3GPP TSG SA WG3 Security — S3#33 **S3-040279**

10 - 14 May 2004

Beijing, China

Title:	**EAP method policies and release 6 non-compliant implementations**
Source:	**Nokia, Ericsson**
Document for:	**Discussion and decision**
Agenda Item:	
Work Item:	**WLAN-IW**

1 Introduction

This paper studies EAP method policies and implications of ME and AAA server implementations which do not conform to release 6 specifications. Different cases are presented from the viewpoint of AAA server and ME policy. Recommendations about AAA server and ME EAP method policies are proposed.

2 Discussion

2.1 AAA policy

2.1.1 AAA Server allows EAP-SIM for USIM subscribers

If the AAA server policy allows EAP-SIM for USIM subscribers, then a malicious terminal can try to impersonate as a subscriber and initiate EAP SIM with the subscribers IMSI even if the subscriber has USIM. The attacker might initiate EAP-SIM in order to exploit some weakness that is only present in EAP-SIM but not in EAP-AKA. It is not possible to avoid this problem by any EAP method negotiation protection, because the AAA server's EAP method policy accepts EAP-SIM when the rogue terminal claims not to support EAP AKA.

2.1.2 AAA Server does not allow EAP-SIM for USIM subscribers

If the AAA server policy does not allow EAP SIM when the subscriber has a USIM, then it will never run EAP SIM for that subscriber. If the user has a R6 non-compliant ME that doesn't support EAP AKA, then the user will not be able to make connections. This compatibility problem is well known in advance, so it only occurs if the operator wants to enforce such a policy. With this policy the operator effectively blocks WLAN access with less secure legacy terminals and forces the subscribers to update their terminals.

2.2 ME policy

2.2.1 ME allows EAP-SIM for USIM subscribers

If a Mobile Equipment policy accepts EAP SIM even if a USIM is inserted, then a malicious access point can initiate EAP SIM. It is not possible to avoid this problem by adding protection to EAP method negotiation, because the terminal's EAP method policy accepts EAP SIM when the rogue network claims not to support EAP AKA.

2.2.2 ME does not allow EAP-SIM for USIM subscribers

If the ME policy does not accept EAP SIM when a USIM is inserted, then it will never run EAP SIM for that subscriber. If the operator has a R6 non-compliant AAA server that doesn't support EAP AKA, then the user will not be able to make connections. Note: the operator can avoid the compatibility problem by making sure that its AAA servers support EAP AKA, if the operator has issued USIM cards.

3 Conclusions

The only way to avoid EAP method downgrading attacks is to enforce EAP method policies that do not accept EAP-SIM for USIM subscribers in both the ME and the AAA server. Hence, the default policies in both the ME and the AAA server shall not accept EAP-SIM if the subscriber has USIM.

However, these EAP method policies will cause incompatibility problems with R6 non-compliant ME and AAA server implementations that do not support EAP AKA. It is not possible to avoid the incompatibilities securely by adding protection to EAP method negotiation. The only way to avoid the incompatibilities is to allow configuring an EAP method policy that allows EAP-SIM even if the subscriber has a USIM. Such an EAP method policy has some undesired security implications, so it should only be used during a transition period when R6 non-compliant equipment are used, and the policies could changed back to the default once most of the equipment have been upgraded to release 6 compliant.

It is proposed that the following EAP method policy rules are adopted:

- When an operator that has deployed R6 non-compliant AAA servers issues USIM cards to subscribers, it is recommended to ensure that the AAA servers support EAP-AKA.

- The default ME EAP method policy shall not accept EAP-SIM authentication if a USIM has been inserted.

- The default AAA server EAP method policy shall not accept EAP-SIM authentication for USIM subscribers.

- In order to interoperate with R6 non-compliant AAA servers, ME implementations may allow enabling an EAP method policy that accepts EAP-SIM even if a USIM has been inserted. The drawback of this EAP method policy is that an active attacker impersonating as the network may initiate EAP-SIM authentication with the terminal.

- In order to interoperate with R6 non-compliant ME implementations, AAA servers may allow configuring an EAP method policy that accepts EAP-SIM authentication for USIM subscribers. The operator may use this configuration option, if many USIM subscribers are expected to use R6 non-compliant ME implementations that do not support EAP-AKA. The drawback of this EAP method policy is that an active attacker impersonating as a terminal may initiate EAP-SIM authentication with the AAA server. The operator should disable EAP-SIM for USIM subscribers in the AAA server policy, when most of the deployed ME's support EAP-AKA.

- Due to the security issues discussed above, it is strongly recommended that even those devices that do not conform to R6 specifications implement both EAP-SIM and EAP-AKA protocols. Note that these protocols can be implemented independent of whether the actual use of the device happens in an environment that deploys SIMs or USIMs."