Um Ambiente Anti-Clonagem para Telefonia Móvel

Alessandro Brawerman e John A. Copeland

[1]School of Electrical and Computer Engineering
Georgia Institute of Technology
Atlanta - GA, USA

{ale,copeland}@ece.gatech.edu

Abstract. *The mobile telephony is one of the services that evolves the fastest in the world. In Brazil, for instance, the number of mobile devices is already bigger than the number of traditional telephones. Despite several advantages presented by the mobile telephony, there are still a lot to discuss regarding security. One of the more dangerous threats is cloning. Besides illegal billing, cloned units increase the competition of shared resources, the network congestion and degrade network services. In this paper an anti-cloning framework for mobile telephony is proposed. Different from previuos work, in this framework the mobile device together with the Wireless Operator is responsible for detecting if it has been cloned or not. Another key point is that the framework is independent of the wireless communication technology, working well for different cellular technologies, communication over satellite networks and the Internet. New pieces of hardware and new protocols are specified to avoid network services being used by cloned units. Proofs that analyze correctness of the protocols are also presented. Finally, practical experiments that attest the feasibility of the framework are described.*

Resumo. *A telefonia móvel é um dos serviços que mais cresce no mundo. No Brasil, por exemplo, o número de telefones celulares já ultrapassou o número de telefones fixos. Apesar das diversas vantagens que a telefonia móvel apresenta, ainda há muito o que se discutir a respeito de segurança. Uma das maiores ameaças é sem dúvida a clonagem. Além de cobrança ilegal, unidades clonadas aumentam a competição por recursos compartilhados, o tráfego na rede e degradam os serviços oferecidos pelas operadoras. Neste artigo, um ambiente anti-clonagem para telefonia móvel é proposto. Diferente de trabalhos prvios, no ambiente proposto, o dispositivo móvel junto com a operadora telefônica é responsável por detectar se foi clo-nado ou não. Outro ponto chave é que o ambiente é independente de tecnologia, funcionando perfeitamente para qualquer tecnologia celular (TDMA, CDMA, GSM, etc), comunicação via satélite e a Internet. Para evitar que os serviços da rede sejam utilizados por unidades clonadas, o ambiente especifica novos hardwares e novos protocolos. Provas que analizam os protocolos também são apresentadas. Por fim, experimentos práticos que atestam a potencialidade do ambiente são descritos.*

1. Introdução

Uma das ameaças mais perigosas em telefonia móvel é a clonagem de celulares e PDAs. Clonar estes aparelhos é considerado crime federal nos Estados Unidos. De acordo com as operadoras de telefonia móvel e o serviço secreto americano [1], as perdas devido a fraudes no sistema de telecomunicação são estimadas em mais de um bilhão de dólares anuais somente nos Estados Unidos. Uma grande parte dessa perda, mais de 60%, é devido à clonagem de celulares e PDAs.

Além de ilegal, unidades clonadas ampliam a competição por recursos compartilhados, aumentam o congestionamento na rede e degradam os serviços oferecidos pelas operadoras. Em consequência, a dificuldade para estimar um modelo de tráfego de informações e planejar a evolução da rede é muito elevada.

Este artigo apresenta um ambiente anti-clonagem para telefonia móvel que não só identifica e nega serviços para unidades clonadas, mas também garante que nenhuma unidade possa ser clonada quando da utilização de serviços oferecidos pelas operadoras de telefonia móvel. O ambiente é desenvolvido para prover um conjunto de tecnologia de hardware e software que estabelece a base para um ambiente livre de unidades clonadas.

Diferente de qualquer outro, neste novo ambiente proposto, o dispositivo de telefonia móvel é consciente do problema de clonagem. Ele é capaz de, por si só, identificar se é uma unidade válida ou clonada. No caso de identificação de clonagem, o dispositivo executa os procedimentos necessários para bloquear o uso de qualquer serviço.

Como uma medida de segurança extra, mas necessária, as operadoras de telefonia móvel também são responsáveis por detectar unidades clonadas e bloquear o uso de qualquer serviço que estas unidades possam necessitar. Uma outra vantagem desta proposta é que o ambiente é independente de tecnologia, funcionando para qualquer tecnologia celular atual ou futura (TDMA, CDMA, GSM, UTMS, etc), para redes via satélite e para a Internet.

Para obter dispositivos móveis conscientes do problema de clonagem, um pacote de hardware resistente a ataques e novos protocolos são definidos. O pacote de harware resistente a ataques armazena informações vitais, tais como o identificador universal do aparelho e a sua respectiva credencial de identidade. Mecanismos de verificação, que checam a integridade de diversos elementos do aparelho, também são codificados internamente ao pacote de hardware resistente a ataques.

Os protocolos a serem apresentados definem os passos de obtenção, validação e armazenamento da credencial de identidade de um aparelho; obtenção, validação, armazenamento e instalação do arquivo de configuração, o qual configura o número telefônico do aparelho; e, finalmente, procedimentos que tornam o dispositivo consciente do problema de clonagem.

O restante do artigo está organizado da seguinte maneira. Na seção 2 assuntos relevantes a clonagem e tecnologias celulares são apresentados. Na seção 3 o ambiente é especificado com maiores detalhes. A seção 4 apresenta as provas formais e a seção 5 os experimentos práticos. Finalmente, a seção 6 conclui o artigo.

2. Assuntos Relevantes

Esta seção apresenta assuntos relevantes a fim de proporcionar ao leitor uma maior compreensão das diversas tecnologias celulares e suas respectivas falhas de segurança.

2.1. AMPS

A tecnlogia AMPS - Advanced Mobile Phone System - [2, 3] é o sistema de telefonia móvel analógico, introduzido nos Estados Unidos durante o começo da década de 80.

Apesar do fato de ser um grande avanço em sua época, o AMPS apresentava várias falhas de segurança e múltiplas cópias de dispositivos clonados eram criadas sem grandes dificuldades. A grande falha do AMPS era que o seu identificador universal era transmitido junto com o número do telefone celular sem proteção alguma.

2.2. GSM

A tecnologia GSM - Global System for Mobile communication - [2, 3, 4], é a tecnologia celular digital aceita mundialmente na atualidade. O esquema de autenticação GSM se baseia em códigos criptográficos especiais para autenticar os clientes e cobrá-los de forma apropriada.

Um cartão personalizado, chamado SIM - Subscriber Identity Module, armazena uma chave secreta que é usada para autenticar o cliente. Conhecimento da chave é suficiente para clonar o dispositivo móvel. O cartão SIM é facilmente removível para que o usuário possa usar outros aparelhos. A desvantagem é que alguém que possua acesso físico ao cartão pode copiar a informação por ele armazenada para outro cartão, clonando desta forma a informação de autenticação do usuário.

Copiar o cartão SIM é uma falha relevante, porém uma falha mais grave foi descoberta. Em [5] é comprovado que os códigos criptográficos usados pelo esquema de autenticação não são fortes o suficiente para resistir a ataques. Para explorar esta vulnerabilidade, um indivíduo poderia interagir repetidamente com o cartão SIM para aprender a chave secreta e assim seria hábil de clonar o dispositivo sem precisar copiar todas as informações do cartão SIM.

Apesar do ataque ser demonstrado tendo-se acesso físico ao dispositivo, é mencionado que ataques sobre o ar, utilizando ondas de rádio, também são possíveis, tornando clonagem de dispositivos GSM uma ameaça real e grave.

2.3. UMTS

A tecnologia UMTS - Universal Mobile Telecommunications System - [2, 3, 6] é um padrão a ser utilizado na geração 3G de telefonia móvel. Esta tecnologia provê maior velocidade de transmissão de dados e aprimora a segurança de várias falhas encontradas na tecnologia GSM.

Apesar das vantagens desta nova tecnologia, a UMTS também armazena informações vitais no cartão SIM. Desta forma, pode-se copiar as informações do cartão SIM da mesma maneira que é feito na tecnologia GSM.

Uma outra desvantagem diz respeito ao blocos de criptografia KASUMI. Estes blocos são o coração do mecanismo de integridade e confidencialidade da rede

UMTS. Para implementação destes blocos são necessários cerca de 10000 portas lógicas e operações criptográficas devem atingir taxas da ordem de 2Mbps. Desta forma, um esforço considerável deve ser apresentado para implementar hardwares de alta performance que sejam capazes de executar as operações dos blocos KASUMI.

Esquemas mais simples que somente detectam unidades clonadas, mas não previnem o problema da clonagem foram propostos em [7, 8].

2.4. Trusted Computing Group - TCG

O TCG é composto por um grupo de industrias de telecomunicação e informática com o objetivo comum de aumentar a segurança do ambiente computacional em diversas plataformas. Eles dizem que irão apresentar especificações formais para o desenvolvimento de hardwares de computação confiável em diversas plataformas, incluindo PCs, PDAs - Personal Digital Assistants - e aparelhos celulares.

Até o presente momento, eles apresentaram uma primeira especificação para o ambiente de PCs [9]. Alguns dos benefícios incluem mais segurança para armazenamento local de dados e um menor risco de roubo de identidade.

Apesar do fato desta especificação realmente apontar e resolver alguns problemas de segurança, ela não atingiria a performance necessária se empregada nos dispositivos de telefonia móvel, já que estes dispositivios apresentam baixo poder de processamento, baixa quantidade de memória e usam uma rede de baixas taxas de transmissão de dados.

3. Especificação do Ambiente Anti-Clonagem

O ambiente anti-clonagem é composto por novos pacotes de hardware, novos protocolos e novos módulos e mecanismos de verificação. A Figura 1 apresenta a arquitetura necessária para um celular ou PDA ser capaz de executar o ambiente anti-clonagem. Os módulos e conectores pontilhados representam a contribuição deste trabalho.

Note que o *Device Manager* (Gerenciador do Dispositivo) é responsável pelo gerenciamento de toda comunicação feita com o mundo exterior e por requerer os serviços de cada módulo interno quando necessário. O *Environment Discoverer* (Detector de Ambiente) é responsável por detectar quais tecnologias estão disponíveis no ambiente atual ao qual se encontra o aparelho. Finalmente, o *CFG Manager* (Gerenciador do CFG) é responsável por gerenciar o arquivo de configuração atualmente instalado.

A nomenclatura usada para especificar o ambiente é apresentadana Tabela 1. O tamanho de cada chave empregada no ambiente varia de acordo com a tecnologia usada. A opo de menor chave igual a 128-bits e não há limites no tamanho máximo.

3.1. Entidades e suas Responsabilidades

Existem quatro entidades que participam e possuem diferentes responsabilidades no ambiente anti-clonagem. A lista abaixo apresenta estas entidades, bem como suas responsabilidades.

1. Produtor: produz o aparelho celular ou PDA, gera a EK, informa a agência de credenciamento sobre a EK gerada e calcula e armazena Att(EK) no dispositivo móvel.

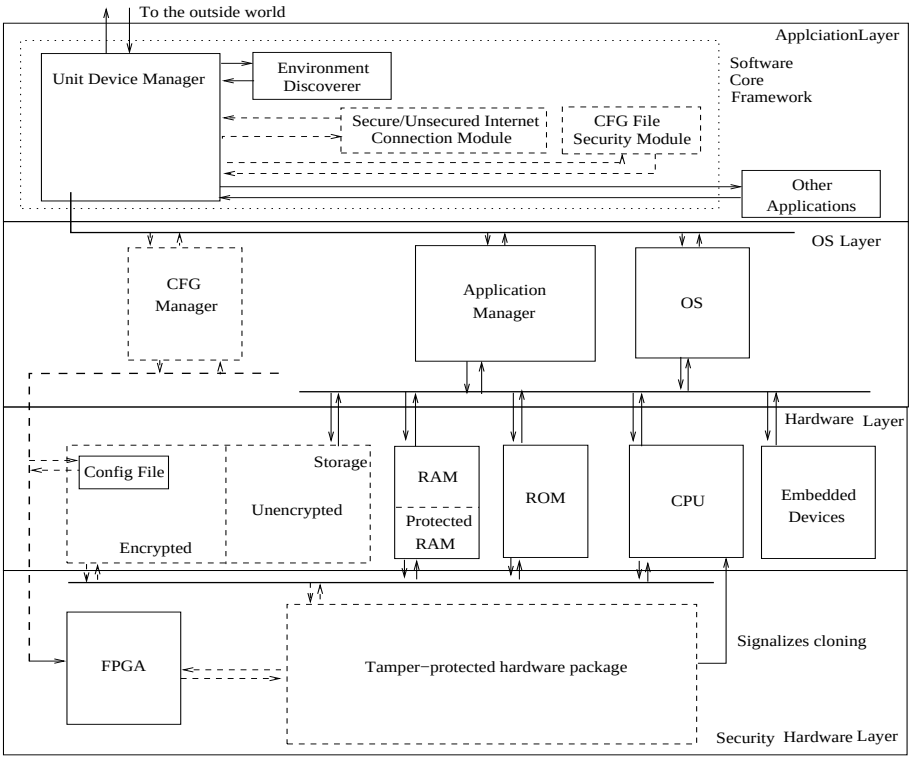

Figura 1. Arquitetura de um dispositivo móvel para o novo ambiente anti-clonagem.

2. Operadora Telefônica - OT: vende o dispositivo móvel, provê serviços, gera o CFG, autentica o aparelho para usar os serviços da rede e detecta unidades clonadas.
3. Agência de Credenciamento - AgC: gera o par de chaves de verificação (par AK) e a credencial de identidade (AC) e disponibiliza estes itens, juntamente com a chave pública da OT, ao aparelho.
4. Dispositivo Móvel: utiliza os serviços da rede, realiza o download do arquivo CFG e detecta se é uma unidade clonada ou válida.

A Figura 2 demonstra o relacionamento entre as diversas entidades do ambiente anti-clonagem. O Produtor envia a EK para a AgC. A AgC gera o par AK e a AC, e envia estas informações e a chave pública da OT para o aparelho. O aparelho obtém o arquivo CFG da OT e está apto a utilizar os serviços da rede telefônica.

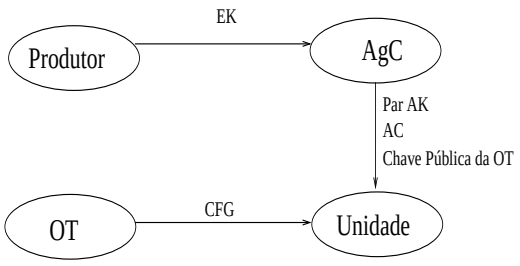

Figura 2. O relacionamento entre as entidades.

Tabela 1. Definições básicas.

C	um número randômico de 48 bits.
$K_Y\{C\}$	C é codificado pela chave Y.
$MD(Z)$	hash de Z.
$[C]_{Alice}$	C é codificado usando a chave privada de Alice.
$\{C\}_{Alice}$	C é decodificado usando a chave pública de Alice.
Verificação	Usada para checar a integridade de um certo componente. Definida como a função Att(X), que resulta no hash do componente X.
Chave de Verificação (AK)	Usada para obter a credencial de identificação do aparelho. Composta pela chave de verificação privada (AK_{priv}) e pela chave de verificação pública (AK_{pub}).
Credencial de Identidade (AC)	Usada para identificar o aparelho celular ou PDA. É assinada pela Agência de Credenciamento e é apresentada toda vez que o aparelho acessa algum serviço da rede. $AC = [hash(AK_{pub})]_{AgC}$.
Chave de Endosso (EK)	Identificador universal do aparelho. Não é revelada em momento algum pelo aparelho.
Arquivo CFG	Usado para configurar o número telefônico do aparelho. É assinado pela operadora telefônica. $CFG = [Phone\#]_{OT}$.
Estado Temporário	Um aparelho que não é capaz de se identificar para a rede. Ainda não possui o AC ou CFG.
Estado Válido	Um aparelho capaz de se identificar para a rede. Já possui o AC e o CFG.

3.2. O Pacote de Hardware Resistente a Ataques - PHRA

O PHRA deve ser fisicamente protegido contra ataques e invasão. Isto inclui conectá-lo fisicamente com as outras partes físicas do aparelho de forma que o PHRA não possa ser facilmente desmontado e transferido para outras unidades. O pacote deve ainda limitar sondas e escaneamentos eletro-magnéticos.

O PHRA é composto por dois chips resistentes a ataques: $TRC1$, somente para leitura, e $TRC2$, no qual pode-se ler e escrever dados. O TRC1 contém a EK, os mecanismos de verificação responsáveis por medir, informar e comparar valores de integridade de elementos, e um hardware especializado em gerar números randômicos. O TRC2 contém o mecanismo de verificação responsável por armazenar valores de integridade e memória não volátil para armazenar as chaves necessárias.

Os mecanismos de verificação são divididos em mecanismo de verificação para medição (AM-Eng), mecanismo de verificação para armazenamento (AS-Eng), mecanismo de verificação para informação (AR-Eng) e mecanismo de verificação para comparação (AC-Eng). A Tabela 2 apresenta as funções de cada mecanismo de verificação.

A Figura 3 ilustra o PHRA assim que a confecção do dispositivo móvel é finalizada pelo Produtor. Hardwares similares ao PHRA podem ser encontrados em [10].

Tabela 2. Mecanismos de verificação e suas funções.

AM-Eng	Calcula Att(EK) e Att(CFG). Envia os resultados para o AR-Eng.
AR-Eng	Armazena Att(EK) e Att(CFG) em seus registradores $R0$ e $R1$.
AR-Eng	Lê e informa os valores dos registradores do AR-Eng.
AC-Eng	Compara os valores dos registradores, recebidos do AR-Eng, com os valores calculados pelo AM-Eng.

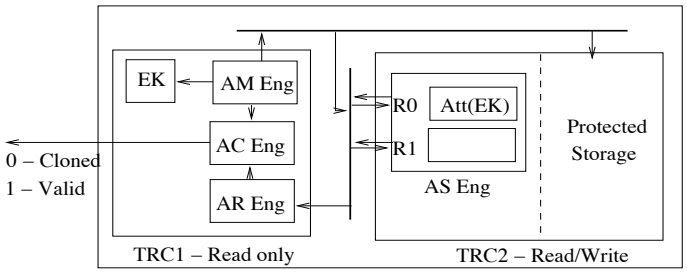

Figura 3. O PHRA ao deixar o produtor.

3.3. Atingindo o Estado Válido

O aparelho celular ou PDA chega as lojas em um estado inválido, ele não possui o AC, e assim, não pode se identificar para a rede telefônica, e também não possui o arquivo CFG, ou seja, não possui um número telefônico.

A Figura 4 apresenta os estados de transição que a unidade deve percorrer até atingir o estado válido e ser capaz de utilizar os serviços da rede telefônica. Note que se for necessário, por qualquer motivo, a troca do número telefônico no futuro, o aparelho voltará ao estado temporário, realizará o download e instalação de um novo arquivo CFG, e retornará ao estado válido.

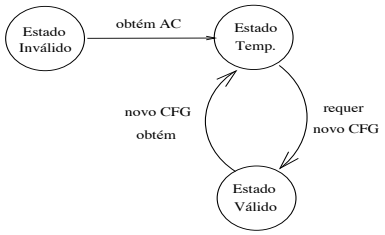

Figura 4. Estados de transição.

3.4. O Protocolo para Obtenção da Credencial de Identidade - PCI

Para obter uma credencial de identificação válida, a unidade precisa executar o protocolo para obtenção da credencial de identidade. O PCI é um processo de comunicação entre o aparelho celular ou PDA e a AgC. Este protocolo é executado apenas uma vez para cada chave de endosso e é totalmente transparente ao usuário final. A Figura 5 apresenta o PCI passo a passo.

Os passos do PCI são definidos como se segue: primeiro, o aparelho contacta a AgC e envia $R0 = Att(EK)$. A AgC procura um valor igual em sua base de dados. Se

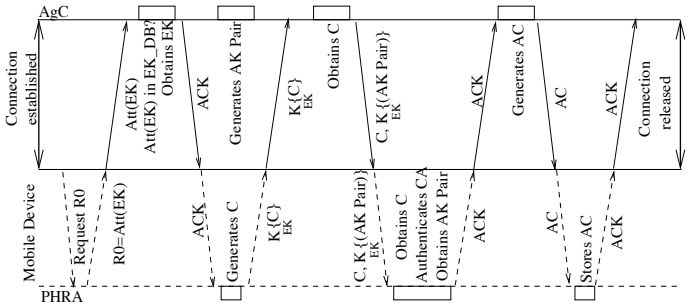

Figura 5. O protocolo para obtenção da credencial de identidade.

encontra este valor, a AgC obtém a EK daquela unidade e informa o aparelho. Se não encontra MD(EK) igual, ou o Produtor não informou a AgC sobre esta EK ainda, ou esta EK é inválida. Em casos em que não há MD(EK) igual na base de dados, a AgC não fornece a credencial de identidade para o aparelho celular ou PDA.

Após obtida a EK do aparelho, a AgC gera o par de chaves de verificação e a unidade autentica a AgC. Após autenticação, a unidade recebe o par de chaves de verificação.

Finalmente, a AgC gera a AC e a envia codificada para a unidade. Esta recebe a AC, decodifica-a e armazena-a no pacote de hardware resistente a ataques. Este passo é seguido pela finalização da conexão.

3.5. O Protocolo de Atualização do CFG - PAC

Com a AC armazenada, o passo final para atingir o estado válido é a execução do PAC para obtenção de um arquivo CFG válido. Este protocolo é executado toda vez que a unidade necessita de um novo numero telefônico. Também é totalmente transparente ao usuário. A Figura 6 apresenta o PAC passo a passo.

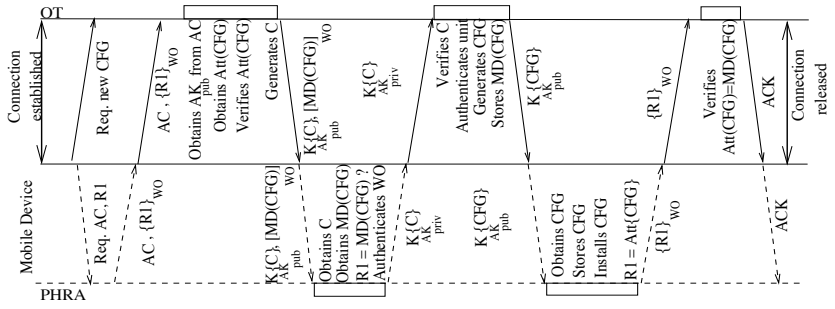

Figura 6. O protocolo de atualização do CFG.

Após conectar com o servidor da operadora telefônica, a unidade envia sua AC e o valor em $R1 = Att(CFG)$ junto com um número randômico codificado C.

Quando a OT recebe AC, verifica se este valor é nulo. Se a comparação é positiva, esta unidade é uma unidade clonada e a OT finaliza a conexão e executa as medidas cabíveis. Caso contrário, o PAC continua normalmente.

A OT identifica a unidade e procura por um valor $MD(CFG)$ em sua base de dados que seja igual ao $Att(CFG)$ recebido. Caso não encontre este valor, esta unidade é

considerada inválida, ou seja, ou ela é uma unidade clonada, ou um ataque está ocorrendo. Em ambos os casos, as medidas cabíveis são executadas pela OT.

Por outro lado, se a OT encontra $MD(CFG) = Att(CFG)$, a unidade é válida e os passos para autenticação mútua são executados.

Após ambas as partes serem corretamente autenticadas, a OT gera um novo CFG, armazena MD(CFG) em sua base de dados e envia o novo arquivo CFG codificado para a unidade. Ao receber o novo CFG, a unidade decodifica-o, instala-o e armazena-o em seu PHRA.

No passo final, o AM-Eng da unidade calcula Att(CFG) e escreve este valor em $R1$. A OT recebe este valor codificado e verifica se é igual ao que havia calculado anteriormente. Em casos positivos, a OT informa a unidade que o protocolo foi executado com sucesso e a conexão é terminada. Em casos negativos, a OT informa que houve um erro na obtenção do CFG e a parte final do protocolo é executada novamente.

Com o AC e o CFG armazenados internamente e instalados corretamente, o dispositivo móvel atinge o estado válido. Portanto, a unidade está pronta para ser usada. A Figura 7 ilustra o PHRA quando o dispositivo móvel atinge o estado válido.

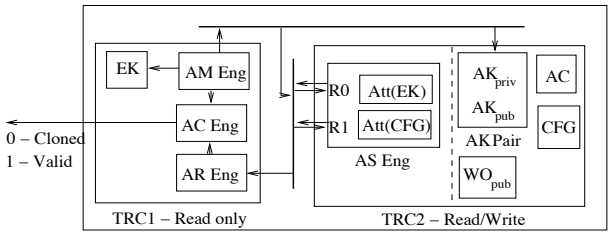

Figura 7. O PHRA no estado válido.

3.6. Procedimentos Anti-Clonagem

Os procedimentos conscientes do problema de clonagem são implementados em ambos os lados, no aparelho celular ou PDA e na OT. Eles são responsáveis por detectar se a unidade é válida ou se é uma unidade clonada.

Após a unidade ter estabelecido uma conexão com a OT e requerido um serviço, os procedimentos anti-clonagem tem início, primeiro no lado do aparelho celular ou PDA e logo após na OT.

No dispositivo móvel, novos valores Att(EK) e Att(CFG) são calculados e enviados para o AC-Eng, o qual também recebe os atuais valores dos registradores $R0$ e $R1$ fornecidos pelo AR-Eng.

O AC-Eng compara os valores recebidos e sinaliza 1 para unidade válida, se $Att(EK) = R0$ e $Att(CFG) = R1$, ou 0 para unidade clonada, se $Att(EK) \neq R0$ ou $Att(CFG) \neq R1$. Desta maneira, a unidade de aparelho celular ou PDA é consciente do problema de clonagem. A Figura 8 demonstra o procedimento. Se o aparelho é uma unidade válida, a AC é enviada para a OT e o procedimento anti-clonagem no lado da OT é iniciado.

No lado da OT, o procedimento funciona basicamente como um módulo de

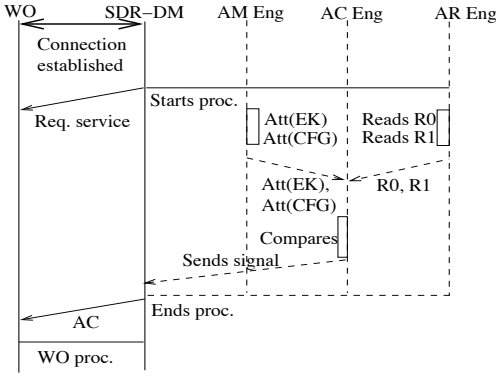

Figura 8. Procedimento anti-clonagem: lado do aparelho celular ou PDA.

autenticação. A OT obtém a AC e verifica se é válida ou nula. Se nula, a OT finaliza conexão e executa os procedimentos cabíveis, pois a unidade foi clonada.

Caso contrário, AC não nula, a OT se prepara para autenticar a unidade. Se a unidade é corretamente autenticada, a OT permite o uso dos serviços requeridos. Por outro lado, se há uma falha na autenticação da unidade, a OT conclui que é um ataque e nega o uso dos serviços. A Figura 9 demonstra o procedimento.

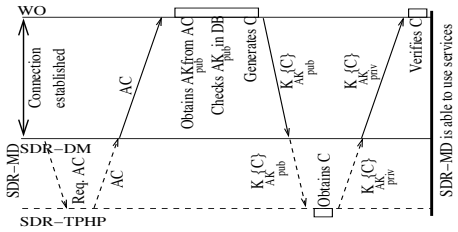

Figura 9. Procedimento anti-clonagem: lado da OT.

4. Analisando o Ambiente Anti-Clonagem

Nesta seção o ambiente anti-clonagem e seus protocolos são analisados, através de lemas e teoremas. O primeiro lema confirma que somente um dispositivo móvel que tenha uma EK válida recebe uma credencial de identidade AC. O segundo lema mostra que um dispositivo móvel recebe um CFG somente quando sua identidade é autenticada com sucesso. Finalmente, o terceiro lema demonstra que somente CFGs válidos, isto é, CFGs que foram gerados e assinados digitalmente pela OT, podem ser instalados no dispositivo móvel.

Esta seção é finalizada com mais 2 teoremas. O primeiro teorema prova que não há possibilidade alguma de clonar um dispositivo móvel pelo ar, usando ondas de rádio. O segundo teorema garante que somente um dispositivo móvel válido pode usar os serviços da rede telefônica.

Lema 1 *A AgC atesta somente a identidade de dispositivos móveis que possuem EKs válidos.*

Como a AgC possui uma base de dados indexadas por EKs válidos, e esta base de dados é armazenada de forma segura, qualquer dispositivo móvel que requesitar uma AC, porém enviar um valor MD(EK) inválido, isto é, hash de EK que não é gerado pelo Produtor, tem seu AC negado.

Um ataque de replay não é possível já que o PCI é executado somente uma vez para cada EK. Personalização do dispositivo móvel, isto é, um ataque de dissimulação (masquerade attack), é notado pelo passo de autenticação. As chances de coliso da funo hash so muito pequenas, j que o hash gerado de 128 bits.

Lema 2 *Dispositivos móveis somente obtém um arquivo CFG quando suas identidades são autenticadas com sucesso.*

De acordo com a definição do PAC, somente após ser autenticado com sucesso pela OT, o dispositivo móvel recebe seu novo CFG. Este passo elimina a possibilidade de ataques de dissimulação e ataques de replay. Somente após responder corretamente ao desafio gerado pela OT, o dispositivo móvel recebe o CFG. Portanto, há nenhum dispositivo é dado um novo CFG a não ser que este prove sua identidade.

Lema 3 *Somente arquivos CFGs válidos são instalados em um dispositivo móvel.*

Para instalar um novo CFG o dispositivo móvel deve executar o PAC. De acordo com a definição do PAC, antes de receber um novo CFG, o dispositivo móvel autentica a OT. Desta forma, ataques de dissimulação e ataques replay são eliminados.

Após o processo de autenticação, o dispositivo móvel recebe o novo $CFG = [Phone\#]_{OT}$*. Como ataques de dissimulação e ataques replay são eliminados, somente a OT poderia ter enviado esta mensagem. Portanto, o CFG é considerado válido e o PHRA armazena e instala o novo CFG.*

Teorema 1 *É garantido que não há possibilidade alguma de clonar um dispositivo móvel pelo ar usando o ambiente anti-clonagem.*

Para clonar um dispositivo móvel pelo ar, o adversário deve obter a EK da vítima ou uma combinação de par AK, AC e CFG válidos.

Como a EK e a $AK_{privada}$ *nunca deixam o dispositivo, não há possibilidade alguma do adversário conseguir a EK e o par AK da vítima pelo ar. Como o CFG é assinado digitalmente pela OT, ele não pode ser duplicado. Além disto, de acordo com o Lema 2, o adversário deve provar sua identidade para obter um CFG válido. Portanto, se o adversário usa um AC que não o pertence, a OT irá notar o ataque e negar um novo CFG.*

A única possibilidade restante para clonar um dispositivo móvel pelo ar, seria capturar a AC do aparelho quando transmitida. Entretanto, o procedimento anti-clonagem executado pela OT irá detectar que a AC capturada não pertence a unidade em questão e irá negar a utilização de qualquer serviços.

Teorema 2 *É garantido que se unidades clonadas existirem, elas não são capazes de usar os serviços oferecidos pela OT.*

De acordo com o procedimento anti-clonagem da OT, para usar os serviços da rede, o dispositivo móvel deve apresentar sua AC válida. Pelo Lema 1, somente dispositivos com EKs válidas conseguem obter uma AC válida. Portanto, uma unidade com uma EK inválida não possui uma AC válida e não pode usar os serviços oferecidos pela OT.

De acordo com o Teorema 1, não há maneira alguma para se clonar um dispositivo móvel pelo ar, além do mais, ataques de dissimulação e ataques replay são notados pelo procedimento anti-clonagem da OT. Portanto, a única outra maneira para clonar um dispositivo é tendo acesso ao seu PHRA.

Entretanto, se o adversário desconectar com sucesso o PHRA do aparelho, sem causar nenhum dano ao PHRA, e for capaz de copiar as informações do PHRA para outra unidade, o Lema 3 e o procedimento anti-clonagem do aparelho garantem que o dispositivo que recebeu as informações copiadas irá negar o acesso aos serviços da rede. O valor de R2 da unidade clonada e o valor atual do MD(CFG) da unidade que recebeu a cópia serão diferentes. Portanto, o dispositivo móvel bloqueia o acesso aos serviços da rede.

Como o procedimento anti-clonagem do dispositivo bloqueia o acesso aos serviços da rede e o procedimento anti-clonagem da OT nota ataques de dissimulação, é garantido que somente um dispositivo válido poderá utilizar os serviços da rede.

5. Experimentos Práticos

Esta seção apresenta experimentos práticos que avaliam a performance do ambiente anti-clonagem e uma comparação com o esquema GSM. Os experimentos foram realizados usan-do a linguagem de programação J2ME [11]. A configuração das máquinas utilizadas nos experimentos é ilustrada na Figura 10. As entidades envolvidas são especificadas na lista abaixo:

1. Os servidores da AgC e da OT: Toshiba Pentium 4 com CPU de 3.06 GHz, 1GB RAM, e Linux SO.
2. O dispositivo móvel: Sharp Zaurus PDA CL-760 com CPU de 400 MHz, 64MB SDRAM, Linux SO, e J2ME support.
3. O roteador: Netgear 108Mbps wireless firewall. Modelo WGT624. O roteador tem funo semelhante ao de uma antena usada pelas operadoras de telefonia celular.

No primeiro experimento, o tempo total para que um dispositivo móvel atinja o estado válido é calculado. No segundo experimento, uma comparação entre o PAC e o método atual para que o usuário troque de número telefônico é apresentada. Finalmente, no terceiro experimento, o tempo total para execução dos procedimentos anti-clonagem é calculado e uma comparação com o esquema de autenticação utilizado pela tecnologia GSM é feita.

Em todos experimentos o algoritmo SHA-1 é utilizado para obter os valores de 128 bits hash dos elementos, a chave EK é uma chave AES 128-bits, e as chaves públicas/privadas são chaves RSA 128-bits, em um primeiro momento, e RSA 512-bits,

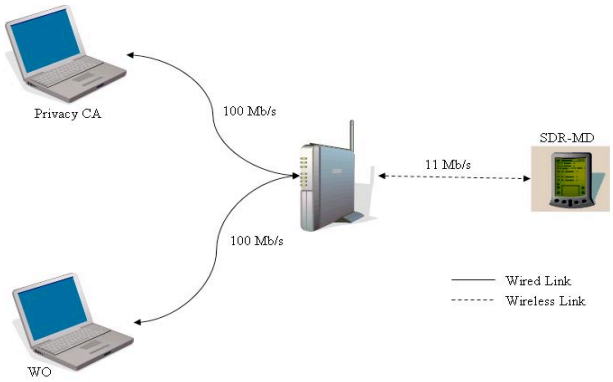

Figura 10. Setup dos experimentos.

em um segundo momento. Esta variação no tamanho das chaves públicas/privadas é interessante para comparação de desempenho do ambiente quando se utilizando chaves menores, mas menos seguras, e chaves maiores, porém mais seguras.

5.1. Experimento 1 - Atingindo o Estado Válido

Neste experimento, é calculado o tempo total para um dispositivo móvel, recentemente comprado, atingir o estado válido. O gráfico da Figura 11 mostra o desempenho do PCI, do PAC e o tempo total para que o dispositivo atinja o estado válido usando chaves RSA de 128-bits e 512-bits. Note que a diferença de performance quando usando chaves de 128-bits e 512-bits é mínima.

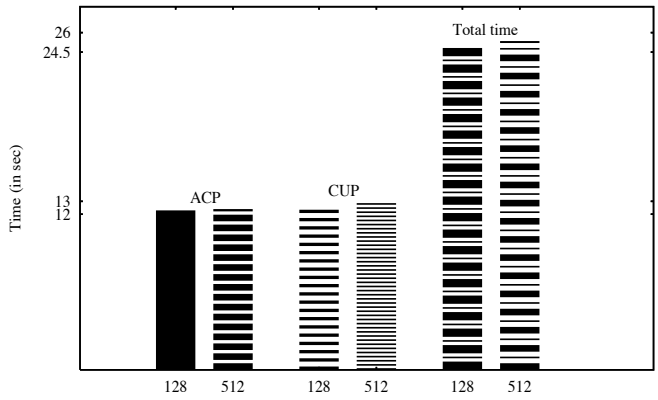

Figura 11. Tempo total para atinjir o estado válido.

Lembre que o PCI é executado apenas uma vez para cada EK e antes do usuário estar apto a usar seu aparelho. Portanto, o desempenho deste protocolo não é tão importante quanto o do PAC.

Como pode ser notado, o tempo para completar o PCI, quando usando chaves públicas/privadas de 128-bits, é aproximadamente 12 segundos. Enquanto que o tempo para executarmos as mesmas operações quando usando chaves de 512-bits, é aproximadamente de 13 segundos. Esta diferença é mínima, e dependendo da performance dos procedimentos anti-clonagem, o uso de chaves de 512-bits é indicado. O mesmo pode ser observado da performance do PAC. Não há novamente uma grande diferença quando se usando chaves de 128-bits ou chaves de 512-bits.

Um fato importante em ambos os protocolos é o tempo para se gerar um número randômico de 48 bits. O dispositivo móvel usado nestes experimentos não possui o hardware específico para gerar números randômicos, portanto o tempo para gerar o número randômico é o passo mais demorado, ao redor de 11 segundos. Este tempo representa cerca de 90% do tempo total do PCI e do PAC quando usando chaves de 128-bits e mais de 80% quando usando chaves de 512-bits.

5.2. Experimento 2 - Tempo Total para Mudança de Número Telefônico

Este experimento apresenta uma comparação entre o tempo total para mudar o número telefônico do dispositivo móvel quando aplicado o PAC e quando aplicado os métodos atuais utilizados pelas operadoras de telefonia móvel.

O primeiro ponto a ser comentado é quanto a transparência do processo ao usuário final. Lembre que o PAC é totalmente transparente, não há necessidade do usuário interagir com o protocolo. O PAC irá realizar o download, instalar e atualizar ambos o registrador no dispositivo e a base de dados da OT. A única função que o usuário possui é a de iniciar o protocolo enviando uma mensagem para a OT.

Por outro lado, o usuário tem uma grande participação nos métodos atuais. Ele deve ligar para a OT, obter um novo número telefônico, reprogramar este novo número no aparelho por si só e esperar por algum tempo para que a base de dados da OT seja atualizada.

Assuma por um minuto que o usuário é realmente familiar com este processo e que o atendente da OT possui alguma experiência. Após ligar para a OT, o usuário é colocado em uma linha de espera. Depois de alguns minutos ele finalmente fala com alguém e explica o que deseja. Então, o novo número é obtido e o usuário deve reprogramar, por si só, este novo número no seu aparelho. Quando o processo parece estar terminando, ainda é necessário uma espera de 30 a 60 minutos para usar o dispositivo. Este é o tempo para a atualização da base de dados da OT.

O segundo ponto a ser discutido é a performance superior do PAC. Os resultados são apresentados na Tabela 3. Note que leva menos de 15 segundos para a atualização do CFG, ou seja, para a atualização do número telefônico, quando o PAC é aplicado e mais de 1 hora quando as operadoras usam os métodos atuais.

Tabela 3. Tempo para atualização do número telefônico.

PAC chaves de 128-bits	12.5 seg
PAC chaves de 512-bits	13 seg
Métodos Atuais	ligação de 15 min + 30 a 60 min atualização da bd da OT

5.3. Experimento 3 - Tempo para Autenticação

Para completar o passo de autenticação, os procedimentos anti-clonagem devem ser executados em ambos os lados, no dispositivo móvel e na OT. Primeiro, o dispositivo executa seu procedimento anti-clonagem para descobrir se é uma unidade válida ou um clone. Então, a OT executa o seu procedimento anti-clonagem para autenticar o dispositivo e evitar que unidades clonadas usem os serviços da rede.

Como os procedimentos anti-clonagem são executados toda vez que o dispositivo móvel tenta usar os serviços da rede, performance neste passo é muito importante.

Lembre que o procedimento anti-clonagem do dispositivo é basicamente uma comparação dos valores atuais de R0 e R1 e os valores calculados pelas funções Att(EK) e Att(CFG). Por outro lado, o procedimento anti-clonagem da OT funciona como um módulo de autenticação e requer operações de criptografia no lado do dispositivo móvel.

O gráfico da Figura 12 ilustra os resultados quando aplicamos chaves públicas/privadas de 128-bits e 512-bits. Note que do tempo total para autenticação, cerca de 60% é gasto no procedimento executado pela OT. Isto deve-se aos fatos de que neste passo já há utilização da rede telefônica e uma certa quantidade de tempo é gasta pelo dispositivo ao executar operações criptográficas.

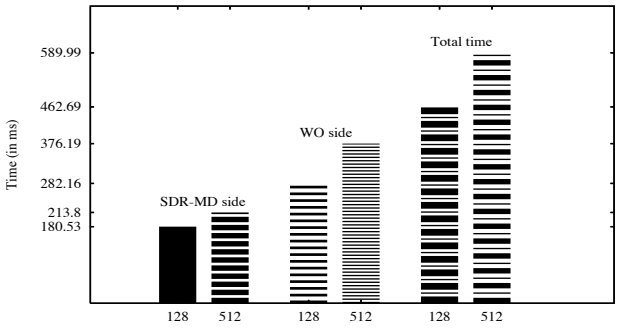

Figura 12. Tempo para autenticação.

Apesar do tempo de performance do esquema de autenticação usado pela tecnologia GSM não ser explicitamente mencionado na literatura, o tempo total para se obter o primeiro pulso de uma ligação GSM é de cerca de 4 segundos em média [3].

Suponha que estes 4 segundos também seriam necessários para se obter serviços da rede quando usando o ambiente anti-clonagem. Então, o tempo para execução dos procedimentos anti-clonagem quando utilizando-se chaves de 512-bits é somente de 15% do tempo total para obter-se os serviços requeridos. Deste forma, os procedimentos anti-clonagem atingem uma performance satisfatória e o uso de chaves públicas/privadas é indicado.

6. Conclusão

Este artigo apresentou um ambiente anti-clonagem para telefonia móvel. O ambiente foi desenvolvido para prover um conjunto de tecnologias de hardware e software que estabelecem a base para um ambiente livre de unidades clonadas.

Diferente de outros trabalhos, no ambiente aqui apresentado, o dispositivo móvel é capaz de descobrir por si só se é uma unidade válida ou clonada. Como uma medida extra de segurança, a operadora telefônica também é responsável por detectar unidades clonadas.

O ambiente é composto por um pacote de hardware resistente a ataques, protocolos que geram a credencial de identidade e o arquivo CFG e procedimentos anti-clonagem em ambos os lados, no dispositivo móvel e na operadora telefônica.

Experimentos práticos mostraram que a diferença em performance quando se usa chaves públicas/privadas de 128-bits e 512-bits é mínima. Portanto, para melhorarmos o esquema de segurança chaves de 512-bits devem ser usadas.

Quando comparando o processo usado para atualização do número telefônico ao utilizar o PAC e os métodos atuais, o PAC mostrou ter performance muito superior, além do fato de ser totalmente transparente ao usuário. Levou, por exemplo, menos de 15 segundos para atualizarmos o número telefônico de um aparelho usando o PAC e cerca de 45 a 60 minutos usando os métodos atuais.

Os experimentos ainda mostraram que o tempo total para a execução dos procedimentos anti-clonagem é satisfatório. Levou apenas 463 milisegundos quando usamos chaves de 128-bits e 590 milisegundos quando usamos chaves de 512-bits.

Quando comparado ao tempo total para obter-se o primeiro pulso de uma ligação GSM, o tempo para execução dos procedimentos anti-clonagem é cerca de somente 15% do tempo total.

Provas para comprovar que o ambiente anti-clonagem é realmente seguro e viável também foram apresentadas.

Referências

[1] U.S. Secret Service Financial Crimes Division. *http://www.secretservice.gov/financial_crimes.shtml*.

[2] RAPPAPORT, T., *Wireless Communcications - Principles and Practice*. Prentice Hall, 2002.

[3] SMITH, C. and GERVELIS, C., *Wireless Network Performance Handbook*. McGraw-Hill, 2003.

[4] GSM, "The GSM security technical whitepaper for 2002." *http://www.hackcanada.com/blackcrawl/cell/gsm/gsm_security.html*.

[5] WAGNER, D., "GSM cloning." *http://www.isaac.cs.berkeley.edu/isaac/gsm.html* Internet Security, Applications, Authentication and Cryptography Group - UC Berkeley.

[6] UMTS Security Features. *http://www.umtsworld.com/technology/security.htm*

[7] FREDERICK, M., "Cellular telephone fraud anti-fraud system," *US Patent 5,448,760*, 1995.

[8] NOTARE, M., "Wireless communications: security management against cloned cellular phones," in *Proc. of the IEEE Wireless Communications and Networking Conference*, Sept. 1999.

[9] THE TCG PC SPECIFICATION. *http://www.trustedcomputinggroup.org/downloads*.

[10] Intel. "Intel Wireless Trusted Platform: Security for Mobile Devices". *http://www.intel.com/design/pca/applicationsprocessors/whitepapers/300868.htm*

[11] Java 2 Micro Edition Technology website. *http://www.wireless.java.sun.com/j2me*