3GPP TSG SA WG3 Security S3-010072

Meeting S3#17

Göteborg, 27 Feb – 2 Mar, 2001

Source: Siemens AG

Title: Considerations on trust and risk

Document for: Discussion / Decision

Work item: Access security for IP-based services

Agenda item: tbd

This document presents arguments which are meant to help in the decision between the alternatives security architectures for the IM domain presented at S3#16. In particular, it is proposed that trust assumptions for the IM domain and associated potential risks be made explicit in contributions. This contribution further considers attacks which become possible when trust assumptions are not justified, and concludes that S3 should adopt the same trust model for the IM domain than for the PS and CS domain.

1 Proposed approach to decision on security architecture

There has been a lack of progress in the discussions on the alternative proposals for a security architecture (cf. Ericsson's TD S3-000699 and Siemens's TDs S3-000689). Partly this seems to be due to a lack of clarity regarding the underlying assumptions on the system to be protected.

Any security architecture should build on:

- A definition of security objectives, including a trust model
- A view of the security-relevant parts of the system to be protected
- A threat and risk analysis
- Security requirements

S3 was very careful in performing these steps before the UMTS Rel'99 security architecture was defined. The results were laid down in TR 33.120 and TR 21.133. A trust model is implicit in these documents. It is believed to be well-understood as it largely carries over from GSM, at least as far as the core network entities are concerned.

If the security objectives and the view of the system for the IM domain are largely similar to that for the PS- and CS-domains then the threat and risk analysis and the security requirements are likely to carry over from the previous analyses.

If, however, the assumptions on the system, e.g. the trust model, are significantly different so as to affect the security architecture of the system then these assumptions and their consequences, in particular new risks, should be made explicit in contributions to S3.

But so far, only one contribution raising the issue of a new trust model for the IM domain was submitted to S3 (Motorola's S3-000679), and this contribution is not very explicit on the new trust assumptions. Furthermore, it disagrees with both alternatives for a security architecture presented to S3 by Ericsson and Siemens, respectively.

2 Considerations on trust and risk

The security architecture proposed by Siemens in TD S3-000689 assumes that the same trust model as for the PS domain may also be applied to the IM domain. With this model it is sufficient to terminate access security in the visited IM domain, and to have user-independent protection between IM domain nodes (network domain security, e.g. provided by IPSec tunnels).

What risk could occur if the trust of the home IM domain in the visited IM domain to handle authentication and integrity checks correctly was not justified?

Fraud by forging call control messages: The P-CSCF could commit fraud against the S-CSCF e.g. by pretending that a call was still going on while in fact it was not. As the S-CSCF is located in the home domain it has full visibility of all call control signalling, including the duration of the call and the agreed QoS parameters, so the P-CSCF would have to actively make up fake call control messages. But for how long could this go on undetected? How long would a roaming relationship with such an operator be maintained? Why should there be a stronger requirement for home control in this scenario than for the CS- and PS domain? After all, it takes more sophisticated measures in the IM domain to commit this type of fraud.

Fraud by tampering with QoS: while the S-CSCF is in control of the services, the P-CSCF is in control of resource allocation and Quality of Service. If it may be assumed that a P-CSCF may show so much skill and criminal energy as to forge call control messages it may also be assumed that the P-CSCF may commit fraud by forging Call Detail Records (CDRs). This will be more difficult to detect as QoS for a multi-media call will be more complex to understand for the user than for a voice call, and the user will not always be able to judge the QoS he should be getting, or the data volume he generated. So, what is the extent of the security gained in letting the home domain check the integrity of call control messages if fraud can still be committed by tampering with QoS?

Stealing of cryptographic keys from the P-CSCF: if an attacker was able to steal cryptographic keys he could make calls at somebody else's expense until the keys were changed in a new authentication. But the same is, of course, true for keys stored in an SGSN or an RNC or VLR, or an S-CSCF (assuming keys were stored there). What reason is there (if any) to assume that the P-CSCF is more vulnerable to such attacks than these other nodes? Who will pick up the bill if keys are stolen in the S-CSCF? Does the P-CSCF have to trust the S-CSCF more than the other way around?

Manipulating cryptographic code in the P-CSCF: if an attacker could disable security checks in the P-CSCF then fraud could be committed until the correct code was restored or the node was disabled. It is true that locating the final authentication check in the HSS is likely to reduce the chance of this attack regarding authentication, as the HSS must be assumed to more resilient against attacks in general, but how likely is this attack against a P-CSCF to happen at all, and how much more likely is it to happen against the P-CSCF than the S-CSCF, SGSN, RNC or VLR?

3 Conclusion

The above paragraphs shed some light on the consequences of certain attacks which become possible if trust assumptions are not justified, and a number of question were raised doubting the practical security gain provided by home control. It is not argued that such a gain may not exist under any circumstances, but as long as there are no convincing answers to the above questions it is proposed to stick to the CS and PS domain trust model.