As Tecnologias TDMA e GSM Relacionadas com o Roubo de Celulares

Esta **Série Especial de Tutoriais** apresenta os trabalhos premiados no III Concurso Teleco de Trabalhos de Conclusão de Curso (TCC) 2007.

O conteúdo deste tutorial foi obtido do artigo classificado em segundo lugar no concurso, de autoria de Rômulo Tavares da Silva.

O objetivo do tutorial é demonstrar a relação das tecnologias GSM e TDMA com o roubo de celulares, prática esta muito comum em nossos dias.

Para dar ênfase a este tema foram demonstrados alguns conceitos dessas tecnologias, a forma como o roubo ocorre em cada uma delas e o que tem contribuído atualmente para que esses índices aumentem.

Além disso, são apontadas as causas e as conseqüências do roubo de celulares, e as prováveis soluções para que este ato seja reduzido de forma significativa.

Rômulo Tavarez da Silva

É Tecnólogo em Redes de Telecomunicações pelo Centro Federal de Educação Tecnológica do Piauí (CEFET, PI). Está cursando Bacharelado em Direito pela Universidade Estadual do Piauí (UESPI).

Atuou como Recenseador no Instituto Brasileiro de Geografia e Estatística – IBGE.

E-mail: egeu22t@yahoo.com.br

Duração estimada: 15 minutos

Publicado em: 24/12/2007

Em vista do aumento de roubos de aparelhos celulares e das várias conseqüências ruins destes atos, tentamos da melhor forma possível e objetiva contribuir com a explanação desse tema, usando o conhecimento obtido ao longo do curso de Redes de Comunicação, em especial nas matérias sobre telefonia celular. E com isso ampliarmos nossos conhecimentos em relação a esse problema que afeta a todas as camadas sociais independentemente de qualquer poder aquisitivo.

Como este tutorial envolve a relação das tecnologias TDMA e GSM com roubo de celular, primeiramente são abordadas essas tecnologias de forma suscita para então formar uma base para o tema central deste tutorial. As tecnologias TDMA e GSM são encontradas em muitas fontes de pesquisas com explicações objetivas e fáceis de entender, sendo possível a sua explanação nesse artigo.

Já o tema “roubo de celulares” é pouco abordado por autores, estudantes e profissionais da área de telecomunicações em geral. Porém, com a junção de alguns artigos, reportagens, opiniões e livros que levemente tangenciam o tema em debate foi possível destacar partes desses conhecimentos e, com pesquisas no campo, foi possível tecer vários comentários a fim de explicar algumas possíveis causas para o aumento do “mercado negro” de celular e também tentar criar possíveis soluções com intuído de enfraquecer este mercado, que nos últimos anos tem crescido de forma bastante expressiva.

São explicações objetivas baseadas na realidade de muitas observações, leituras, entrevistas com profissionais da área e que de modo direto podem ser adicionadas às alternativas já existentes que tentam evitar o roubo de aparelhos celulares.

Hoje quando se fala em desenvolver soluções para o aumento de segurança contra roubo de algum bem, pensa-se também nos possíveis caminhos alternativos que o contraventor poderá desenvolver para burlar os dispositivos ou normas de segurança existentes para com isso se desenvolver dispositivos que possam apresentar maiores dificuldades para a ação desses contraventores.

Em vista desses caminhos alternativos, fica muito arriscado em se falar que existe solução única e 100% aprovada contra roubo já que não existem soluções definitivas para essa prática, pois se encontrarmos uma solução **x** hoje contra roubo, cedo ou mais tarde o contraventor poderá desenvolver uma ação **y** que iniba a solução **x**, e assim conseguir extraviar o bem protegido por **x**.

Com vista nessa realidade, um caminho sensato a seguir é observar o que existe hoje contra roubo de celulares e desses dispositivos selecionar qual realmente funciona e para qual ou quais os ladrões conseguem criar alternativas para obterem suas pretensões. Esses dispositivos que realmente funcionam devem ser aperfeiçoados com base nos defeitos que os outros apresentam e assim deve-se tentar criar novos sistemas que dificultem em muito a ação dos ladrões.

É com essa linha de pensamento (criar novos sistemas) que se pretende neste trabalho escrever sobre o roubo de celular e sua relação com as tecnologias GSM e TDMA, mostrando as possíveis causas que, de alguma forma, vêm contribuindo para que os índices de extravio desse bem aumentem e também demonstrar as possíveis soluções para que esses índices tenham considerável redução.

Pretende-se também relatar o que existe na atualidade concernente ao assunto, e de forma crítica descrever o que é ou não a favorável ao combate desta prática tão comum em nossos dias.

A Tecnologia TDMA

Time Division Multiple Access, ou melhor, Divisão de Tempo com Acesso Múltiplo, é uma das tecnologias digitais mais usadas pelo mercado norte-americano, que transforma sinais analógicos de voz em dados digitais e aumenta em três vezes a capacidade de atendimento a usuários em relação ao da tecnologia analógica (na tecnologia GSM o aumento é de 6 vezes).

A tecnologia TDMA é usada em comunicação de telefones celulares digitais para dividir cada canal celular em três slots para aumentar a quantidade de dados transmitidos. O AMPS e o TDMA (IS-136) apresentam, portanto, a mesma arquitetura básica apresentada na figura a seguir:

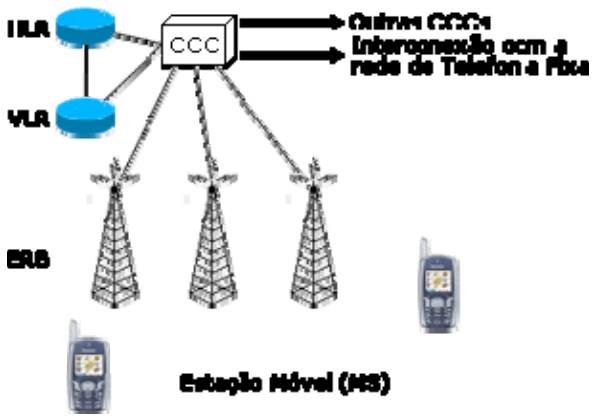

Figura 1: Rede TDMA.

Mobile Station (MS)

Ou Estação Móvel é o terminal utilizado pelo assinante. A estação móvel é identificada por um MIN (*Mobile Identification Number*). O equipamento dispõe ainda de um número de série eletrônico (ESN).
Estação Rádio Base (ERB)

A ERB é o equipamento encarregado da comunicação com as estações móveis em uma determinada área que constitui uma célula. A ERB ocupa o centro de uma célula. Seu objetivo é estabelecer o radio enlace com os celulares operando dentro de sua área de cobertura. Para isso, uma ERB dispõe das seguintes instalações e equipamentos:

- Armário, onde ficam instalados os equipamentos;
- Torre, usada para dar sustentação às antenas;
- Antenas, usadas para estabelecer a comunicação com os celulares.

Central de Comutação e Controle (CCC)

A CCC é a central responsável pelas funções de comutação e sinalização para as estações móveis localizadas em uma área geográfica designada como a área da CCC.

Home Location Register (HLR)

Ou Registro de Assinantes Locais é a base de dados que contém informações sobre os assinantes de um sistema celular.

Visitor Location Register (VLR)

Ou Registro de Assinantes Visitantes é a base de dados que contém informações sobre os assinantes em visita (roaming) a um sistema celular.

A Tecnologia GSM

O GSM tem a estrutura básica dos sistemas celulares e oferece as mesmas funcionalidades básicas dos demais sistemas celulares associadas à mobilidade como roaming e handover (transparência) entre células. O sistema pode operar em três faixas:

- **900 MHz** (890-960 MHz);
- **1800 MHz** (1710-1880 MHz, utilizadas pela OI, TIM, CLARO);
- **1900 MHz** (1850-1990 MHz, utilizada pela VIVO).

É um sistema TDMA/FDMA/FDD, isto é, um sistema que usa simultaneamente o múltiplo acesso (MA) por divisão de freqüência das portadoras (FDMA), o múltiplo acesso por divisão de tempo (TDMA) de cada portadora e usa uma faixa de freqüência para cada sentido de transmissão (FDD = *Frequency Division Duplex*).

O sistema utiliza um espectro de 25 MHz (para largura do canal Tx/Rx, sendo Tx-upload e Rx-dowload) em cada sentido de transmissão, ou seja, a freqüência Tx está 25 MHz em relação a de Rx e vice-versa. Cada portadora subdivide-se em oito intervalos de tempo, que proporcionam um total de 1000 canais em cada sentido de transmissão.

A arquitetura de referência de um sistema GSM é apresentada na figura a seguir:

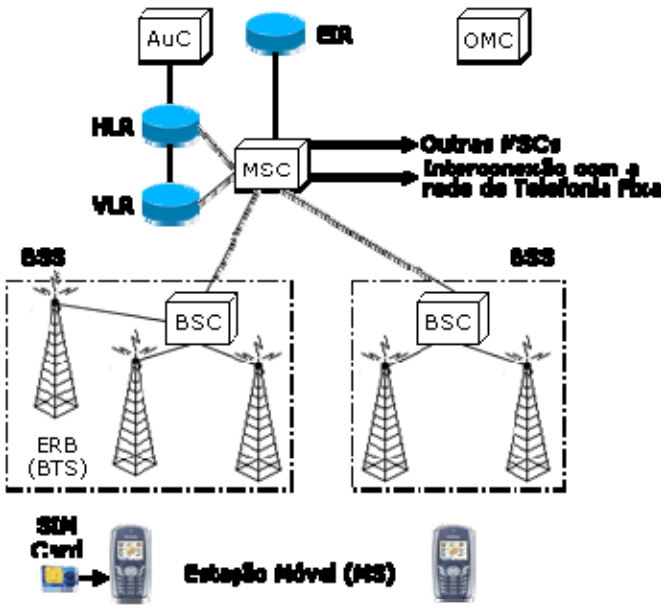

Figura 2: Rede GSM.

Mobile Station (MS)

Ou Estação Móvel é o terminal utilizado pelo assinante quando carregado com um cartão inteligente conhecido como SIM Card ou Módulo de Identidade do Assinante (*Subscriber Identity Module*). **Sem o SIM Card a Estação Móvel não está associada a um usuário e não pode fazer nem receber chamadas**.

Uma vez contratado o serviço junto a uma operadora o usuário passa a dispor de um SIM card que ao ser inserido em qualquer terminal GSM faz com que este passe a assumir a identidade do proprietário do SIM Card.

O SIM card armazena entre outras informações um número de 15 dígitos que identifica unicamente uma dada Estação Móvel denominado IMSI ou Identidade Internacional do Assinante Móvel (*International Mobile Subscriber Identity*).

As Estações Móveis (*Mobile Stations*) são formadas pelo Equipamento Móvel (*Mobile Equipment*) e pelo módulo SIM (*Subscriber Identity Module*). O Equipamento Móvel possui o hardware (transmissor e o receptor) e o software responsáveis pela comunicação com a estação base através da interface aérea.

O módulo SIM é formado por um processador seguro, por uma memória ROM (buffer, Tx/Rx) que abriga o micro sistema operacional do SIM e suas funções criptográficas, por uma memória EEPROM que guarda as informações pertinentes aos usuários (International Mobile Subscriber Identity - IMSI, chaves criptográficas e senhas) e por uma memória RAM, usada como buffer de recepção e transmissão Em síntese, é o módulo SIM que contém todas as informações que identificam os usuários.

Já o terminal é caracterizado por um número também com 15 dígitos, atribuído pelo fabricante, denominado IMEI ou Identidade Internacional do Equipamento Móvel (*International Mobile Station Equipment Identity*).

Base Station System (BSS)

É o sistema encarregado da comunicação com as estações móveis em uma determinada área. É formado por várias *Base Transceiver Station* (BTS) ou ERBs, que constituem uma célula, e um *Base Station Controller* (BSC), que controla estas BTSs.

Mobile-Services Switching Centre (MSC)

Ou Central de Comutação e Controle (CCC) é a central responsável pelas funções de comutação e sinalização para as estações móveis localizadas em uma área geográfica designada como a área do MSC.

A diferença principal entre um MSC e uma central de comutação fixa é que a MSC tem que levar em consideração a mobilidade dos assinantes (locais ou visitantes), inclusive o handover da comunicação quando estes assinantes se movem de uma célula para outra.

O MSC encarregado de rotear chamadas para outros MSCs é chamado de Gateway MSC.

Home Location Register (HLR)

Contêm toda a informação administrativa sobre o assinante do serviço e a localização corrente do terminal. É através do HLR que a rede verifica se um terminal móvel que se está a procurar ligar possui uma assinatura

do serviço válida. Caso a resposta seja afirmativa o MSC envia uma mensagem de volta ao terminal a informar que se está autorizado a utilizar a rede.

O nome da operadora aparece então no visor, informando que se pode efetuar e receber chamadas. Quando o MSC recebe uma chamada destinada a um terminal móvel ele vai ao HLR verificar qual a localização (determinada pelo *polling*). Paralelamente, o terminal de tempos a tempos envia uma mensagem para a rede, para informá-la do local onde se encontra (este processo é chamado de *polling*).

Visitor Location Register (VLR)

Ou Registro de Assinantes Visitantes é a base de dados que contém a informação sobre os assinantes em visita (roaming) a um sistema celular.

Authentication Center (AUC)

Ou Centro de Autenticação é responsável pela autenticação dos assinantes no uso do sistema. O Centro de Autenticação está associado a um HLR e armazena uma chave de identidade para cada assinante móvel registrado naquele HLR possibilitando a autenticação do IMEI do assinante. É também responsável por gerar a chave para criptografar a comunicação entre MS e BTS.

Equipment Identity Register (EIR)

Ou Registro de Identidade do Equipamento é a base de dados que armazena os IMEIs dos terminais móveis de um sistema GSM. Juntamente com o *Authentication Center* (AUC) ambos são utilizados para questões de segurança.

O EIR contém uma lista de IMEIs de terminais que foram declarados como furtados ou que não são compatíveis com a rede GSM. No caso do terminal móvel se encontrar nessa lista "negra", o EIR não permite que ele se ligue à rede.

Dentro do AC encontra-se uma cópia do código de segurança do SIM. Quando decorre a autorização o AC cria um número aleatório que é enviado para o terminal móvel. Os dois equipamentos de seguida utilizam esse número, juntamente com o código do SIM e um algoritmo de encriptação denominado de A3, para criar outro número que é enviado de volta para o AC.

Se o número enviado pelo terminal for igual ao calculado pelo AC, o utilizador é autorizado a usar a rede, caso contrário o mesmo terá restrição na rede. O EIR das operadoras é interligado ao banco de dados do **CEMI** (Centro de Estações Móveis Impedidas) desde novembro de 2005.

Operational and Maintenance Center (OMC)

Ou Centro de Operação e Manutenção é a entidade funcional através da qual a operadora monitora e controla o sistema.

Base Station Controller (BSC)

O BSC gere os recursos de rádio de um ou mais BTS. Entre as suas funções incluem-se o *handoff*, que ocorre quando o utilizador se desloca de uma célula para outra, permitindo que a ligação se mantenha, o estabelecimento dos canais de rádio utilizados e mudanças de freqüências.

Finalmente, estabelece a ligação entre o terminal móvel e o *Mobile service Switching Center* (MSC), o coração do sistema GSM.

TDMA e o Roubo de Celulares

O celular TDMA possui uma identificação incorporada ao próprio aparelho que é denominado ESN. Esta sigla significa *Eletronic Serial Number*, ou seja, Número Serial Eletrônico. É um número atribuído a cada estação móvel no momento de sua fabricação. Geralmente, o fabricante o escreve na parte posterior do aparelho, onde é colocada a bateria. Pode vir escrito na forma decimal (11 dígitos numéricos) ou hexadecimal (8 dígitos alfanuméricos).

Os três primeiros algarismos no número em decimal ou os dois primeiros em hexadecimal indicam o fabricante. Com isso a identificação do celular nessa tecnologia é feita através da combinação entre o número do telefone e o ESN. Como o registro é centralizado, o usuário, cada vez que compra um novo aparelho, necessita comunicar o fato à operadora.

Cada vez em que um celular de tecnologia TDMA é ligado, o celular executa um procedimento conhecido como registro. Durante esse processo, a combinação número do telefone + ESN é checada em um banco de dados da operadora associado a CCC (Central de Comutação e Controle), o qual irá caracterizar o aparelho em alguma cor relacionado com seu devido significado, junto ao banco de dados da operadora, tal como:

- **Verde** = Celular regularizado (autorizado);
- **Cinza** = Celular suspeito de roubo ou fraude (suspeito);
- **Preto** = Celular roubado e não pode ser utilizado (impedido).

Esse banco de dados da operadora por sua vez está também interligado nacionalmente ao CEMI (Cadastro de Estações Móveis Impedidas). Esse cadastro nacional foi lançado em 13 de novembro de 2000 pela ACEL (Associação Nacional dos Prestadores de Serviço Móvel Celular), o qual contabiliza até hoje cerca de 4,5 milhões de celulares roubados ou furtados. Esse sistema tem como objetivo impedir que um aparelho roubado ou furtado seja habilitado fora de sua área de concessão original.

O acesso ao banco de dados é reservado apenas às empresas de telefonia, que também são responsáveis pela inclusão dos códigos de série dos terminais roubados no cadastro. Para nós seria uma espécie de SERASA, SPC, etc.

A sistemática de inclusão de um celular roubado no CEMI funciona da seguinte maneira. Logo que um usuário tem seu aparelho extraviado, o mesmo entra em contato com a operadora de seu celular extraviado e comunica o fato a mesma. Com isso a operadora irá incluir a combinação do número do celular extraviado + o ESN, do mesmo, no CEMI.

Essa combinação durante sete dias ficará caracterizada pela cor cinza, período em que o proprietário deverá apresentar a operadora o BO (Boletim de Ocorrência), para assim depois de apresentado o BO a cor da combinação mude para Preto. Com esta cor o aparelho estará impossibilitado de funcionar em qualquer operadora que compartilhe do CEMI.

Em suma, a pessoa que roubou este aparelho que agora esta caracterizado pela cor preta não poderá fazer nada com o mesmo, a não ser usar como sucata para venda de peças, algo bem menos lucrativo do que vender pronto para funcionar, apesar de roubado, como ocorre na tecnologia GSM, o que veremos logo a seguir.

No GSM, por sua vez, para se identificar em uma rede, o aparelho realiza um complexo conjunto de operações matemáticas com base nas informações gravadas no SIM chip. No SIM chip é armazenado as informações pessoais do usuário, tais como:

1. **International Mobile Subscriber Identity (IMSI)** - número de identificação do assinante;
2. **Subscriber identification key** - chaves de criptografia do usuário; e
3. Agenda telefônica e demais informações pessoais, etc. Através do uso do SIM chip é possível garantir maior facilidade para o usuário, que pode trocar de telefone sem precisar ir à loja ou até mesmo pegar um telefone emprestado e utilizar como se fosse o seu próprio aparelho.

Outro ponto importante do sistema GSM é o *International Mobile Equipment Identity* (IMEI), um número de identificação do aparelho com 15 algarismos, que é programado na fábrica. O IMEI, ao contrário do ESN dos demais sistemas celulares digitais, não tem participação ativa no cadastro do usuário. Um SIM chip (ou usuário) pode utilizar diversos aparelhos ou IMEI diferentes.

Em 12 de fevereiro de 2002 o site *The Register* noticiou o roubo de 26 mil celulares GSM ocorrido em Londres. O prejuízo estimado do roubo foi de seis milhões de dólares. As perdas com o roubo de celulares GSM vêm aumentando sistematicamente nos últimos anos. Amsterdan observou, entre os anos de 2000 e 2001, um aumento de 50% nos roubos de celulares.

No Brasil as autoridades competentes não revelam dados concretos, até mesmo porque muitos usuários que têm seus celulares roubados não registram BO ou em alguns casos nem sequer ligam para sua operadora para comunicar o ocorrido. Mas profissionais da área celular informam que sem dúvida nenhuma a entrada do sistema GSM no Brasil fez subir significativamente a ocorrência de roubo de celulares em nosso país.

A razão para este aumento encontra-se em parte no uso de SIM chips e **IMEI**. Como o **SIM chip** pode ser utilizado por diversos aparelhos, um usuário mal intencionado pode fazer uso de aparelhos roubados mais facilmente.

Ao contrário dos sistemas atuais o GSM permite ao usuário trocar de modelo sem necessitar realizar novamente a habilitação, ou seja, ao se extraviar um celular basta a introdução de um novo chip no mesmo para que volte a funcionar normalmente. Para reduzir os transtornos causados pelo furto de celulares, várias operadoras, em consciência do fato, vêm tentando impedir o uso de celulares roubados em suas redes.

Assim cada vez em que é ligado, o celular executa um procedimento conhecido como registro. Durante este processo, o IMEI do celular é checado em um banco de dados chamado **EIR** - *Equipment ID Register*. Nesta base de dados o aparelho pode ser caracterizado como **verde**, **cinza** ou **preto**. **Verde** representa que o celular encontra-se regularizado, **cinza** que o celular é suspeito de roubo ou fraude e que o celular é roubado e não pode ser utilizado.

O EIR é hoje o principal mecanismo de combate ao roubo de celulares. Já começam a surgir no mundo grandes bases de dados que alimentam os bancos de dados das operadoras com o IMEI de aparelhos roubados; algo como um SPC dos celulares roubados.

Com isso a ACEL, operacionalizado pelo Comitê Gestor de Roaming (CGR) sob a direção do Alcides Maya, resolveu interligar as diversas IER ao CEMI (Cadastro de Estações Móveis Impedidas) que antes só continha dados de celulares TDMA e CDMA, mas que a partir de novembro de 2005 também passou a conter dados de celulares GSM extraviados.

Teoricamente esse sistema funcionaria, não fosse um detalhe quase despercebido: O IMEI de um aparelho pode ser trocado com kits que custam aproximadamente quinze dólares. Ao trocar o IMEI do celular roubado, o ladrão seria capaz de "limpar" o celular. Apesar de alguns países já pensarem em proibir a venda desses kits, a história mostra que dificilmente esta estratégia obterá algum sucesso.

Procurando minimizar o problema, foram criados vários sistemas capazes de traçar perfis do usuário. Através desse tipo de sistema, um usuário que fizesse uso de muitos aparelhos (IMEI) diferentes seria facilmente identificado e poderia ter seu comportamento questionado pelas operadoras ou monitorado pela polícia.

Trata-se de uma solução semelhante aos sistemas de combate à fraude, já utilizados. No entanto, os sistemas podem não funcionar tão bem quanto se imagina. Considerando que o IMEI pode ser alterado basta mudar o IMEI do celular roubado para um IMEI já mapeado como legítimo para o sistema não ser capaz de identificar a fraude, ou seja, a famosa clonagem do IMEI roubado para um legítimo. O fluxograma abaixo representa essa questão mais facilmente.

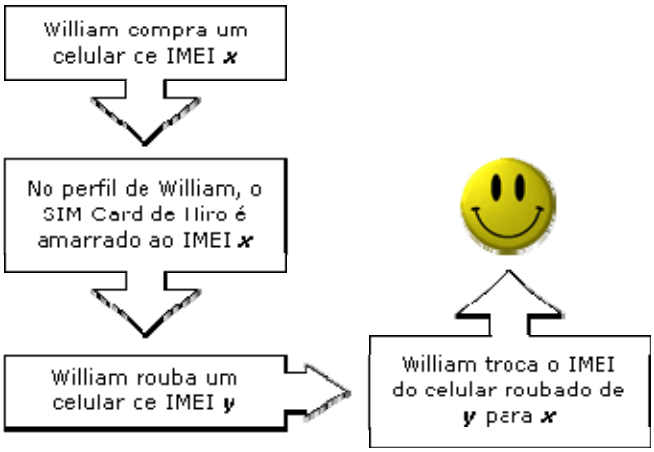

Figura 3: Troca de IMEI em celulares.

Sem dúvida alguma a solução para o problema é complexa. Ainda em 2000 o pesquisador grego Diomidis Spinellis publicou um artigo sobre uma possível proteção. A técnica está baseada em um questionamento periódico feito pela operadora.

O sistema da operadora consultaria o aparelho sobre algumas informações que garantissem que aquele aparelho era o comprado pelo usuário daquele SIM chip. Outra solução poderia estar no uso de circuitos resistentes a modificações (*tamper-proof*) nos aparelhos celulares, o que talvez encarecesse os equipamentos, além de não ser totalmente eficiente.

No que concerne ao kit para troca do IMEI dos aparelhos roubados, as operadoras estão identificando aparelhos com números de IMEI alternados e com características diferentes do original, por exemplo, um aparelho Motorola com um IMEI de um Samsung e vice-versa.

A única certeza é de que o GSM tem suas grandes inovações como envio de fotos, vídeos, acesso a internet e vários outros, porém em questão as facilidades para o roubo do mesmo ser lucrativo ao criminoso é bem notório. Mas ao final deste artigo propus algumas possíveis soluções que tende a dificultar a ocorrência desses roubos.

Possíveis Causas e o Mercado Negro do Celular

Algumas das possíveis causas que influenciam o mercado negro de celulares são apresentadas a seguir.

Facilidades na Compra do Chip

Muitas vezes quando alguém adquire um celular que foi retirado de outrem, vai a alguma loja filiada a uma das operadoras e adquire um novo chip sem nenhuma dificuldade, reabilitando assim o celular irregular.

Isso decorre porque nessas filiais não existe nenhum tipo de fiscalização para se saber em qual celular o novo chip será utilizado, isto é, se será utilizado em celular regular ou em celular roubado. Neste caso, as operadoras, além de exigirem o cadastro, deveriam também amarrar a identidade do aparelho ao SIM card.

A Garantia de Receptadores

Esta causa é um dos principais elementos propulsores do mercado negro do celular. Só existe roubo de celular porque existe alguém que compre este celular para uso próprio ou para revender por preços bem abaixo dos padrões normais.

Infelizmente nessa gama de receptadores existem até lojas conceituadas que adquirem o celular roubado e os revendem como celular novo ou usado (dependendo do estado de conservação do mesmo) mediante nota fiscal adulterada.

Facilidades da Tecnologia GSM

Este aspecto já foi comentado anteriormente no tópico sobre o GSM e o roubo de celular. Como a linha de um celular GSM fica vinculada a um simples chip, basta uma simples troca desse chip para que o celular funcione com outro número.

Com isso os ladrões aproveitam essa facilidade ao roubar um celular e trocar o chip anterior por um novo, para assim repassar o mesmo com uma maior facilidade para a revenda. Já com a tecnologia TDMA é bem diferente, pois o número fica vinculado ao aparelho através do ESN, conforme já comentado.

Em conseqüência disso, ao se roubar um aparelho TDMA e se o mesmo for bloqueado, este só servirá como “sucata” de peças.

Programas Geradores de IMEI

Hoje quando uma operadora é informada por um cliente seu o qual teve seu celular roubado, ela logo procura bloquear o número desse celular contido no chip e o IMEI do mesmo que é incluído no CEMI. Porém com a existência de kits que trocam o IMEI por outro legalizado, a prática do roubo torna-se lucrativa para os maus intencionados.

Esse IMEI na verdade não é inventado aleatoriamente, mas sim copiado de algum outro celular regular que não tem seu IMEI incluso no CEMI para com isso o celular roubado funcionar normalmente.

O que geralmente acaba ocorrendo e assim este celular roubado será vendido com muita facilidade. Atualmente o novo sistema integrado que as operadoras estão adotando, IMEI diferente do original no aparelho, IMEI não cadastrados e IMEI iguais serão restringidos e não funcionarão.

Conseqüências do Roubo de Celular

Algumas das possíveis conseqüências do roubo de celulares são apresentadas a seguir.

Prejuízo Financeiro

Talvez esta seja uma das maiores conseqüências do extravio desse bem, conseqüência esta interligada com as outras que serão citadas abaixo. Como no mercado existem celulares com preços os mais variados possíveis, alguns chegando à cifra 2.000 reais, ninguém estará disposto a perder este valor empregado e não ser ressarcido. Infelizmente é o que acaba ocorrendo na maioria dos casos em que o proprietário tem seu bem extraviado.

Com isso na maioria dos casos quando o proprietário de um requintado celular tem o mesmo retirado de sua posse, recorrerá a um celular mais simples para não correr o risco de ter outro prejuízo semelhante. Enfim, esta é a conseqüência base do roubo e/ou furto do celular.

Perda de Dados do Celular

Aqui entenda-se dados como as diversas informações contidas no aparelho. Com a subtração dessas informações muitos transtornos são gerados, como por exemplo, a perda da agenda telefônica, fotos, imagens e outros. Para algumas pessoas esta perda de dados pode não significar tanto, mas para alguém que trabalhe com vendas ou outro ramo que necessite de manter muitos contatos diariamente, será uma perda e um transtorno muito grande.

Afinal para recompor parte desses dados, levará algum tempo e em conseqüência certo prejuízo financeiro com as perdas de contato. Mas atualmente as operadoras estão disponibilizando através de seus menus no software do aparelho uma aplicação que possibilita transferir os dados de sua agenda ao sistema das operadoras o qual armazenará os dados a qualquer tempo. Porém este serviço é tarifado e não se aplica a fotos, vídeos, etc.

Trauma Psicológico do Proprietário

Há pouco tempo quando algum ladrão assaltava um cidadão, exigia no ato do assalto a bolsa contendo seus pertences pessoais. Hoje o que se percebe ao conversar com vítimas de assaltos ou em informações recolhidas em delegacias, é que na maioria dos casos os ladrões pedem só o celular no ato do assalto.

Nesses casos eles não pedem ou nem perguntam se a vítima tem dinheiro, querendo apenas o celular, deixando transparecer que é bem mais “lucrativo” roubar um celular que uma bolsa. Pois com o celular em mãos, o ladrão já sabe que garantia de dinheiro, o que não é garantido ao se roubar uma bolsa.

Estes roubos quase sempre vêm acompanhados de grave ameaça, ou seja, o ladrão com manuseio de arma branca (facas ou outro instrumento cortante e pontiagudo) ou arma de fogo (revolveres, ou semelhante de fabricação caseira) ameaça grosseiramente atentar contra a vida da pessoa assaltada.

É aqui onde a vítima fica traumatizada com o excesso de truculência de muitos assaltantes, que além da humilhação verbal partem para agressão física sem nenhuma necessidade. Causas estas que acabam levando a vítima a fica com algum trauma psicológico e que em alguns casos podem levar meses para a vítima se recuperar.

Uso em Prisões para Auxilio na Prática de Crimes

Após ser roubado, quando o celular não vai para a revenda no mercado negro com preços bem abaixo do mercado formal, o mesmo tem como destino garantido as penitenciárias.

Apesar de algumas penitenciárias já possuírem bloqueadores, o celular é ainda hoje o principal instrumento para o planejamento de crime a partir das prisões. É com ele que as organizações criminosas coordenam as atividades delituosas praticadas extra-muro.

A resultante dessa conseqüência está bastante presente na mídia de nossa atualidade. Em que muitos policiais civis, militares e até bombeiros são assassinados a mando de grupos que organizam muitos atentados dentro de uma penitenciária por meio de um simples celular.

Então de alguma forma podemos concluir que o roubo de celular contribui de alguma forma expressiva para a morte de muitos inocentes. E isso deve ser levado com muita importância para se desenvolver possíveis soluções que possam inibir o extravio desse bem.

Apesar da gravidade do problema, algumas soluções podem ser listadas como forma de tentar evitar o roubo de celulares.

Maior Fiscalização das Revendedoras de Celular na Venda de Chips

Hoje para se adquirir um chip em alguma operadora não é tarefa das mais difíceis, pois algumas vezes o vendedor não irá perguntar para qual celular o chip será direcionado e muito menos se pede a nota fiscal deste celular. Isso facilita muito para um meliante com um aparelho irregular habilitar o mesmo, dando impulso ao mercado negro de celular.

Em vista disso, intensificando a fiscalização ao se exigir a nota fiscal do celular em que se direcionará o chip a ser comprado, estará se formando mais uma barreira contra o roubo do celular, pois vários dados do proprietário como nome, CPF, endereço, IMEI do aparelho e outros dados serão checados, presumindo-se assim a procedência legal do celular apresentado.

Selo de Segurança na Nota Fiscal

Como em alguns lugares para se comprar um chipe, exige-se a nota fiscal como referência da procedência legal do celular, muitos ladrões utilizam de sua sapiência para forjar notas fiscais verdadeiras, a qual na verdade só contém dados falsos.

Como muitas das notas fiscais fornecidas pelo vendedor de celular ao cliente não tem nenhum selo de segurança e ainda algumas são preenchidas sem o uso do computador, fica muito fácil para o meliante falsificar uma nota fiscal de um celular roubado.

Em posse dessa nota fiscal falsa, o meliante terá uma maior facilidade de vender o celular roubado como um celular regular.

Maior Eficiência no Envio de Dados ao CEMI

Após uma pessoa ter seu celular extraviado, o procedimento a ser seguido é em primeiro lugar entrar em contato com a operadora comunicando tal fato e logo em seguida ir a uma delegacia, responsável pela região onde ocorreu o roubo, portando a nota fiscal do celular roubado e sua carteira de identidade com o intuito de formalizar o boletim de ocorrência.

Em posse desse B.O., ir o mais rápido possível a operadora do celular para cancelar o IMEI do celular e o mesmo ser inserido no CEMI. Essa é o procedimento mais eficaz para se evitar ao máximo que a ladrão utilize o aparelho roubado com facilidade.

Porém, em virtude do trauma psicológico ou da exaltação de ânimo da vítima desse roubo, aquelas etapas descritas não são percorridas o que acaba facilitando para o ladrão em habilitar novamente o celular roubado.

Com isso, por mais que a pessoa fique chateada com o roubo, o que não é por menos, a vítima deve logo que puder comunicar o fato à operadora munido do B.O. para que assim o envio dos dados ao CEMI seja mais eficiente.

Ação Periódicas dos Órgãos de Segurança Pública

Essa ação seria em duas vertentes:

- Descobrir quem são os maiores receptadores desses roubos para que assim os mesmos pudessem ser punidos exemplarmente, enfraquecendo consideravelmente assim um dos componentes que mais propulsiona esse mercado negro que só tem crescido ultimamente.
- Fazer vistorias surpresa às mais variadas assistências técnicas de celular com o intuito de verificar a procedência legal dos celulares ali encontrados. Pois quando um celular tem seu IMEI bloqueado é em alguma assistência técnica que o meliante irá tentar desbloqueá-lo. Então fiscalizar estas assistências é de suma importância para o enfraquecimento do mercado negro de celular, além de se exigir das operadoras uma maior exigência dos clientes ao comprar um chip, como nota fiscal do celular.

Uso Mais Discreto do Celular

Essa possível solução para se evitar o roubo de celular está diretamente relacionada com o comportamento do usuário do celular em público. Tais dicas não vão evitar 100% que o celular seja roubado, mas com certeza irão contribuir em muito para que o aparelho não seja roubado.

Algumas dicas são:

- Evitar exibir o aparelho e deixa-lo amostra;
- Mantenha-o dentro do bolso da camisa, do paletó ou bermuda;
- Evite deixa-lo sobre a mesa de restaurante, bares, lanchonete ou outros lugares;
- Guarde-o na bolsa;
- Preste muita atenção à sua volta quando for atendê-lo;
- Evite ao máximo manter conversações no celular em lugares abertos como ruas, praças e outros.

O tema aqui trabalhado sobre as tecnologias GSM e TDMA relacionadas com o roubo de celular foi aqui debatido com o objetivo de demonstrar quais motivos tem contribuído para que esse ato só aumente ultimamente, assim como as causas, as consequências e as possíveis soluções relacionados ao tema.

O objetivo foi contribuir de forma significativa para o esclarecimento desse tema buscando relacionar as peculariedades que o roubo de celular tem suas características peculiares para cada tecnologia e que no GSM o roubo tem sido mais facilmente contornado pelos ladrões devido a facilidade que esta tecnologia apresenta para tal ato.

Espera-se que com a leitura deste tutorial, o leitor possa voltar sua atenção para este tema tão relevante no nosso meio e que por muitos passa desapercebido até o momento de ser vítima da abertura que estas tecnologias oferecem às pessoas mal intencionadas.

Porém, apesar dessas facilidades que tais tecnologias oferecem, entende-se que se as possíveis soluções citadas forem postas em práticas, irão contribuir em muito para que o roubo de celular diminua em nosso meio de forma bastante relevante.

Referências

ALENCAR, Marcelo Sampaio de. Telefonia Celular Digital. 1. Ed. São Paulo: Érica, 2004.

FERRARI, Antônio Martins. Telecomunicações: Evolução & Revolução. 9. Ed. revisada e atualizada. São Paulo: Érica, 2005.

NASCIMENTO, Juarez do. Telecomunicações. 2. Ed. São Paulo: Pearson Education do Brasil, 2000.

TUDE, Eduardo. Tutoria sobre TDMA e AMPS. Rio de Janeiro, teleco, 2003.

Sites pesquisados:

- www.teleco.com.br/tutoriais
- www.agora-online.com.br
- www.correioweb.com.br
- www.portaladsl.com.br
- www.wirelessbrasil.com.br
- www.clipping.planejamento.gov.br

1. Quais são os componentes que fazem parte da arquitetura básica das redes AMPS/TDMA?

- Mobile Station (MS), Estação Rádio Base (ERB), Central de Comutação e Controle (CCC), Home Location Register (HLR) e Roaming Location Register (RLR).
- Mobile Station (MS), Estação Rádio Base (ERB), Softswitch (SSW), Home Location Register (HLR) e Visitor Location Register (VLR).
- Mobile Station (MS), Estação Rádio Base (ERB), Central de Comutação e Controle (CCC), Home Location Register (HLR) e Visitor Location Register (VLR).
- Headend (HE), Estação Rádio Base (ERB), Central de Comutação e Controle (CCC), Home Location Register (HLR) e Visitor Location Register (VLR).

2. Quais são os componentes que fazem parte da arquitetura básica das redes GSM?

- Mobile Station (MS), Base Station System (BSS), Mobile-Services Switching Centre (MSC), Home Location Register (HLR), Visitor Location Register (RLR), Authentication Center (AUC), Equipment Identity Register (EIR), Operational and Maintenance Center (OMC) e Base Station Controller (BSC).
- Mobile Station (MS), Base Station System (BSS), Mobile-Services Switching Centre (MSC), Home Location Register (HLR), Visitor Location Register (RLR), Authentication Center (AUC), Equipment Routing Register (ERR), Operational and Maintenance Center (OMC) e Base Station Controller (BSC).
- Mobile Station (MS), Base Station System (BSS), Mobile-Services Switching Centre (MSC), Home Location Register (HLR), Visitor Location Register (RLR), Authentication Center (AUC), Equipment Identity Register (EIR), Operational and Maintenance Center (OMC) e Main Station Controller (MaSC).
- Mobile Station (MS), Base Station System (BSS), Mobile-Services Switching Centre (MSC), Home Location Register (HLR), Roaming Location Register (RLR), Authentication Center (AUC), Equipment Identity Register (EIR), Operational and Maintenance Center (OMC) e Base Station Controller (BSC).

3. Quais das alternativas abaixo representam possíveis causas de roubo de celular?

- Facilidades na Compra do Chip.
- A Garantia de Receptadores.
- Facilidades da Tecnologia GSM.
- Programas Geradores de IMEI.
- Todas as alternativas anteriores.