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

Tdoc ⌘S3-050180

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.234** **CR** **058** ⌘ **rev** **2** ⌘ 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 **X**

Title:	⌘	WLAN AN providing protection against IP address spoofing
Source:	⌘	SA WG3
Work item code:	⌘	WLAN
Date:	⌘	25/02/2005
Category:	⌘	**F**
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:	⌘	For WLAN Direct IP Access there exists potential IP address spoofing attack if the charging is based on IP address. It's WLAN AN's duty to defeat this kind of attack.
Summary of change:	⌘	Add a description of IP address spoofing attack against WLAN AN in the Annex C3.3.
Consequences if not approved:	⌘	WLAN provider may not be aware of this threat of IP address spoofing attack against WLAN Direct IP Access.

Clauses affected:	⌘	Annex C3.3

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

Other comments:	⌘	

*** BEGIN OF CHANGE ***

C.3.3 Attacks at the WLAN AN Infrastructure

Attacks can be performed at the WLAN AN infrastructure, e.g. Access Points (AP), the LAN connecting the APs, Ethernet switches etc. To perform any type of attacks "inside" the WLAN AN, the attacker needs access to the network in some way. For ordinary wired networks, an attacker needs to somehow hook up to the wires to get access. The WLAN AN is partially a wired network, and an attacker may hook up to that part of the network. In public spaces the APs and corresponding wired connections may be physically accessible by attackers. Simply connecting a laptop to the wired LAN "behind" the APs may give the attacker free access to WLAN services as well as access to other user's data and signalling traffic.

Depending on where charging data is collected, an attacker with access to the wired LAN of the WLAN AN can also interfere with the charging functions. If the volume based charging model is applied, an attacker could e.g. inject packets with any chosen source or destination MAC and IP addresses, just to increase a user's bill.

For WLAN Direct IP Access if the charging is based on IP address, there exists a threat of IP address spoofing attack against the WLAN AN, which may generate incorrect accounting message for users.

NOTE: 3GPP suggest WLAN operators not to use IP address based accounting; unless there are sufficient countermeasures implemented against IP address spoofing attack in the WLAN AN.

*** END OF CHANGE ***