3GPP TSG SA WG3 Security — S3#23 **S3-020230**

14th – 17th May, 2002

Victoria, BC Canada

Source:	**Nortel Networks**
Title:	**Network Handling of 'Badly Behaved' IMS Clients**
Document for:	**Discussion/Decision**
Agenda Item:	**6.14, UE Functionality Split**

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 considers 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 has been clarified by SA1 in S3-020038 that Release 5 networks should be secure against attacks by such clients. It is recommended 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 badly behaved IMS clients is merited. Furthermore, in its liaison statement S3-020038, SA1 has clarified that Release 5 networks should be secure against attacks by badly behaved clients. It is recommended to include in draft TS 33.203 a set of recommended handling rules by which the IMS network may mitigate its vulnerabilities. Section 3 of this paper contains text that is recommended for inclusion in 33.203 in this regard.

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 badly behaved IMS clients and discuss to what degree mitigation solutions should be standardized. The remaining text in this section is recommended for inclusion in draft TS 33.203. The intention is to capture in standards recommended handling rules by which the IMS network may mitigate its vulnerabilities.

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. It is important to protect limited computing and other IMS system resources against abuse, and to safeguard the IMS user community against the actions of others with malicious intent. While specific handling rules are beyond the scope of standardization, a set of general principles for the handling of misbehaving IMS clients is put forth. It is recommended that IMS network element implementations take these principles into consideration.

Faulty clients

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)

Protection against SIP protocol faults can be achieved by careful implementation of the IMS network elements handling the SIP protocol [2]. Incoming messages should be checked for protocol faults and appropriate error handling action taken if faults are detected. The system design should be such that it is not be possible to achieve "theft of service" or disruption of service to other users by sending SIP messages with protocol faults.

IMS clients that issue a large number of SIP messages in rapid succession may not be functioning properly. If protective measures are not in place, large amounts of visited network IMS resources may be consumed without accomplishing any useful work; potentially, service to other IMS users may be disrupted for lack of available resources. Protective measures should be in place that discard messages from users when certain rate-based thresholds are reached. To be most effective, such measures should be implemented at the IP/port level rather than at the SIP (application) level. Ideally, the IMS network elements themselves (e.g., P-CSCF) should not have to handle large numbers of repetitive or otherwise unproductive SIP messages.

Maliciously modified clients

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]

Protective measures against intentional DoS attacks should function in a similar way as those described above for faulty ('babbling') clients. Rate-based discarding of messages under flood conditions can preserve resources for providing service to as many IMS users as possible.

Protective measures against spoofing and disruption of service attacks should be implemented in a conservative fashion. To accommodate future IMS system enhancements and additional service offerings, visited IMS network elements (i.e. the P-CSCF) should forward unrecognised SIP elements to SIP entities upstream. On the other hand, P-CSCF implementations should be responsive to particular attacks as they are identified and mitigation methods are standardized by 3GPP.

REFERENCES

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

[2] IETF RFC 3261, "SIP: Session Initiation Protocol", May 2002.