3GPP TSG SA WG3 Security **S3-020508**

8th – 11th October, 2002

Munich, Germany

Agenda Item: 7.17

Source: Ericsson

Title: Working Assumptions and Open Issues in Presence Security

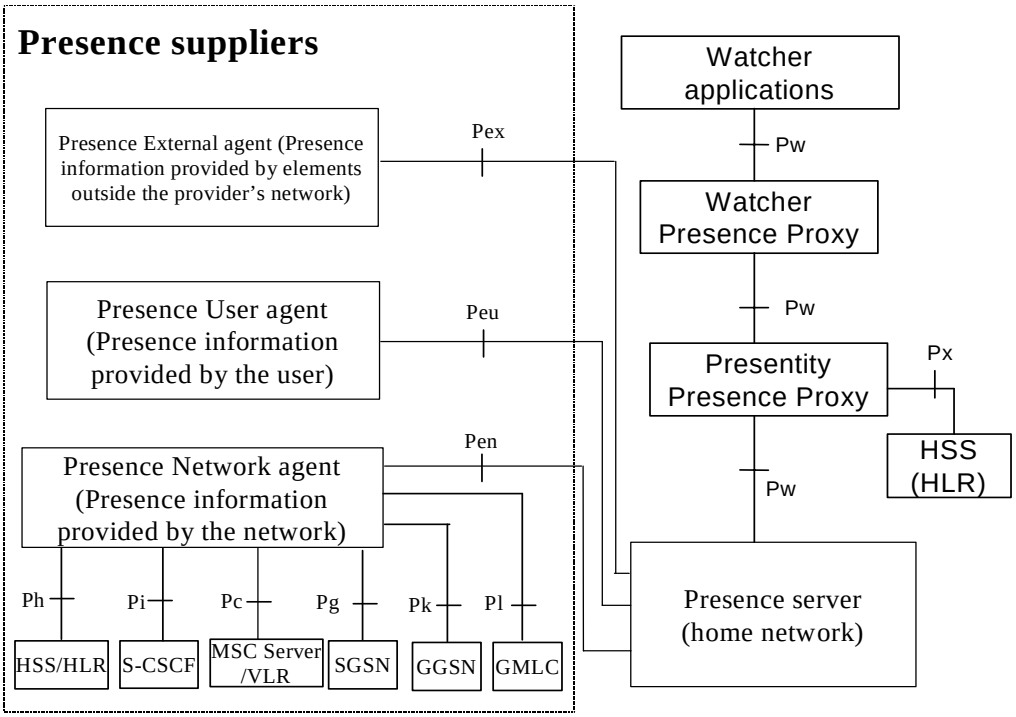
Document for: Discussion/Decision

1. Introduction

This paper compares the Presence Reference Architecture to existing UMTS security mechanisms. The goal of the paper is to identity working assumptions and open issues for SA3.

2. Presence Architecture and Security Requirements

Figure 1 describes reference architecture for presence services. The architecture is very general and can be realized over various technical systems, e.g. IMS, WAP or SMS. This paper discusses each protocol interface in different contexts, and identifies working assumptions and open issues for SA3.



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 [TS23141]

2.1 Presence External Agent - Presence Server (Pex)

Presence External Agent (PEA) provides presence information outside the provider's network. Since PEA and Presence Server (PS) both situate in the home network, the Pex interface is generally 'secure'.

The following issues are open and for future study:

- Security between PEA and external information source: Presence External Agent must be able to trust on the real source of the presence information. This security is currently outside the Presence Architecture but it has significant influence on the trustworthiness of the system.

- False presence information inside the network: It is not realistic to assume that communication between the presence suppliers (i.e. Pex, Peu and Pen) and the PS is secured end-to-end. However, there is a threat for internal attacks. In theory, anybody (inside some network) could feed false presence information to the Presence Server, and Presence Server would forward this information to the watchers without real security checking.

2.2 Presence User Agent - Presence Server (Peu)

A presentity may provide presence information using a Presence User Agent (PUA). Presentity may also use PUA to manage access rules, and activate/deactivate the presence service.

PUA may situate in UE (e.g. IMS based PUA) or in the network (e.g. WAP or SMS based PUA).

2.2.1 IMS based Presence User Agent

In IMS, the Presence User Agent will be situated in the UE. PUA will send presence information using some SIP method (e.g. UPDATE) and utilizing the existing IMS architecture. The following security services can be re-used from IMS:

- Authentication, integrity protection and replay protection: The Presence Server and UE can trust that IMS covers these security services.

- Anonymity: The presentity may not want to reveal its real identity. For this purpose, the presentity may register an anonyme identity (IMPU).

The following issues are open and for future study:

- Confidentiality: Encryption provided by the access network (e.g. UMTS) may not be enough for end-user privacy. The use of IPsec encryption between the UE and P-CSCF may be required.

- False presence information inside the network: It is not realistic to assume that communication between the presence suppliers (i.e. Pex, Peu and Pen) and the PS is secured end-to-end. However, there is a threat for internal attacks. In theory, anybody (inside some network) could feed false presence information to the Presence Server, and Presence Server would forward this information to the watchers without real security checking.

- Degree of anonymity: It is not clear what is the degree of anonymity that can be achieved by using 'anonyme' IMPUs. For example, some information in SIP message may reveal that some IMPUs are actually related to the same UE.

- Protocols: It is not clear yet which protocols will be used in Peu interface. Peu may include protocols for web access (e.g. HTTP for access list manipulation and registrations), and consequently there may be a need for additional security.

2.2.2 Non-IMS based Presence User Agent

The following issues are open and for future study:

- Non-IMS accesses: Ability of WAP/SMS/WV etc to fulfil the security requirements should be studied.

2.3 Presence Network Agent - Presence Server (Pen)

Presence Network Agent (PNA) will provide presence information from various network elements in the home network. Since PNA and Presence Server (PS) both situate in the home network, the Pen interface is generally ‘secure’.

The following issues are open and for future study:

- False presence information inside the network: It is not realistic to assume that communication between the presence suppliers (i.e. Pex, Peu and Pen) and the PS is secured end-to-end. However, there is a threat for internal attacks. In theory, anybody (inside some network) could feed false presence information to the Presence Server, and Presence Server would forward this information to the watchers without real security checking.

2.3.1 HSS/HLR – Presence Network Agent (Ph)

No additional security requirements.

2.3.2 S-CSCF – Presence Network Agent (Pi)

No additional security requirements.

2.3.3 Presence Network Agent – MSC Server/VLR (Pc)

No additional security requirements.

2.3.4 Presence Network Agent – SGSN (Pg)

No additional security requirements.

2.3.5 Presence Network Agent – GGSN (Pk)

No additional security requirements.

2.3.6 Presence Network Agent – GMLC (Pl)

No additional security requirements.

2.4 Watcher applications – Presence Server (Pw)

The Watcher application (WA) is used to fetch or subscribe presence, presence list and/or watcher information. In practice, there are at least two different instances of Pw interface. Firstly, a subscriber can acts as a Watcher. Secondly, a subscriber can act as a Presentity subscribed to the watcher information. The both cases are discussed here even though the second case may belong to Peu interface (open issue in SA2).

2.4.1 IMS based Watcher applications

In the first case, the IMS Watcher subscribes to the Presence Server situated in the home network of the Presentity. The IMS Watcher and this home network may not have any security relationships.

In the second case, the IMS Presentity subscribes to the watcher information in the Presence Server. This functionality is needed in order to informing the Presentity on watcher information and new Watchers. If a Watcher is not included in the access lists, the Presentity needs to update the access rules in order to allow the subscription. The Presence Server situates in the home network of the Presentity, and consequently, they have an existing security relationship.

The following security services can be re-used from IMS:

- Authentication:

  - The Presence Server can trust that the Watcher Presence Proxy has authenticated the identities of the IMS Presentities and Watchers.
  - The Presentities and the Watchers can trust that the their own Watcher Presence Proxy has a trust relationship with the Presence Servers.

- Integrity and replay protection: The messages between the Presentity/Wacher and the Presence Server are integrity and replay protected between the UE and P-CSCF. The path between the P-CSCF and the Presence Server is trusted.

The following new security services should be considered:

- Anonymity: The Watcher may not want to reveal its real identity. For this purpose, the Watcher may register an anonyme identity (IMPU).

The following issues are open and for future study:

- Confidentiality: Encryption provided by the access network (e.g. UMTS) may not be enough for end-user privacy. The use of IPsec encryption between the UE and P-CSCF may be required.
- Authentication: The Presence Server may need additional mechanism for authenticating the Watchers. For example, the Presentity may provide passwords for Watcher authentication.
- Authentication: The Presentity may need additional mechanism for authenticating the Watchers. For example, the Watcher may provide a token or electronic signature for authentication.
- Degree of anonymity: It is not clear what is the degree of anonymity that can be achieved by using ‘anonyme’ IMPUs. For example, some information in SIP message may reveal that some IMPUs are actually related to the same UE.
- Anonymity: The Watcher may not want to reveal its real identity. The Watcher may want to request that its identity (IMPU) is hidden from the Presentity.

2.4.2 Non-IMS based Watcher applications

The following issues are open and for future study:

- Non-IMS accesses: Ability of WAP/SMS/WV etc to fulfil the security requirements should be studied.

2.5 Presentity Presence Proxy – HSS (Px)

This interface assists locating the Presence Server of the presentity. There are no additional security requirements related to Px interface.

3. Conclusions

It is suggested that SA3 adopts the following working assumptions related to Presence:

1) Peu: Existing IMS security architecture fulfils the security requirements related to authentication, integrity protection, replay protection and anonymity.
2) Ph: No additional security requirements.
3) Pi: No additional security requirements.
4) Pc: No additional security requirements.
5) Pg: No additional security requirements.
6) Pk: No additional security requirements.
7) Pl: No additional security requirements.

8) Pw: Existing IMS security architecture fulfils the security requirements related to authentication, integrity protection and replay protection.

It is suggested that SA3 further studies the following open issues related to Presence:

1) Pex: Security between PEA and external information source should be further studied.

2) Pex, Peu & Pen: Threats and potential solutions for false presence information inside the network should be further studied.

3) Peu & Pw: IMS may need to be enhanced by IPsec encryption between UE and P-CSCF in order to fulfil the confidentiality requirement.

4) Peu & Pw: The degree of anonymity provided by 'anonymous IMPU' should be further studied.

5) Peu & Pw: Ability of non-IMS accesses (e.g. WAP/SMS/WV) to fulfil the security requirements should be further studied.

6) Pw: The Presence Server may need additional mechanism for authenticating the Watchers. For example, the Presentity may provide passwords for Watcher authentication.

7) Pw: The Presentity may need additional mechanism for authenticating the Watchers. For example, the Watcher may provide a token or electronic signature for authentication.

8) Pw: IMS may need to be enhanced by a security mechanism for the Watcher to request anonymity.

It is suggested that LSs related to the following issues are sent to other 3GPP working groups:

1) Peu: It is not clear yet which protocols will be used in Peu interface. Peu may include protocols for web access (e.g. HTTP for access list manipulation and registrations), and consequently there may be a need for additional security.

4. References

[TS23141] 3GPP, Presence Service; Architecture and Functional Description, Release 6.