3GPP TSG SA WG3 Security — S3#35 **S3-040749**

5 - 8 October 2004

St Paul's Bay, Malta

Title: **Use of MAC addresses**

Source: **Ericsson**

Document for: **Discussion and decision**

Agenda Item: **6.10 WLAN interworking**

Work Item: **WLAN-IW**

1 Introduction

This discussion paper analyzes the suitability of using the MAC address to identify the user's device in WLAN interworking.

In TS 33.234, the use of the MAC is currently specified in order to check if a certain user is connecting to the WLAN access network with different devices. These devices get access to a single (U)SIM in order to authenticate and authorize against the 3GPP AAA server.

2 Discussion

The MAC address can be described this way:

Media Access Control address or MAC address is, in computer networking, a unique identifier physically stored inside a network card or similar network interface and used to assign globally unique addresses. When connected to the Internet from a computer or host, a correspondence table relates the IP address to the computer's physical (MAC) address on the LAN.

In WLAN, the MAC address is the physical address of the WLAN network card installed in the computer or other device willing to access the WLAN access network.

WLAN interworking in 3GPP foresees that the devices accessing the WLAN will not host the (U)SIM needed for authentication, but other existing devices (e.g. a mobile phone) will be accessed for this purpose. Recently, in TS 33.234 it was introduced that the MAC address had to be sent to the 3GPP AAA server. With this, it was intended to control that not more than one device, was being authenticated with one (U)SIM, that is, if the MAC addresses received for the same user, in two authentication processes, were different, that meant that two devices wanted to access the WLAN using the same (U)SIM. Nevertheless, it has to be noted the following facts:

- Although physical MAC addresses are permanent by design, several mechanisms allow modification, or "spoofing", of the MAC address that is reported by the operating system. The MAC address is not authenticated, that is, there is no guarantee that it hasn't been spoofed or tampered.

- If an attacker wanted to spoof the MAC address of subsequent devices accessing a WLAN with the same (U)SIM, it wouldn't work as in a LAN environment the MAC addresses have to be unique (for layer 2 routing purposes).

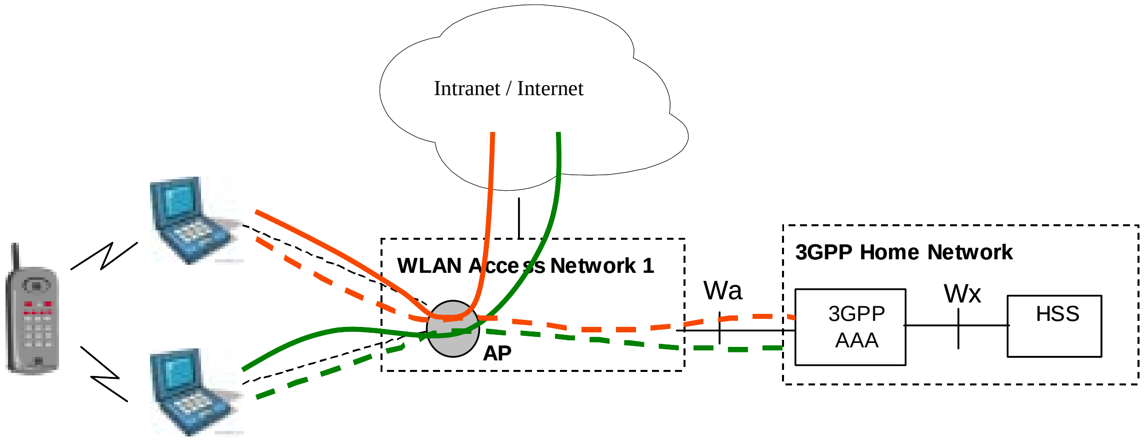
- Otherwise, the attacker can make the two (or more) devices to attach to different WLAN access points. In that case, the MAC addresses could be made equal and the attack would work because the AAA server wouldn't detect it.

- In case of scenario 3, not only the MAC address can be spoofed but also the WLAN access point information, because the WLAN AN does not participate in the authentication/authorization process by any means.

Taking into account these observations, we can differentiate four different situations in which the attack we want to mitigate can be launched. For simplicity, it will be assumed that the attacker wants to mount the attack with two devices.

Same WLAN access network, scenario 2

In this situation, the attacker has two WLAN capable devices, and wants to get access to the WLAN access network for both devices, which are attached to the same WLAN access point



As the AAA server will receive the WLAN access point information (by means of the NAS-IP address attribute), it will know that the authentication requests are coming from the same WLAN access point. In that case, there is the certainty that the two devices cannot own the same MAC address, so if a subsequent authentication request is received for the same user but with different MAC address, the AAA server will certainly know that a new different device is trying to get access on behalf of that user, and will be able to block the access.

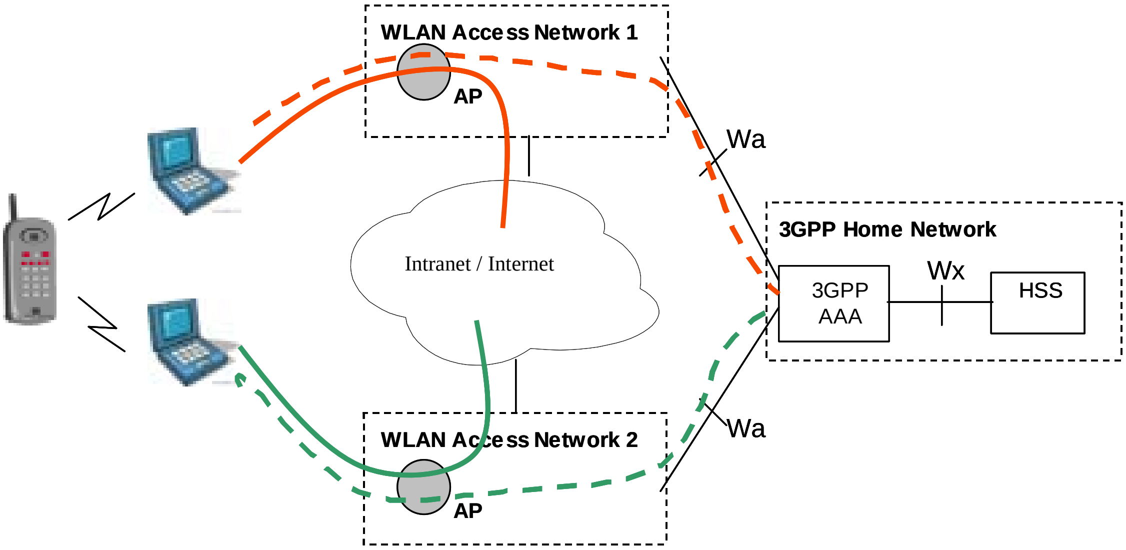
However, some devices can legally own two or more MAC addresses, simply by means of owning two or more WLAN network cards. But the case in which a computer uses two or more WLAN network cards to access the same WLAN access network does not seem realistic, so we can conclude that in this situation the sending of the MAC addresses helps to mitigate the fraud situation.

Note that the Home AAA server will receive the WLAN access network name by means of the Location Name attribute but this does not give accurate enough information as it does not reflect the access point where the WLAN capable devices are attached.

Different WLAN access points, scenario 2

This situation can happen in places where the same area is served by more than one WLAN access provider, or there are several WLAN access points that handle independent MAC address spaces. The attacker has two

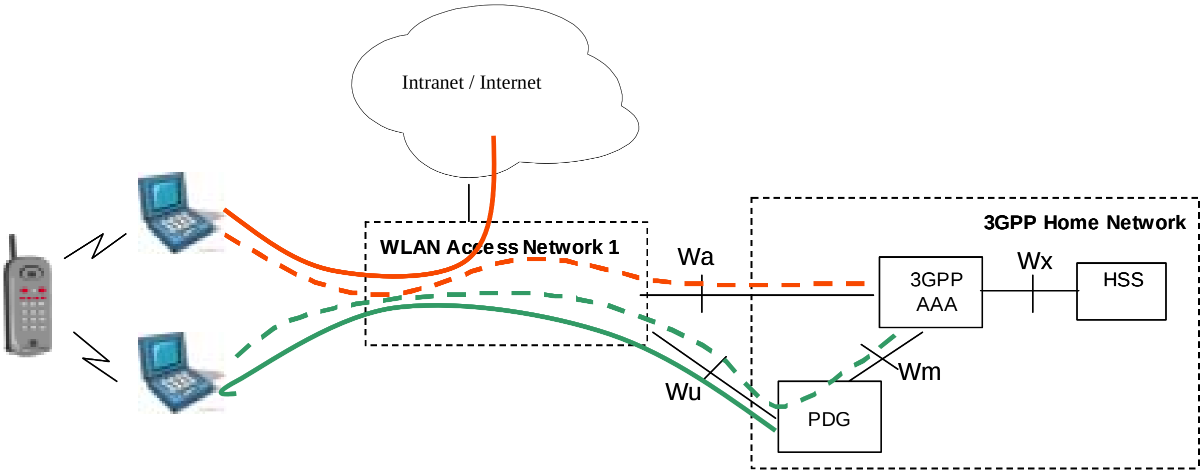
WLAN capable devices, and wants to get access for both but in different WLAN access points. These different WLAN access point can be in the same WLAN access network or in different ones. The picture shows when they are in different ones.



The AAA server, if it receives the MAC addresses and the WLAN access point information, can detect that the two devices are in different WLAN access points (by means of the NAS-IP access attribute) and likely in different WLAN access networks (by means of the Location Name attribute). But if the MAC addresses are equal it can be because of: 1-one of the devices has spoofed the MAC address to make it equal to the other, or 2-it is the same device that is pre-authenticating in other WLAN access point. As the AAA server has no means to distinguish between these two situations, the simultaneous access cannot be forbidden as it could correspond to situation 2 which is perfectly legal, so the sending of the MAC address does not help in this case.

Simultaneous access to scenarios 2 and 3

The attacker in this case wants to get access to the WLAN AN and to 3GPP network services, one with each device.



As explained above, in this situation it doesn't matter if the devices are in the same of different WLAN access point, because the AAA server will never have reliable information of the WLAN access point, for the device(s) authenticating via scenario 3. Hence, the WLAN access point information has to be discarded as parameter to rely on.

The only parameter to check would be the MAC addresses of the two devices. However, as said before one device can legally have more than one MAC address. And recalling the recent LS from SA1 S3-040597:

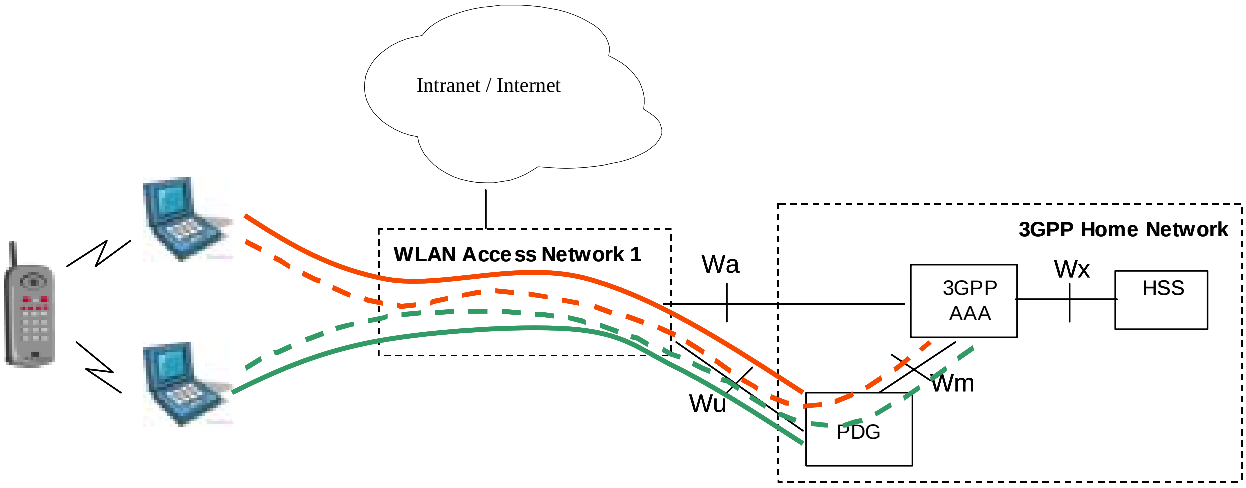
"…there is no requirement to preclude access to PS based services from access networks other than I-WLAN."

the access to scenario 3 doesn't have to be made necessarily via a WLAN, it can be for example with a LAN. So the situation in which a user, with one device, accesses the WLAN with a WLAN card and 3GPP network services with an Ethernet LAN is perfectly possible, and this implies that two authentication requests, for the same user, with different MAC addresses, has to be allowed.

Then, the sending of the MAC addresses in this situation does not help as the AAA server cannot distinguish between a fraud and a legal situation.

Two devices accessing simultaneously to scenario 3

In this situation the attacker will have two devices accessing the PDG in the 3GPP network, regardless the type of connection they are using (WLAN, LAN, etc.).



As there is no WLAN access point information available (and trusted), the attacker can connect its devices to different networks and spoof the MAC addresses to make them equal. Then, the MAC addresses here do not help to detect the attack.

3 Conclusions

The previous analysis shows that only in one case the MAC addresses are reliable parameters to detect this type of fraud, but in the rest they don’t help.

Therefore, the AAA server has to be able to detect this situation (the first case) and enforce policies only in that case. In the rest of the situations, the MAC addresses should be discarded if received. If the AAA server is not able to determine the trustfulness in the MAC address (for example because the WLAN access point information is not available), it is recommended to NOT enforce any policy, based on the MAC addresses.