3GPP TSG SA WG3 Security — S3#14 **S3-000457**

1-4 August, 2000.

Oslo.

Source: **Motorola**

Title: **WI proposal on UMTS network protection for DoS attacks**

Document for: **Discussion**

Agenda Item: **tbd**

Work Item Description

Network security in combating denial-of-service attacks

1. 3GPP Work Area

	Radio Access
X	Core Network
X	Services

2. Linked Work Items

- Network-based end-to-end security
- Core network security – full solution

3. Justification

The convergence of mobile communication and Internet brings Internet-like services directly to mobile users, while it also exposes the UMTS network to various Internet attacks. Eavesdropping, tampering, impersonation and communication interruption can happen anywhere along the end-to-end route.

This WI aims to address the communication interruption issue caused by Internet Denial-of-Service attacks to the UMTS network. The UMTS PLMN can be easily congested and therefore paralysed by bogus traffic from the Internet. Examples of denial-of-service attacks to the UMTS networks are:

1. Launching massive UDP packets to a PLMN: This can be done by finding a few IP addresses of a PLMN, sending massive UDP packets to those addresses until the traffic reaches its capacity limit at Gn interface(or Iu, Iub etc), and then the UMTS network will be flooded.
2. Utilising the well-known Internet SYN flood attack to send massive TCP Connection Request packets(TCP packets with SYN=1 and ACK=0) to many mobile stations.
3. Utilising the well-known Internet smurf or broadcast attacks, or Path-Discovery to launch massive ICMP traffic to the UMTS network, and hence to flood the network. Those attacks will happen only if those Internet diagnostic services are supported by UMTS.

The current UMTS system architecture and protocols are designed to accommodate some Internet services, including informative service, job dispatching, information casting, home automation, and messaging services etc. Most of the services are *PULL* type services, which are invoked by the MS. Other services are *PUSH* type that are invoked by the Network Node and delivered to the MS without negotiation with the MS on a case-by-case basis.

If the service is based on UDP/IP(video or audio services) no matter whether it is PULL or PUSH type, the UMTS border gateway(or firewall residing at the UMTS border) can only perform packet filtering based on IP source and destination addresses, or in conjunction with UDP port numbers. However, it is quite easy to spoof an address on the Internet and also very easy to forge an IP address.

For the PUSH type services, although they may be implemented on top of TCP/IP, the UMTS network can be flooded easily by SYN flood attacks. A 2 Mbps UMTS air interface can be totally blocked when a 200-octet TCP Connection Request packet is sent to an MS at 1 millisecond intervals. A feature designed in the UMTS R99 permits the launching of this type of attack because the core network allows network initiated PDP context activation(for supporting PUSH type services).

The network initiated PDP context activation is triggered by an arriving UDP or TCP Connection Request PDU under the condition that there has not been any PDP Context established for the UDP flow or TCP connection. After the GGSN initiates the Network-Requested PDP Context Activation, an RAB-setup is performed over air interface to build a signal connection and to reserve the necessary radio resources for the traffic. Hence this can overload the DCCH channel and RACH buffer; and exhaust RAB.

From the network operator’s perspective, business success largely depends on the fact that networks run properly so that the services can be delivered to customers. It is also essential that their network be utilised as much as possible in order to produce maximum profit. The former point requires limitation of traffic types coming into UMTS network(i.e., limit the service type offered to the end-user) in order to reduce the chance of DoS attacks. However, the later point determines that the UMTS network has to support all user-demanded services. The issue is how to protect Network Operator’s UMTS network whilst allowing various services being provided to end-users.

4. Objective

This WI aims to address the communication interruption caused by Internet Denial-of-Service attacks to the UMTS network. The output of the WI will be a set of proposals for DoS countermeasures in UMTS, and also CRs to SA and CN TSG to address the security holes in the current standard specification.

The objective of the WI can be further classified as:

- Understand DoS attacks and therefore conduct a threat analysis for PUSH type services, other services build on top of UDP/IP, and Internet diagnostic messages(ICMP Echo Req, ICMP Echo Resp, Path MTU discovery, etc.).
- Propose countermeasures within UMTS network to combat the DoS attacks, or to reduce the chance of launching this type of attacks to UMTS network.
- Produce CRs to SA2, CN3, and SA5 to address the security holes resulted from the DoS attacks.

5. Service Aspects

Input from S2 will be required on service architecture, type of services for UMTS and addressing in order to fully understand the nature of the services supported for UMTS R00. Also input from N3 will be require on the internetworking aspects in order to support various Internet services.

Input from and output to S5 on charging related DoS countermeasures.

6. MMI Aspects

Not yet investigated

7. Charging Aspects

Charging policy in a UMTS network is highly related to the WI. Employing different charging policy can directly affect the probability of launching DoS attacks to UMTS network.

- Flat-rate - This method is simple and easy to implement. Although radio resource is scarce, mobile subscribers do not expect to pay for signalling messages in managing mobile attachment and PDP context. However, this may cause radio interface congestion by both PULL and PUSH type services.
- Volume based - An alternative charging method is to count the bytes sent or received by the mobile. This seems to be accurate. However, we need to investigate how to charge the PUSH type services and signalling messages in order to prevent DoS attacks.
- Service based - Would operators be willing to charge differently for the use of different services? If YES, how to classify those services and attach different tariffs in order to prevent DoS attacks?

8. Security Aspects

The work item is a security item.

9. Impacts

Affects:	USIM	ME	AN	CN	Others(S2, S5)
Yes				X	X
No					
Don't know	X	X	X		

10. Expected Output and Time Scale(to be updated at each plenary)

Meeting	Date	Activity
S3#14	August 1-4, 2000	Presentation to S3 of the WI proposal
S3#15	September 2000	Approval of the WI Threats analysis of DoS attacks
S3#16	November, 2000	Security requirements analysis for combating DoS attacks LS to CN3, SA2&5
	Dec 2000	Security features specification CRs to be approved in SA3 and SA2&5
	Feb 2001	Security architecture specification CRs to New Document approved at TSG level
	April 2001	Detailed security feature specification CRs to be approved by SA3
	June 2001	CRs approved at TSG level

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
TS 23.121		Architectural Requirements for R99		
TS 29.060		GTP across Gn and Gp		
TS 23.060		R99 Service description		
TS 24.008		Mobile radio interface layer 3 specification, core network protocols - stage 3		
TS 32.105		3G Charging: Call Event Data		
TS 23.003		Phase 2+; Numbering, addressing and identification		

11. Work Item Raporteurs

Rong Shi	Dan Brown
Motorola	Motorola
16 Euroway	1501 W.SHURE DRIVE
Blagrove	Arlington Heights
Swindon, UK	Illinois 60004
SN5 8YQ	USA

12. Work Item Leadership

TSG SA WG3

13. Supporting Companies

14. Classification of the WI (if known)

(X)	Feature (go to 14a)
	Building Block (go to 14b)
	Work Task (go to 14c)