# ITU-T Workshop

## "New Horizons for Security Standardization"

## Abstract

**Geneva, 3 –4 October 2005**


Speaker: **Michel LEBER**

**Senior Marketing Manager**

**TEKELEC France**


Session: **7: Overview of some specific areas of current interest for security standardization**

Title of Presentation: **SS7 and the vulnerability of the networking infrastructure**


When SS7 was defined in a monopolistic operator environment a long time ago, there was the assumption that the SS7 network will be a closed network with limited carriers & interconnection. Therefore, the main concern was rather to secure telecom building access rather than to secure the protocols itself from intrusion.

Deregulation, multiplication of service providers, new services & applications, as well as interconnection with other types of networks like IP, has completely changed the situation. And it's clear that there was a lack of encryption or authentication.

SS7 outages are coming both from various internal & external reasons:

- software bugs
- accidents of configuration errors
- network overloads through fraud & "commercial" spam (SMS)
- network attacks by hackers with intention to put network down
- ….

In 1990 & 1991, several SS7 outages were due to software bugs and faulty software patches.

In 1998, ETSI has published a document on SS7 vulnerabilities & best practices. In the meantime, new scenarios and contexts have emerged.

- The world will be hybrid for the years to come: SS7 & IP-based networks will co-habit and this is increasing possibilities of vulnerability.
- The knowledge of signalling networks has been spread out. The Web is full of ideas on how to attack telecom infrastructure. Telecom is clearly in the Top 4 terror targets.

In the past, SS7 network attacks examples were:

- at Signalling Transfer Point (STP) level with creation/manipulation of SS7 network management messages, generating isolation or congestion of network sub-parts

- on IN-services servers (INAP protocol) where service logic is concentrated
- on circuit management (reduction of available voice channels)

Generalisation & improvement of advanced screening functions on STPs have limited such kind of problems.

Mobile networks have brought new vulnerabilities to international SS7 network with non-call related SS7 traffic (MAP, CAMEL), and in 2001 several international SCCP gateways have crashed due to roaming & SMS traffic peaks. Today in Western Europe, 95% of signalling messages on international links are SCCP, only 5% are ISUP.

Fraud & security are often related. SMS Spoofing & SMS Faking with signalling & identity manipulation are now common. (Examples are in the slides).

More complexity in case of mobile networks and globally multiplication of services like LNP, call transfer, short codes, etc… has increased strongly the average number of signalling messages per call. Therefore, there is an explosion of signalling bandwidth needs, solved by SS7 High Speed Links or SS7 over IP transport. And SS7oIP is bringing different security challenges.

With old POTS terminals, there was no risk to put a telecom network in danger. There are now also threats were terminals can be involved:

- On ISDN accesses: hackers can spoof the source address & create/introduce ISDN User Part (ISUP) messages
- Mobile Smart-phones with OS like PCs are targets for malicious code, and SMS can be used to spread “attack code” with the aim to overload the SS7 network

Other problems impacting Fraud & Security have also to be mentioned:

- new “exotic” operators dangerous for meshed SS7 networks: non-ethic behaviour, missing monitoring solutions
- lack of competences due to Opex saving,
- bad outsourcing of network management

Network architecture is changing rapidly, with the move from circuit-switched to packet-based networks. Since telecom signalling is now a terrorism target, it may let us see that traditional way and procedures for setting up new standards may be too slow for the subject of network security. Collaboration between different organizations is needed, but new relevant ideas for speeding up the process are necessary. It’s certainly one of the objectives of this workshop.

Convergence of wireline & wireline networks with IMS architecture (IP Multimedia Subsystem) & related new signalling protocols fully based on IP, replacing SS7, will certainly bring a portfolio of new services to customers, but also new security challenges to solve.