S3-020392 Agenda Item: x.x

Title: WLAN Interworking Security WID

Source: BT Group

Work Item Description

Title

WLAN Interworking Security WID

1 3GPP Work Area

X	Radio Access
X	Core Network
X	Services
X	Terminals

2 Linked work items

Access Security for IP based Services

Subscription Management

UE Management

Network Domain Security (if secure distribution of authentication between roaming partners is necessary) Lawful Interception

WLAN inter-working WID in SA1 and SA2

3 Justification

There is an increasing demand for wireless 'local area' access in very different scenarios. Wireless access to Internet is provided to public users by the use of currently existing WLAN technology such as IEEE 802.11b. In companies wireless access is provided to portable computer users by use of the same technology. For residential use wireless access is also increasing. 3rd generation technologies and systems will provide bearers for similar packet switched services, with greater mobility and wider area coverage albeit with reduced data rate.

WLAN technology can complement 3GPP based networks in deployment environments with high user density and demand for higher data rates. However, in order to provide flexible use of both technologies in these environments and to provide mobility of services between the two technologies it is sensible that some degree of interworking exists between the two technologies/systems.

The current study within SA1, described in the "3GPP system – WLAN Interworking" WID, covers requirements aspects of WLAN-3GPP System Interworking [S1-020638]. In addition SA2 have a complimentary WID, which is identifying and analysing potential Interworking architectures [S2-02-0908]. It is therefore considered to be necessary for SA3 to develop Security Architecture suitable for implementation to enhance these work items.

4 Objective

In co-ordination with SA1 and SA2, SA3 is to produce a Technical Report and subsequent Technical Specification for WLAN Interworking. These documents will be developed based on the following deliverables:

- 1. A review of the security of existing and relevant technologies i.e. IEEE, 3GPP and IETF, including RAN technologies and network technologies
- 2. An elaboration of a Trust model and inter-working scenarios
- 3. An analysis of potential threats
- 4. Recommendations of appropriate access control mechanisms including Authentication, Authorisation, and key management including symmetric as well as asymmetric technologies
- 5. Recommendations of appropriate mechanisms for the confidentiality and integrity protection for different hops and layers i.e. first hop (e.g. link layer) and network hop (e.g. PIC&IPSec etc)
- 6. A definition of the security requirements, to include any requirements for Lawful Interception

These documents will then: -

- □ Ensure that any changes to the 3GPP Specifications, resulting from this work are implemented within 3GPP via the standard 3GPP CR process.
- □ Ensure that any changes to the IEEE Specifications, resulting from this work are implemented within IEEE via the IEEE CR process.

5 Service aspects

Security architecture will meet the service requirements defined by SA1

6 MMI aspects

MMI aspects will need to address the configuration and visibility within the terminal and the network of the security status from the perspective of both the end user and the service provider.

7 Charging Aspects

Non Identified

8 Security Aspects

This is a Security Item

9 Impacts

Affects:	USIM	TE	MT	UE	AN WLAN	AN RAN	CN	Others
Yes	X	X	X	X	X	X	X	
No								
Don't know								

10 Expected Output and Time scale (to be updated at each plenary)

			Deliverables	
No.	Title	Prime rsp. WG	Completion Date	Comments
1	3GPP & IEEE WLAN Interworking Security Review	SA3	SA3#25 8-11 th October 2002	A Review of the security of existing 3GPP and IEEE WLAN security from a theoretical and practical perspective. http://www.ieee802.org/11/
				http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm
				http://www.cs.umd.edu/~waa/1x.p df
				http://www.isaac.cs.berkeley.edu/is aac/wep-faq.html
				http://slashdot.org/articles/01/02/1 5/1745204.shtml
2	3GPP & IEEE WLAN Interworking Security Risk Analysis	SA3	SA3#25 8-11 th October 2002	Determination of the security risks associated with various deployment environments and interworking scenarios. (SA2 Technical Report will be presented for info at SA #17 9 th – 12 th September)
3	Wireless Local Area Network (WLAN) Interworking Security Technical Report		SA3#26 19 th – 22 nd November 2002	
4	Wireless Local Area Network (WLAN) Interworking Security Technical Specification		SA3#27 Feb 2003	
	CR,s approved to existing specifications		SA3#27 Feb 2003	How do we handle any CR's to IEEE specs?

			New sp	ecifications		
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments
TR xx.xxx	Wireless Local Area Network (WLAN) Interworking Security	SA3	SA1 SA2	SA#18 9 th –12 th December 2002	SA#19 17 th – 20 th March 2003	TR Incorporates deliverables 1&2 from above list
TS xx.xxx	Wireless Local Area Network (WLAN) Interworking Security	SA3	SA1 SA2	SA#19 17 th – 20 th March 2003	SA#20 9 th – 12 th June 2003	TS To Include recommendations

	Affected existing specifications 3GPP				
TS	21.133	3G security; Security threats and requirements			
TS	33.106	Lawful interception requirements			
TS	33.107	3G security; Lawful interception architecture and functions			
TS	33.108	3G security; Handover interface for Lawful Interception			
TS	33.200	Network Domain Security - MAP			
TS	33.203	3G security; Access security for IP-based services			
TS	33.210	3G security; Network Domain Security (NDS); IP network layer security			

Affected existing specifications IEEE				
IEEE 802.11, 1999	ISO/IEC 8802-11: 1999) IEEE Standards for Information Technology			
Edition	Telecommunications and Information Exchange between Systems			
	Local and Metropolitan Area Network Specific Requirements Part			
	11: Wireless LAN Medium Access Control (MAC) and Physical Layer			
	(PHY) Specifications			
IEEE 802.11a-1999	(8802-11:1999/Amd 1:2000(E)), IEEE Standard for Information			
	technology—Telecommunications and information exchange between			
	systems—Local and metropolitan area networks—Specific			
	requirements—Part 11: Wireless LAN Medium Access Control (MAC)			
	and Physical Layer (PHY) specifications—Amendment 1: High-speed			
	Physical Layer in the 5 GHz band			
IEEE 802.11b-1999	Supplement to 802.11-1999, Wireless LAN MAC and PHY specifications:			
	Higher speed Physical Layer (PHY) extension in the 2.4 GHz band			
	Amendment to IEEE 802.11-1999, (ISO/IEC 8802-11) Information			
IEEE 802.11d-2001,	technologyTelecommunications and information exchange between			
	systemsLocal and metropolitan area networksSpecific requirements			
	Part 11: Wireless LAN Medium Access Control (MAC) and Physical			
	Layer (PHY) Specifications: Specification for Operation in Additional			
	Regulatory Domains			
IEEE	Draft Standard 802.11i, D2.1 (March 2002): Specification for Enhanced			
802.11i	Security.			

Affected existing specifications ETSI BRAN			
ETSI TS101 761-2	Broadband Radio Access Networks (BRAN) HIPERLAN Type 2 Data		
V1.3.1	Link Control (DLC) layer; Part 2: Radio Link Control (RLC) sublayer.		

Work item rapporteurs

If supported by SA3 at SA3#24 Ericsson can take the rapporteur role.

Work item leadership

SA3

Supporting Companies

Alcatel, BT Group, Cisco, Ericsson, Lucent, Motorola, Nokia, Nortel, Siemens Sonera, Telenor, Telia, Vodafone,

The above supporting companies, active in SA3, support the "3GPP System – WLAN Interworking" WID in SA1 and SA2 and it will need to be confirmed that they support this WID by the SA3#24 meeting 9^{th} - 12^{th} of July 2002

14 Classification of the WI (if known)

X	Feature (go to 14a)
	Building Block (go to 14b)
	Work Task (go to 14c)

- 14a The WI is a Feature: List of building blocks under this feature
- 14b The WI is a Building Block:
- 14c The WI is a Work Task: parent Building Block