

Roubos de celulares, o que muda com a chegada do GSM.

Por **André Fucs de Miranda, CISSP**, <afucs@cfsec.com.br>

IRRESTRITO / PÚBLICA / ORDINÁRIA

Grupo de Restrição: Irrestrito	Emissão: 29.07.2002
Arquivo: YSP_0003	Versão: 29.07.2002

Declaração de exoneração de responsabilidade

Este documento foi publicado pela CFSEC Security Architects com o intuito de fornecer, de forma rápida, informações precisas e atualizadas. A CFSEC Security Architects tentará corrigir qualquer erro que possa estar presente neste documento, tão logo seja avisada.

Entretanto, a CFSEC Security Architects não pode garantir que as informações apresentadas no mesmo estejam corretas.

A CFSEC Security Architects alerta ainda para os seguintes aspectos:

- O material difundido comporta exclusivamente informações de caráter geral, que não pretendem referir a situação específica de um indivíduo ou de uma entidade;
- Este documento pode incluir informações que não devem necessariamente estar completas, ser exaustivas e exatas ou estarem atualizadas;
- Este documento remete para sites externos, sobre os quais a CFSEC Security Architects não tem qualquer controle e relativamente aos quais declina todas as responsabilidades;
- As informações disponíveis neste documento não são pareceres de caráter profissional ou jurídico.

Todas as informações são providas pela CFSEC somente em uma base "no estado". Em nenhum evento a CFSEC será responsável pelos possíveis danos diretos, indiretos, especiais ou de qualquer outro tipo, derivados do uso deste web site, ou de qualquer outro web site que esteja ligado a este, incluindo, sem limitação, qualquer perda de lucros, interrupção de negócios, perda de programas ou outros dados de informação relacionados ao seu sistema, incluindo o caso de que nos seja expressamente informado a possibilidade de tais danos.

CFSEC Security Architects é marca registrada da CFSEC Sistemas Ltda. As demais marcas registradas são respeitadas.

Agradecimentos

Aos amigos Edmo Suassuna, Eduardo Starling, Gustavo Zeidan, Hiro Kozaka, Jotapê França, Marcelo Borges e Vitor Conceição,

Mais um santo salvador

O GSM chegou ao Brasil. Aleluia ou Salve-se quem puder? Nem um nem o outro. Apesar de todo o sucesso prometido pelo novo sistema, a nova face dos roubos de celulares, cada vez mais comum nos países que adotam o GSM, é praticamente desconhecida dos brasileiros.

Através deste documento procuramos apresentar algumas características técnicas com direta influência no número de furtos de aparelhos celulares no exterior. **Esse artigo, entretanto, não afirma que este problema existe, como aqui descrito, nas redes GSM em implantação e/ou operação no território Brasileiro.**

As diferenças entre o sistema atual e o GSM

Nos celulares CDMA e TDMA, a identificação de um aparelho é feita através da simples combinação do número do telefone com o número serial do aparelho (**ESN**). Como o registro é centralizado, o usuário, cada vez que compra um novo aparelho, necessita comunicar o fato à operadora.

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** são armazenadas 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
- 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.

O roubo de aparelhos

Em 12 de fevereiro de 2002 o site The Register noticiou¹ 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. Amsterdam observou, entre os anos de 2000 e 2001, um aumento de 50% nos roubos de celularesⁱⁱ. 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. Para reduzir os transtornos causados pelo furto de celulares, várias operadoras vêm tentando impedir o uso de celulares roubados em suas redes.

Primeira tentativa

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 **preto** 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.

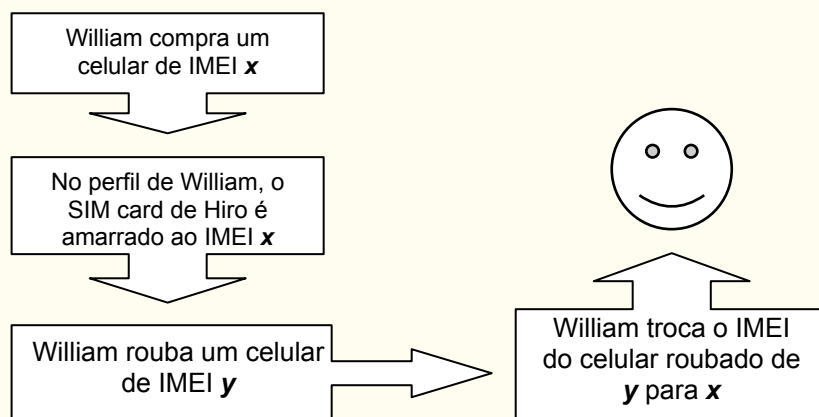
Teoricamente esse sistema funcionaria, não fosse um detalhe quase desapercibido: O **IMEI** de um aparelho pode ser trocado com kits que custam aproximadamente quinze dólares. Ao trocar o **IMEI** do celular roubado, o ladrão seria capaz de **limpar** o celular. Apesar de alguns países já pensarem em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

Lá se vai o barraco

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. O fluxograma abaixo representa essa questão mais facilmente.



Ainda restam esperanças

Sem dúvida alguma a solução para o problema é complexa. Ainda em 2000 o pesquisador grego Diomidis Spinellis publicou um artigoⁱⁱⁱ 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 encareceria os equipamentos, além de não ser totalmente eficiente.

A única certeza é de que o GSM chegou e talvez até seja mais seguro... Mas até quando?

ⁱ The Register, The Great Mobile Phone Robbery, <http://www.theregister.co.uk/content/7/24037.html>

ⁱⁱ Amsterdam bombards muggers, http://www.minjust.nl/b_organ/dpjs/engels/sec_netherlands.htm

ⁱⁱⁱ Diomidis Spinellis. Reflection as a mechanism for software integrity verification. *ACM Transactions on Information and System Security*, 3(1):51-62, February 2000.