some of their End Users's communications. For various reasons IPsec is the protocol they choose to secure the communications. Currently, IPsec is not adapted to Multiple Interfaces Environment. IPsec can hardly be configured in a proper way which may result in breaking End Users' communications. At least, it makes it very hard for the End Users to combine Security with MIF enhancements. MOBIKE partly address the problem for a single Interface. This draft provides the problem statement and defines the IPsec Security Requirements for MIF.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 30, 2012.

Copyright Notice

Table of Contents

1. Requirements notation 3
2. Introduction 3
3. Problem Statement 3
3.1. Adding Interfaces Dynamically 3
3.2. Removing Interfaces Dynamically 4
3.3. Multihoming 5
3.4. Hard Handover Mobility 5
3.5. Soft Handover Mobility 5
3.6. Selecting Traffic 6
3.7. Conclusion 6
4. Multiple Interfaces Offload Security Requirements 7
5. Position toward MOBIKE 9
6. Security Considerations 10
7. IANA Considerations 10
8. Acknowledgment 10
9. Normative References 10
Authors' Addresses 11

1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Introduction

Current Radio Access Network (RAN) infrastructure will not be able to deal with the next future traffic increase. Consequently ISPs are willing to offload the RAN traffic on alternate networks like WLAN. RAN and WLAN have different characteristics, and compared to RAN, WLAN may be untrusted, unreliable and the Network Interface management is performed by the End User (EU). As a consequence, when a EU switches a non-secured communication from RAN to WLAN, it MUST be able to secure it. Then communications on WLAN takes advantage of Multiple Interfaces to enhance the EU experience on WLAN. Thus, such communications MUST have their security appropriately configured to keep the communication secured and avoid that Security breaks the communication.

Section Section 3 describes the Problem Statement: an IPsec secured communication cannot benefit from MIF features. Then, section Section 4 provides the IPsec Security Requirements for Multiple Interfaces, Mobility and Multihoming. Section Section 5 positions MOBIKE [RFC4555] toward the Security Requirements, and provides the additional features MUST be defined for MOBIKE.

3. Problem Statement

3.1. Adding Interfaces Dynamically

The EU may be connected through multiple WLAN Access Points for bandwidth aggregation. Eventually, splitting flows among various Access Points may also be one way to overcome WLAN Access Points unreliability. The EU may be able to add or remove an Interface on a given communication. Protocols like SCTP or MPTCP have especially been designed for that purpose. In fact, SCTP through AS-CONF message is able to dynamically add Interfaces to a given SCTP association.

When the EU is being offloaded, the communication may be secured with IPsec. In this draft we consider two scenarios: (1) One where the communication is encapsulated to a Security Gateway through multiple IPsec tunnels (one per Interface). This scenarios may not require the Server to see the EU with Multiple Interfaces. (2) The other

scenario considers a communication where the EU is connected via Multiple Interfaces directly to the Server. In that case, the communication is secured with IPsec transport mode. The main motivation for using End-to-End security is to limit Security Gateway latencies and limit the security overhead.

When the nodes discovers a new Interface, we expect that IPsec adds this Interface. From the existing IPsec Security Associations related to the communication, IPsec MUST be able to derive for both the EU and the Server the IPsec configuration for the ADDed Interface. More specifically, if the EU is connected to a Security Gateway, the EU MUST configure a new IPsec Tunnel so that the communication can be tunnelled from the new Interface to the Security Gateway. With communication, we mean that the EU may send or receive packets related to the communication. If the EU is directly connected to the Server, the EU MUST configure IPsec so that the communication can be also protected by using the new Interface. Note that IPsec does not define which interface SHOULD be used. IPsec is configured so that other protocols in charge of carrying the traffic may be able to choose one or the other Interface.

Currently IPsec does not provide such mechanisms. This means that any time the EU discovers an Interface, it will have to initiate an IKEv2 negotiation that authenticates the EU and the Server and derives the key material. We want to avoid multiple negotiations for a given communication.

An alternative would be to use MOBIKE Multihoming, which provides the opportunity to the EU to add the new Interface with the ADDITIONAL_IP*_ADDRESS Notify Payload. This would make the new Interface being considered as an Alternate Interface. In other words, this Interface could be used only if the EU would become unreachable on the running Interface. This does not provide Multiple Interfaces. A single Interface is used at a time, and this is what MOBIKE has been designed for. Furthermore MOBIKE only considers the Tunnel mode, which would only address the Security Gateway scenario.

3.2. Removing Interfaces Dynamically

The EU may use Multiple connections on WLAN, section Section 3.1 explains why the EU may be able to dynamically ADD interfaces to a given communication. Similarly, this section shows that the EU MUST also be able to REMOVE Interfaces from a communication. There may be multiple reasons to REMOVE an Interface. The Interface may not be reachable, the EU may not want to use this Interface anymore... On a security point of view, when an Interface is not used for a secure communication, IPsec MUST explicitly DISCARD all traffic on that Interface.

Currently IKEv2 provides the possibility to DELETE a Security Association. However, this requires a per Security Association Negotiation. With frequent Interface changes, and the Multiple Interfaces of the EU, this negotiations require too many Notify Payload. The EU, simply wants to advertise the Server to REMOVE an Interface with a single Notify Payload.

MOBIKE overcomes this management issue by using a single Interface. Consequently there is only one active Interface.

3.3. Multihoming

Multihoming is the ability to provision Interfaces in case the running Interface is not reachable anymore. For a secure communication, the EU wants to provide one or a range of Alternate IP addresses that MUST be used in case the Primary Interface is not reachable. The difference with ADDing an interface to an given communication is that with Multihoming the Alternate MUST be used only if the Primary Interface is not reachable. On an IPsec point of view, it means that IPsec MUST be configured to DISCARD any packets of the communication unless the Primary Interface is not reachable. When the Primary Interface is not reachable, then IPsec MUST be configured to PROTECT or BYPASS the traffic for the given communication.

Currently MOBIKE provides Multihoming. However, MOBIKE does not make possible to assign a list of Alternate Interfaces to a specific communication. The reason is that MOBIKE only considers a single working interface.

3.4. Hard Handover Mobility

Hard Handover Mobility is the ability for a host to update an Interface with another. This generates the packets of the Network to be discarded. In an IPsec point of view, updating the Security Association results in DISCARDing packets sent or received on the new Interface, and accepting (BYPASSing or PROTECTing) packets on the old Interface not anymore used.

IPsec with MOBIKE provides this facility. However, it is only provided for the Tunnel mode.

3.5. Soft Handover Mobility

Soft Handover is the ability to switch from an old Interface to the a new Interface with a state where both old and new Interfaces can send or receive traffic so to avoid loosing the packets in the network. Soft Handover can be done with a combination of ADD and REMOVE

operations described in section Section 3.1 and section Section 3.2

As mentioned in section Section 3.1 and section Section 3.2, they are currently NOT handled by MOBIKE.

3.6. Selecting Traffic

The EU MUST be able to ADD / REMOVE an Interface, to provide Alternate Interface for Multihoming, or perform some Mobility with Soft Handover or Hard Handover. However in the previous sections such operations have been considered as a global policy for the EU. In fact the EU may not have the same policy for all its traffic. Thus such operations MUST be provided for a given traffic. Motivations may be that the EU may keep some corporate traffic inside a corporate network (private IP addresses, confidentiality...) whereas Internet traffic can use any Interface and especially the one providing the highest bandwidth.

MOBIKE does not provide this kind of facility since it considered a single Interface in use.

3.7. Conclusion

This section address common scenario for an EU being offloaded on the a WLAN. The EU may be connected to a Security Gateway or directly connected to the Service. In both cases, the EU MUST be able to:

- ADD an Interface: When the EU has discovered a new Interface, it MUST be able to add this Interface to its current configuration. This means, that IPsec MUST be configured to be able to receive or send traffic on all its interfaces.
- REMOVE an Interface: When the EU notice that one Interface is not active, it MUST be able to remove this Interface to its current configuration. This means that IPsec MUST NOT PROTECT any traffic on this Interface.
- Mobility: The EU MUST be able to perform Hard Handover as well as Soft Handover.
- Multihoming: When one link fails, the EU MUST be able to automatically switch the traffic to an Alternate IP address. This means that IPsec MUST be configured to be able to receive or send traffic on that Interface.
- Traffic Selectors: The EU MUST be able to perform all the above operations globally or for a given traffic. Thus, it MUST be able to indicate which traffic the operation MUST be applied to.

4. Multiple Interfaces Offload Security Requirements

Then follows the Multiple Interfaces Offload Security Requirements. Note they only concern the Security layer. The only purpose of those Requirements is to properly configure the EU Security Layer so that the Security Layer does not stall or affect the EU communication. Since this draft considers IPsec [RFC4301] and IKEv2 [RFC5998], Multiple Interfaces, Multihoming and Mobility address two different channels:

- The DATA channel: i.e. EU communication. In that case, Security Requirements means how to secure properly the IPsec Security Policy Database and Security Association Database, so that IPsec do not block the EU communication. This is like configuring a firewall.
- IKEv2 channel i.e. IKEv2 application. IKEv2 is the IPsec application that configures the IPsec Databases. The application MUST be Multiple Interfaces, Multihoming and Mobility aware so to configure properly the IPsec Databases for the DATA channel.

Here are the following Security Requirements:

- Multiple Interfaces:
    - DATA channel: For the DATA channel, Multiple Interfaces means that the EU MUST be able to ADD or REMOVE an IP address to a given secured communication. Suppose an EU has established a communication with a Server using an Interface I_OLD. When it detects an new Interface I_NEW, the EU MUST be able to configure IPsec Databases so that the communication can go through I_OLD or I_NEW without being discarded. Note that how the DATA traffic is handled and effectively routed on one or the other or both Interfaces is out of scope of the draft. Similarly, when the EU is communicating to the Server with Multiple Interfaces, it MUST be able to configure IPsec Databases so that one or multiple interfaces MUST NOT accept / handle any traffic.
    - IKEv2 channel: For the IKEv2 channel, we suppose using one interface is sufficient. The IKEv2 channel only carries signalization messages. If the EU wants to change the Interface for IKEv2, then it SHOULD perform a Mobility.
- Multihoming:
    - DATA channel: For the DATA channel, Multihoming means that the EU MUST be able to provide Alternate Interfaces to the Server. In the case the Primary (or running) Interface fails, the communication with the Server MUST be able to go on on the Alternate Interface. More specifically, this means that when the Primary Interface is detected as being down, the EU and the Server MUST

configure the IPsec Databases so that the communication can use the Alternate Interface. The difference with ADDing and Interface in the Multiple Interfaces case is that until the Primary Interface is down, the Alternate Interface does not receive or transmit any traffic. Alternate Interfaces DISCARD such traffic.

- IKEv2 channel: For the IKEv2 channel, Multihoming means that when the Primary Interface is down, IKEv2 MUST be able to switch to the Alternate Interface to send IKEv2 signalization messages to the Server. Once IKEv2 has recovered from the Primary Interface crash-down, it can proceed to the DATA channel IPsec configuration.

- Mobility:
  - DATA channel: For the DATA channel, Mobility means that the EU MUST be able to UPDATE the IPsec Databases and change an old Interface (I_OLD) by a new Interface (I_NEW). There are two ways to do so. With a Hard Handover, I_OLD is replaced by I_NEW. Packets that are in the network or in the network stack of the Server and EU when the update occurs will be DISCARDED by the EU. With Soft Handover, the EU ADDs I_NEW and configures its IPsec Databases to receive / send traffic on both I_OLD and I_NEW. Then it REMOVEs I_OLD when no traffic is anymore expected on that Interface. Note that Soft Handover is performed according to the Multiple Interfaces Requirements.
  - IKEv2 channel: For the IKEv2 channel, as mentioned in the Multiple Interfaces item, Hard Handover may be sufficient, since the channel only carries signalization messages. Once IKEv2 has moved the IKEv2 channel, it configures IPsec Databases for the DATA channel.
- Traffic Selector:
  - DATA channel: For DATA channel Traffic Selector MUST specify which traffic the Mobility, Multihoming, Multiple Interface action MUST be performed.
  - IKEv2 channel: For the IKEv2, Mobility and Multiple Interface operation may be done with a Hard Handover. However, for Multihoming the channel SHOULD be consider as a specific traffic.

Note that when this draft considers Mobility, Multiple Interfaces or Mobility, only the IPsec configuration is affected. However, in some cases, the configuration of the IPsec Databases may affect the communication of the EU. In fact, if the EU is securing its communication with IPsec and the Tunnel mode, a modification of the outer Interface results in moving the communication. In that case, communication mobility results as a side effect of IPsec Database configuration and this is what is used in MOBIKE [RFC4555]. This case does not happen with the IPsec Transport mode, and the

communication mobility MUST be handled by other protocols then IPsec (application, SHIM6, SCTP, MPTCP...

5. Position toward MOBIKE

Multihoming Security Requirements are partly handled by IPsec MOBIKE [RFC4555] extension. MOBIKE has been designed for the VPN Mobility and Multihoming use case with a single interface. Thus MOBIKE only addresses the Security Gateway, with the IPsec Tunnel mode. More specifically, MOBIKE does neither address the Transport mode, nor the case of Multiple Interfaces.

Here are the Mobility and Multihoming MOBIKE features:

- MOBIKE Mobility: MOBIKE provides Mobility by UPDATING the outer IP address. Because MOBIKE considers a single interface, the UPDATE occurs for both the IKEv2 channel and the DATA channel. Furthermore, Because MOBIKE only considers the Tunnel mode, UPDATing the IPsec Databases results in moving the communication as a side effect. Because the EU has a single interface, Mobility is always a Hard Handover.
- MOBIKE Multihoming: MOBIKE provides Multihoming mechanism. The two peers are able to exchange Alternate IP addresses. In case the the Primary IP address is not reachable, IKEv2 tests the Alternate IP address is still reachable with a COOKIE2 exchange. If the Alternate IP address is still reachable, MOBIKE triggers a MOBILITY and UPDATEs the Primary Address by the Alternate IP address. Because the EU has only a single interface, both DATA and IKEv2 channels are updated. Because MOBIKE only considers the Tunnel mode, only communications with Tunnel mode will be updated.

MOBIKE provides Mobility and Multihoming features. However, MOBIKE currently partly addresses the Security Requirements:

- Multiple Interfaces: This is NOT addressed by MOBIKE. This means that currently EU with communications involving Multiple Interfaces will need to establish an IKE channel on each Interface. This also means that there is no Security Interface Management facilities, and for example Soft Handover is NOT possible.
- Mobility: MOBIKE addresses Mobility only for Hard Handover with IPsec Tunnel mode protection. As a result the Security Gateway Scenario is partly addressed. To completely address it with Soft Handover, MOBIKE needs to be extended for Multiple Interfaces. Furthermore, to address End-to-End security with the Server, MOBIKE also needs to be extended for the Transport mode.

- Multihoming: MOBIKE Multihoming features currently address the Security Requirements at least for the IKEv2 channel. For the DATA channel, Multihoming may be extended for Multiple Interface by providing Alternate IP addresses for each Interface.

A a result, MOBIKE requires the following extensions:
- Mobility for Transport: to support all offload architecture, especially those with End-to-End Security.
- Mobility for Soft Handover: to make possible Soft Handover for both Transport and Tunnel mode. Note that Soft Handover is related to Multiple Interfaces Management.
- Multihoming for Multiple Interfaces: Multihoming SHOULD be provided with different Alternate IP addresses depending on the network the connection is currently working. Note that it is also related to Multiple Interface Management.
- Multiple Interfaces Management: MOBIKE MUST consider Multiple Interfaces Management for operations it has been designed for like Mobility and Multihoming. It MUST also provide generic extension to make Multiple Interface Management, such as ADDing or REMOVing an Interface.
- Traffic Selector: the EU MUST be able to explicitly specify which traffic the operation applies.

6. Security Considerations

The whole draft is about security.

7. IANA Considerations

There is no IANA consideration here.

8. Acknowledgment

We would like to thank Daniel Palomares, Pierrick Seite, Brian Carpenter, Hui Deng and Jong-Hyouk Lee for their useful comments.

9. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4555] Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", RFC 4555, June 2006.

[RFC5998] Eronen, P., Tschofenig, H., and Y. Sheffer, "An Extension for EAP-Only Authentication in IKEv2", RFC 5998, September 2010.

Authors' Addresses

Daniel Migault
Francetelecom - Orange
38 rue du General Leclerc
92794 Issy-les-Moulineaux Cedex 9
France

Phone: +33 1 45 29 60 52
Email: mglt.ietf@gmail.com

Carl Williams
MCSR Labs
Philadelphia, PA 19103
USA

Phone: 650-279-5903
Email: carlw@mcsr-labs.org