3GPP TSG SA WG3 Security — S3#21b **S3z020031**

31st January - 1st February, 2002

Antwerp, Belgium

Source: **Nortel Networks**

Title: **Network Handling of Untrusted IMS Clients**

Document for: **Discussion**

Agenda Item: **IMS-8, Further Contributions to TS 33.203**

Abstract

In an open, competitive environment, IMS (SIP) clients of different kinds and from a variety of manufacturers will appear on the consumer market. This contribution suggests that SA3 consider the vulnerabilities that the IMS network may have to IMS clients that are "badly behaved" (i.e. either faulty or modified with malicious intent). It may be appropriate to include in draft TS 33.203 a set of recommended handling rules by which the IMS network may mitigate its vulnerabilities.

1. Introduction

An open environment for the IMS likely will encourage the proliferation of available IMS (SIP) clients for a variety of applications and from a variety of manufacturers. In operation, the IMS network may find itself vulnerable to the actions of IMS clients that do not behave properly. This "bad behavior" may be due to either faulty software or to software that has been modified with malicious intent. The next section outlines possible vulnerabilities that fall into each of these categories.

It is likely to be of interest to IMS network operators to protect limited computing and other system resources against abuse, and to safeguard the IMS user community against the actions of others with malicious intent. Thus, consideration by SA3 of the threats posed by untrusted IMS clients is merited.

2. Possible IMS Network Vulnerabilities

IMS clients may appear on the consumer market without having been adequately tested. The following kinds of problems with faulty clients may be seen:

- SIP protocol faults (e.g., missing obligatory headers, syntax errors within headers)
- Babbling (rapid, unwarranted repetition of messages)

Threats posed by maliciously modified IMS clients may include the following:

- Denial of Service (DoS) attacks targeted at particular IMS network elements
- Disruption of service attacks aimed at individual IMS users
- Spoofing attacks, such as the one described in [1]

3. Recommendation

It is recommended that SA3 give consideration to the threats posed by untrusted IMS clients and discuss to what degree mitigation solutions should be standardized. It may be appropriate to include in draft TS 33.203 a set of recommended handling rules by which the IMS network may mitigate its vulnerabilities.

REFERENCES

[1] 3GPP TSG SA3 document S3-010633 [Ericsson]: "The 'Fraudulent User' Attack Against the IMS"