TSG-SA WG 3 (Security) meeting #9
Oslo, Norway 17th - 21st July 2000

Source: Nortel Networks
Subject: **Security requirements for access to R'00 IM subsystem**

Introduction

This contribution identifies security requirement for the IM CN subsystem to minimize the opportunity for fraudulent activity and promote a smooth evolution path.

IM CN Subsystem Security Architecture

In the PS domain, service is not provided until a security association is established between the mobile equipment and the network. IM CN subsystem is essentially an overlay to the PS-Domain and is not embedded in the SGSN or GGSN nodes consequently a second security association is required between the multimedia client and IM CN subsystem before access is granted to multimedia services. The IM CN Subsystem Security Architecture is shown in the following figure.

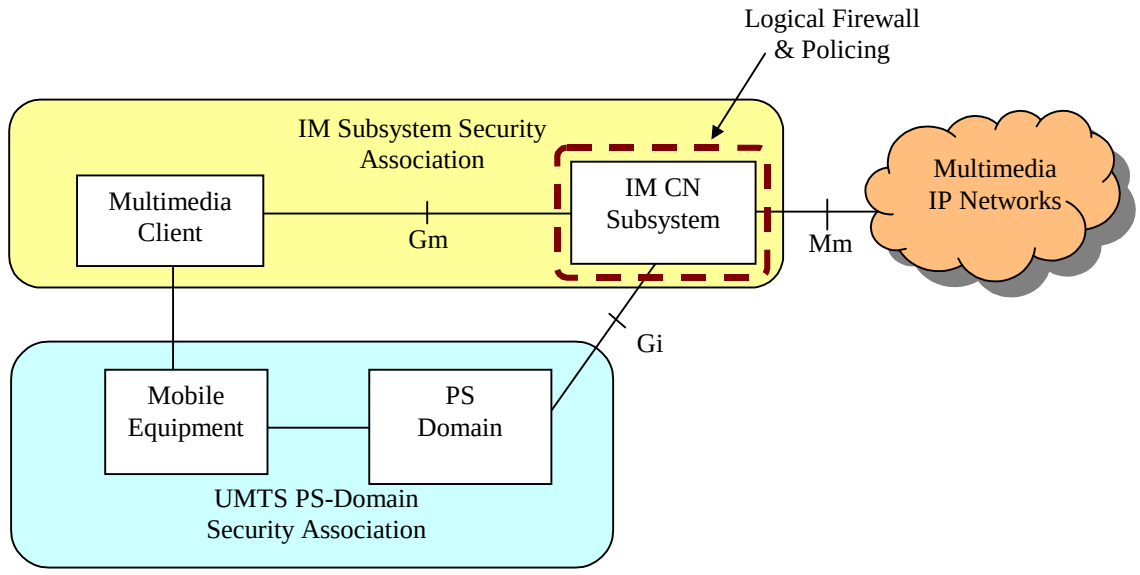

Figure 1: IM CN Subsystem Security Architecture

IM CN Subsystem Security Architecture Requirements

- IM CN Subsystem Security shall be independent of physical implementation entities.

The physical coupling of a multimedia client within the terminal may look secure, however given the availability of powerful computing platforms and communications test equipment, it would be unwise to rely on this as the primary defence mechanism. A far better approach would be to standardize a mechanism, which would provide adequate registration and authentication of the multimedia client by the IM CN subsystem, regardless of where the multimedia client is physically located.

- IM CN Subsystem Security shall be independent of lower layer security

A requirement of 3GPP is the consideration of access independence, which opens the possibility in future releases for a multimedia client to access the IM CN Subsystem via alternative access technologies e.g. xDSL, Cable Wireless. Therefore, it is essential that the IM CN Subsystem Security does not rely on the security provided by the PS-Domain and provides a smooth evolution path that would allow access via alternative access technologies. In addition, the IM CN subsystem security mechanism shall be consistent with security techniques employed in the Internet as this likely to be the termination point of the majority of traffic.

An independent IM CN Subsystem security mechanism provides additional protection against security breaches. For example, if the PS-Domain security is breached the IM CN Subsystem would continue to be protected by it's own security mechanism.

Finally, the multiple layers of security allow independent evolution to address future security needs but also allows enhancements to the individual security associations in the event of a security breaches.

- Multimedia clients located in the user device or external IP network shall not be trusted

In the past there has been a trust relationship between the voice client in the GSM terminal and the GSM network providing the service. In the more open Internet environment software clients can be developed extremely easily e.g. on home computers. This opens the possibility for rogue or badly written applications to threaten the integrity of the network. Therefore, it essential that firewalls and policing functions are installed in the network to protect against virus attacks and rogue software client. This would be inline with the internet model on which the IM CN subsystem is being built, and would not run the risk of what could happen if the trust relationships are broken.

Conclusion

The combination of appropriate firewalls, policing functions and a peer-to-peer security association between the Multimedia client and the IM CN subsystem, will both provide the best solution in terms fraud prevention and allows independent evolution of both the user device and IM CN Subsystem. Therefore, it is proposed to include the sections "IM CN Subsystem Security Architecture" & "IM CN Subsystem Security Architecture Requirements" in TS 33.102.