Security Implications of the Session Identifier

(draft-tschofenig-nsis-sid-00.txt)

Authors:
H. Tschofenig
H. Schulzrinne
R. Hancock
A. McDonald
X. Fu
Background

- **Discussions** about the session ownership problems already started with the requirements work.

- We spend some time at the New York *interim meeting* to discuss some issues.

- I promised to **capture** the *current status* of our discussions and to make them available to other working group members (to get a bigger audience).
Problem

- We discussed the problems several times already.
- However, no real progress seen so far.
- Mobility (in combination with security) is still somewhat fuzzy.
Goal

- Point to
  - the **implications** to the signaling protocol with regard to certain solutions
  - the **problems** with the presented problem and the corresponding solutions
  - the relationship to mobility

- As part of the mobility related NSIS signaling the following question must be addressed: **What is the expected functionality?**
Several proposals, which have been discussed in the past, are described:

These proposals are categorized into
- Global (applicable to all nodes along the path)
- Local (applicable to particular domains only e.g. visited network)

Details can be obtained from the draft (and will not be discussed here).

Important part:
- Solutions give the reader information about the assumptions and the consequences
Pending Issues

- Which is the authorizing entity?
- Which action might be authorized by whom?
- Is the Session Identifier concept useful? (tradeoff benefit vs. additional overhead)
- How should mobility signaling work in detail (e.g. always end-to-end signaling messages assumed)?
- How should replay protection be handled?

Hannes.Tschofenig@siemens.com