3GPP TSG SA WG3 Security — S3#37
Sophia Antipolis, France 21 - 25 February 2005

Tdoc ⌘S3-050032

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.234** **CR** **056** ⌘ **rev** **-** ⌘ Current version: **6.3.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☒ Core Network ☐

Title:	⌘	Threat of users accessing each other in link layer and corresponding security requirements of user traffic segregation.
Source:	⌘	ZTE Corporation
Work item code:	⌘	WLAN
Date:	⌘	22/01/2005
Category:	⌘	**B**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change:	⌘	There is no description about threat of user accessing each other in link layer and corresponding security requirements of user traffic segregation in current specification.
Summary of change:	⌘	Adding threat of user accessing each other in link layer and security requirement of user traffic segregation. Some editorial corrections is also included.
Consequences if not approved:	⌘	Specification is not complete.

Clauses affected:	⌘	4.2.6(new), C.1, C.2.2.2

	Y	N		
Other specs affected: ⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

*** BEGIN OF CHANGE1 ***

4.2.5 Link layer security requirements

Editors note: This section is FFS, LS (S3-030167) sent to SA2 group on 1) the need for requiring 802.11i in TS 23.234. SA2 to explain the impact (if any) a change of technology from 802.11i to WPA would have on the standardisation work. 2) SA2 to study the architectural impacts of implementing protection on Wa interface 3) SA2 to Investigate the importance of specifying specific WLAN technologies to be used for the WLAN access network.

Most WLAN technologies provide (optional) link-layer protection of user data. Since the wireless link is likely to be the most vulnerable in the entire system, 3GPP-WLAN interworking should take advantage of the link layer security provided by WLAN technologies. The native link-layer protection can also prevent against certain IP-layer attacks.

Areas in which relevant requirements are defined are:

- Confidentiality and integrity protection of user data;
- Protection of signalling;
- Key distribution, key freshness validation and key ageing.

These requirements are out of scope of 3GPP. IEEE has defined the security requirements and features for the link layer in WLAN access networks, see IEEE 802.11i [6]. Other WLAN access technologies are not excluded to be used although not described here.v

4.2.6 User traffic segregation requirements

User traffic should be segregated in WLAN AN.

- Users should not access each other in link layer, unless permitted by operators.
- One user should not access another user's WLAN UE by IP address directly, unless permitted by operators.

*** END OF CHANGE1 ***

*** BEGIN OF CHANGE2 ***

C.1 Security for Public WLAN Access

These questions related to security in the 3GPP-WLAN architecture, must be addressed:

- What needs to be protected? i.e. what are the assets, and to whom are they valuable?
- What trust relations can be assumed? i.e. who can trust whom, and to what degree? The Trust Model is described in Annex B.
- What are possible attacks against the assets, how can they be performed, and what is done to detect/prevent them?

In section ~~3~~ C.2 the relevant ~~assents~~ assets and threats to those assets are identified. Section ~~4~~ C.3 contains examples of possible attacks. Countermeasures are not discussed in this ~~contribution~~ section but the threats and specific attacks should be taken into consideration when defining security mechanisms for 3GPP-WLAN interworking.

*** END OF CHANGE2 ***

*** BEGIN OF CHANGE3 ***

C.2.2.2 User Data and Privacy

The user expects that the data he sends/receives while accessing to WLAN services, ~~and~~ personal information (such as identity, which services he/she uses or where he/she is located at a given time) is kept away from unauthorised parties, and data stored in his/her WLAN equipment is not accessed by unauthorized user.

The following threats are relevant:

- An attacker obtains the information that the user sends/receives while accessing to WLAN services. This includes user credentials transferred during the authentication phase, as well as any other data (e.g. documents) exchanged once the user has gained access to the WLAN services. The attacker might know or not who the user is;
- An attacker manipulates or substitutes the information that the user sends/receives while accessing to WLAN services. The attacker might know or not who the user is;
- An attacker analyses the information sent/received by users (even if it is mostly concealed) in order to derive some personal information about the users (such as which services they are using or where they are located at a given time).
- An attacker obtains information about the user (permanent identity etc.) and traces where and when the user has been accessing WLAN services.
- An attacker (also a legal user) accesses the user's WLAN equipment in link layer without the user's permission.

*** END OF CHANGE3 ***