3GPP TR 33.865 V0.2.1 (2013-04)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security aspects of WLAN network selection for 3GPP terminals (Release 12)

MCC selects keywords from stock list.

Keywords
<keyword[, keyword]>

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

This clause is optional. If it exists, it is always the second unnumbered clause.

1 Scope

The present document studies the security aspects of WLAN Network Selection for 3GPP Terminals. In particular, the goals of this document are:

-To work on security impacts and threats of key issues and solutions of SA2's specifications.

-To identify potential conflicts between security mechanisms provided by non-3GPP providers via Hotspot 2.0 and security mechanisms provided by 3GPP operators, and define security solutions if needed.

-To identify possible impacts to the current authentication method of non-seamless WLAN offload.

Editor Notes: Need to update the scope with relevant TS and TR.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 23.865: " WLAN network selection for 3GPP terminals".

[3] WFA: "Hotspot 2.0 Technical Specification v1.0.0".

[4] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

[5] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3".

[6] IEEE: 802.11u, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 9: Interworking with External Networks".

3 Definitions, symbols and abbreviations

Delete from the above heading those words which are not applicable.

Clause numbering depends on applicability and should be renumbered accordingly.

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [x] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [x].

Definition format (Normal)

<defined term>: *<definition>.*

example: text used to clarify abstract rules by applying them literally.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

Symbol format (EW)

<symbol> <Explanation>

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [x] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [x].

Abbreviation format (EW)

<ACRONYM>	<Explanation>
AAA server	
AN	
ANDSF	Access Network Discovery and Selection Function
ANQP	
AP	
BSS	
EAP-AKA	
EAP-SIM	
IE	
SSID	
WLAN	

4 Description of key issues of security aspects of WLAN network selection for 3GPP terminals

Editor's note: This clause is intended to provide an overview of the security issues which arise from the use cases and functionalities specified by TR 23.865[2] and WFA Hotspot 2.0 specifications [3].

4.1 Key issue - Use WLAN Access Network Type and Venue Information for network selection

4.1.1 Issue details

As described in clause 5.7 of TR 23.865 [2], access network type and venue related information of WLAN access networks is recommended to be considered by the Access Network Discovery and Selection Function (ANDSF) as operator policies preferences for WLAN network selection decisions.

The Access Network Type IE identifies a WLAN network as a private, public, free, personal, emergency, etc. type of network. The Venue information such as venue type and venue name helps to identify the venue where WLAN network may be deployed, e.g. school, hospital, hotel, professional office, etc. This type of information would allow operators and service providers to apply different policies for different types of WLAN networks such as public hotspots, home or enterprise based WLAN networks. In some places, there is possibility that the same SSID is used for public hotspots which are charged and hotel hotspots that are free of charge.

4.1.2 Threats

An example deployment is shown in figure 1, where type (including Access network Type and Venue information) 1 implies the WLAN is public and charged while type 2 means that WLAN is hotel and free of charged. It is assumed that the priority of type 2 WLAN is higher than type 1 WLAN, and SSID B has higher access priority than SSID A when the type is the same.

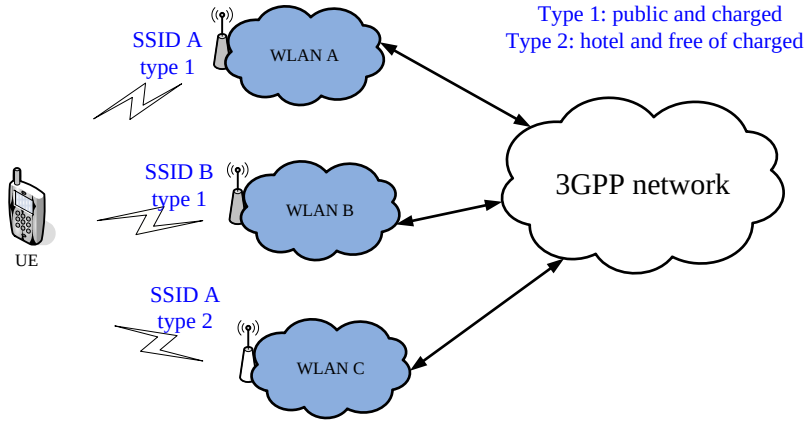

Figure X.1 use WLAN Access Network Type and Venue information for network selection

According to Hotspot 2.0 [3], access network type and venue related information of WLAN access networks can be discovered by UEs prior to association and authentication procedures. The information is transported to UE by a Hotspot 2.0 compliant AP in clear text, it means that users including attackers can get these information. A malicious WLAN A which has a subscription agreement with 3GPP operator and has the lowest selection priority may pretend to be WLAN C which has higher selection priority than WLAN A by transmitting SSID A and type2 to UE, and the UE may select a lower priority WLAN network. It would also result in additional costs if WLAN A charged higher than WLAN B. Additionally, the signal quality of the lower priority WLAN network may be poor, there is a risk that the users may change the operator due to the bad user experience.

In general, from a security point of view, using the access network type and venue related information in WLAN selection policies can cause security issue as discussed above. Thus there is a need to discuss how to use the access network type and venue related information in a secure manner.

4.1.3 Security requirements

Editor's Note: This clause is intended to capture the security requirements for solving the key issue. The requirements are mapped to the relevant threats.

Editor's Note: It is FFS whether a security mechanism can and should be provided to solve this issue.

4.2 Key issue - Support WLAN access through roaming agreements

4.2.1 Issue details

More and more 3GPP operators rely on roaming agreements for supporting WLAN access, an example deployment is shown in Figure 1 below, where the 3GPP operator has roaming agreements with Partner X and Partner Y. Each of these partners acts as a "roaming consortium" and maintains its own roaming agreements with individual hotspot providers (shown as WLAN A, B and C).

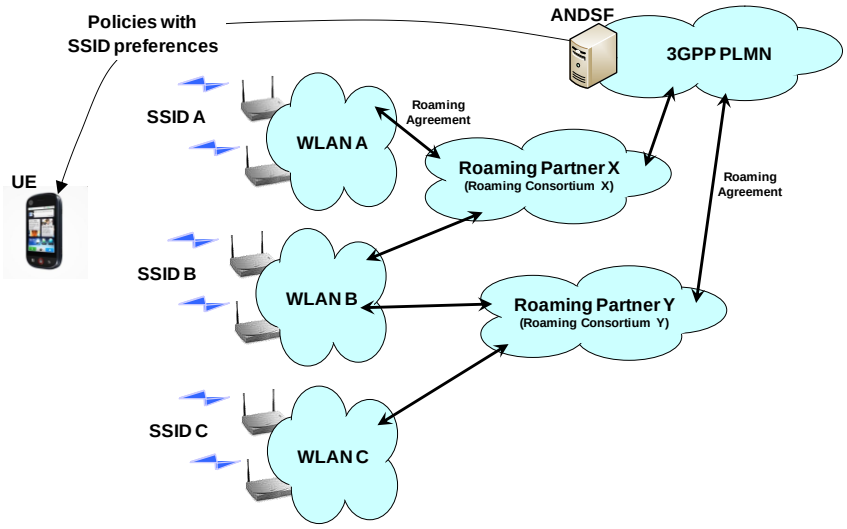

Figure Y.1 Supporting WLAN access through roaming agreements

The ANDSF may send policies to UE based on Realms and/or OUIs to indicate for example that "WLANs that interwork with Realm=PartnerX.com have the highest access priority". The UE uses the Realms and/or OUIs as an alternative way (instead of using SSID) to identify and prioritize the discovered WLAN access networks.

4.2.2 Threats

The Realms and/or OUIs are broadcasted by HS2.0 AP in its beacon or transmitted in probe response frames. A Hotspot 2.0 compliant UE is also capable to discover the Realms and/or OUIs by using the applicable discovery procedures (e.g. based on the ANQP protocol). The information is transmitted to UE without security protection. The Realms and/or OUIs may be tampered by a man-in-the-middle (MitM) attack on radio interface which may lead to useless of the policies based on the information. Besides, a malicious HS2.0 AP which has a low priority subscription agreement with 3GPP operator is able to send a fake OUI to claim a high access priority, in order to seduce UE to choose. It would result in an additional cost to UE.

In addition, using SSIDs in WLAN selection policies can also create several different attacks, as what have been mentioned above.

4.2.3 Security requirements

Editor's Note: This clause is intended to capture the security requirements for solving the key issue. The requirements are mapped to the relevant threats.

Editor's Note: It is FFS whether a security mechanism can and should be provided to solve this issue.

4.3 Key issue - Interaction between WLAN network selection and network-provided policies for WLAN selection

4.3.1 Issue details

As TR 23.865 [2] described, an operator may provide ANDSF policies to the UE in order to allow the UE to route traffic to specific WLAN access network (e.g. a specific SSID) based on the policy rules. Current policy rules could be enhanced by adopting parts of the WFA Hotspot 2.0 specifications [3] that allow for developing policies for WLAN network selection by making use of IEEE 802.11u [6] ANQP query response mechanisms, use of realms information, venues information, network load, etc.

For example, a 3GPP operator wants to have policies whereby traffic can be offloaded to its roaming partners but only in a certain time window and at a particular geographic location, e.g. during rush hour in a busy downtown area. Assume operator A has relationship with operator #1 with SSID1 and operator #2 with SSID2. The ANDSF rules specify that if you are in location x and between time y and z then prefer SSID1 but for other location or times prefer

SSID2. The PLMN priority list in the UE has SSID2 higher in preference than SSID1. Now if the user is at location x between time y and z, the conflict resolution between ANDSF rules and PLMN priority list is needed.

Editor's Note: It is FFS whether there is threats related to this key issue.

4.4 Key issue - Use WLAN load information for network selection

4.4.1 Issue details

As TR 23.865 [2] described, providing network selection policies to the UE that take load or congestion indication from WLAN networks into account can improve the existing WLAN network selection decisions.

An AP compliant with Hotspot 2.0 broadcasts the BSS Load information and supports the WAN Metrics ANQP Element. The BSS Load information element contains information on the current mobile device population and channel utilization in the BSS. The WAN Metrics ANQP element provides information about the WAN link of a WLAN access network.

The WFA Hotspot 2.0 specifications [3] take into account the BSS Load and backhaul parameters to specify BSS Load policy to prevent a mobile device from joining a WLAN network that may be overly congested with traffic and/or interference.

Editor's Note: It is FFS whether there is threats related to this key issue.

5 Solutions of key issues

5.1 Solution 1: Authenticity of WLAN information

5.1.1 Description

This solution addresses key issue "Use WLAN Access Network Type and Venue Information for network selection" and Key Issue "Support WLAN access through roaming agreements".

According to Hotspot 2.0 specification [3], UE with (U)SIM card shall support EAP-SIM/EAP-AKA protocol for authentication .

In addition to the technical solutions, some non-technical methods (e.g. operator management, customer report, etc.) can be adopted by 3GPP operator to supervise the behaviour of WLAN operator, to prevent malicious but legal WLAN AP from sending fake WLAN information to UE. The details of non-technical method are out of 3GPP scope.

5.2 Solution 2: Solution of supporting security parameters of selection policies

5.2.1 Description

In current specification TS33.402 [4], the EAP-AKA' procedure is used for mutual authentication and key agreement when the non-3GPP access is treated as trusted non-3GPP access network. In this case, the UE and HSS derives a new authentication vector by using the access network identity (i.e., "WLAN" as the access network identity for WLAN AN) as one of input parameters. The UE can check that the identity it has received over the air is the same as the identity the AAA server has given via EAP-AKA' which is specified in TS33.402 [4] and TS24.302 [5].

However, if the UE does not choose a trusted access network, the EAP-AKA' procedure will not be performed. Then the UE cannot be able to check the access network identity.

It can be achieved by extending the ANDSF selection policies to support security parameters of selection policies. When the UE sends a request to ANDSF server for selection policies, the ANDSF sends a response to UE which includes the security related information and the policy. The security related information can be the trust relationship of non-3GPP access network which can be used to indicate that for example "trusted WLAN have the higher access priority than untrusted WLAN". The UE stores the received security related information and the policies based on it if these information is not stored or changed in UE. Based on these stored information, the UE selects the most suitable trusted WLAN access network for accessing and initiates EAP-AKA' authentication procedure for establishing connection with the selected WLAN access network. In addition, the security related information and the corresponding policies can also be transmitted to UE by policy update procedure which is triggered by ANDSF.

Editor's Note 1: It is FFS how to extend ANDSF policies for security selection preferences. It is FFS which threats this solution solves.

Editor's Note 2: The analysis should take into account that an ANDSF security policy to prefer trusted WLAN accesses may be in contradiction with other preferences for network selection.

Editor's Note 3: Untrusted WLAN access network may also use EAP-AKA' procedure which is specified in clause 6.4 in TS 33.402 [4].It should be analysed if that has impact on the proposed ANDSF security policy.

5.2.2 Impacts on existing nodes or functionality

The ANDSF access selection policies need to be extended in order to include additional selection preferences

Annex <A>:
<Annex title>

Annexes are labelled A, B, C, etc. and are "informative"(3G TRs are informative documents by nature).

A.1 Heading levels in an annex

Heading levels within an annex are used as in the main document, but for Heading level selection, the "A.", "B.", etc. are ignored. e.g. **A.1.2** is formatted using ***Heading 2*** style.

Bibliography

The Bibliography is optional. If it exists, it shall follow the last annex in the document.

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

Bibliography format

- <Publication>: "<Title>".

OR

<Publication>: "<Title>".

Annex <X>: Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2013-01	-	-	-	-	Initial version- Addition of S3-130156, S3-130158, S3-130085, S3-130159 with the changed discussed during SA3#70	-	0.1.0
2013-04	S3#71	S3-130551	-	-			0.2.0
2013-04	-	-	-	-	MCC clean-up of S3-130551	0.2.0	0.2.1