3GPP TSG SA WG3 Security — S3#25 **S3-020539**
8 - 11 October 2002
Munich, Germany

Source: Ericsson

Title: 3G-WLAN – Security Endpoint

Document for: Discussion and approval

Date: 03-10-2002

1 Introduction

While 3GPP standards will not specify the exact architecture and mechanisms of WLAN Access Networks, setting requirements seem inevitable to guarantee the same level of security in WLAN Access Networks (AN) as in 3G cellular networks.

One important issue in this scope is the location of the security endpoint for traffic protection; and, consequently, the method of protection.

This discussion paper argues that the security endpoint must be physically secure; and, hence lie "deeper" in the WLAN AN than the WLAN access point. Traffic protection alternatives are also discussed and a solution using IPsec is sketched.

2 Background and Motivation

Most WLAN technologies provide (optional) link-layer protection between the WLAN UE and the WLAN AP. Present day public access WLAN deployments, however, typically disable such protection. Although this behaviour is expected to change for 3G-compliant WLAN AN:s, it is not clear that UE-AP air interface protection will suffice to meet 3GPP's stringent security requirements.

There are both technical and business/operational arguments for placing the security endpoint (or alternatively "a" security endpoint) further from UE:

- The security properties of different link-layer mechanisms may (and, currently, do) differ significantly, making a uniform security solution based on link-layer protection alone difficult. [If all WLAN technologies meet 3GPP's security requirement then a heterogeneous solution may be acceptable.]
- WLAN AP:s for public access will have to operate in public places, where physical security of the AP:s and their fixed side connections may be difficult to guarantee. [It may suffice to mandate physical security of all WLAN AP:s their fixed network connections in a 3GPP-compliant WLAN AN.]
- Public access WLAN operators with a non-3GPP user base may wish to offer access to both 3GPP-compliant clients and others simultaneously with little or no modification to their existing operations (i.e. allow other forms of authentication, and perhaps even leave the air interface unprotected). Thus, a 3GPP-specific "add-on" solution may be preferable to protect only roaming 3GPP customers. [Interoperability with existing deployments may not be a strong requirement.]
- For time or volume based charging per-packet integrity protection appears necessary between the UE and the node collecting/generating charging information. [Modern WLAN AP:s with built-in AAA(RADIUS) functionality may perform this task.]

Arguably, the above points indicate that traffic protection to a node behind the WLAN AP:s would be preferable (although sensible counter-arguments are also given in brackets). As a side effect, a 3GPP-specific node or module in the WLAN AN can provide advantages other than traffic protection (e.g. DIAMETER/RADIUS translation).

3 Protection Alternatives

This section assumes that the security endpoint resides on a node with (at least in part) 3GPP-mandated functionality. For brevity, this node/function will be referred to as the "3GPP-module".

Independent of the specific method of traffic protection, the security association should be cryptographically tied to the AKA authentication by using keying material derived from the AKA parameters. The basic assumption is that the procedure specified in EAP-AKA can be used. As witnessed by the temporary identity handling (and a potential reauthentication) extension, EAP-AKA is quite flexible; so, it may be possible to include a simple security mode setup negotiation in it.

Since the relevant WLAN technologies are Ethernet-like (or emulate Ethernet) and the main purpose of public access WLAN is to offer IP connectivity, the two main candidates for traffic protection in WLAN AN:s are the IEEE 802.10 Standard for Interoperable LAN/MAN Security at the link layer (L2) and the IETF IP Security solution at the IP/network layer (L3).

A third alternative could be to extend the link-layer protection offered natively by the respective WLAN technology to a node behind the WLAN AP. Such an approach may involve some technical difficulties due to the tight integration of link-layer security and other MAC-layer features. Also, the IEEE 802.11i task group, for example, decided that nodes beyond the wireless link are outside their scope.

3.1 Pros and cons of the L2 solution

The 802.10 security solution is attractive, because it is completely transparent to both the WLAN AP:s and the higher layer applications on the WLAN UE, including security mechanisms on the network and transport layers.

The use of 802.10 would require that the 3GPP-module is placed on a node reachable on L2 from the UE. This constraint does not appear to be too limiting, since the access router could be a natural choice for the 3GPP-module's location.

The major drawback of an 802.10-based solution, however, is that the standard is not widely used or even implemented.

3.2 Pros and cons of the L3 solution

IPsec is a more mature, widely deployed technology. It would also allow more freedom in the placement of the 3GPP-module (in case that mattered). On the other hand, a full-blown IPsec client, complete with IKE negotiation and policy management, is unnecessarily heavy in this specific scenario.

In addition, a usual IPsec-based solution for WLAN traffic protection is likely to interfere with an IPsec-based VPN client the WLAN user may wish to use for corporate access. Unless all uses of IPsec in the WLAN UE are coordinated, conflicts between different IKE processes attemtping to bind to the same well-known port (UDP 500) may render all (but perhaps one) IPsec-based solutions inoperable. Ensuring the correct order of IPsec tunnels (i.e. the corporate tunnel should run inside the WLAN tunnel and not vice versa) may prove difficult if not impossible without coordination.

The presence of NAT devices between the UE and the security endpoint could also present problems for an IPsec-based solution. Since NATs are not expected to be deployed in the WLAN AN, this is mainly relevant if the security endpoint is located outside.

3.3 A potential L2.5 solution for 3GPP

A possible approach to combine the best of the L2 and L3 solutions could be to implement a simple IPsec tunnel extension on L2.5 (i.e. between L2 and L3), in the WLAN driver. Since the WLAN UE will need a 3GPP-specific software update to support EAP-AKA, there would be no incremental logistic impact due to this solution.

The security association would be keyed directly from EAP-AKA, thus eliminating the need for and avoiding conflicts with IKE. If desired, a simple security mode setup procedure could be added to the EAP-AKA exchange. Alternatively, a preset IPsec mode (e.g. ESP/AES/SHA) could be mandated by 3GPP.

The application of IPsec at L2.5 would also guarantee the correct tunnel order. Furthermore, just like 802.10, this protection method would be completely transparent to the UE's IP stack, while keeping the advantages of IPsec.

Unfortunately, the potential problems with NATs and IPsec still persist, although a simple solution may be possible for this special case.

4 Air interface protection

As the 3GPP security requirements could be met by the IPsec solution at L2.5, extra link-layer protection on the WLAN air interface may seem unnecessary. Note, however, the wireless link is likely to be the most vulnerable in the entire system, and the native link-layer protection can thwart certain IP-layer attacks. Hence, if enabled, the WLAN link-layer security should still be used.

Since the 802.1x/EAP authentication would be initiated through the WLAN AP even in this scenario, the 3GPP-module would need to intercept the EAP traffic (this would also be necessary for security mode setup or RADIUS/DIAMETER translation), and generate the key sent to the AP based on a (3GPP-specified?) key derivation method. A simple application of a cryptographically secure one-way function to derive the AP key from the key passed from the AAA Server would suffice.