3GPP TSG SA WG3 Security — S3#32 **S3-040046**
09 - 13 February 2004
Edinburgh, Scotland, UK

Source: **Ericsson**
Title: **The Spreading of Vulnerabilities between WLAN and GSM**

Document for: **Discussion**
Agenda Item: **WLAN**

1. Introduction

The spreading of GSM vulnerabilities to WLAN networks has been discussed in SA3#31 [1], and Colin Blanchard's contribution [2] discusses the spreading of WLAN vulnerabilities to GSM networks. This paper discusses under which conditions the vulnerabilities can or can not spread from one network to another.

The paper is organized as follows. Assuming certain nodes in the network can be compromised, the knowledge of the compromised can leak out. In order to assess the impacts of this, it is necessary to understand what knowledge is held by the different nodes in the network. Section 2 discusses this. Section 3 shows the relationships of the different quantities. Section 4 presents an analysis.

We assume a split UE scenario in this paper. While the design of the specific protocol mechanisms for this is still under discussion, we assume that it is based on either the termination of EAP in the cellular terminal (alternative 2 in [3]) or the derivation of the MK in the cellular (alternative 3).

2. Knowledge of the Nodes

The cellular network nodes have the following information:

- SIMs know the challenges (RANDs or AUTNs), and are responsible for storing long term keys and the replay protection counters (in UMTS). The SIMs are also responsible for generating responses and session keys (Kc or CK/IK).

- Cellular terminals know the challenges, responses, session keys, and replay counters.

- Visited network nodes such as the MSC/VLR know the challenges, responses (even before the terminals respond), session keys, and replay counters.

- Home network nodes such as the HLR/HSS generate challenges, responses, and session keys. The nodes also store long-term keys and replay protection counters.

We divide the Wireless LAN nodes as follows:

- Home AAA server is the authoritative AAA server that responds to an authentication request.

- Proxy AAA server(s) are the intermediate nodes that pass authentication and accounting requests along, but do not respond to them themselves.

- Access Points are the nodes that provide Wireless LAN access and request the clients to authenticate themselves. The access points delegate the remainder of the authentication exchange to the Home AAA server.

- Laptops are the devices that have a wireless LAN connection.

- Cellular terminals house the SIM cards that the laptops use for authentication in a split UE case.

The Wireless LAN nodes have the following information:

- The home AAA server knows the challenges, replay protection counters, responses, and the Master Session Key (MSK). Depending on protocol design, the home AAA server may also know the original session keys (Kc and CK/IK), and may know these and the response even before the user has authenticated.

- The proxy AAA servers know the challenges and replay protection counters. They also know the responses the MSK, but only after the user has already authenticated.

  (For the purposes of simplifying the discussion, we ignore the fact that some of the nodes know only a part of the MSK known as the Pairwise Master Key, PMK.)

- The access points know the MSK and the link-layer keys derived from it. The access points also see the challenges, responses, and replay protection counters as they pass through it.

- The laptop knows the MSK and the link-layer keys derived from it. Depending on how the split UE scenario is implemented, it may also know additional information. If EAP is terminated on the cellular terminal, it does not know anything additional. If Master Key (MK) calculation is done in the cellular terminal, then the laptop also learns the MK and the Transient EAP Keys (TEKs) used within the EAP method.

- The cellular terminal knows the challenges, responses, session keys, and replay counters. Depending on its role in the split UE scenario, the terminal may also know the MK, TEKs, and the MSK.

3. Relationships of Cryptographic Quantities

The following relationships can be seen between the different cryptographic quantities. Unless otherwise indicated, the relationships are one way. In other words, if Q can be used to derive P, it is not possible to derive Q from P unless a strong cryptographic function such as SHA1 is broken.

- The long term keys and challenges can be used to derive responses and session keys.

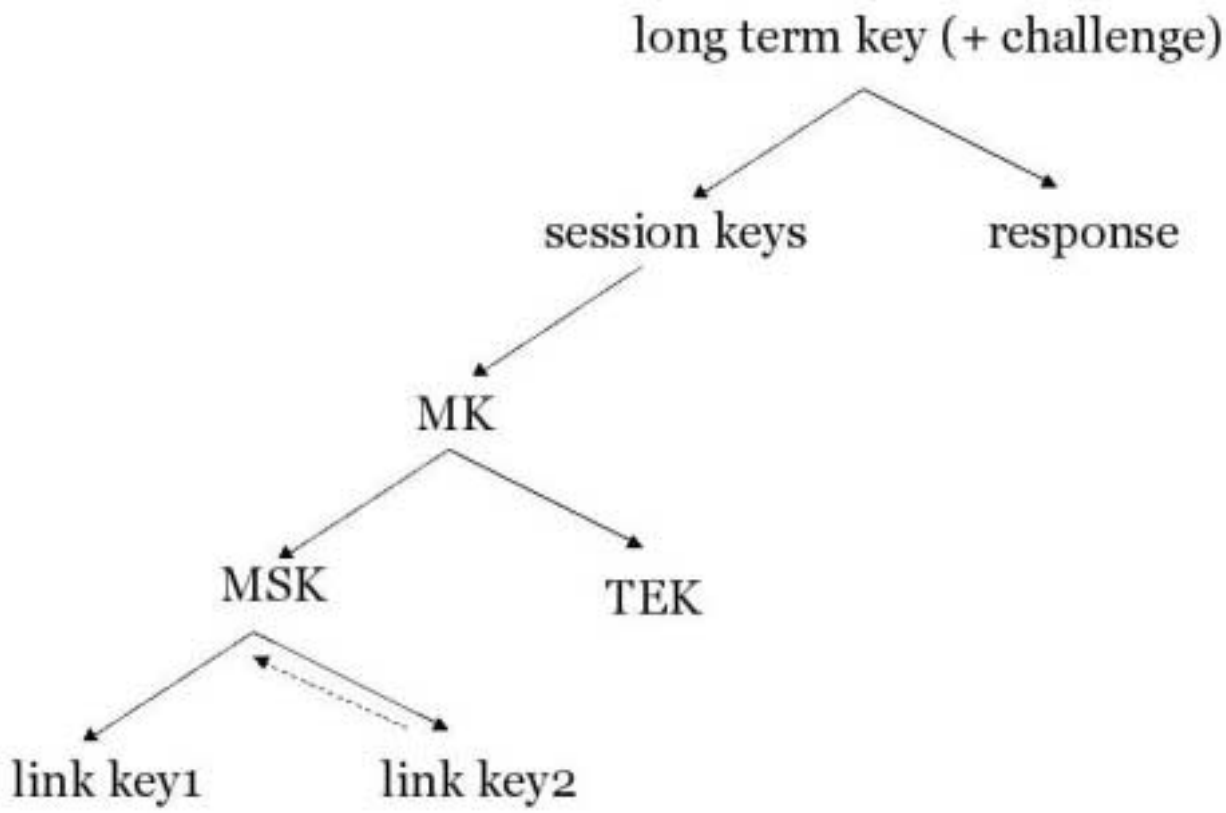
- The session keys can be used to derive MK.

- MK can be used to derive TEKs.

- MK can be used to derive MSK.

- MSK can be used to derive link-layer keys. (If the link layer keys are not derived from the MSK using a one-way function, the compromise of the keys may reveal the MSK as well. Fortunately, link layers such as 802.11i and WPA use a one-way function.)

This is also illustrated in the below figure.



4. Analysis

With the help of the above facts, we can analyze the implications of compromising the nodes related to Wireless LAN access:

1. Home AAA server

   A compromise of the AAA server would reveal information necessary to authenticate both cellular and Wireless LAN users, such as the challenges, responses and session keys.

   This enables attacks to GSM and UTMS authentication.

2. Proxy AAA servers

A compromise of a proxy AAA server would reveal the used challenges, responses (after the authentication), and the MSK.

Given that a one-way function is employed to derive both the MK and the MSK, this does not help in deriving the corresponding cellular quantities, Kc or CK/IK. Therefore, an attack against GSM or UMTS authentication is not possible via a proxy AAA server.

In the case of a GSM SIM, the compromise of the challenges, responses, and the MSK would make it possible to replay the same authentication in Wireless LAN, if the client did not have any affect on the EAP conversation. However, in EAP SIM the client introduces a nonce, which prevents this. Thus, the compromise of a proxy AAA server does not help in attacks against wireless LAN authentication either. (But of course, a compromise of a proxy AAA server makes it possible to provide access to unauthorized clients working together with the proxy, for instance, by responding to authentication requests without forwarding them to the home network.)

A compromise of the MSK makes it possible to retrieve the used link-layer session keys. Thus it becomes possible to inspect the user's traffic, or send traffic on the behalf of the user over this particular Wireless LAN session.

3. Access point

   A compromise of the access point reveals the same quantities as in item 2 above. Thus, this does not help in an attack against GSM or UMTS authentication, or the replay of the same Wireless LAN authentication in another situation.

   A compromise of the access point compromises also the user's cleartext traffic, as link-layer protection is terminated on the access point.

4. Laptop

   The compromise of a laptop would reveal at least the MSK and the link-layer keys derived from it, possibly also the MK and TEKs.

   Given that the MK, TEKs, and MSK are derived via one-way functions, the corresponding cellular quantities (Kc or CK/IK) cannot be derived. Therefore, an attack against GSM or UMTS authentication is not possible via a laptop.

5. Cellular terminal

   The compromise of a cellular terminal reveals all quantities except the long-term keys.

   This can be used to perform attacks against GSM and UMTS authentication or WLAN authentication, posing as the SIM card that the terminal houses. It does not provide a means to attack authentication related to other SIM cards.

5. Conclusions

It can be assumed that access points and laptops are relatively vulnerable to compromise, given their number, location and typical construction. Proxy AAA servers may be vulnerable to compromise, though this is far less likely. Home AAA servers, HLR/HSS, and MSC/VLR are not expected to be easily compromised.

Based on our analysis, the compromise of proxy AAA nodes, access points, and laptops does **not** result in any vulnerability against GSM or UMTS authentication.

The compromise of the home AAA server **does** result in vulnerabilities even for GSM and UMTS, though the exact nature of the threat depends on the detailed protocol design. As a result, we recommend a similar level of protection for this node as is already provided for the HLR/HSS. On a practical note, it seems that the main purpose of this node in the architecture is to act as a "translation agent" between IETF AAA protocols and the HLR/HSS, to avoid a modification in the HLR/HSS itself. Thus it seems natural that the node is kept at a central location in the cellular network. Put in another way, the Wx interface should not cross-administrative boundaries, and the AAA server should be in a physically secure location.

As is obvious, the compromise of a cellular terminal opens attacks in GSM and UMTS. These attacks carry on to the Wireless LAN. As discussed in [1], limiting the use of A5/2 on terminals that provide also Wireless LAN access helps mitigate this attack. A more long-term solution is to provide key separation, but that would require new GSM and UMTS functionality as a change in the highest part of the key hierarchy would be needed.

6. References

[1] S3-030733, Implications of the A5/2 Attack for 3GPP WLAN Access Ericsson, TeliaSonera
[2] S3-040009, Protecting GSM/GPRS networks from attacks from compromised WLAN networks when interworking, British Telecom.
[3] S3-030747 Pseudo-CR to TS 33.234 on Requirements on UE split, Siemens