3GPP TSG SA WG3 Security — S3#37 **S3-050033**
February 21 - 25, 2005
Sophia Antipolis, France

Source: ZTE Corporation

Title: Discussion about MSK MIKEY Message Reception in the ME

Document for: Discussion and decision

Agenda Item: MBMS

1 Introduction

In clause 6.4.6.1 of 3GPP TS33.246 v6.1.0, SP payload has been stored before the MSK MIKEY message is verified. This vulnerability can be used to perform some attack. This paper discusses the reception of MSK MIKEY message and proposes that SP payload should be stored after the MSK message is validated.

2 Discussion

Security Policy (SP) payload includes information for the security protocol such as algorithms to use, key lengths, initial values for algorithms etc. In MBMS, SP payload only defines a set of policies that apply to SRTP. SP payload is independent of the policies (such as algorithms) which are used to verify the MSK message. Therefore it will not impact the validation of MSK message when SP payload is stored in ME.

If the SP payload is stored before the MSK message is verified, attacker can take advantage of it and carry out some attacks. For example, attacker can forge a MSK message with a malicious SP payload. When UE receives the spurious message, malicious SP payload is stored in ME. Even though MGV-F will return failure to ME, SP stored in ME may be changed so that UE can not decrypt the SRTP packet. By this means, an attack to availability may be performed.

3 Proposal

Since it is insecure to store SP payload in ME before MSK message is verified, SP payload should be stored after MSK message is verified. We propose to change the corresponding description in section 6.4.6.1. A CR implementing the change is also provided.