3GPP TSG SA WG3 Security — S3#22 **S3-020277**
14 - 17 May 2002, Victoria, Canada

CR-Form-v5

CHANGE REQUEST

⌘ **33.210 CR CRNum** ⌘ **rev - ⌘** Current version: **5.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM □ ME/UE □ Radio Access Network □ Core Network ☒

Title:	⌘	Strengthening the requirements on IV construction to prevent attacks based on predictable IV		
Source:	⌘	Qualcomm/Telenor		
Work item code:	⌘	SEC-NDS-IP	***Date:*** ⌘	22.04.2002
Category:	⌘	**F**	***Release:*** ⌘	REL-5
		Use one of the following categories: ***F*** *(correction)* ***A*** *(corresponds to a correction in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.		*Use one of the following releases:* *2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *REL-4 (Release 4)* *REL-5 (Release 5)*

Reason for change:	⌘	A recent publication [1] has irrevocably demonstrated that IPsec ESP CBC based encryption is susceptible to adaptive chosen-plaintext attacks ~~for~~ based on predictable IVs. The current description on how to construct IVs in the IPsec RFC allows for predictable IVs.
Summary of change:	⌘	To strengthen the requirements on how IVs are constructed in the NDS/IP context.
Consequences if not approved:	⌘	If the CR is not approved NDS/IP implementations ~~will~~ might be vulnerable to ~~the~~ - attacks like those described in [1].

Clauses affected:	⌘	2, 5.3.5 (new)		
Other specs affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘	
Other comments:	⌘	Reference: [1] Attacking predictable IPsec ESP Initialization Vectors Antti Nuopponen (Netseal) and Sami Vaarala (Netseal) Helsinki University of Technology (HUT) Available at: http://www.hut.fi/~svaarala/hakkeri2002/espiv.pdf		

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 21.133: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Threats and Requirements".

[2] 3GPP TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[3] 3GPP TS 23.002: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Network architecture".

[4] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2".

[5] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2".

[6] 3GPP TS 29.060: "3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface".

[7] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".

[8] 3GPP TS 33.103: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Integration guidelines".

[9] 3GPP TS 33.120: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Principles and Objectives".

[10] 3GPP TS 33.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Access security for IP-based services".

[11] RFC-2393: "IP Payload Compression Protocol (IPComp)".

[12] RFC-2401: "Security Architecture for the Internet Protocol".

[13] RFC-2402: "IP Authentication Header".

[14] RFC-2403: "The Use of HMAC-MD5-96 within ESP and AH".

[15] RFC-2404: "The Use of HMAC-SHA-1-96 within ESP and AH".

[16] RFC-2405: "The ESP DES-CBC Cipher Algorithm With Explicit IV".

[17] RFC-2406: "IP Encapsulating Security Payload".

[18] RFC-2407: "The Internet IP Security Domain of Interpretation for ISAKMP".

[19] RFC-2408: "Internet Security Association and Key Management Protocol (ISAKMP)".

[20] RFC-2409: "The Internet Key Exchange (IKE)".

[21] RFC-2410: "The NULL Encryption Algorithm and Its Use With IPsec".

[22] RFC-2411: "IP Security Document Roadmap".

[23] RFC-2412: "The OAKLEY Key Determination Protocol".

[24] RFC-2451: "The ESP CBC-Mode Cipher Algorithms".

[25] RFC-2521: "ICMP Security Failures Messages".

[26] Internet Draft: "On the Use of SCTP with IPsec ", available as "draft-ietf-ipsec-sctp-03.txt"

[27] RFC-1750: “Randomness Recommendations for Security.

5.3.5 Requirements on the construction of the IV

The following strengthing of the requirements on how to construct the IV shall take precedence over the description given in the implmentation note in RFC-2405 [16] section 5, the description given in RFC-2451 [24] section 3 and all other descriptions that allow for predictable IVs.

- The IV field shall be the same size as the block size of the cipher algorithm being used. The IV shall be chosen at random, and shall be unpredictable to any ~~other~~ party other than the originator.
- It is explicitly not allowed to construct the IV from the encrypted data of the preceding encryption process.

The common practice of constructing the IV from the encrypted data of the preceding encryption process means that the IV is disclosed before it is used. A predictable IV exposes IPsec to certain attacks irrespective of the strength of the underlying cipher algorithm. The second bullet point forbids this practice in the context of NDS/IP.

These requirements imply that the network elements must have a capability to generate random data. RFC-1750 [27] gives guidelines for hardware and software pseudorandom number generators.