3GPP TSG SA WG3 Security — S3#26 **S3-020624**
19- 22 November 2002
Oxford, UK

Source: Nokia

Title: WLAN Identity Privacy with Cryptographic Temporary Identifiers

Document for: Discussion and approval

Agenda item: TBD

1 Introduction

The current working assumption in SA2 is that identity privacy on WLAN is implemented with temporary identifiers. This submission discusses the security implications of architectural choices and proposes a mechanism based on cryptographic temporary identifiers.

2 Identity Privacy Considerations

In order to achieve the same level of identity in the 3GPP-WLAN interworking system as currently in 3GPP, the identity privacy solution needs to take into account the special characteristics of WLAN networks. Contrary to other 3GPP radio access networks, false WLAN access points are relatively cheap and easy to install and hence active attacks are easier to mount over WLAN than over other 3GPP radio access networks. Therefore, it is desirable that the 3GPP-WLAN interworking system should be able to resist both passive and active attacks against the privacy of the subscriber identity.

EAP/SIM and EAP/AKA protocols support the use of temporary identifiers. They include a mechanism to transport a new temporary identifier from the 3GPP AAA server to the UE as part of the authentication procedure. If the UE has a temporary identifier when starting full USIM/SIM authentication, the UE uses it instead of the permanent IMSI-based identity. In order to provide true unlinkability, so that an observer cannot link the user's sessions together, the temporary identifiers should not be re-used. Therefore, the 3GPP AAA server should send a new temporary identifier as part of every full SIM/USIM authentication procedure.

The EAP/SIM and EAP/AKA protocols also include means for the network to request for the permanent IMSI-based identity in cases when the network is not able to decode a temporary identifier that the UE has used. However, the UE has no way of telling whether the EAP request for the permanent identity originates from a valid 3GPP AAA server or from an active attacker that is trying to learn the true identity of the subscriber.

One way to protect against such active attacks on the UE is to ignore requests to send the permanent identity if the UE has a valid temporary identifier available. This is possible if the UE can assume that the network is able to maintain the temporary identifiers that the network assigned and sent to the UE. For example, the UE could assume that if it has received a temporary identifier less than a month ago, the network should still recognize it. Such policy on the UE is infeasible if the network can lose the temporary ID for example due to a 3GPP AAA server malfunction, because the policy would prevent the UE from authenticating with a valid 3GPP AAA Server after reboot. Depending on the UE implementation, it may also be possible that with an explicit intervention by the user, the UE policy of not sending its permanent identity could be temporarily overridden.

To facilitate the described protection against active attacks, the home 3GPP network needs to store the temporary identifiers in a reliable manner, as carefully as it stores any other permanent or semi-permanent subscription data. The home network should be able to decode the temporary identifier to the permanent

IMSI-based identity, even if the 3GPP AAA server changes, and even if there are 3GPP AAA servers from different vendors. Still it would be desirable not to require any inter-AAA server protocols just to transfer temporary identifier information.

The UE may fail to store a temporary identifier sent to it as part of full USIM/SIM authentication. In this case, the UE will typically use the previous temporary identifier on the next connection. Hence, the home 3GPP network must be able to decode the previously used temporary identifier (because the UE may use it again) and any temporary identifiers issued after it.

3 Cryptographic Temporary Identifiers

Instead of storing each assigned temporary identifier in a database, we propose that the 3GPP AAA server composes cryptographic temporary identifiers that contain the encrypted IMSI. The cryptographic temporary identifier needs to be composed in a randomised manner so that a different identifier is obtained each time when composing a temporary identifier for a given IMSI.

The temporary identifier should be a self-contained "opaque token" so that the 3GPP AAA server does not need to store any subscriber-specific or temporary identifier specific data in order to be later able to decode the identifier. The home network only needs to store the common cryptographic keys and other common parameters that may be required to decode the temporary identifiers. Hence the 3GPP AAA server does not need to maintain any subscriber specific data for users that do not have active sessions.

We also propose that the format of the cryptographic temporary identifier is standardized in SA3 in order to ensure that different 3GPP AAA server implementations are able to decode each other's temporary identifier.

This proposal does not have any impact on the EAP/SIM and EAP/AKA protocol specifications. The UE does not need to know how temporary identifiers are allocated.

4 Proposal

We propose the following requirements be agreed as a starting point for the identity privacy design:

- Cryptographic temporary identifiers that contain the encoded IMSI are used for identity privacy
- Temporary identifiers are allocated and decoded by a 3GPP AAA server
- SA3 shall specify the format of the cryptographic temporary identifier in order to achieve interoperability among different 3GPP AAA server implementations
- It shall be possible to change regularly the keys that are used for cryptographic temporary identifiers
- The home network should store the keys used for encoding and decoding temporary identifiers reliably
- The same temporary identifier keys should be available for all 3GPP AAA servers in the home network
- The 3GPP AAA server should allocate a new temporary identifier on every full SIM/USIM authentication, so that the UE does not need to use the same temporary identifier more than once.