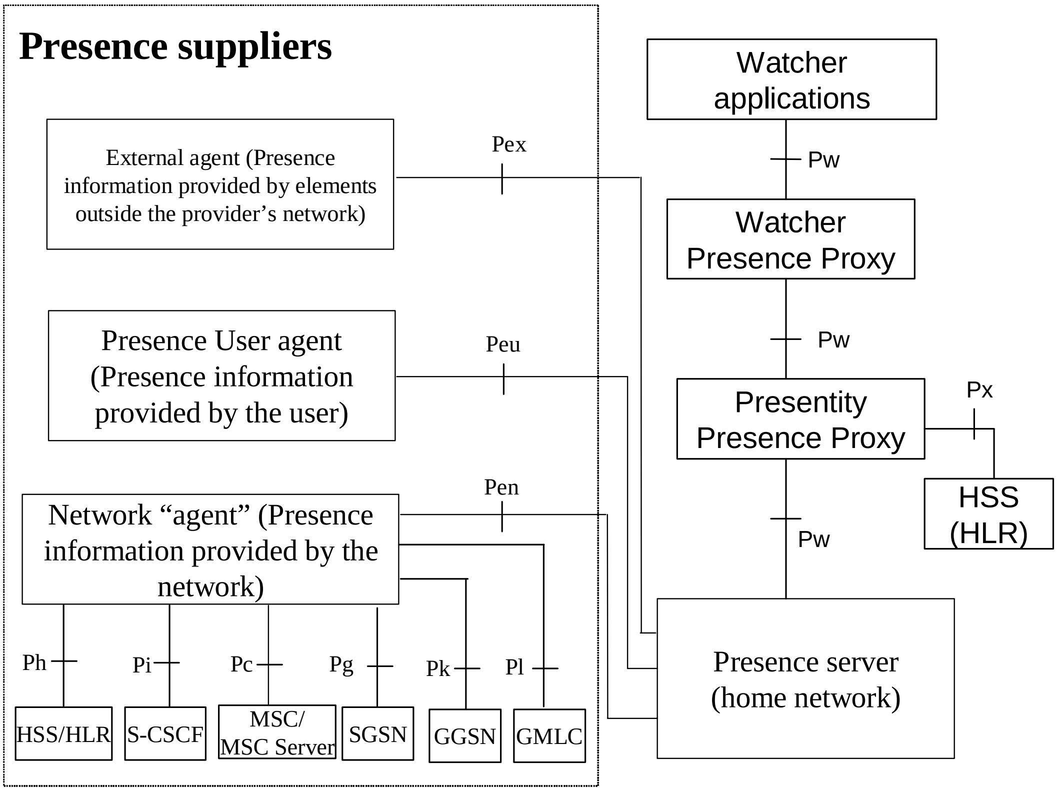
3GPP TSG-SA3 Meeting #25 ***S3-020502***
Munich, Germany, 8-11October, 2002

Title: **Presence Security Proposal**
Source: **Nortel Networks**
Agenda Item: **xx**

1. Introduction

In this contribution we propose a solution for securing the information exchanged between the Presence Server and Watcher applications. This is indicated as Pw reference point in the 3GPP presence reference architecture as shown below:



Presence suppliers
External agent (Presence information provided by elements outside the provider's network)
Presence User agent (Presence information provided by the user)
Network "agent" (Presence information provided by the network)
Pex
Peu
Pen
Ph
Pi
Pc
Pg
Pk
Pl
HSS/HLR
S-CSCF
MSC/ MSC Server
SGSN
GGSN
GMLC
Watcher applications
Pw
Watcher Presence Proxy
Pw
Presentity Presence Proxy
Px
HSS (HLR)
Pw
Presence server (home network)

Interfaces Ph, Pi, Pc, Pg, Pk and Pl are based on existing R5 procedures e.g. CAMEL, MAP, CAP, RADIUS, ISC, Cx, Sh.

Figure 1: Reference architecture to support a presence service

This interface supports both subscription and notify operations in order to support the presence service (i.e., SIP SUBSCRIBE and NOTIFY messages). The security requirements as defined in TS 22.141 [1] for these operations are authentication, confidentiality and integrity protection of the information exchanged between the Watcher and the Presence Server.

2. Authentication

Before any Watcher/Presentity (or its proxy) entity (referred to as simply watcher) can exchange Subscription requests and Notify replies with the Presence Server, it needs to be authenticated. Here we propose a mechanism to accomplish the security requirements if the Presence Service based on the IETF draft “Session Initiation Protocol (SIP) Extensions for Presence” [2].

There are two possible scenarios for authenticating subscription requests for presence information, namely, intra-domain (local administrative domain) and inter-domain authentication.

2.1 Intra-Domain

In a single administrative domain, it is assumed that all the entities that want to communicate with the Presence Server have shared secrets. Therefore, we can use the message digest authentication (MD5) over Transport Layer Security (TLS).

When a watcher wants to subscribe to the presence service, it should establish a TLS connection with the Presence Proxy or the Presence Server. The Presence Server offers its certificate to prove its identity to the watcher. On receiving a valid certificate from the Presence Server, the watcher creates the subscribe request and sends it to the presence server. The Presence Server should challenge the request with Authentication required response. On receiving the challenge the watcher replies with the message digest (MD5).

Once the challenge response is accepted by the Presence Server, the watcher should keep this TLS connection open, so that the presence server can act as a proxy, in cases where it needs to forward the subscribe requests to servers in other domains.

2.2 Inter Domain

In inter domain scenarios, establishing an authenticated identity of the watcher application is based on transitive trust, i.e., when a watcher generates Subscribe request to its local domain presence proxy, it should use SIP proxy digest authentication over a TLS connection, to identify itself to the target Presence Server. The subscribe request is forwarded to the target domain presence server over a TLS connection. It is assumed that the trust relationship between the domains is that the forwarding domain has authenticated all the watcher subscribe requests.

3. Encryption

Encrypting the entire Subscribe requests end-to-end for confidentiality is not appropriate. The intermediaries such as proxy servers need to view certain header fields in order to route the requests correctly. However, for privacy reasons the contents of the notification responses has to be encrypted.

The S/MIME could be used to encrypt the body (if any) of both subscribe request and the notify response messages. The encryption can be performed using the key of the watcher from the subscribe request.

4. References

[1] 3GPP TS 22.141: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects Service Aspects; Presence Service"

[2] Internet-Draft (draft-ietf-simple-presence-07.txt): “Session Initiation Protocol (SIP) Extensions for Presence”