SIEMENS

3GPP TSG SA WG3 Security **S3-010077**
joint S2/S3 meeting, Göteborg, 27 Feb 2001

Considerations on trust and risk

Source: **Siemens AG**

Document for: **Discussion**

Agenda item: **?**

Steps in security architecture definition (1)

- Definition of security objectives, including trust model
- View of the security-relevant parts of the system to be protected
- Threat and risk analysis
- Security requirements

Steps in security architecture definition (2)

- Pertinent UMTS Rel'99 docs: TR 33.120 and TR 21.133
- **If** security objectives and system view for IM domain are largely similar to PS- and CS-domains
  then threat and risk analyses and security requirements carry over from Rel'99
- **If** security objectives and system view for IM domain are significantly different
  then these differences and their consequences, in particular new risks, should be made explicit in S3 contributions

Considerations on trust and risk

- **It has been argued that the P-CSCF should not be trusted by the home network**
- **The following slides examine potential risks when important security functions are located at an untrustworthy P-CSCF**
- **The objective of this risk analysis is to see whether**
  - the risk is significantly different from that in the CS- and PS-domains
  - a certain degree of trust in the P-CSCF is unavoidable

Potential risk when P-CSCF terminates access security (1)

Fraud by forging call control messages:

- S-CSCF home domain sees all call control messages
- P-CSCF could deceive S-CSCF about session state only by actively forging messages

QUESTIONS:

- 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?
  (Fraud more sophisticated in the IM domain)

Potential risk no matter where access security terminates

Fraud by tampering with QoS:

- P-CSCF is in control of resource allocation and Quality of Service
- P-CSCF may forge Call Detail Records (CDRs) regarding QoS
- QoS important factor in call charge
- Impossible to detect for S-CSCF (even when S-CSCF terminates integrity)
- Difficult to detect for user (complex QoS, volume charges)

QUESTION:

- How much security is gained in letting the home domain check the integrity of call control messages if fraud can still be committed by tampering with QoS?

Potential risk when P-CSCF terminates access security (2)

Stealing of cryptographic keys from the P-CSCF:

- If successful attacker can make free calls until new authentication
- But the same is true for keys stored in an SGSN, RNC or VLR, or an S-CSCF

QUESTION:

- 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 when keys are stolen from S-CSCF?
  (Does P-CSCF need to trust the home network?)

Potential risk when P-CSCF terminates access security (3)

Disabling security checks in the P-CSCF by hacking:

- if successful attacker can make free calls
  until the correct code was restored or the node was disabled.
- final authentication check in the HSS could reduce risk if HSS especially tamper-resistant (but not for integrity checks)

QUESTIONS:

- How likely is this attack against a P-CSCF?
- Why would it be more likely than in the PS and CS domains?

Conclusion

- **Practical security gain by home control doubtful**