MIF Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 2, 2012

D. Migault
Francetelecom - Orange
C. Williams
MCSR Labs

March 1, 2012

Multiple Interfaces Security Requirements for Offload
draft-mglt-mif-security-requirements-00.txt

Abstract

Current Radio Access Network (RAN) infrastructure will not be able to deal with the next future traffic increase. As such traffic is being offloaded on alternate networks like WLAN. Contrary to RAN, WLAN MAY not be trusted networks, so the End User has to secure offloaded communications. Current offload architectures consist in tunneling the End User traffic to a Security Gateway. Alternatively, ISPs MAY provide End-to-End security and connect directly the End User to the Server. Because WLAN network are not managed by ISPs, WLAN Access Points MAY not be reliable making End User willing to benefit from multiple connections.

This draft presents the Security Requirements for an offloaded End User with multiple interfaces. From the Security Requirements, the draft explains why IPsec is the most appropriated security protocol, and points the Multihoming feature current IKEv2 Extension MOBIKE are lacking.

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 2, 2012.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Requirements notation 3
2. Introduction 3
3. Offload Security Requirements 4
4. Problem Statement 6
5. Security Considerations 7
6. IANA Considerations 7
7. References 7
7.1. Normative References 7
7.2. Informative Reference 7
Authors' Addresses 8

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

ISP main motivation is to provide services to its End Users. This means providing the infrastructure that supports the mobile data traffic generated by its End Users as well as the best Quality of Service. Current ISP RAN architecture will not be able to support next future mobile data. The most effective way to deal with that traffic is to take advantage of deployed WLAN and offload the RAN traffic to WLAN. This architecture requires the End User to deal with at least two different interfaces connected to two distinct networks that provides different level of Trust and different level of Quality of Service.

For example, IWLAN is the proposed offload architecture by 3GPP. The End User connected to a WLAN set up an IPsec tunnel with the ISP Tunnel Terminating Gateway (TTG), and forwards its traffic. Communications with an ISP service hosted application are forwarded to the Gateway GPRS Support Node (GGSN), otherwise Internet communications are forwarded to the Packet Data Gateway (PGD).

However, this IWLAN architecture offloads the whole traffic of the End User, and ignores services specificities. For example, services are good candidates for offloading their traffic - like hight bandwidth ISP service hosted. Other services MAY not be offloaded and use only RAN - either for confidentiality or Quality of Service Motivations. A third category of services MAY not be offloaded and redirected to the ISP CORE Network, but instead should go directly on the Internet. As such, there are different offload policies based on the services. In fact the Security Gateway introduces some latencies, and possibly routing indirections that MAY affect some Real Time Applications.

In addition to the offload policies, services MAY behave differently during offload. One example described in [Lee] is the "on-the-spot" strategy that takes advantage of WLAN higher bandwidth to reduce the overall downloading time and thus save battery. With the "on-the-spot" strategy, if no WLAN is accessible, the application interrupts the download until a WLAN is accessible - instead of switching to the RAN. Of course, if after a pre-defined delay, no WLAN has been found, then the application switches to the RAN. This strategy especially targets services that do not have real time requirements

and experimentations show that this increases offloaded data up to 29%, and saves 20% of the battery.

As a results applications MAY have different interests toward offload which makes ISPs consider not only offloading the whole End User traffic, but also apply offloading policies on a per-service basis.

In an offload situation, security and other service based features such as transport policies MAY be adapted. Then security and other services based features MAY depend on the network, the End User is attached to. For example, WLAN managed by the ISP MAY not modify consequently the level of trust compared to RAN. On the other hand a WLAN provided by a third entity MAY be considered as untrusted. ISPs have a good knowledge of the Quality and level of trust of network the End User is attached to and so are good candidates for proposing an offload service for their own application or as service for third party services.

In an offload situation, the End User is expected to be able to perform:

- Offload Mobility between a trusted network (for example RAN) to an untrusted Network (for example WLAN)
- Offload Mobility from one WLAN access Point to another WLAN Access Point.
- Offload Multihoming for WLAN Access Point Fail over
- Offload Multihoming for simultaneous use of multiple Interfaces

This draft concerns both Multihoming and Security. As such Offload Mobility operations are out of scope of the draft.

3. Offload Security Requirements

From section Section 2 this section lists the security requirements.

A first list of requirements provides generic requirements that defines the granularity the Offload Security protocols SHOULD base their policy on, the layer secured by the Offload Security, the network architectures the Security Layer will be integrated to, as well as the authentication methods that SHOULD be supported.

Granularity: Offload Security policies are established according to various criteria such as sub network and IP addresses to identify the network, ports and protocols to identify the service

Security Layer: Offload Security SHOULD NOT require modification of the code of a running service

Architecture: Offload Security MUST fit architectures with a Security Gateway that secure a global traffic, as well as architectures with a direct connection between the End User and the Service.

Authentication: Offload Security MAY provide authentication mechanisms from the WLAN that are similar to those provided on the RAN. This would provide the opportunity for End User to access their service directly from the WLAN rather being authenticated by the RAN and then offloaded on the WLAN.

Then follows the Multihoming related Security Requirements:

Failover: WLAN Access Point MAY not be maintained by the ISP, and so MAY be unreliable. When the End User is connected to a service or to a Security Gateway using a Primary IP address, the End User MUST be able to provide a list of Alternate IP addresses which MAY be used in case the Primary IP address is not reachable. Alternate IP addresses are provided for a given communication, a Primary IP addresses is replaced by an Alternate IP address, and Primary and Alternate are not used simultaneously for the same communication.

Simultaneous Interfaces: Another way to get around WLAN unreliability is that the End User is connected simultaneously to various WLAN Access Points. This makes the End User to split its traffic between various WLAN Access Points, limiting the impact of an Access Point Failure. More specifically, this would in the worst case require restarting a subset of the applications rather than all the applications. How the End User splits its traffic is out of scope of the draft. The End User can assign various services to different WLAN Access Points, or splits flows of a given service between the different WLAN Access Points. The advantage of having multiple simultaneous connections to various WLAN Access Points, is that the End User can measure and estimate the best path, and manage its traffic according to its measurements. As such, the Security Requirements for Offload Multihoming with Simultaneous Interfaces are: 1) When the End User has established a secure communication with the server, it MUST be able to ADD an Interface to that communication. 2) When the End User detects that one WLAN provides better connectivity, it MUST be able to switch the traffic from one Interface to another. 3) Then when the End User is not anymore attached to one WLAN, it MUST be able to advertise the Server, the interface is not valid anymore and to REMOVE it.

4. Problem Statement

Comparing TLS [RFC5246] /DTLS [RFC5238] and IPsec with the generic Security Requirements of section Section 3 shows that IPsec [RFC4301] is advised to Offload Security. TLS/DTLS does not provide other granularity than a service granularity (port). In other words, DTLS/ TLS provides a secure version of a given service. Then TLS/DTLS main drawback is that it requires code modifications, and thus makes ISP Offload service hard to be deployed for third party. Furthermore, TLS/DTLS has mainly been designed for End-to-End connectivity, and MAY not fit all requirements of a Security Gateway Architecture. At last TLS/DTLS does not provide EAP [RFC3748] framework for authentication. On the other hand, IPsec addresses all the security requirements. IPsec defines Security Policies according to various Traffic Selectors that includes subnetworks, IP addresses, ports, and upper layer protocols. Then it secures the IP layer in the kernel, which does not impact the service, and thus makes possible an ISP to provide a Secured Offload for a third party service. IPsec has two modes: the Transport mode for End-to-End connectivity and the Tunnel mode to secure the link between the End User and a Security Gateway. At last IPsec [RFC5998] provides an EAP framework making authentication mechanisms [RFC4186] [RFC4187] on RAN possible on WLAN. In the remainder of this draft we will consider IPsec only.

Multihoming Security Requirements are partly handled by IPsec MOBIKE [RFC4555] extension. MOBIKE has been designed for the Tunnel mode only, and provides Mobility and Multihoming Failover for a connection protected with the Tunnel Mode. More specifically, with MOBIKE, IKEv2 can exchange Alternate IP addresses. Once the application detects the primary interface is not available it MAY switch running IPsec tunnel connections on the Alternate IP addresses by UPDATING the Security Associations. However, MOBIKE does not provide Multihoming Failover for communication protected with the Transport Mode. Furthermore, MOBIKE does not provide mechanisms for the use of simultaneous Interfaces. MOBIKE has been designed to UPDATE Security Association, which makes possible to change the outer IP address of the IPsec Tunnel. In conjunction of mechanisms for the use of simultaneous Interfaces, UPDATE can be used for traffic management with Tunnel mode. This traffic management facility is available for the Tunnel Mode and has to be extended to the Transport Mode.

A a result Security Requirements are:

- Extend MOBIKE Failover for communication protected with the IPsec Transport Mode

- Extend MOBIKE UPDATE for communication protected with the IPsec Transport Mode
- Extend MOBIKE Multihoming for simulatenous use of multiple interfaces for both IPsec Transport and Tunnel Mode

5. Security Considerations

The whole draft is about security.

6. IANA Considerations

There is no IANA consideration here.

7. References

7.1. Normative References

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

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[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.

[RFC5238] Phelan, T., "Datagram Transport Layer Security (DTLS) over the Datagram Congestion Control Protocol (DCCP)", RFC 5238, May 2008.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

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

7.2. Informative Reference

[Lee] Lee, K., Rhee, I., Lee, J., Yi, Y., and S. Chong, "Mobile data offloading: how much can WiFi deliver?", SIGCOMM ACM,

oct 2010.

[RFC4186] Haverinen, H. and J. Salowey, "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)", RFC 4186, January 2006.

[RFC4187] Arkko, J. and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC 4187, January 2006.

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