3GPP TSG SA WG3 Security S3-020247

May 14 – May 17, 2002

Victoria, Canada

Agenda Item:	6.9
Source:	BT Group
Title:	Some Consideration for WLAN Inter-working
Document for:	Discussion

1 WLAN security from a theoretical and practical perspective

WLAN is not a single radio technology, several different technologies fall into the category called WLAN.

1. The existing industry standard IEEE 802.11b operating at 2,4 GHz ISM band.
2. Bluetooth as a new technology for the same band

3. A new technology (IEEE 802.11a) developed for the 5GHz band.

4. ETSI BRAN Hiperlan2 are being developed for the 5GHz band.

Despite the different radio technologies, all these WLAN systems are commonly used for transportation of IP datagrams. So that the specific WLAN technology used in each wireless IP network is not very visible for the layers above IP.

SA3 will need review the security that is available with each of these technologies. This will summarise and verify the conclusions from the extensive research that has been published on both the theoretical perspective of the strength of the solution and the practical constraints of typical implementations eg default settings left unchanged etc

Examples of some of the issues

WEP (Wired Equivalent Privacy)

The 802.11 standards define WEP as a simple mechanism to protect the over-the-air transmission between WLAN access points and network interface cards (NICs). Working at the data link layer, WEP requires that all communicating parties share the same secret key. To avoid conflicting with U.S. export controls that were in effect at the time the standard was developed, 40-bit encryption keys were required by IEEE 802.11b, though many vendors now support the
optional 128-bit standard. WEP can be easily cracked in both 40- and 128-bit variants by using off-the-shelf tools readily available on the Internet. On a busy network, 128-bit static WEP keys can be obtained in as little as 15 minutes.

- **RC4 Stream Cipher**: WEP uses the RC4 stream cipher. The IEEE 802.11 standard describes the use of the RC4 algorithm and key in WEP, but does not specify specific methods for key distribution. Without an automated method for key distribution, any encryption protocol will have

implementation problems due to the potential for human error in key input, escrow, and management.

- **The initialisation vector:** As the initialisation vector (IV) is transmitted as plaintext and placed in the 802.11 header, anyone sniffing a WLAN can see it. At 24 bits long, the IV provides a range of 16,777,216 possible WEP chose to use a 24-bit IV and does not dynamically rotate encryption keys, these shortcomings are demonstrated to have practical applications in decrypting.

- **Message Integrity Check;** Another concern with WEP is its vulnerability to replay attacks due to the cyclic redundancy check (CRC)-32 checksum function as performed by standards-based WEP. With CRC-32, it is possible to compute the bit difference of two CRCs based on the bit difference of the messages over which they are taken. In other words, flipping bit n in the message results in a deterministic set of bits in the CRC that must be flipped to produce a correct checksum on the modified message. Because flipping bits carries through after an RC4 decryption, this allows the attacker to flip arbitrary bits in an encrypted message and correctly adjust the checksum so that the resulting message appears valid.

2 Security risks associated with various Deployment Environments and Inter-working Scenarios

2.1 Environments

The environments and some of their characteristics may be summarised as follows:

- "Public" environment includes all areas where there is unrestricted public presence, including outdoor areas, streets, transportation centres, retail stores, hotels, restaurants and public spaces and lobbies in major civic buildings. Here, for example, the WLAN operator is expecting general access and will likely have a system policies and equipment suitable for 3GPP interworking.

- "Corporate" environment includes offices and factories where the users are restricted to employees of the business. Restricted visitor access may also be accommodated in this environment. The Corporate WLAN operator is providing service primarily for internal uses, and access to other networks may be screened (i.e. with a "firewall"). There may be several WLANs deployed within the corporation, not all of which are to be interworked with 3GPP. Thus, interworking between Corporate WLAN and 3GPP may involve some different policies and techniques than for other environments.

- "Residential" environment includes individual homes and apartments where the users are restricted to the residents and their guests. Here, the WLAN owner and user are most likely the same. However, in a multi-tenant building, there may be a single WLAN (i.e. owned by the landlord) serving many users. The interworking of residential WLAN with 3GPP may involve some different policies that for other environments.

The security capabilities and policies will differ between public, corporate and residential WLANs. These differences may lead to different interworking methods between 3GPP and WLANs in these environments. Hence, it is to be recognised that secure interworking may not be possible in all cases for both technical and non-technical considerations.

2.2 Interworking Scenarios

3GPP System and WLAN interworking can be implemented in steps from a quite simple interworking to fully seamless inter system operation. This is can best be considered by defining a number of different scenarios for interworking that provide an indicative roadmap for development.

Although success will vary from scenario to scenario, the overall aim is to avoid changes to WLAN standards and to minimise changes in existing 3GPP specifications encompassing Release 99, Release 4 and Release 5,

Six interworking scenarios have been identified by 3GPP SA1 in TR 22.934 v1.0.0 [1]

Each scenario realises an additional step in integrating WLAN in the 3GPP service offering and naturally includes the previous level of integration of the previous scenario.
The 3GPP System – WLAN interworking scenarios may be considered with the aid of the simplified reference diagram in figure 1. This reference diagram illustrates the elements of the 3GPP and WLAN systems being interworked. These may be interconnected in a variety of ways to develop the progressive scenarios outlined in this section.

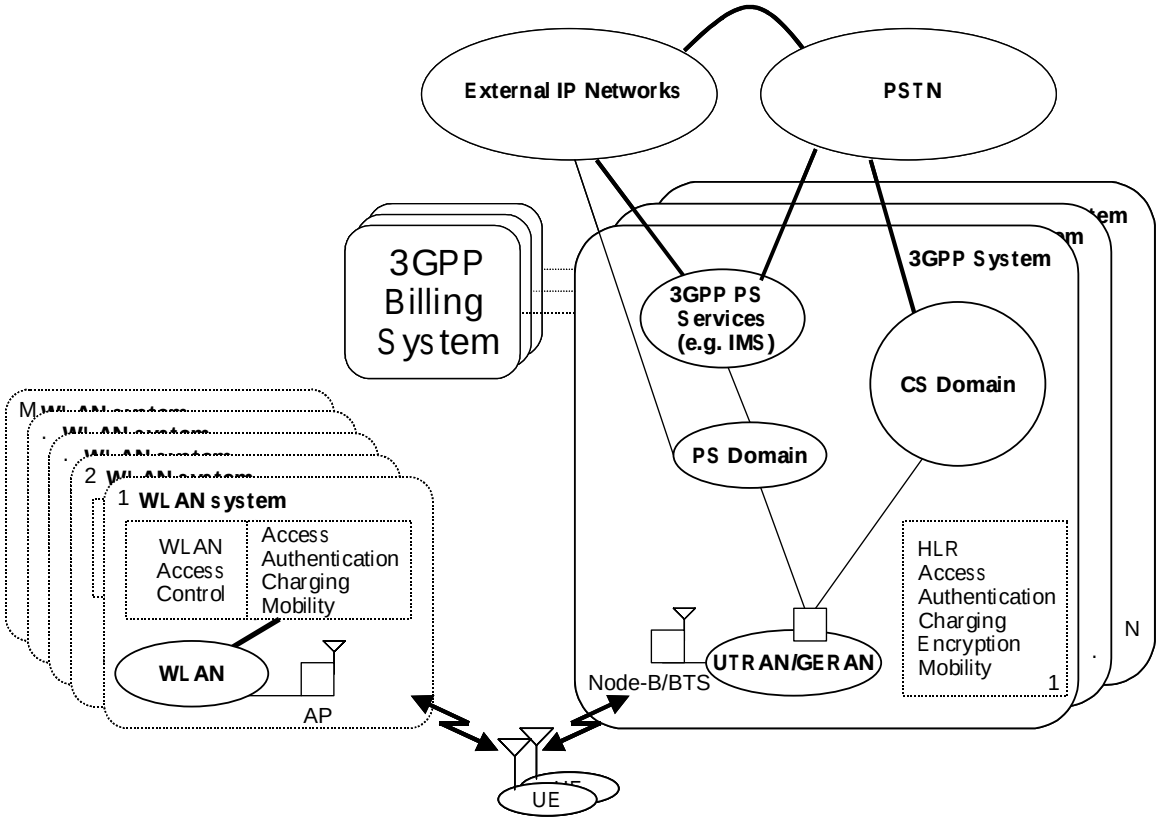

Figure 1: 3GPP System – WLAN interworking simplified reference model

- **Scenario 1 - Common Billing and Customer Care:** This is the simplest scheme of interworking. The connection between WLAN and 3GPP *is that there is a single customer relationship*. The customer receives one bill from the mobile operator for the usage of both 3GPP and WLAN access services. Integrated Customer Care allows for simplified service offering from both operator and subscriber's perspective. The security level of the two systems may be independent. This scenario does not pose any new requirements on 3GPP specifications.

- **Scenario 2 - 3GPP system based Access Control and Charging:** This is the scenario where *authentication, authorization and accounting are provided by the 3GPP system*. The security level of

these functions applied to WLAN is in line with that of the 3GPP system. This ensures that the user does not see significant difference in the way he is granted access. This may also provide means for operator to charge access in a consistent manner over the two platforms. Reusing the 3GPP system access control principles allows for additional benefits seen from a user and 3GPP system operator standpoint. First of all the 3GPP system operator may easily convert the subscribers within his existing 3GPP system customer base to becoming WLAN-3GPP system subscribers with a minimum effort both for the subscriber and the operator. In addition the maintenance of the subscriber may also be simplified. No requirements are put upon the set of services to be offered in the WLAN part beyond those inherently offered by being addressable in an IP network.

- **Scenario 3: Access to 3GPP system PS based services:** The goal of this scenario is to *allow the operator to grant access to 3GPP system **PS** based services through the WLAN access*. These services may include e.g. IMS based services, location based services, instant messaging, presence based services, MBMS and any service that is built upon the combination of several of these service components. Even though this scenario allows access to all services, it is an implementation question whether only a subset of the services is actually provided. However, service continuity between the 3GPP system part and the WLAN part is not required

- **Scenario 4: Service Continuity:** The goal of this scenario is to allow that the *services supported in Scenario 3 to survive the process of change of access network technology between WLAN and a 3GPP system*. However some services may not survive. The solution for providing service continuity between WLAN and a 3GPP system could also be used for providing service continuity between two WLAN subnets. The criteria and decision mechanism for change of access network is FFS. Change in service quality may be a consequence of mobility between access technologies, due to varying capabilities and characteristics of access technologies.

- **Scenario 5: Seamless services:** The goal of this scenario is to provide seamless service continuity between the access technologies, for the services supported in Scenario 3. *I.e. minimizing aspects such as data loss and break time during the switch between access technologies.*

- **Scenario 6: Access to 3GPP CS Services**: The goal of this scenario is to *allow the operator to grant access to 3GPP system **CS** based services through Circuit Switched WLAN access.* Seamless mobility for CS services will be provided.

2.3 Security considerations with International Roaming

SA3 will need identify potential solutions to support services when the user is connected to a WLAN that is outside the country where their account is held e.g. at a foreign airport. Certain authentication schemes e.g. based on GSM or 3GPP SIM cards and AuC (see IETF proposals in 3.2.2 below) may allow this to be achieved more easily. For example for transfer of a limit set of authentication vectors to a visited network.

3 Access Control Schemes

Operators who wish grant access to 3GPP system **PS and CS based** services through the WLAN access will require access control related functions within user equipment with a similar level of security that exists in 3GPP user equipment. It is unlikely that existing WLAN access control and encryption will meet this need.

3.1 Subscription security issues

3.1.1 Naming and Addressing

SA3 will need to determine what naming conventions need to be adopted or translations that may be required to allow inter-working eg if the user identification for 3GPP based access control needs to be based on be based on Network Access Identifier (NAI) format (user@realm) /RFC 2486/.

3.1.2 User identity confidentiality

In GSM users are allocated temporary *identity (TMSI*) which has meaning only in the local area and for a short period of time. SA3 must determine if an equivalent functionality is required when interoperating with WLANs.

3.2 Authentication

3.2.1 EAP/802.1X, LEAP

A proposal jointly submitted to the IEEE by Cisco Systems, Microsoft, and other organizations introduced an end-to-end framework using 802.1X and the Extensible Authentication Protocol (EAP) to provide this enhanced functionality. Central to this proposal are two main elements:

- EAP allows wireless client adapters, that may support different authentication types, to communicate with different back-end servers such as Remote Access Dial-In User Service (RADIUS)

- IEEE 802.1X, a standard for port based network access control

When these features are implemented, a wireless client that associates with an AP cannot gain access to the network until the user performs a network logon. When the user enters a username and password into a network logon dialog box or its equivalent, the client and a RADIUS server perform a mutual authentication, with the client authenticated by the supplied username and password. The RADIUS server and client then derive a client-specific WEP key to be used by the client for the current logon session. User passwords and session keys are never transmitted in the clear, over the wireless link.

EAP/802.1X, is sometimes referred to as LEAP,

A specific implementation of this has been proposed by Nokia using both GSM and 3GPP SIM cards in the client and an instance of a GSM AuC as the Radius Server.

3.2.2 IETF Proposals

EAP/SIM: EAP SIM Authentication (draft-haverinen-pppext-eap-sim-02.txt) This document specifies an Extensible Authentication Protocol (EAP) mechanism for authentication and session key distribution using the GSM Subscriber Identity Module (SIM).

- EAP type for GSM authentication
- Can be implemented with an authentication gateway - no other changes required to GSM network
- GSM operator roaming can be used
- Key distribution as part of the authentication procedure
- Enhancements to GSM authentication:
- EAP/SIM includes a MAC_RAND parameter for mutual authentication and to prevent an active attacker from querying SRES's from the client
- EAP/SIM can use several GSM triplets at a time for stronger authentication and to generate longer keys
- IMSI privacy supported
- Usage scenarios: PPP, WLAN access authentication

EAP/AKA: AKA within EAP, the new version (draft-arkko-pppext-eap-aka-01.txt) has been modified according to some requests in the IETF mailing list, e.g. the exact way used to signal that GSM authentication is not acceptable has been changed. Also, a new (optional) feature allowing identity privacy in a manner similar to EAP SRP has been added.

- EAP type for the UMTS Authentication and Key Agreement (AKA)
- EAP/AKA supports all the UMTS AKA scenarios
- basic authentication, sequence number synchronization etc.
- Similar IMSI privacy support as in EAP/SIM
- EAP/AKA includes GSM compatible mode
- basic GSM authentication without the enhancements of EAP/SIM
- The home server knows if this particular user has been given an old GSM SIM or a newer UMTS USIM
- Client can refuse GSM-only authentication

3GPP SA1 in TR 22.934 v1.0.0 have also identified that an option to realise the requirement "access control related functions within user equipment with a similar level of security that exists in 3GPP user equipment" is to have a UICC card containing SIM or USIM application in the UE.
Some constraints have been identified, for example;

1. Deployed WLAN devices (according WLAN standards, e.g. 802.11, HiperLan 2 etc), that meet interworking requirements, e.g. security, shall be supported without upgrading the functionality.

2. The user involvement in enabling scenario 2 interworking functionality in terminals shall be minimised (e.g. installation of SW) and by the reuse of existing 3GPP permanent subscriber database (e.g. HLR)

3.2.3 IPSec

Though IPSec is used primarily for data confidentiality, extensions to the standard allow for user authentication and authorisation to occur as part of the IPSec process.

SA3 will need to determine if the combination of USIM authentication and IPSec can be used alone or can be combined into a workable solution for WLAN UMTS interoperation.

4 Confidentiality and integrity protection of operators / users data

4.1 WEP (Wired Equivalent Privacy)

If LEAP or its equivalent is implemented, some of the concerns with WEP may no longer apply

4.2 IPSec

IPSec is a framework of open standards for ensuring secure private communications over IP networks. IPSec VPNs use the services defined within IPSec to ensure confidentiality, integrity, and authenticity of data communications across public networks, such as the Internet. IPSec also has a practical application to secure WLANs by overlaying IPSec on top of cleartext 802.11 wireless traffic.

When deploying IPSec in a WLAN environment, an IPSec client is placed on every PC connected to the wireless network and the user is required to establish an IPSec tunnel to route any traffic to the wired network. Filters are put in place to prevent any wireless traffic from reaching any destination other than the VPN gateway and DHCP/DNS server. IPSec provides for confidentiality of IP traffic, as well as authentication and antireplay capabilities. Confidentiality is achieved through encryption using a variant of the Data Encryption Standard (DES), called Triple DES (3DES), which encrypts the data three times with up to three different keys.

SA3 will need to determine an appropriate scheme based on an analysis of the strengths of WEP LEAP and IPSec.

5 Charging and Billing Security Issues

5.1 Fraud Management

It will be important to ensure that any final solution generates sufficient information to allow fraud to be detected and managed. SA3 should make recommendations on such issues as format of call/ session records, reporting of authentication failures, QoS changes and service termination mechanisms.

5.2 Service Termination in Real Time

As the charging information affects the service rendered, a mechanism may be required to allow the 3GPP system to indicate to the WLAN system that the service rendered should be terminated, interrupted or modified (for example for pre-paid users).

5.3 QoS issues

Although the specifications shall permit a technical implementation of handover between a 3GPP System and a WLAN, there may be a temporary change of QoS on bearer services at the time of handover. Any non-temporary change in the QoS shall be seen at the service access points as a network initiated renegotiations of QoS. If the newly negotiated QoS is not acceptable, the UE/user may terminate the connection/context.

SA3 will need to determine if there are any security issues with such a change in QoS e.g. repudiation of a legitimate service charge and make appropriate recommendations.