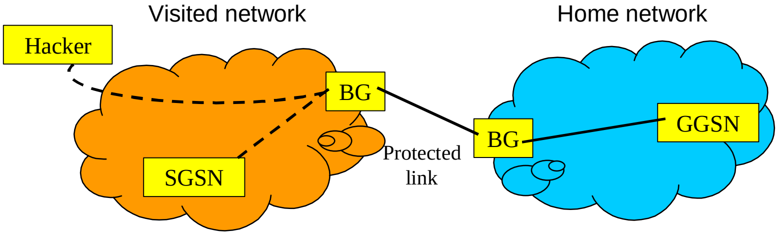
TSG-SA WG 3 (Security) meeting #18 TSG S3 (01) 0198
Phoenix, USA 21-24 May 2001 Agenda Item:

Source: France Telecom (contact: Sebastien Nguyen Ngoc, sebastien.nguyennngoc@francetelecom.com, +33 1 45 29 47 31)
Title: GTP security issue
Document for: Discussion/Decision

Issue

France Telecom is concerned with a potential security risk linked to the lack authentication between the SGSN and GGSN when roaming.
In a roaming situation, if a hop by hop security solution is used, it is likely that the signaling traffic will be protected between border gateways, but that protection within the PLMN of an operator is not always enforced (and it is actually impossible for an operator to know whether it is enforced). Therefore there is a potential attack scenario where the network of an operator can be attacked through the badly protected network of an operator it has a roaming agreement with (see figure below).



In this case, if an attacker can break into the backbone of the visited network, he can send valid signaling messages through the BG to the home network.

Proposal

France Telecom proposes that for R5 the protection of the signaling messages between the SGSN and GGSN is done end to end when roaming in order to guarantee the security of operators’ networks.