



Artigo: Segurança em redes 3G - UMTS

André Ligieri Straccialano

Evolução das Redes Celulares no Brasil

Nos anos 50, as concessões dos serviços de telecomunicações eram distribuídas indistintamente pelos governos federal, estaduais e municipais, propiciando que empresas operadoras surgissem e se expandissem de forma desordenada, com custos onerosos e sem qualquer compromisso com a qualidade, gerando problemas operacionais e resultando falhas de interconexões entre as regiões do país. Diante deste cenário surge a necessidade de interação por parte do Governo Federal, e diante deste cenário foi aprovado pelo Congresso Nacional, em 27 de agosto de 1962, a Lei 4.117, instituindo o Código Brasileiro de Telecomunicações, responsável pela transformação radical do panorama do setor, disciplinando os serviços telefônicos e colocando-os sob o controle da autoridade federal.

O Código Brasileiro de Telecomunicações implementou a política básica do setor, além de definir um modelo tarifário e transformar todas as empresas em um único Sistema Nacional administrado pelo Conselho Nacional de Telecomunicações, subordinado a Presidência da República, com as atribuições de coordenar, supervisionar e regulamentar o setor de telecomunicações;

No início da década de 70 o serviço de telefonia de longa distância apresentava um bom nível de qualidade e a telefonia urbana era deficiente. Como solução foi autorizada a criação de uma sociedade de economia mista através da Lei 5792, de 11 de julho de 1972. Assim nascia a Telecomunicações Brasileiras S/A - TELEBRÁS, vinculada ao Ministério das Comunicações, com atribuições de planejar, implantar e operar o sistema.

Foi nesse período que a TELEBRÁS implantou em Campinas, o Centro de Pesquisa e Desenvolvimento - CpQD, que buscava a pesquisa e desenvolvimento de um modelo de telecomunicações brasileiro com foco em redução de importações e consequentemente independência de mercados externos e justamente com este cenário que surge na cidade de Brasília o primeiro grupo de estudos em telefonia móvel no Brasil, que utilizava o sistema ITMS (Improved Mobile Telephone System) que operava com baixa capacidade de acesso e tinha na rede apenas 150 terminais.

No ano de 1973, as operadoras do sistema TELEBRÁS são eleitas responsáveis pelo fornecimento do serviço e começa os estudos para a definição do modelo de sistema adotado no Brasil, mas somente no ano de 1983, inicia-se em São Paulo os testes com o modelo adotado, que correspondia a tecnologia AMPS (Advanced Mobile Phone System) que foi utilizado em todos os países do continente Americano e em alguns outros da Ásia e Austrália. Esta tecnologia utiliza como acesso múltiplo a divisão de frequência (FDMA) e consiste em 416 canais, sendo que 21 são usados para controle, nos canais de voz são utilizados uma frequência para transmissão em outra para recepção, com banda de 30Khz cada, utilizando modulação de frequência.

Inicialmente o sistema adotado compreende no AMPS e logo através de análise de demanda foi instituído o sistema estendido E-AMPS, que entrou em operação na cidade do Rio de Janeiro no ano de 1990, portanto esta foi o início do modelo comercial de telefonia no Brasil, sendo também no ano seguinte implementado em Brasília e logo após nas cidades de Campo Grande, Belo Horizonte e Goiânia. As operações na cidade de São Paulo e no interior iniciaram em 06 de Agosto de 1993, sendo que representou o último dos grandes mercados mundiais a receber a tecnologia.

Diante deste cenário e a tendência mundial de inovação e novos serviços, o sistema de telecomunicações brasileiro demandava novos e altos investimentos, o estado no entanto não injetava os recursos necessários em relação ao tempo e demanda que o mundo apresentava novas soluções, além do que estruturas estatais carregavam a máquina administrativa nacional e



Artigo: Segurança em redes 3G - UMTS

visando aumento de competitividade orientado para universalização das telecomunicações foi aprovado pelo Congresso Nacional a Emenda nº 8 à Constituição Federal, em 8 de agosto de 1995, permitindo ao Governo Federal outorgar concessões para exploração de serviços de telecomunicações ao setor privado. A Lei nº 9.295/96 permitiu a licitação de concessões de telefonia celular da banda B e em julho de 1997 o Congresso Nacional aprovou a Lei Geral das Telecomunicações (Lei nº 9.472), a base regulatória para o setor, que também continha as diretrizes para a privatização do Sistema Telebrás. A venda ocorreu no dia 29 de julho 1998 através de 12 leilões consecutivos na Bolsa de Valores do Rio de Janeiro, pela venda do controle das três holdings de telefonia fixa, uma de longa distância e oito de telefonia celular, configurando a maior operação de privatização de um bloco de controle já realizada no mundo. Com a venda, o governo arrecadou um total de R\$ 22 bilhões, um ágio de 63% sobre o preço mínimo estipulado.

Diante deste cenário, no ano de 1997 com a abertura de mercado de telefonia móvel, o espectro de frequência foi dividido em duas bandas: a Banda A de 825.03 a 834.99 MHz, abrangendo os canais de 1 a 333 e a Banda B de 845.01 a 846.48 MHz, abrangendo os canais de 334 a 666. Ambas as bandas possuem uma faixa expandida (E-AMPS) que varia para a Banda A de 824.04 a 825.03 MHz, abrangendo os canais de 991 a 1023 MHz, e a Banda B de 846.51 a 848.97 MHz abrangendo os canais de 717 a 799. Nesta mesma época a Anatel não impõe regras quanto a migração para o sistema de segunda geração 2G, o novo sistema digital, onde as operadoras de telefonia celular ficaram livres para escolher o padrão que melhor se adapta a sua situação.

Com a ampla utilização do sistema AMPS, a saturação de banda tornaria-se inevitável e a oferta de serviços limitada, pois a tecnologia de primeira geração não previa outros negócios, como dados, fax, SMS e outros, inclusive os altos investimentos também obrigavam as empresas buscar um acréscimo de receita e a solução foi a migração para sistemas digitais. Como premissa para as novas tecnologias de segunda geração (2G), o sistema deveria operar sobre as mesmas bandas existentes, evitando assim alterações na planta já instalada, também foi considerado o uso mais eficiente do espectro, tornado a tecnologia capaz de atender mais usuários. Diante disto, duas tecnologias propostas foram introduzidas comercialmente no Brasil, o D-AMPS e o CDMA, que juntamente com o GSM Europeu caracterizaram a segunda geração (2G) de telefonia móvel, ainda voltada para serviços de voz, porém já suportando um determinado número de serviços adicionais.

O D-AMPS (Digital AMPS), padronizado inicialmente pelo padrão IS-54 e aperfeiçoado pelo IS-136, utiliza diretamente a estrutura de canais de 30 kHz, mantendo portanto uma compatibilidade plena com o sistema analógico já implantado, justificando o nome inicial. Os canais de transmissão e recepção de 30 kHz compartilham no tempo 3 intervalos comutados digitalmente, numa técnica conhecida como TDMA (Time Division Multiple Access ou Acesso Múltiplo por Divisão de Tempo). Logo no início da implantação comercial, o nome do sistema D-AMPS foi abandonado na prática, sendo totalmente substituído pelo nome da tecnologia, com a utilização de 3 slots de tempo, foi possível aumentar em 3 vezes a capacidade em relação ao sistema AMPS. No Brasil esta tecnologia foi inicialmente utilizada pelas operadoras de banda B, pois oferecia além de melhor capacidade (canal RF x Usuários), um índice de MOS (Mean Opinion Score) superior ao sistema analógico, portanto seria uma estratégia comercial aderir uma tecnologia digital, podendo além de operar em roaming em redes AMPS, ofertar novos serviços, como identificador de chamadas e mensagens de texto.

O CDMA (Code Division Multiple Access ou Acesso Múltiplo por Divisão de Código), no padrão IS-95, revolucionou os padrões da época, pois a base dos sistemas que tinham como herança os sistemas analógicos FDM e permaneceu nos sistemas digitais através de compressão de sinais em modulação multi nível tinham como objetivo minimizar o uso da banda, propondo assim uma economia do uso do espectro que ao contrário no CDMA, utilizava espelhamento



Artigo: Segurança em redes 3G - UMTS

espectral, sendo que como conceito utiliza toda a banda disponível em um determinado canal, em muitos casos, muito mais do que o suficiente para um único sinal. Esta tecnologia utiliza canais de 1,23Mhz e utiliza como modo de acesso multiplexação através de códigos, gerados do telefone até a estação base e vice versa, contudo a capacidade do modelo esta diretamente ligada ao mecanismo de controle de potencia e sinais de interferência, quanto menor a potência utilizada maior será a capacidade. Em valores teóricos, a capacidade do sistema CDMA é 7 vezes maior que o AMPS, e também oferece novos serviços, como mensagens, identificador de chamadas e outros, esta tecnologia no Brasil foi introduzida para ofertar maior maior eficiência de espectro e melhora de qualidade no sistema, sendo a alternativa para as operadoras principalmente denominadas banda A, que foram adquiridas no leilão de privatização pelos grupos Portugal Telecom e Telefonica Mobile em alguns dos principais mercados dos países.

O Brasil durante os anos de 1998 até inicio de 2002 possuía operações das tecnologias TDMA e CDMA com serviços digitais e a planta inicial através de AMPS em todo território nacional, portanto para aumentar a oferta de serviços para os usuários foi introduzindo novos concorrentes nos conforme previsto pela LGT, sendo assim foi efetuado o leilão da banda C em 02 de Fevereiro de 2001, tendo fracassado devido ao inicio das licitações das redes de terceira geração na Europa, demandado altos investimentos, outro fato interessante foi os altos custos solicitado pelo governo para compra das licenças, que introduzia no país o sistema GSM (Global System For Mobile Communications), amplamente utilizado na Europa, inclusive a frequência ofertada neste leilão de 1,8Ghz é exclusiva para uso militar nos Estados Unidos. Outro fato interessante que marcou o leilão da banda C foi a impossibilidade de participação de operadoras de telefonia fixa, fato este que com a disponibilidade para os leilões da banda D e E o vencedor da área I foi a concessionária desta localização, e com isso iniciou-se no Brasil a oferta de tecnologia GSM.

No ano de 2002 após o leilão das bandas D e E e utilizando a faixa de frequência DCS 1800Mhz, que corresponde a 1710Mhz a 1785Mhz para subida e 1805Mhz a 1880Mhz novos concorrentes introduziram a tecnologia GSM no Brasil, este sistema teve origem através de estudos realizados em conjunto por Franceses e Alemães e foi acordado por diversos países europeus, sendo encaminhando para constante desenvolvimento no ano de 1989 para a ETSI (European Telecommunications Standards Institute), com isso diversos outros países, como Austrália e outros do continente asiático adotaram este modelo. O GSM teve algumas fases, introduzindo novos recursos e funcionalidades, uma de suas principais características foi a inserção de um modelo de autenticação baseado na identidade o usuário, com a capacidade de mobilidade para outro equipamento móvel.

O GSM utiliza no espectro DCS 1800 373 canais de RF, com banda de 200Khz para o par de frequências de transmissão e recepção, utilizando modulação digital 0,3GMSK (Gaussian Minimum Shift Keying), utilizando taxa de dados de 270Kb/s, operando com divisão de 8 slots de tempo através de TDMA. No seu canal de RF de 200Khz o GSM possui capacidade de 8 chamadas, fato este proporcionado pela melhor modelo de reutilização de frequências.

Em 2003 o cenário da telefonia celular no Brasil teve uma importante alteração, a fusão das empresas pertencentes ao Grupo Portugal Telecom e Telefônica criaram a marca Vivo, formada basicamente pelas operadoras de Banda A e a aquisição pela Telecom Américas das operadoras de banda B, formando a marca Claro, com isso o mercado nacional de telefonia celular a atendido com mais de 95% pelas empresas Claro, Vivo, Oi e TIM.

Diante deste cenário, ocorre o inicio da migração de clientes que utilizam a tecnologia TDMA para as redes GSM, durante o ano de 2002, auge da tecnologia no Brasil, 60% dos clientes acessavam as redes através de TDMA, cenário este no final de 2003 já apresentava queda de 15% e permaneceu até os dias atuais com desativação total devido a necessidade de utilização do espectro para tecnologia de terceira geração, no entanto neste mesmo ano, a tecnologia GSM apresenta juntamente com o CDMA um inicio de uma disputa por modelo de comunicação de dados mais eficiente, dando inicio a geração 2,5 no Brasil.



Artigo: Segurança em redes 3G - UMTS

A tecnologia de transmissão de dados com velocidades teóricas superiores as convencionais dos celulares de segunda geração já não era novidade no Brasil, contudo a oferta de apenas uma operadora não impulsionou o mercado durante o ano de 2002, sendo que o em 2003 com novas ofertas alavancou o mercado. Os ofertas baseavam-se basicamente na tecnologia CDMA2000 1RxTT, que utilizava um canal de 1,25Mhz para o oferecimento de serviço de dados, combinado com modulação mais eficiente, e as redes com acesso TDMA, no Brasil exclusivamente a tecnologia GSM com o serviço GPRS, que operava com a utilização dos 8 slots de tempo de GSM, sem reserva de recursos. Uma questão importante foi a introdução da comutação de pacotes pela rede GPRS, este serviço possibilitou a cobrança por demanda, e a maior cobertura GSM no Brasil impulsionou esta tecnologia.

No ano seguinte, a demanda por aumento de largura de banda para dados acelerou o processo de implantação de tecnologia CDMA2000 EV-DO, que corresponde a uma melhoria no sistema de modulação e uma melhora na codificação de envio de dados em relação aos erros de transmissão possibilitando taxas teóricas de 2,4Mb/s, no entanto as redes GSM introduziram em 2004 o EDGE, que basicamente melhorou a eficiência da modulação e aumentando a taxa do GPRS em três vezes.

Esta evolução para demanda de serviços de dados com maiores taxas levou as operadoras a planejar o modelo de evolução para redes de terceira geração, a adoção da tecnologia GSM pela Vivo inclui no cenário nacional uma cobertura de mais de 85% da base, contudo para o oferta de redes de terceira geração, que no cenário nacional já é representado pelo EV-DO, surge a necessidade de utilização da evolução do modelo GSM, mantendo interoperabilidade entre os dois sistemas, com isso a tecnologia abordada é a UMTS (Universal Mobile Telecommunications System), que apresenta um conceito de novos serviços, e ingressa as redes celulares em modelos convergentes futuros, com o acesso aos serviços IP, já utilizados em escala global através da internet.

Diante disto, a Anatel ofertou através de leilão espectros específicos para esta tecnologia porem, o reaproveitamento de frequências utilizadas na banda B impulsionou o lançamento da tecnologia no ano de 2007, fazendo com que o serviço iniciado possa ser implantado gradativamente em novas regiões, ofertando a nova tecnologia para todo o Brasil.



Artigo: Segurança em redes 3G - UMTS

Arquitetura Redes 3G - UMTS (Universal Mobile Telecommunications System)

A rede celular de terceira geração, que utiliza a notação International Mobile Telecommunications 2000 - IMT 2000 pela ITU (International Telecommunication Union) e UMTS (Universal Mobile Telecommunications System) reconhecida na Europa e possui notação mais reconhecida no Brasil, é considerada a sucessora do GSM, pois preserva os investimentos realizados nas evoluções da planta já instalada e opera em conjunto com as redes UMTS, portanto prove migração suave aos sistemas GSM já implantados. Outro fato importante compreende na arquitetura de serviços, que foi planejado para ofertar uma infinidade de serviços, juntamente com uma estrutura universal de roaming, preservando as configurações pessoais de cada cliente.

Na sua primeira versão, a rede UMTS foi concebida para prover os seguintes serviços:

- **Teleserviços** (Voz, SMS, Identificador de Chamadas, Chamadas em espera, conferências e outros...)
- **Portadores** (Fornecem serviços com a necessidade de controle de capacidade de transferência entre os acessos, estes serviços possuem parâmetros distintos para atraso, jitter e taxa de erros)

Entretanto, tanto serviços orientados a conexão como os não orientados a conexão possuem capacidade de conexões ponta a ponto e ponta a multiponto, com isso as taxas oferecidas aos serviços são:

- 144Kb/s - Rural Indoor
- 384Kb/s - Urbano/Suburbano outdoor
- 2Mb/s - Indoor/Outdoor curto alcance.

Com relação a qualidade de serviço, o sistema possui algumas classes pré determinadas:

- Conversação (Voz, Video Chamadas e Serviços Interativos tempo real)
- Streaming (Serviços Multimídia, video sob demanda e webcast)
- Interativa (Navegação Internet, Jogos rede, acesso a aplicativos)
- Background (e-mail, SMS, Downloads)

Os serviços oferecidos podem ser customizados pelas operadoras, e ofertam conforme parcerias estratégicas uma infinidade de conteúdo para as redes UMTS, entretanto os serviços de Voz, Fax, SMS e Chamadas de Emergência são padronizados, pois necessitam de interface com outros concorrentes, como exemplo de serviços podemos citar alguns:



Artigo: Segurança em redes 3G - UMTS

Informação

- *Navegação Internet*
- E-Commerce
- Notícias

Ensino

- Aulas Virtuais
- Pesquisas a bibliotecas on-line

Entretenimento

- Musicas sob demanda
- Games
- Video Clips
- Turismo Eletrônico

Serviços à comunidade

- chamada de emergência
- serviços administrativos

Serviços de negócios

- escritório móvel
- *business TV*
- grupos de trabalho virtuais

Serviços de Comunicação

- vídeo chamadas
- vídeo conferência
- localização pessoal

Serviços financeiros

- banco virtual
- E-Payments

Serviços especiais

- tele-medicina
- monitoramento

A arquitetura da rede UMTS, é subdividida e três domínios, que correspondem a :

- **User Equipment** : Corresponde ao terminal móvel juntamente com seu modelo de identificação do usuário USIM (Universal Subscriber Identity Module)
- **UTRAN** : UMTS Terrestrial Radio Access Network) Prove a rede de acesso so terminal móvel
- **Core Network**: Responsável pelos domínios de comutação de circuitos e pacotes

A Figura 1 representa a arquitetura da rede UMTS e apresenta seus elementos:

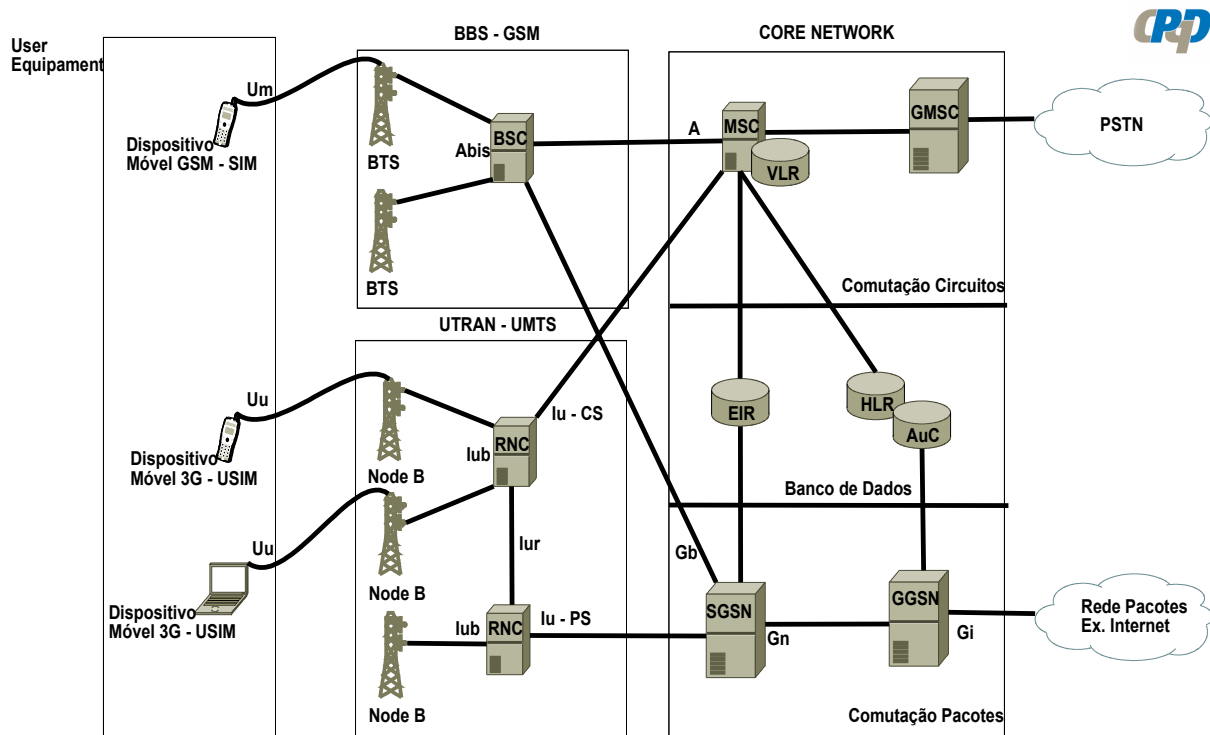


Figura 1

User Equipment

Neste domínio o telefone do cliente e o USIM (Universal Subscriber Identity Module), prove acesso a rede celular de terceira geração, o USIM corresponde a um cartão de memória que contém informações responsáveis para prover autenticação, identificação, armazenamento de aplicações e configurações do usuário. Como identificação o USIM armazena o IMSI (International Mobile Subscriber Identity, utiliza um número 15 dígitos, sendo que os três primeiros apresentam o MCC (Mobile Country Code), que corresponde a identificação do país, os dois ou três subsequentes para o MNC (Mobile Network Code) apresentando o número de identificação da operadora, variando de 2 dígitos para padrão Europeu e três para Americano, e os posteriores correspondem a MSIN (Mobile Subscriber Identification Number), associado ao número do cliente na rede, por exemplo 724 (Brasil) 07 (CTBC) 1234567890 (Número Identificação Rede). Outros elemento armazenado é a chave de autenticação Ki (Authentication Key) que utiliza uma chave criptografada em 128 bits assinada pela operadora durante o processo de inicialização e validação do USIM Card, esta chave também é armazenada no centro de autenticação localizado no core da rede para segurança no processo de autenticação e utilização dos serviços de terceira geração. Outros elementos são o ICC-ID (Integrated Circuit Card ID) que identifica universalmente o cartão, o LAI (Local Area Identity) que armazena o código de área para o cliente e informações utilizadas para SMS, contatos ou outras aplicações específicas. O cartão também armazena o PIN (Personal Identification Number) que é utilizado junto com as informações do IMSI e Ki para o processo de autenticação, este código é importante, pois inseri outra camada de segurança no processo, correspondente a interação humana do usuário.



Artigo: Segurança em redes 3G - UMTS

UTRAN - UMTS Terrestrial Radio Access Network

A rede de acesso para os serviços de terceira geração utiliza a interface Uu, sendo implementada através de WCDMA-FDD (Wideband Code Division Multiplex Access - Frquency Division Duplex), que compreende na utilização de 2 canais de subida e descida de 5Mhz, separados por uma banda de guarda. O acesso múltiplo dos usuários aos canais é o DS-CDMA (Direct Sequence CDMA), que utiliza através diferentes códigos com espalhamento espectral.

Na domínio UTRAN as funções do NODE B e RNC são as seguintes:

Node-B

- Transmissão/recepção
- Modulação / Demodulação
- Codificação do canal físico CDMA
- Micro diversidade
- Tratamento de erro
- Closed loop power control

RNC

- Controle de recursos de rádio
- Controle de admissão
- Alocação do canal
- Parâmetros de controle de potência
- Controle de Handover
- Macro Diversidade
- Encriptação
- Segmentação / Reunião
- Sinalização de Broadcast
- Open Loop Power Control

A partir do release 5, as bases de radio GSM passaram a utilizar a interface Iu já padronizada pelo UMTS, com isso um dispositivo multi rádio poderá ofertar similaridade de serviços, inclusive incluir outros mecanismos de acesso, como WLAN.

Core Network

O core network tendo como base o aproveitamento da planta GSM já implantada pode ser analisada como três domínios distintos:

Comutação de Circuitos

Neste subdomínio podemos citar como elemento principal o MSC (Mobiles Services Switching Centre), responsável pela Comutação, Sinalização, Paging, e InterMSC handover. Outro elemento presente é a VLR (Visitor Location Register), que executa função de registro temporário para terminais em deslocamento. O GMSC (Gateway Mobiles Services Switching Centre) é o responsável pela interconexão entre a rede UMTS e as diversas redes de telefonia.



Artigo: Segurança em redes 3G - UMTS

Comutação de Pacotes

Este domínio fornece as funções gerência e conexões entre a rede UMTS e as redes de dados, tendo como exemplo a Internet, o SGSN (Serving GPRS Support Node) estabelece a conexão lógica entre o terminal e a rede, exercendo como ponto principal o controle dos terminais, já o GGSN (Gateway GPRS Support Node) estabelece o acesso entre o backbone da rede de pacotes e o core da rede de pacotes UMTS.

Banco de Dados

Este domínio estabelece funções de registro de informações para ambas as divisões do núcleo, pacotes e circuitos, tendo como elementos o HLR (Home Location Register) que contem as informações definitivas dos assinantes, como perfil do cliente, situação e ponto local de acesso. O AUC (Authentication Center) armazenas as chaves de identidade para cada usuário que possui registro na HLR, provendo mecanismo de autenticação para o IMSI, e gerando as chaves para comunicação segura entre o terminal e a estação rádio de acesso. Outro elemento presente neste domínio é o EIR (Equipment Identity Register) que armazena a identidade do terminal móvel, IMEI (International Mobile Equipment Identity) estando este associado a uma base central prove controle de terminais proveniente de roubos e fraudes.

Core UMTS associado a IMS (Internet Protocol Multimedia System).

O IMS é patrocinada pelo 3GPP/2 com apoio dos principais órgãos de padronização com o intuito de fornecer serviços baseados em redes IP e tendo como principal meta a integração de voz e dados em uma base de informações única, com administração centralizada e integrada a diversas redes de acesso existente. Esta arquitetura possui três camadas, e em conjunto com a rede UMTS é dividida entre Aplicação, que contem a plataforma existente para os serviços, como por exemplo um serviço de e-mail, a camada de controle, que inclui também o gerenciamento das sessões, utilizando como base da convergência o protocolo SIP e a camada de acesso, que prove a conexão entre o equipamento, como por exemplo a rede UMTS/WCDMA, Redes Wireless LAN e outras. Esta arquitetura inicialmente desenvolvida para redes celulares despertou grande interesse das operadoras fixas, pois prove integração em suas infra estruturas e permitem um novo conjunto de serviços, agregando novas receitas a sua operação, a figura 2 representa este modelo.

Services in all-IP Domain:

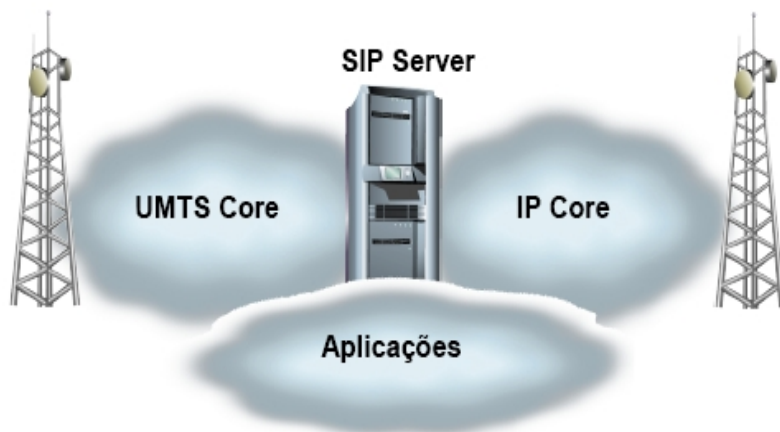


Figura 2

Segurança em Redes UMTS

A idéia de implementação de um modelo de segurança que garanta a confidencialidade das chamadas e prevenção de fraudes surge com a própria evolução das tecnologias. Nas redes AMPS interceptar uma conversação consistia em uma tarefa com poucas dificuldades, pois qualquer pessoa portando um scanner de rádio capturava a frequência de transmissão e recepção tinha acesso as informações, além do que o ESN (Eletronic Serial Number) que provia a autenticação do sistema era enviado em texto claro, possibilitando a captura e clonagem dos terminais. Com a evolução para os sistemas de segunda geração a inserção de codificação de voz, modulação digital através de GMSK (Gaussian Minimum Shift Keying) em conjunto com os sistemas de multiplexação baseadas em código e tempo dificultaram estas operações, mas ainda um invasor determinado a executar sua operação podia clonar um terminal e interceptar as chamadas, pois ainda não havia um meio de autenticação poderoso, que estabelecesse através de chaves cifradas o transporte as informações. A rede GSM e UMTS abordam em sua arquitetura um modelo que prove autenticação e confidencialidade a identidade do assinante e as respectivas sinalizações e informações, e em conjunto com relação ao serviço de dados aborda os aspectos de controle nos sistemas de bilhetagem por demanda.

Confidencialidade em redes UMTS

Processo de identificação em redes GSM/GPRS/UMTS

Nas redes GSM, o usuário possui registrado em seu SIM Card o IMSI, que possui função semelhante ao ESN nas redes analógicas, portanto para evitar a captura e clonagem do terminal, é utilizado o recurso TMSI(Temporary Mobile Subscriber Identity) que opera em conjunto com um código de registro de área LAI (Local Area Identity) evitando ambiguidades de registros, portanto, quando o terminal móvel é iniciado, o IMSI é enviado a rede, quando é inserido no VLR, ocorre um estabelecimento entre o IMSI e o TMSI gerado para a operação, com isso o TMSI é transportado, o IMSI somente será utilizado quando ocorrer falha na rede o no terminal, o TMSI é gerado a cada troca de VLR ou mediante a uma requisição. Nas redes GPRS o processo é semelhante, a diferença ocorre com o uso de um TLLI (Temporary Logical Link Identity), que é tratado pelo SGSN, ao contrário do GSM que opera o TMSI pelo MSC, outra alteração é o uso de um RAI (Routing Area Identity) que substitui o LAI na identificação de localidade, nas redes UMTS o processo de uso de um TMSI/TLLI é idêntico as redes GSM/GPRS.

Processo de autenticação em redes GSM/GPRS/UMTS

Necessidade de um sistema de autenticação

O processo de autenticação em redes celulares garante ao sistema que ele realmente é o que diz ser, ao ser registrado na rede ele obtém seu perfil para uso de funcionalidades na rede, como geração de chamadas de voz, acesso a rede de dados e outras, portanto se um usuário se identificar como outro ele poderá usufruir dos recursos sendo que a cobrança pelos serviços e responsabilidade jurídica pela utilização recairá para outro usuário, além do que receber suas informações e quebrar a confidencialidade do sistema. A figura 3 representa um modelo de ataque que através do core da rede UMTS poderá ocorrer a alteração da identidade de um usuário.

UMTS – Tipos de Ataques

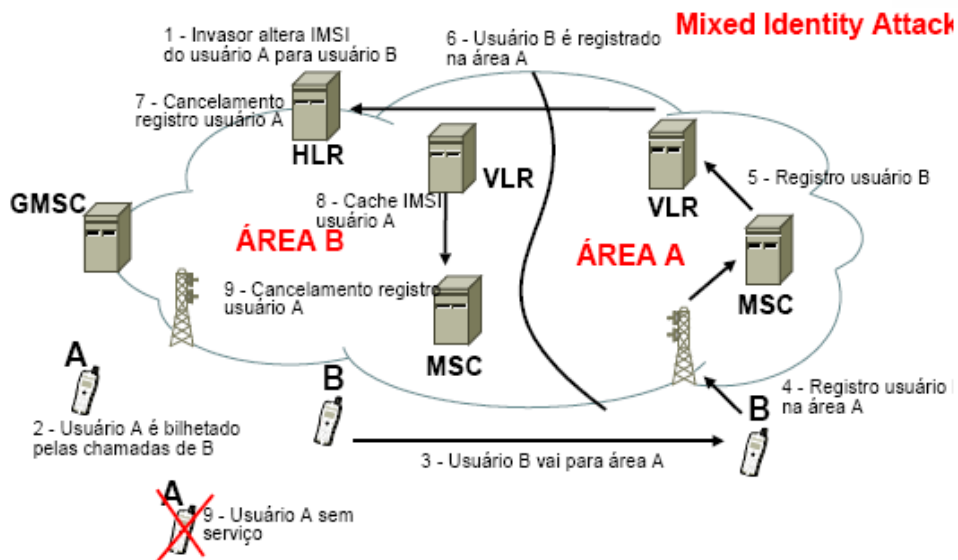


Figura 3

Processo de identificação e autenticação em redes UMTS

As redes UMTS utilizam como método de identificação e autenticação um processo diferente das redes GSM/GPRS pois tanto em redes estrangeiras como em home network cinco elementos são usados no processo:

- RAND: Número aleatório
- XRES: Resposta de autenticação
- Ck: Chave de ciframento
- Ik: Chave de Integridade
- AUTN: Token de autenticação

Para compreendermos a operação, segue a descrição do processo de autenticação mútua entre o usuário e a rede, que após a operação conhece a chave que é compartilhada entre eles, e está disponível apenas para o USIM e o AUC, este método de desafio e resposta mantém a compatibilidade com redes GSM existente, permitindo a autenticação quando uma rede UMTS não está disponível, este sistema garante a migração suave das redes já implantadas para UMTS.



Artigo: Segurança em redes 3G - UMTS

- Encaminhamento pela VLR/SGSN requisição autenticação para a HLR
- Resposta da requisição fornecida pela HLR
- Armazenamento pelo VLR/SGSN vetores de autenticação
- Encaminhamento da VLR/SGSN para o terminal da requisição de autenticação (RANDi) + AUTN(i)
- Verificação do AUTN(i) e geração do RES(i) pelo terminal
- Terminal envia a resposta RES(i) para a VLR/SGSN
- VLR/SGSN compara a RES(i) e XRES(i)
- Terminal gera a CK(i) and IK(i) e VLR/SGSN seleciona para uso.

Confidencialidade da Informação

Outro ponto necessário para manter a confidencialidade em sistemas celulares UMTS compreende no mecanismo de proteção de acesso ao rádio, pois caso o espião consiga compreender o mecanismo toda a confidencialidade da comunicação de voz e dados estará comprometida. Diante deste cenário, o UMTS adiciona como camada de segurança de proteção o UMTS Encryption Algorithm UEA que possui uma grande vantagem sobre os modelos utilizados nas redes GSM/GPRS A5 e GEA, pois ele não é secreto, fazendo com que sua força não esteja em seu desconhecimento e sim na própria robustez, tornando-se eficaz contra ataques de engenharia reversa.

O modelo de stream cipher implementado no UEA foi denominado F8, que possui como referência o algoritmo KASUMI, que vem do block-cipher japonês Misty. O F8 possui chave de 128 bits, tornando ataques como o Birthday Attacks e força bruta inviáveis. Nas redes UMTS o estabelecimento de chaves não é determinado como padrão, com isso uma das garantias é que as chaves geradas recentemente não foram usadas, isto é possível através de um número sequencial que chega cifrado até o USIM card e o sistema trata como já utilizado ou não, com isto são geradas duas chaves com o mesmo parâmetro (RAND) em dois algoritmos distintos, um denominado F3 para gerar Ck, que garante a confidencialidade e F4 para Ik, que será usado para garantir a integridade. Para garantir este requisito, o F9 foi padronizado para a rede UMTS.

A implementação do UEA é realizado sobre a camada RRC, mais precisamente sobre o terminal do usuário e o RNC, este trata-se de uma função hash que calcula um MAC-I (Message Authentication Code-Integrity) e encaminha junto com as informações de sinalização, quando o receptor recebe o MAC-I, ele utiliza a mesma chave Ik para calcular o XMAC-I (eXpected MAC-I), se ambos coincidirem haverá integridade durante a transmissão e recepção.

Vulnerabilidades e Possíveis Ataques

Para Garantir a migração suave entre os sistemas baseados no GSM e rede UMTS os elementos já existentes foram aproveitados na evolução da tecnologia, portanto alguns ataques já conhecidos em redes GSM podem ser implementados em redes UMTS, segue abaixo alguns exemplos:

Acesso sinalização rede GSM

Nas redes GSM, não ocorre o ciframento no núcleo de sua estrutura, portanto caso um atacante consiga acesso a alguns elementos ele irá obter as informações transmitidas, como por exemplo o RAND, SRES e a chave Kc além do que interceptar a própria chamada, outro fato possível seria uma ação contra o HLR, podendo recuperar as chaves Ki de todos os assinantes,



Artigo: Segurança em redes 3G - UMTS

obviamente que o nível de proteção ao HLR é relativamente alto, mas caso exista esta oportunidade os benefícios para o invasão será muito grande.

Interceptação de chave através de falsa base

Como observamos anteriormente o terminal pode ser solicitado para responder a desafio elaborado pela rede GSM, portanto caso o atacante utilize uma falsa base sobrepondo o sinal da legítima ele poderá inundar o terminal de solicitações e reconstruir a chave através de suas respostas. Este tipo de ataque não poderá ocorrer nas redes UMTS, pois possui modo de proteção contra falsa base, mas devido a operação em conjunto ainda representa uma vulnerabilidade.

Interceptação através do AuC

Este tipo de ataque pode ser executado buscando o Ki através da AuC, que responde a pedidos executados pela rede GSM e retorna triplas válidas para autenticação no terminal móvel, sendo que uma das principais vantagens para o espião é a velocidade de resposta do AuC em relação ao USIM Card, devido a este fato, implementar níveis severos de segurança no AuC é decisivo para sucesso neste tipo de ataque.

Ataques Através da Rede IP

Com a inserção de redes UMTS agregadas em novos serviços convergentes através da arquitetura IMS, o acesso a rede IP para fornecimento de acesso e transporte providencia uma infinidade de problemas já relacionados ao "Mundo IP" para as redes celulares, uma das possibilidades está relacionado a ataques de negação de serviço (DOS), agindo diretamente na disponibilidade dos serviços, a seguir algumas possibilidades de ataques.

- Lançamento maciço de pacotes UDP a uma PLMN: Isto pode ser feito conhecendo alguns endereços IP da PLMN e enviando grande quantidade de pacotes UDP até que o tráfego alcance seu limite de capacidade na interface lu ou lub e então a rede UMTS será inundada.
- Utilização de ataques SYN-flood, bem conhecidos, para o envio maciço de pacotes de requisição por conexão TCP (pacotes TCP com SYN = 1 e ACK = 0) para muitas estações móveis.
- Utilização de ataques smurf ou de broadcast, bem conhecidos, ou ataques pathdiscovery para o lançamento de tráfego ICMP maciço à rede UMTS, e, por conseguinte inundar a rede. Estes ataques acontecerão apenas se UMTS suportar serviços de diagnóstico.

Modelo de Segurança

Como pudemos observar, as redes UMTS implementam uma arquitetura de segurança robusta com relação as redes GSM, a melhoria no modelo de identificação e autenticação aliado ao sistema criptográfico forte prove mecanismos seguros para o fornecimento de novos serviços, porém com a agregação dos serviços IP um plano de ação pró ativo deve garantir que atividades indesejadas interfiram no funcionamento do sistema, com isso um plano de operação é apresentado na figura 3.

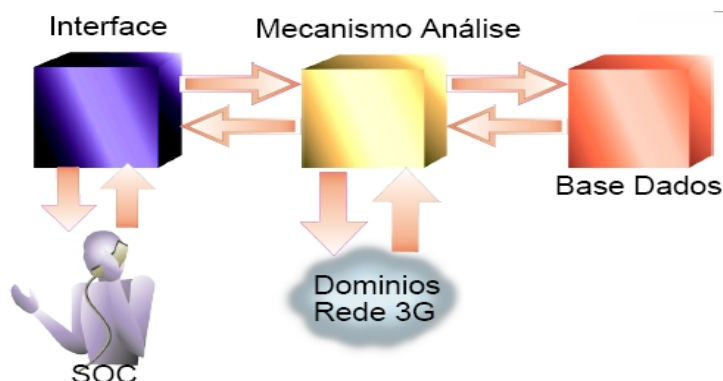


Figura 4

Este modelo apresenta um conjunto de elementos funcionais que devem ser analisados na arquitetura das redes UMTS, segue a descrição dos blocos:

- Interface
 - Elemento que executará a interface entre o SOC (Security Operation Center) e as atividades registradas na base de dados
- Base de dados
 - Deverá conter um registro de atividades suspeitas em ambos os domínios da rede UMTS, armazenando as informações para tratamento imediato ou posterior.
- Mecanismo de análise
 - Elemento que executará a checagem nos domínios e efetuará uma comparação com atividades registradas na base de dados
- SOC (Security Operation Center)
 - Grupo responsável por analisar os incidentes ou atividades e agir de forma pró ativa, garantindo a operação correta do sistema.

Conclusão

O sistema UMTS implementa melhorias significativas com relação aos sistemas GSM, mas abre oportunidades para vulnerabilidades e ataques provenientes do mundo IP. A integração com arquitetura IMS fornece convergência e meios para oferta de internet services, porém é preciso atuar de forma pro-ativa nos incidentes de segurança focados nos domínios da rede 3G.



Artigo: Segurança em redes 3G - UMTS

CPqD

O CpqD atua em soluções de segurança em redes UMTS ofertando a seus clientes:

- Análise de vulnerabilidades nos domínios da rede UMTS
- Plano de continuidade de negócios
- Auditoria na arquitetura de redes UMTS

A instituição estuda a implementação de um modelo de tratamento de incidentes e análise de vulnerabilidades pró ativa, monitorada por um centro de operações de segurança que fornecerá de forma integral as respostas para todas atividades irregulares nas operações de redes de voz, dados e multimídia, baseadas na arquitetura UMTS.