Harald Orlamünder 16. Mai 2008

Auszug aus dem Protokoll der
Protokoll der 19. Sitzung der neuen ITG-Fachgruppe 5.2.3
Next Generation Networks
am 10. April 2008 in Darmstadt

5. Fachthemen

5.1 Security for SIP-based Peer-to-Peer Internet Telephony (Lyubomir Lyubenov)

Während bei „klassischen“ SIP-Netzen zentrale Knoten für die Registrierung und Suche des Kommunikationspartners benutzt werden, ist die Information über die Lage der Knoten bei Peer-to-Peer SIP verteilt und die Suche geschieht z.B. über Distributed Hash Tables (DHT). Das Problem dabei ist, dass nun Informationen nicht mehr in einem geschützten Bereich – dem Server – liegen, sondern bei den Clients am Rand des Netzes. Aber die Sicherheit soll nach wie vor gewährleistet bleiben.

Nach einer kurzen Vorstellung des Projektstandes an der FH Mannheim wurden sie Sicherheitsaspekte erörtert. Die klassischen Schutzziele wie Geheimhaltung, Authentifizierung, Integrität, Verfügbarkeit und Verbindlichkeit gelten natürlich auch für die SIP-basierte Sprachverbindung. Als Mittel der Wahl gilt die Verschlüsselung, wobei die verschiedenen Verfahren wie symmetrische und asymmetrische Verschlüsselung, hybride Verfahren und Signaturen präsentiert wurden.

Interessant waren die Verfahren, die Skype einsetzt. Obwohl diese nicht offen gelegt sind, weiß man inzwischen doch schon einige Details. So werden bei Skype die Informationen im Super-Peer verschlüsselt abgelegt. Vergleichbar zu SSL wird zuerst mit einem asymmetrischen Schlüssel ein symmetrischer Schlüssel vereinbart, der dann für die eigentliche Kommunikation benutzt wird.

Interessant ist auch die Frage, wann und wie die IP-Adressen ausgetauscht werden. Das sollte erst beim wirklichen Verbindungsaufbau stattfinden und aus Sicherheitsgründen über zwischengeschaltete Proxies (was allerdings dem „reinen“ Peer-to-Peer-Gedanken widerspricht).

Eng mit dem Thema Sicherheit verwandt ist das Thema „Lawful Interception“, also das gesetzliche Abhören. Hie muss es trotz verschlüsselten Verkehrs für die Bedarfsträger möglich sein, gezielt einen Teilnehmer abzuhören. (Bei Skype ist das heute nicht der Fall!)

Und ein weiterer Aspekt ist nicht außer Acht zu lassen: die Gefahr von SPIT (SPAM over Internet Telephony), denn Nachrichten, die ein Server generieren kann, können auch in großer Zahl erzeugt und verbreitet werden.

5.2 NGOSS Standard (Volker Smoljko)

Das Thema Netzmanagement hat im Laufe der Jahre eine Wandlung erfahren: nicht nur, dass die Prozesse immer komplexer werden und daher Unterstützung durch intelligente System erfordern, Netzmanagement ist heute nicht mehr nur ein Mittel zur Prozessverbesserung sondern Voraussetzung für die Einführung neuer Dienste.

Unter dem Begriff „New Generation Operations Systems and Software program“ (NGOSS) hat das Telemanagement-Forum (TMF), ein Konsortium von ca. 400 Netzbetreibern, Dienstanbie-

tern, Herstellern und Systemintegratoren, ein umfangreiches Rahmenwerk geschaffen. Der Fokus wird auf die Themen *Process*, *Application*, *Data* und *Messaging* gelegt. Entsprechend werden 4 Bereiche behandelt:

- *Business Process Framework* mit der „Enhanced Telecom Operations Map“ (eTOM),
- *Enterprise-wide Information Freamework* mit dem „Shared Information and Data Model“ (SID),
- *Applications Framework* mit der „Telecom Applications Map“ (TAM), und
- *Systems Integration Framework* mit der „Technology Neutral Architecture“ (TNA/SOA).

Dazu kommen die übergreifenden Aspekte:

- *Compliance and Conformance Testing Criteria* und
- *Lifecycle and Methodology*.

Die Datenwelt (IT) hat mit der „IT Infrastrcture Library“ (ITIL) ein eigenes Rahmenwerk definiert. Durch das Zusammenwachsen von Informations- und Kommunikationstechnik, wird jetzt teilweise auch im TK-Bereich ITIL gefordert. Eine Koexistenz von eTOM und ITIL ist wahrscheinlich, wobei es hierbei nur um die ITIL-Prozesse im Bereich Operations (Problem-, Incident,- und Change Management Prozess) geht. Eine Harmonisierung von ITIL und eTOM ist von TMF aufgenommen worden, wobei es im Wesentlichen um die Harmonisierung der Begriffe geht.

Das generelle Problem der Einführung neuer Verfahren beim Netzbetreiber ist die Forderung nach ununterbrochenem Dienst – der Kunde soll seine Dienste stets zu Verfügung haben, denn dahinter steht das Geschäft und damit die Einkünfte der Betreiber. Änderungen in den Betreiberinternen Prozessen sollen sich also nicht nach Außen auswirken. Das erfordert eine ausgefeilte Migrations-Strategie.

5.3 Ethernet Update (Thomas Knoll)

Aus den aktuellen Entwicklungen zum Thema „Carrier Ethernet“ wurden VPN-Lösungen vorgestellt. Benutzten seither die Geschäftskunden IP-VPNs, oder L3-VPNs (wie MPLS-VPN oder IPsec Tunnel), sind in Zukunft auch Ethernet VPNs gefordert. Erste Ansätze sind der „Virtual Private Wire Service“ (VPWS) und der „Virtual Private LAN Service“ (VPLS), bei denen Ethernet über MPLS transportiert wird.

Das Metro Ethernet Forum (MEF) hat sich seit 2001 dem Thema „Carrier Ethernet“ angenommen und definiert die Anforderungen:

- Standardized Servies,
- Scalability,
- Service Management,
- Reliability und
- Quality of Service.

Diese unterschieden sich deutlich vom klassischen Ethernet-LAN. Das MEF hat inzwischen 19 Dokumente veröffentlicht, die sich mit Ethernet-Diensten und deren Tests beschäftigen. (http://www.metroethernetforum.org/)

Die Technik hinter den verschiedenen Diensten benutzt das VLAN-Tagging (IEEE 802.1q), das „VLAN-Stacking“ (IEEE 802.1ad), bei dem zwei VLAN-Tags benutzt werden, sowie eine Technik bei der dem Ethernet-Rahmen ein weiterer Header vorangestellt wird – unter dem Begriff „MAC-in-MAC“ oder „Provider Backbone Bridges“ (PBB) bekannt (IEEE 802.1ah). Mit diesem umgeht man den begrenzten Adressvorrat des VLAN-Tags (nur 4096 Werte) und vor allem die Verwendung der Kunden-MAC-Adressen im Betreibernetz.

Die letzte Entwicklung in dieser Reihe ist PBB-TE, wobei „TE“ für „Traffic Engineering“ steht, oder kurz „PBT“ (IEEE 802.1 Qay). Kernpunkt dieser Erweiterung ist das Einrichten von Pfaden per Management, wobei in Zukunft dieses per GMPLS erfolgen wird, womit sich ein Kreis zum MPLS schließt.

Denn auch MPLS begegnet der Kritik, es sei „zu komplex und Ethernet ja viel einfacher“ mit einer Variante, die nur eine Untermenge vom klassischen MPLS darstellt, dem „Transport-MPLS“ (T-MPLS). Dabei wird ein Ethernet-Rahmen in MPLS transportiert; E-LSP und L-LSP werden unterstützt und neben unidirektionalen LSPs sind auch bidirektionale LSPs möglich.

Da man Ethernet immer ähnlicher zur klassischen Übertragungstechnik gestalten will, sind auch die dortige Schutzmechanismen zu emulieren wie z.B. die Ersatzschaltung (Protection Switching). Interessant ist, dass Arbeiten auf diesem Gebiet der ITU-T überlassen wurden. Eine sinnvolle Entscheidung, denn dort liegt das Know-How auf diesem Gebiet. Für diese Zusammenarbeit wurde im Februar 2008 ein „joint working team (JWT)“ zwischen ITU-T und IETF geschaffen.

Interessant im Bereich der Dienste ist noch der TDM-Support, der es erlaubt, klassische Telekommunikationsschnittstellen wie E1 (2 Mbit/s) oder einzelne Container aus der SDH-Welt über Ethernet zu übertragen. Das wird allerdings mit einem erheblichen Overhead erkauft: so wurde ein Faktor von ca. 5 gemessen!