3GPP TSG SA WG3 Security – S3 #16 **S3-000678**

28-30 November, 2000

Sophia Antipolis, France

Source: **Motorola**

Title: **Internet-based DoS attacks on UMTS network**

Document for: **Discussion**

Agenda item: **tbd**

Abstract

Information is provided for discussion and possible inclusion into 3G TR 33.900 regarding Internet-based DoS attacks that may be launched against a UMTS network.

Section 14 of 3G TR 33.900 discusses UMTS network vulnerabilities that may arise from the delivery of new services. Many of these services may come from sources that are accessed via the Internet. Hence it is suggested that the following text be added to Section 14 of 3G TR 33.900. Alternative placement may also be determined by SA3.

14.3 Internet-based Denial of Service (DoS) Attacks

Attacks commonly referred to as "Denial of Service" (DoS) aim to block the communication of a host, immediate node or link by flooding it with bogus packets. Denial of service attacks can be realised by SYN flood attack, smurf attack, broadcasting attack, path MTU discovery, UDP flooding etc.

DoS attacks can be introduced into UMTS networks from the Internet as a result of introducing various Internet services to MS users. Examples of those services include:

- *PUSH* type services.
- *PULL* type services, built on top of UDP/IP.
- *Internet Diagnostic* services, based on ICMP echo messages and Path MTU discovery messages.

We now describe some UMTS services that may provide the basis for DoS attacks.

14.3.1 PUSH type services

We define *PUSH* type service here as the services being initiated and activated from an Internet node rather than from an MS. This implies that some IP packet(s) need to reach the MS before the service context is established, in other words to allow Internet users to access the UMTS terminals.

Examples of PUSH type services include:

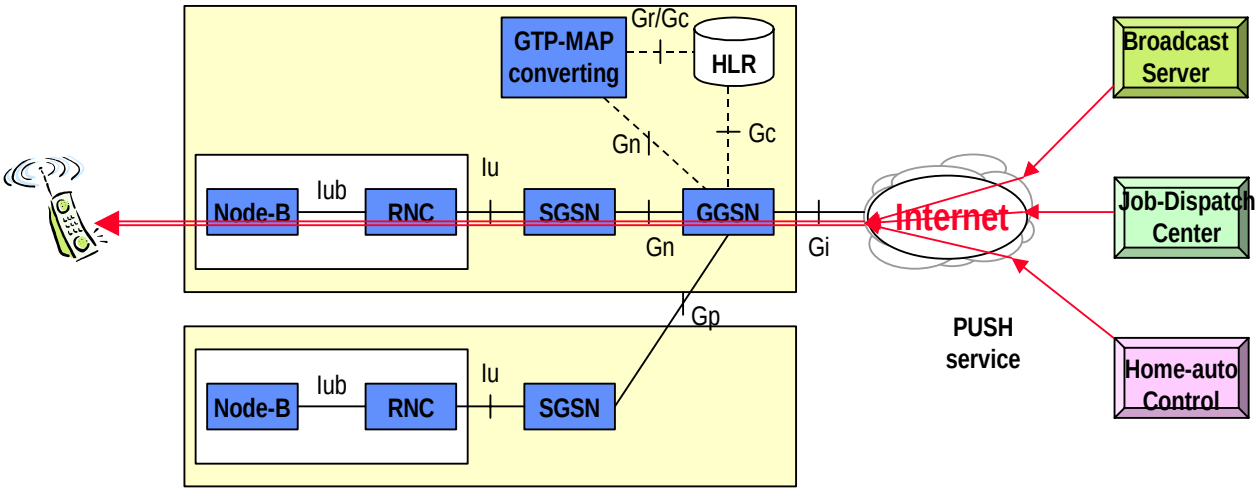
- Multimedia conferencing service initiated from Internet stationary nodes.

– News multicasting: data are distributed to a group of terminals; acknowledgement for receiving those data is not required.

– Job dispatching by narrow-cast: data are distributed to a group of end-user terminals; acknowledgement may or may not be required.

– Real-time event notification in home automation: data are sent to one or a few terminals in a real-time fashion; acknowledgement may or may not required.

The nature of the PUSH type services can be characterised as (1) the server or control centre controls to whom the services are delivered; (2) services are delivered to the mobile terminals in the distribution list if they are attached to the network (but not necessarily activated); (3) some IP packets need to be delivered to the MSs before service context is established.

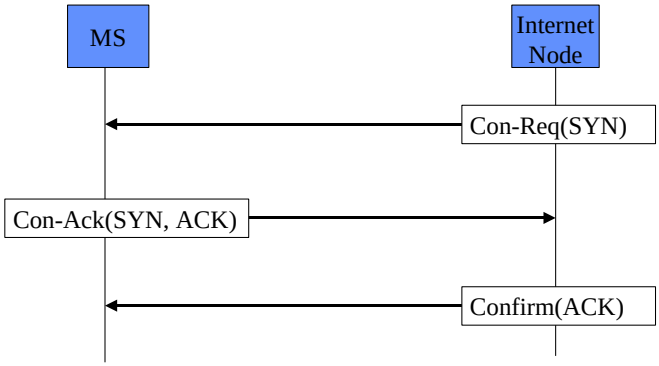


In order to support PUSH type services, certain types of IP packets have to be allowed to reach MSs directly from the Internet stationary nodes(see figure above). The types of IP packets that need to be passed to UMTS MS by the UMTS network are:

(1) PUSH type services built on top of TCP.

A *Passive Open* for a TCP connection is required on MS. This means that MS wishes to accept incoming service requests.

A TCP connection is established by a *Three Way Handshake* procedure(as seen below).



When the Internet Node would like to set up a TCP connection with the MS, a TCP Connection Request is sent to the MS with SYN bit set in the TCP packet header. After the MS receives the Con-Req packet, a corresponding synchronisation message will be sent to the Internet Node and a half opened connection is stored in the MS's buffer. The MS waits for the connection

acknowledgement from the Internet Node. If the Internet Node sends the connection acknowledgement, the connection is set up, otherwise, the connection is half opened.

Apart from the first Con-Req packet, all the follow-up TCP datagrams will have ACK bit set. Hence filtering out the packets that do not belong to a connection is easy to do for a firewall.

Although stateful Firewalls are able to filter out IP packets that do not belong to a TCP connection based on TCP connection information, the TCP Connection Request packets can still be permitted to enter the UMTS network for PUSH type services. Hence a security hole is opened to launch DoS attacks to the UMTS network by sending massive TCP Connection Request packets.

(2) PUSH type services built on top of UDP.

See section 14.3.2.

14.3.2 Pull and push type services built on top of UDP

UDP is based on a connectionless concept. As such, the UDP header does not contain much information apart from source and destination port numbers as well as the packet checksum. When using UDP as a transport protocol, the normal network level Firewall can only perform filtering based on IP addresses and UDP port numbers. This leaves a security hole to launch denial-of-service attacks to UMTS networks and MSs.

14.3.3 Internet diagnostic services

(1) ICMP error messages

ICMP messages are typically sent to report errors that have occurred in the process of datagrams. When UMTS MS acts as a host of an Internet application, the following ICMP error messages can be sent to the MS due to various errors.

- Destination Unreachable, both routers and hosts can send *ICMP Destination Unreachable* messages to source hosts under certain circumstances. One example is that a router may need to fragment a datagram to forward it, but the Do Not Fragment flag may be set.
- Time Exceeded, when a router finds that the Time To Live field of a datagram has been decrement to zero, the datagram will be discarded and a *Time Exceeded* message will be sent to the source host. When Fragmentation is used, the destination host will send a Time Exceeded message if not all the fragments are received within a certain time period.
- Parameter Problem, when a problem found in the IP header parameters, an *ICMP Parameter Problem* message will be sent to the source host.
- Source Quench, when a datagram arrives at a router or host faster than they can be processed, a *Source Quench* message will be sent back to the datagram source.

(2) Internet PING service

PING service is designed to test the reachability of a remote network or host. It utilises the ICMP Echo Request/Reply message pair to perform the function.

The issue is whether UMTS MS should be PING-able. If so, a security hole is left to launch SMURF and PING broadcast attacks.

(3) Path MTU Discovery

In order to avoid performing datagram fragmentation in the end-to-end route and at the same time to transfer those datagrams at the largest possible size, the *Path MTU Discovery* service is provided to set the MTU for an end-to-end route before transferring a large amount of datagrams.

Path MTU Discovery is realised by sending a series of IP datagrams with the “Don’t Fragment” bit set until a packet reaches the destination (The first IP datagram is sent with the size of the first hop) without receiving the ICMP Destination Unreachable. Then the packet size of the last datagram is used as Path MTU.

This is a very powerful service in avoiding segmentation and therefore improving end-to-end QoS. The question is how UMTS domain deals with the Path MTU Discovery messages in order to avoid flooding the network.

References *(may be added per editor’s judgment)*

[1] 3G TS 29.060 v3.4.0 “GPRS Tunnelling Protocol Across Gn and Gp interface”, Mar 2000.

[2] 3G TS 23.060 v3.3.0 “UMTS; GPRS; Service description; Stage 2”, April 2000.

[3] IETF RFC 792, “ICMP – Internet Control Message Protocol”, 09/01/1981.

[4] IETF RFC 1191, “Path MTU Discovery”, Nov 1990.

[5] IETF RFC 1981, “Path MTU Discovery for IP version 6”, Aug 1996.

[6] IETF Internet Draft, “ICMP Traceback Messages”, Mar 2000.