3GPP TSG-SA3#18 **S3-010192**
Phoenix 21-24 May, 2001

Agenda Item:	tbd (NDS WI)
Source:	Siemens Atea
Title:	Protection Profiles for MAP Security
Document for:	Discussion and Decision

1 Scope and Objectives

This contribution further details the definition of Protection Profiles for MAP Application Layer Security.

2 Background

At the SA3 Adhoc meeting in Madrid, the working assumption was taken to define MAP-PP on the basis of MAP operation level. Also a MAP-PG (protection group) was introduced as being a set of protected MAP operations that belong functionally together. Protection profiles can than be individual protection groups or particular combinations of MAP-PGs.

This contribution particularly addresses the MAP-PGs that have to be defined [based on a threat assessment (the basis for this is provided in /2/) that was only performed on the MAP operations that are available in /1/] and how to combine MAP-PGs into standard protection profiles.

As Siemens still believes that MAP-PP shall be defined on the basis of MAP component level, this contribution still includes the indications for protection level. If N4 recommends using MAP-PP on the basis of MAP components, then this contribution can be taken as a starting point. However if N4 decides that it is more suitable to go for MAP-PP on the basis of MAP operation level, the main rationales in this contribution can still be used but may need some editorial rework.

To enhance readability, the protection level Table has been provided in annex.

3 Protection Groups for MAP Security

Within this chapter the protection groups are listed and deviations with respect to TS 33.200 V0.5.0 (/1/) are explicitly listed. The MAP-PGs defined in this paragraph are listed in order of decreasing security risk (except PG(0)).

MAP-PG(0): No Protection

This MAP-PP does not contain any operation and it does not protect any information. It is useful however to have a "null" MAP-PP to use on situations where no security is required or is an option. This protection group cannot be combined with any other protection group.

NOTE: This MAP-PG is mentioned as MAP-PG(0) in /1/ and is unchanged.

MAP-PG(1): Protection for Reset

Application Context/Operation	Protection level
ResetContext-v2/ Reset	1
ResetContext-v1/ Reset	1

NOTE: This MAP-PG is mentioned as MAP-PG(1) in /1/ and is unchanged.

Threat assessment: When receiving a reset message from an HLR, the VLR or SGSN marks all its registered subscribers coming from that HLR with a flag "not confirmed by HLR" which results in a new update location dialogue at the next radio contact. Frequent reception of reset messages will significantly increase update location signalling and processing load and is suitable for denial of service attacks that is very easy to perform.

Conclusion: It is essential that MAP-PG(1) is protected by the first release of MAPsec.

MAP-PG(2): Protection for Authentication Information except Handover Situations

Application Context/Operation	Protection Level
InfoRetrievalContext-v3/ Send Authentication Info	3
InfoRetrievalContext-v2/ Send Authentication Info	3
InfoRetrievalContext-v1/ Send Parameters	3
InterVlrInfoRetrievalContext-v3/ Send Identification	3
InterVlrInfoRetrievalContext-v2/ Send Identification	3

NOTE: This MAP-PG is mentioned as MAP-PG(2) in /1/ and is unchanged.

Threat assessment: In response of the above MAP operations, authentication vectors are delivered from HLR to VLR or SGSN, or transported between 2 VLR's. Authentication vectors can be used for false Base Station attacks.

Conclusion: It is essential that MAP-PG(2) is protected by the first release of MAPsec.

MAP-PG(3): Protection of non location dependant HLR Data

Application Context/Operation	Protection Level
AnyTimeInfoHandlingContext-v3 / AnyTimeModification	1

NOTE: This MAP-PG was mentioned as MAP-PG(5) in /1/) and is unchanged.

Threat assessment: The above MAP-operation changes permanent data in the HLR asked by the gsmSCF. Such data may include insertion and activation of call-forwarding and can be used by a hacker for fraud. As the HLR is the master database in the PLMN, its data shall be protected. There exist other MAP-operations that alter permanent HLR data and that have not been assigned to this MAP-PG (See /2/), which leaves this MAP-PG incomplete.

Conclusion: It is essential that MAP-PG(3) is protected by the first release of MAPsec.

MAP-PG(4): Protection for Authentication Information in Handover Situations

Application Context/Operation	Protection Level
HandoverControlContext-v3/ Prepare Handover (*)	4
HandoverControlContext-v3/ Forward Access Signalling (*)	4
HandoverControlContext-v2/ Prepare Handover (*)	4
HandoverControlContext-v2/ Forward Access Signalling (*)	4
HandoverControlContext-v1/ Perform Handover (*)	4
HandoverControlContext-v1/ Forward Access Signalling (*)	4

(*): The Application Context also contains other operations but only the mentioned Application Context/Operation combinations are protected.

NOTE: This MAP-PG is mentioned as MAP-PG(3) in /1/ and the protection level has been adjusted.

Threat assessment: The MAP operations PrepareHandover and ForwardAccessSignalling that are exchanged between 2 VLRs contain an access-network container that is transparent for the core-network. This container (BSSAP or RANAP-related) includes security relevant information (CK, IK). The potential misuse after obtaining the security relevant information is restricted in time until the next authentication occurs. Signalling messages in the radio network may be altered, or PS or CS data can be eavesdropped, therefor the secrecy of CK and IK shall be guaranteed. It is felt that other MAP operations that introduce permanent changes in the HLR (See /2/), are equally important as this MAP-PG.

Conclusion: It is essential that MAP-PG(4) is protected by the first release of MAPsec.

MAP-PG(x): Protection of Location Information

Application Context/Operation	Protection Level
NetworkLocUpContext-v3/ Update Location (*)	4
GprsLocationUpdateContext-v3/ Update GPRS Location (*)	6
HandoverControlContext-v3/ Prepare Subsequent Handover (*)	6
SubscriberInfoEnquiryContext-v3/ Provide Subscriber Info	3
NetworkLocUpContext-v2/ Update Location (*)	4
HandoverControlContext-v2/ Prepare Subsequent Handover (*)	6
NetworkLocUpContext-v1/ Update Location (*)	4
HandoverControlContext-v1/ Perform Subsequent Handover (*)	6

(*) : The Application Context also contains other operations but only the mentioned Application Context/Operation combinations are protected.

NOTE: This MAP-PG is mentioned as MAP-PG(4) in /1/ and has been updated to introduce the protection Level 6 (2 0 0).

Threat assessment: The above MAP-operations contain location information (Ex. SGSN area, VLR area, RNCid, …) that is exchanged between VLR/SGSN) towards HLR (Update xx Location, ProvideSubscriberInfo) , between VLR’s during handover (PrepareSubsequentHandover). Eavesdropping or altering location information can be misused. It can lead to a denial of service attack against that particular subscriber.

Conclusion: The realization of this protection profile requires lower priority as all the before mentioned. In addition to the MAP operations that are mentioned in MAP-PG(x), the MAP operations needed for LCS shall also be incorporated. Also other MAP operations (Ex. InsertSubscriberData) include location dependant data.

4 Protection profiles for MAP Security

Protection profiles can be individual protection groups or particular combinations of protection groups. MAP protection profiles are coded as a 16 bit binary number where each bit corresponds to a protection group. Currently only 5 groups [MAP-PG(0) .. MAP PG(4)] are defined applicable to the first release of MAPsec, the rest are reserved for future use.

Protection profile bit	Protection group
0	No protection
1	Reset
2	Authentication information except handover situations
3	Non-location dependant HLR data
4	Authentication information in handover situations
Y	Location information
6-15	Reserved

The following Standard Protection Profiles indicated in **bold** are proposed as being part of the first release of MAPsec.

Protection profile name	**Protection group**						
	MAP PG(0) No protection	**MAP PG(1) Reset**	**MAP PG(2) Authinfo except handover situations**	**MAP PG(3) Non-location dependant HLR data**	**MAP PG (4) Authinfo in handover situation**	MAP PG (x) Location information	
Profile A	✓						
Profile B		✓	✓				
Profile C		✓	✓	✓			
Profile D		✓	✓	✓	✓		
Profile E		✓	✓	✓		✓	
Profile F		✓	✓	✓	✓	✓	
Profile G							
Profile I							

The above table deviates slightly from /1/ because of following reasons:

A) AnyTimeModification [included in MAP PG(3)] is only defined at protection level 1.

B) It must be possible for an operator to add MAP-PG(3) separately. Defining Profile C ensures this.

C) All profiles that are coloured grey were indicated in the analysis as being lower priority for inclusion in the first release of MAPsec.

5 Conclusions

Siemens ask SA3 to consider the above standard protection profiles (indicated in bold) and incorporate them into TS 33.200. The reasoning for grouping MAP-operation into MAP-PG has been mentioned and a first risk analysis was done. However not the whole scope of available MAP operations was assessed and some more work is needed (for example on MAP operation that change permanent HLR data).

6 References

/1/ 3GPP TS 33.200 V0.5.0 Network Domain security (Release 4)

/2/ AP99-028 SS7 NETWORK SECURITY THREAT ANALYSIS

7 ANNEX on Protection Level Table

The concept of "protection levels" is introduced to administrate the protection on component level: A protection level of an operation determines the protection modes used for the operation's components according to the following table:

Table 5: MAPsec protection levels

protection level	protection mode for invoke component	protection mode for result component	protection mode for error component
1	1	0	0
2	1	1	0
3	1	2	0
4	2	1	0
5	2	2	0
6	2	0	0