3GPP TSG-SA3
Washington, D.C.
12-14 September 2000

Tdoc 3GPP ***S3-000571***

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

33.900	**CR**	**XXX**	Current Version:	1.2.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	SA #	for approval		strategic		*(for SMG use only)*
list expected approval meeting # here ↑		for information	X	non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)*	(U)SIM		ME		UTRAN / Radio		Core Network	X

Source: Motorola~~T-Mobil~~ **Date:** 05.09.00

Subject: DoS attacks to 3G networks and users

Work item: 3G network protection for Denial-of-Service attacks

Category: *(only one category shall be marked with an X)*

F	Correction	
A	Corresponds to a correction in an earlier release	
B	Addition of feature	X
C	Functional modification of feature	
D	Editorial modification	

Release:

Phase 2	
Release 96	
Release 97	
Release 98	
Release 99	
Release 00	X

Reason for change: Introduction of additional DoS attacks and

Clauses affected: ch. 8.1; ch. 9

Other specs affected:

Other 3G core specifications		→ List of CRs:	TS 33.900
Other GSM core specifications		→ List of CRs:	
MS test specifications		→ List of CRs:	
BSS test specifications		→ List of CRs:	
O&M specifications		→ List of CRs:	

Other comments:

help.doc

<--------- Double-click here for help and instructions on how to create a CR.

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.

2.1 Normative references

[1] 3G TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements".

[2] 3G TS 33.120: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Principles and Objectives".

[3] UMTS 33.21, version 2.0.0: "Security requirements".

[4] UMTS 33.22, version 1.0.0: "Security features".

[5] UMTS 33.23, version 0.2.0: "Security architecture".

[6] 3G TS 23.060: "3rd Generation Partnership Project; Technical Specification Group and System Aspects; Digital cellular telecomunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2".

[7] 3G TS 29.060: "3rd Generation Partnership Project; Technical Specification Group and System Aspects; Digital cellular telecomunications system (Phase 2+); GPRS Tunnelling Protocol Across Gu and Gp interface".

2.2 Informative references

IETF documents:

[8] IETF RFC 792: "ICMP – Internet Control Message Protocol", 09/01/1981.

[9] IETF RFC 1191: "Path MTU Discovery", Nov 1990.

[10] IETF RFC 1981, "Path MTU Discovery for IP version 6", Aug 1996.

[11] IETF Internet Draft: "ICMP Traceback Messages", Mar 2000.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

DoS	Denial of Service
SPC	Signalling Point Code

8 Counteracting envisaged 3G attacks

Many of the security enhancements required to 2G systems are intended to counteract attacks which were not perceived to be feasible in 2G systems. This includes attacks that are, or are perceived to be, possible now or very soon because

intruders have access to more computational capabilities, new equipment has become available, and the physical security of certain network elements is questioned.
In order to perform the attacks the intruder has to possess one or more of the following capabilities:

- **Eavesdropping.** This is the capability that the intruder eavesdrops signalling and data connections associated with other users. The required equipment is a *modified MS*.
- **Impersonation of a user.** This is the capability whereby the intruder sends signalling and/or user data to the network, in an attempt to make the network believe they originate from the target user. The required equipment is again a *modified MS*.
- **Impersonation of the network.** This is the capability whereby the intruder sends signalling and/or user data to the target user, in an attempt to make the target user believe they originate from a genuine network. The required equipment is modified *BS*.
- **Man-in-the-middle.** This is the capability whereby the intruder puts itself in between the target user and a genuine network and has the ability to eavesdrop, modify, delete, re-order, replay, and spoof signalling and user data messages exchanged between the two parties. The required equipment is modified *BS in conjunction with a modified MS*.
- **Compromising authentication vectors in the network.** The intruder possesses *a compromised authentication vector*, which may include challenge/response pairs, cipher keys and integrity keys. This data may have been obtained by compromising network nodes or by intercepting signalling messages on network links.
- **Interruption of the communication.** This is the capability that the intruder sends enoumous amount of bogus traffic to 3G network and users to block the siganlling or user traffic, and therefore cause abusive usage of network resources. This is also called Denial of Service attacks. The nature of the attacks is that the victim can not detect the real sender of the bogus traffic.

The first and the last capability are ~~is~~ the easiest to achieve the following capabilities are gradually more complex and require more investment by the attacker. Therefore, in general, an intruder having a certain capability is assumed also to have the capabilities positioned above that capability in the list. The first two capabilities were acknowledged in the design of 2G systems. 3G security however should thwart all six ~~five~~ types of attacks.
In the following we consider several attacks to 3G systems which may not have been fully addressed in 2G systems and attempt to identify whether the security features and mechanisms provided in the latest version of the 3G security architecture specification counteracts each of these attacks.

8.1 Denial of service

We distinguish between the following denial of service attacks:

8.1.1 User de-registration request spoofing

Description:

An attack that requires a *modified MS* and exploits the weakness that the network cannot authenticate the messages it receives over the radio interface. The intruder spoofs a de-registration request (IMSI detach) to the network. The network de-

registers the user from the visited location area and instructs the HLR to do the same. The user is subsequently unreachable for mobile terminated services.

Does 3G security architecture counteract the attack: Yes

Integrity protection of critical signalling messages protects against this attack. More specifically, data authentication and replay inhibition of the de-registration request allows the serving network to verify that the de-registration request is legitimate.

8.1.2 Location update request spoofing

Description:

An attack that requires a *modified MS* and exploits the weakness that the network cannot authenticate the messages it receives over the radio interface. Instead of the de-registration request, the user spoofs a location update request in a different location area from the one in which the user is roaming. The network registers in the new location area and the target user will be paged in that new area. The user is subsequently unreachable for mobile terminated services.

Does 3G security architecture counteract the attack: Yes

Integrity protection of critical signalling messages protects against this attack. More specifically, data authentication and replay inhibition of the location update request allows the serving network to verify that the location update request is legitimate.

8.1.3 Camping on a false BS

Description:

An attack that requires a *modified BS* and exploits the weakness that a user can be enticed to camp on a false base station. Once the target user camps on the radio channels of a false base station, the target user is out of reach of the paging signals of the serving network in which he is registered.

Does 3G security architecture counteract the attack: No

The security architecture does not counteract this attack. However, the denial of service in this case only persists for as long as the attacker is active unlike the above attacks which persist beyond the moment where intervention by the attacker stops. These attacks are comparable to radio jamming which is very difficult to counteract effectively in any radio system.

8.1.4 Camping on a false BS/MS

Description:

An attack that requires a *modified BS/MS* and exploits the weakness that a user can be enticed to camp on a false base station. A false BS/MS can act as a repeater for some time and can relay some requests in between the network and the target user, but subsequently modify or ignore certain service requests and/or paging messages related to the target user.

Does 3G security architecture counteract the attack: No

The security architecture does not prevent a false BS/MS relaying messages between the network and the target user, nether does it prevent the false BS/MS ignoring certain service requests and/or paging requests. Integrity protection of

critical message may however help to prevent some denial of service attacks, which are induced by modifying certain messages. Again, the denial of service in this case only persists for as long as the attacker is active unlike the above attacks, which persist beyond the moment where intervention by the attacker stops. These attacks are comparable to radio jamming which is very difficult to counteract effectively in any radio system.

8.1.5 Legitimate roaming partner identity spoofing

Description:

An attack that exploits the weakness that the network cannot authenticate the messages it receives over SS7 or IP for supporting internetwork roaming. The intruder spoofs the roaming partner's identity or network node addresses(SPC or IP addr), then send bogus signalling traffics to the victim's networks.

Does 3G security architecture counteract the attack: Yes for IP based signalling; No for the SS7 based signalling

Some Internet Firewalls have the functionality to perform IP packets filtering. Also using IPSec for securing signalling over IP can effectively prevent this type of attacks.

However, for SS7 based signalling, there is no security protection at the SS7 layer. Need further investigation.

8.1.6 Push-service initiator identity spoofing

Description:

An attack that exploits the weakness that the 3G network cannot authenticate the user traffics it receives from a Push service initiator which is located on the Internet. The intruder spoofs the Push-service initiator's IP address, then send bogus IP packets to the victim 3G users to either block the core network traffic channel or radio interface traffic channel.

Does 3G security architecture counteract the attack: No at the moment

Stateful Internet Firewalls may be developed to deal with various PUSH-type services.

8.1.7 Internet router identity spoofing

Description:

An attack that exploits the weakness that the 3G network cannot authenticate the Internet ICMP diagnostic messages it receives from Internet routers. The intruder spoofs the Internet routers IP addresses, then send various ICMP diagnostic messages to 3G network and users to interrupt the communication by abuse network resources.

Does 3G security architecture counteract the attack: Yes if all those diagnostic messages are blocked.

Although some stateful Firewalls can perform selective filtering of ICMP messages, the intruder can still utilise some diagnostic services to launch DoS attacks to 3G networks and users. One example of the diagnostic services is Path MTU Discovery.

9 Network issues

9.1 Security policy

9.1.1 Access control policy

9.1.2 Access control policy for traffic originated from Internet

TBD.

15 Network issues for combating DoS attacks

TBD.