Probleme bei IMS

Von Gunnar Heine

Das IP-Multimedia Subsystem (IMS) als offene Dienstplattform ist zurzeit eine viel versprechende technische Entwicklung im Bereich Next Generation Network (NGN), VoIP und Triple-Play-Services. Doch noch sind nicht alle Stolpersteine beseitigt.

SCHWERPUNKT IMS

Einige wichtige Probleme an denen bei IMS derzeit noch gearbeitet wird, sollen im zweiten Teil der Artikelserie erörtert werden. Eine Schwierigkeit ist der Bereich hereinkommender Telefonate. Von Seiten 3GPP (Third Generation Partnership Project) fehlt bisher die Spezifikation, wie IMS-Teilnehmer für reguläre Telefongespräche aus dem PSTN (Public Switched Telephone Network) angesprochen werden können. Dieser Punkt wurde bereits im ersten Teil der Artikelserie dargestellt. Der Grund erklärt sich unter anderem aus der Historie des IMS als Erweiterung der existierenden Mobilfunknetze: Gespräche aus dem PSTN werden dort auf normalem Weg über die kanalvermittelte Architektur verarbeitet. Die Frage einer IMS-Involvierung stellte sich erst nachträglich. Wir werden im Folgeartikel in der kommenden Ausgabe einen möglichen Lösungsansatz beschreiben. Auch das zweite Problem, nämlich das der Verfügbarkeit von Echtzeit-QoS (Quality of Service) im Zugangsnetz (IP-CAN – Internet Protocol – Connectivity Access Network) wurde bereits beschrieben. Es ist eng verknüpft mit den Schwierigkeiten im Bereich der Zugangsnetze, siehe weiter unten.

Als dritter Punkt ist das Thema der Interoperabilität zu nennen. Wie im Vorfeld dargestellt, gibt es bei IMS-Implementierungen Probleme mit dem Interworking untereinander und zu den unterschiedlichen Endgeräten. Ursachen hierfür sind zum einen die verschiedenen IMS-Standard-Varianten und zum anderen die Tendenz, ein System zu entwickeln noch bevor der zugrunde liegende Standard wirklich fertig ist. Insbesondere der letztgenannte Punkt erfordert vom Hersteller proprietäre Problemlösungen, die dann im Betrieb zu den genannten Interoperabilitäts-Problemen führen.

Ebenfalls eine Schwierigkeit stellt der Zugang aus jedem Zugangsnetz dar. Zumindest im Release 5 des 3GPP-Standards ist der Zugang zum IMS nur von GSM/GPRS- beziehungsweise UMTS-Netzen heraus möglich. Mit Release 6 lässt sich der Zugang zwar auch aus alternativen Zugangstechniken realisieren, diese müssen aber so genannte I-WLANs im Sinne von 3GPP sein. Die Gründe dafür sind unter anderem die beschriebenen Themen wie Verfügbarkeit von Echtzeit-QoS, Identifizierung und Authentisierung beziehungsweise mögliche Sicherheitsrisiken wie Intrusion und Denial-of-Service-Attacken.

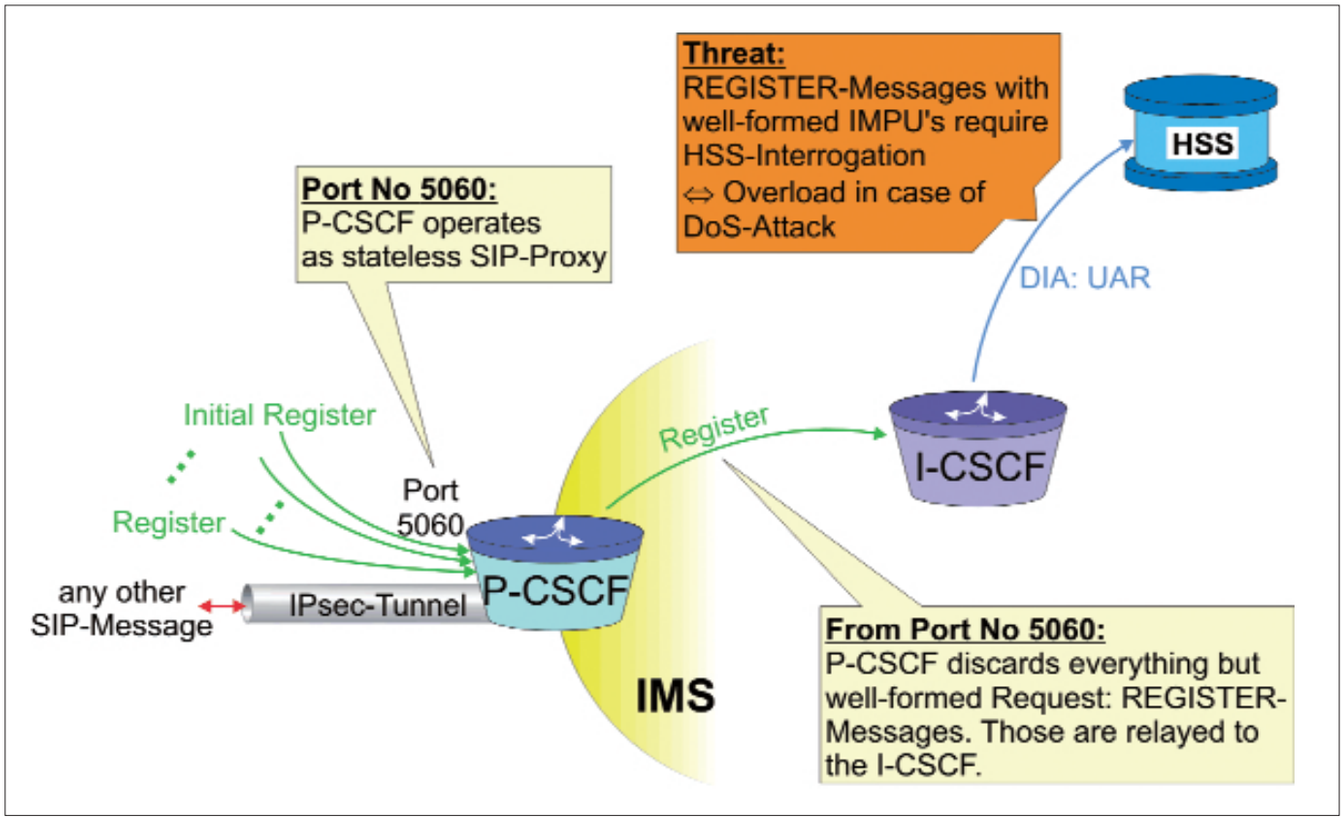
Als weiterer Stolperstein für die Freigabe von jeder Art von Zugangsnetz muss das Thema NAT/NAPT (Network Address Translation/Network Address Port Translation) genannt werden. Da das Session Initiation Protocol (SIP) und vor allem das Session Description Protocol (SDP) mit eingebetteten IP-Adressen und Port-Nummern arbeiten, ist die Verwendung privater IP-Adressen im IMS-Umfeld ohne aufwendige Maßnahmen an den Netzgrenzen nicht möglich. Wir werden uns in der nächsten Ausgabe dieses Problems mit Nachdruck annehmen.

Die Möglichkeit von Intrusion und DoS-Attacken

Der Albtraum eines jeden TK-Netzbetreibers ist das Eindringen von Hackern in sein Netz. Bisher sind TK-Betreiber von diesen Gefahren relativ verschont geblieben, weil TK-Netze keine IP-Netze sind. Dies ändert sich natürlich mit dem Massen-Einsatz des IMS, beziehungsweise allgemeiner ausgedrückt, mit der Migration hin zu IP-basierten Techniken. Eines der Hauptprobleme in diesem Zusammenhang sehen wir im Bereich von DoS-Attacken. Ganz allgemein besteht eine DoS-Attacke darin, dass vom Angreifer derart viele Anfragen an einen Server geschickt werden, dass dieser mit der Bearbeitung nicht mehr nachkommt und seinen Dienst quittieren muss, das heißt sein Dienst für andere Kunden nicht mehr erreichbar ist. Dieses Problem entsteht dadurch, dass der Server für jede Anfrage Prozessor-Leistung und Speicherplatz reservieren muss, alles Ressourcen, die naturgemäß beschränkt sind. DoS-Attacken im IMS-Umfeld von 3GPP-Netzen sind besonders tückisch, da diese sofort ins Herz des Mobilfunknetzes treffen können, nämlich ins HLR (Home Location Register) beziehungsweise HSS (Home Subscriber Server). Damit kann der Gesamtbetrieb eines solchen Netzes, also nicht nur des IMS, lahm gelegt werden. Bild 4 illustriert den Weg einer solchen Attacke.

Dabei ist wichtig, dass laut 3GPP erst während der Registrierung auf einen IPsec-Tunnel umgeschaltet wird. Aber der „normale“ SIP-Port 5060 des IMS beziehungsweise der P-CSCF (Proxy Call Session Control Function) ist offen für jede korrekt formatierte und empfangene SIP-Register-Nachricht. Und jede dieser Nachrichten muss bearbeitet werden, das heißt sie werden an die I-CSCF (Interrogating Call Session Control Function) weitergereicht. Befindet sich in der SIP-Register auch noch eine korrekt formatierte IMPU (IP Multimedia Public Identity – User-ID), dann muss die Anfrage sogar an das oder

Gunnar Heine ist Geschäftsführer der Inacon GmbH, Buchautor und Lehrbeauftragter an der Fachhochschule Wilhelmshaven



Quelle: Inacon

Bild 4: DoS-Attacke auf IMS und HSS (Home Subscriber Server)

eines der HLRs beziehungsweise HSSs geschickt werden. Damit hat der Angreifer den größtmöglichen Schaden angerichtet.

Es stellt sich die Frage, weshalb man bei 3GPP dieses Problem nicht sofort erkannt und adressiert hat. Die Erklärung liefert wieder die im Vorfeld geschilderte Historie des IMS. Das Problem von DoS-Attacken stellt sich ja erst dann, wenn der Zugang von jedem Zugangsnetz aus erlaubt wird, insbesondere von beliebigen WLAN- oder DSL-basierten Netzen ohne echte Zugangskontrolle. Solange man den Zugang auf GSM/GPRS- und UMTS-Netze beschränkt, bleibt das Risiko überschaubar, weil diese Netze eine dedizierte und aufwendige Zugangskontrolle einsetzen. Wir werden im Folgeartikel einen möglichen Lösungsansatz beschreiben.

Wiederum aus der Historie heraus erklärbar ist das Problem der Identifizierung und Authentisierung des Endkunden beziehungsweise des Endgeräts. Bei der IMS-Standardisierung innerhalb von 3GPP konnte man sich auf eine der ganz wesentlichen Errungenschaften von ETSI beziehungsweise von GSM abstützen: Der unbedingten Verwendung von Smart Cards (SIM, USIM – Universal Subscriber Identity Module) durch den Endkunden zu Identifizierungs- und Authentisierungs-Zwecken. Diese harte Forderung hat bisher das Ausmaß von Sicherheitsproblemen im GSM-basierten Mobilfunk in überschaubaren Grenzen gehalten.

Das ganze Verfahren ist allerdings sofort in Frage gestellt, wenn andere Arten von Betreibern und andere Arten von Kunden oder Endgeräten das IMS verwenden wollen (Stichwort: Fixed Mobile Convergence). Man überlege sich einmal die Konsequenzen, wenn nunmehr jedes Festnetz-Telefon und jeder PC mit Softphone-Anwendung eine Smart Card benötigte. Eine solche Forderung lässt sich sicher nicht realisieren.

Auch an dieser Stelle gibt es bis dato keinen konkreten Lösungsweg jenseits von User-ID/Passwort oder zertifikatsbasierten Ansätzen.

Als letztes muss das Problem mit den IP-Adressen angesprochen werden. Welche IP-Adressen-Version soll verwendet werden – IPv4 oder IPv6? Natürlich hatte man innerhalb von 3GPP schon früh die Problematik von NAT und NAPT erkannt und daher von vornherein die Verwendung von IP-Adressen der Version 6 zwingend vorgeschrieben, und zwar für alle IMS-Nutzer. Denn bei IPv6 stehen derart viele Adressen zur Verfügung, dass kein NAT/NAPT mehr nötig ist, und sich die entsprechenden Probleme einfach nicht stellen.

Obwohl diese Annahme natürlich korrekt ist, möchten wir an dieser Stelle auch auf die inhärente Firewall-Funktion von NAT/NAPT-Routern hinweisen, die man nicht übersehen darf. Aus diesem und aus vielen anderen Gründen musste 3GPP letztlich seine Muss-Forderung nach IPv6 wieder aufweichen.

Für viele Hersteller stellt sich daher die Situation heute so dar, dass die Endgeräte mit so genannten Dual-Stacks IPv4/IPv6 ausgestattet werden müssen, um jeder Umgebung gewachsen zu sein. Eine weitere Komplikation in der schönen neuen Welt des IMS.

Fazit

Zweifellos ist das IP-Multimedia Subsystem als offene Dienstplattform zurzeit eine viel versprechende technische Entwicklung. Doch es lassen sich heute noch eine Reihe von Problemen im IMS-Bereich erkennen. In der nächsten Folge der Artikelserie werden wir versuchen, Lösungsansätze für diese Probleme zu erarbeiten und vorzustellen sowie die Chancen dieser Ansätze bewerten. *(GB)*