Ambiente para Proteção de Sistemas Operacionais de Dispositivos Móveis

Luiz Francisco Carvalho Jr.[1], Alessandro Brawerman[2]

[1]Centro Universitário Positivo - UnicenP

[2]Centro Universitário Positivo – UnicenP

carvalhojr@gmail.com, brawerman@gmail.com

Resumo. *Com a constante evolução da telefonia celular e o avanço tecnológico, os telefones celulares estão possuindo um aumento cada vez maior quanto ao poder de processamento. Através deste avanço surgiu também a possibilidade de efetuar troca de dados entre telefones ou acessar a Internet com rápida velocidade. Assim sendo, abriram-se oportunidades para novos problemas de segurança. Alguns deles, ainda pouco explorados em dispositivos móveis, mas que podem vir a causar muitos problemas e perdas de dados, são os vírus e códigos maliciosos.*

Os estudos desta monografia visam prevenir a modificação do sistema básico do telefone celular, de modo a impedir que vírus e códigos maliciosos alterem o sistema operacional. Técnicas de hash e backup em hardware seguro são utilizadas para que exista uma cópia autentica do sistema operacional. Este ambiente para proteção do Sistema Operacional é proposto, implementado e executado em experiências práticas.

1 Introdução

Os estudos deste trabalho visam identificar as formas como o sistema operacional do telefone celular pode ser modificado por um vírus ou algum código malicioso. Descobrindo a maneira como agem os vírus, é possível prevenir ou detectar a infecção do sistema operacional o mais rápido possível, para desta forma evitar que o vírus possa alterar as configurações básicas do sistema.

Através da alteração do sistema, um código malicioso pode tentar efetuar uma falsa autenticação, roubar informações da configuração do telefone celular ou impedir o correto funcionamento do aparelho.

Um ambiente de trabalho é proposto, implementado e executado para impedir a alteração do sistema. Este ambiente é composto da verificação da integridade e da recuperação do sistema operacional original em caso de infecção.

Vírus para telefones celulares ainda não conseguem se disseminar com grande relevância e não são ainda capazes de causar grandes danos. Mas com o aumento da complexidade dos telefones, os códigos maliciosos podem se tornar tão nocivos quanto nos computadores.

Alguns vírus atuais são capazes em alguns casos de desabilitar todas as funções do celular, como enviar e receber chamadas; podem enviar mensagens de texto para todos os contatos; travar o sistema; aumentar o consumo de bateria ou desabilitar completamente o celular.

Estes vírus se propagam nos celulares através de anexos em mensagens (serviço de mensagens multimídia), em transferências usando o protocolo *bluetooth (Szor, 2005)* e em *downloads*. As infecções em massa ainda não existem em celulares devido ao grande número de sistemas operacionais adotados por diferentes fabricantes. Desta forma, até agora os vírus estão restritos a marcas e sistemas dificultando assim a multiplicação.

O objetivo deste projeto é garantir que de nenhuma forma o sistema operacional básico possa ser modificado. Sendo assim, o sistema está livre de vírus ou da tentativa de uma engenharia reversa que, por exemplo, possa tentar alterar o processo de autenticação para que o sistema funcione sem ela.

A alteração do sistema básico indica que algum processo está agindo de maneira duvidosa. Portanto, evitar que isto aconteça é uma maneira de garantir a integridade do sistema. Este projeto propõe o uso da identificação do sistema através de uma função *hash*. Um algoritmo *Hash* é uma função matemática que recebe uma entrada de qualquer tamanho e produz uma saída pequena com tamanho fixo, são exemplos de funções *hash* os algoritmos *MD2, MD4, MD5 e SHA.* (Wikipédia)

A cada inicialização do sistema operacional do celular, ou em outras palavras, a cada vez que o celular for ligado, um teste no sistema operacional é realizado para verificar a sua integridade. Em caso de alteração, um backup do sistema é necessário para sobrescrever e voltar o sistema aos seus arquivos originais, os quais eram confiaveis. Este *backup* fica em local seguro, de forma que não possa ser alterado. A criptografia dos dados armazenados também é necessária, evitando que um possível intruso roube informações sobre o funcionamento do sistema.

O telefone celular deve também ser fisicamente seguro contra ataques e invasão, impedindo que o hardware possa ser facilmente desmontado e transferido, devendo evitar sondas e escaneamentos eletros-magnéticos. Evitar este tipo de alteração é essencial para garantir a segurança dos processos fundamentais de execução do sistema, como: autenticar, receber e efetuar chamadas.

Na implementação deste ambiente é utilizada a linguagem J2ME (*Java 2 Micro Edition Technology website*), assim como uma PDA e a utilização de rede sem-fio para simulação do ambiente de telefonia celular.

2 Trabalhos relacionados

Este trabalho apresenta alguns aspectos que podem ser comparados a outros trabalhos:

- A garantia de correta execução do sistema operacional;
- a verificação de integridade do sistema operacional;
- a recuperação do sistema através de backup e

- o pacote seguro de hardware.

Para buscar como estas funcionalidades foram implementadas em outras soluções na área de segurança é interessante observar como foram construídos. Abaixo segue uma breve descrição sobre as características de cada sistema.

O Trusted Computing Group é uma organização que desenvolve e divulga especificações para proteção e fortalecimento das plataformas de rede, além de criar especificações técnicas para aumento da segurança nos dispositivos de comunicação móvel. Algumas aplicações que foram desenvolvidas por este grupo e que são desejáveis na implementação desta monografia são: execução de sistema operacional confiável, módulo de inicialização confiável (Fonte Trusted Computing Group).

Um ambiente anti-clonagem para telefonia móvel foi apresentado em (Brawerman, 2005). Este estudo apresenta um ambiente anti-clonagem que identifica e nega serviços para unidades clonadas e também garante que nenhuma unidade possa ser clonada quando estiver utilizando os serviços oferecidos pelas operadoras de telefonia móvel. Os aspectos de segurança abordados neste estudo são de suma importância para esta monografia, como também o pacote de hardware que é utilizado e será seguido nesta implementação.

O trabalho apresentado nesta dissertação tem suas particularidades em relação a funcionalidades de outros correlatos pelos seguintes aspectos:

- O *backup* do sistema está localizado em local seguro.

- O protocolo de comunicação entre o telefone celular e o servidor para a recuperação do sistema OPERACIONAL.

O *backup* do sistema está armazenado no servidor, sendo necessário o *telefone* celular efetuar o *download.* Desta forma garante-se a integridade e a versão do sistema que será instalado no telefone celular.

O download do sistema é efetuado após uma conversação entre o celular e o servidor garantindo assim uma troca de informações para o envio do arquivo criptografado.

3 Especificação

O ambiente de proteção deve certificar a integridade do sistema operacional básico, por meio de um *software* utilizando a linguagem de programação *J2ME*. Para simular o funcionamento do dispositivo móvel (telefone celular) é utilizada uma *PDA* com sistema operacional *Linux*.

Em um processo executado durante a inicialização do sistema é verificada a integridade através de uma função hash, em seguida é feita à comparação do código hash gerado com o código hash armazenado. Em caso de igualdade dos dois valores a integridade do sistema esta garantida e o sistema prossegue a sua execução normal. Em

caso de não igualdade, está apurada a alteração do sistema, desta forma o sistema faz a comunicação com o servidor requerendo uma cópia autentica do sistema operacional.

Para requerer a cópia do sistema operacional o software deve seguir um protocolo, como a seguir: Após o software verificar a não integridade do SO é enviada uma requisição de backup para o servidor que responde ao celular perguntado o motivo da requisição. O celular então envia o hash do SO, o servidor então confirma o recebimento. Em seguida ocorre a autenticação do celular, após a autenticação é enviada a copia do SO criptografada, para finalizar o celular comprova ao servidor o recebimento do SO. Ao término do recebimento é efetuada a descriptografia do arquivo e a instalação do novo SO. O protocolo é visualizado na figura 7, com a troca de mensagens ocorrendo em função do tempo.

Antes de ser efetuado o download do *backup* deve ser efetuada a autenticação do celular, isto garante que o arquivo está sendo enviado para um telefone celular autorizado.

3.1 Pacote de hardware

Para garantir a segurança também se faz necessário que o hardware do telefone celular seja protegido, desta forma previne-se que o equipamento possa ser aberto e modificado os conteúdos de sua memória para roubar informações ou tentar alterar as suas configurações.

O pacote de hardware deve ser fisicamente protegido contra ataques e invasão. Isto inclui conectá-lo fisicamente com as outras partes físicas do aparelho de forma que o hardware não possa ser facilmente desmontado e transferido para outras unidades. O pacote deve ainda limitar sondas e escaneamentos eletro-magnéticos (Brawerman, 2005) (Trusted Computing Group) (Intel Wireless Trusted Platform). Como nos trabalhos correlatos o pacote de hardware segue a abordagem do “ambiente anticlonagem de telefonia móvel” de Brawerman.

O hardware 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 chave de criptografia, os mecanismos de verificação responsáveis por medir, informar e comparar valores de integridade de elementos. O TRC2 contém o mecanismo de verificação responsável por armazenar valores de integridade e memória não volátil para armazenar as chaves necessárias (brawerman, 2005).

4 Resultados

Para a validação do *software* foram efetuados testes, que comprovam o funcionamento e garantem a performance do sistema. A comprovação do funcionamento é realizada com a substituição do arquivo em que é realizado o hash, pelo backup que está armazenado no servidor.

Os testes de performance foram feitos levando-se em conta arquivos para o hash e backup com diferentes tamanhos. O arquivo representa o núcleo do sistema

operacional (Kernel).

O kernel representa a camada mais baixa de interface com o hardware, sendo responsável por gerenciar os recursos do sistema computacional como um todo. É no kernel que estão definidas funções para operação com periféricos (interface serial/paralela, teclado, display), gerenciamento de memória. Para que um programa ou possivelmente um vírus use os serviços disponibilizados é necessário ter acesso ao Kernel.

Os arquivos de kernel do Sharp Zaurus possuem entre 1k e 150k, desta forma foram feitos testes com arquivos de backup com tamanhos de 2,5k a 700K, para avaliar o tempo de execução e espera com que o usuário teria para ligar o celular.

Foram efetuados testes de tempo de execução total e intermediário, como:

- Tempo para calcular o hash: consiste no tempo de calculo do hash para os arquivo, em cada inicialização o hash atual é calculado para se comparar com o hash armazenado.
- Tempo total de execução levando em conta a não alteração do arquivo: é o tempo total de execução do *software* sem a necessidade de efetuar o *backup*. Esta avaliação define o tempo de atraso de execução a cada vez que o celular for ligado.
- Tempo de download do arquivo: é o tempo necessário para que o celular receba o *backup* do servidor.
- Tempo de descriptografia: Inicia-se após o recebimento do arquivo, e termina logo após o arquivo infectado ser substituído pelo *backup*.
- Tempo de execução incluído backup do arquivo e descriptografia: é o tempo de execução do software caso o sistema tenha sido infectado.

Cada simulação e tomada de tempos foi realizada individualmente para cada função, não sendo simplesmente o tempo total de execução a somatória de todos os outros tempos, mas sim um teste realizado unicamente. Para cada teste foi realizado a media entre três tempos.

Arquivo com tamanho de 2.5k

Tempo para calcular o hash = 170 ms

Tempo total de execução levando em conta a não alteração do arquivo = 237 ms

Tempo de download de arquivo= 9.387 ms

Tempo de descriptografia= 32.109 ms

Tempo de execução incluído backup do arquivo e descriptografia= 42.029 ms

Arquivo com tamanho de 12k

Tempo para calcular o hash = 824 ms

Tempo total de execução levando em conta a não alteração do arquivo = 841 ms

Tempo de download de arquivo= 34.205 ms

Tempo de descriptografia= 32.409 ms

Tempo de execução incluído backup do arquivo e descriptografia= 67609 ms

Arquivo com tamanho de 180.4k

Tempo para calcular o hash =10.528 ms

Tempo total de execução levando em conta a não alteração do arquivo=10.110 ms

Tempo de download de arquivo= 458.379 ms

Tempo de descriptografia= 32.946 ms

Tempo total de execução incluído backup do arquivo e descriptografia=489.693 ms

Arquivo com tamanho de 750K

Tempo para calcular o hash =32.752 ms

Tempo total de execução levando em conta a não alteração do arquivo=32.041 ms

Tempo de download de arquivo= 805.270 ms

Tempo de descriptografia= 33.540 ms

Tempo total de execução incluído backup do arquivo e descriptografia=901.504 ms

Sem a necessidade do backup o software executa rapidamente, adicionando pouco tempo a inicialização do sistema. Com a necessidade do backup o tempo de espera para o maior arquivo foi no máximo de 15 minutos.

5 Conclusão

A implementação do projeto mostrou ser esta mais uma forma eficiente de prevenir a alteração do sistema do telefone celular. Se o ambiente estiver integrado diretamente ao sistema operacional, pode-se exaurir o usuário do seu conhecimento, sendo possível garantir que o sistema operacional está integro e sempre em sua correta execução. Outra utilidade possível deste ambiente é manter o sistema operacional atualizado em sua versão mais recente, bastando para isso um controle de versões, com isto é possível prevenir vírus que utilizem falhas do sistema operacional para agir.

Referências

BURNETT, S; PAINE, S. Criptografia e Segurança – O guia oficial RSA,

Campus 2002.

BRAWERMAN, A; COPELAND, J. A. *Um Ambiente anti-clonagem para telefonia móvel*. - 2005 - Departamento de Engenharia de computação, Centro Universitário Positivo, Curitiba - PR, Brasil; School of Electrical and Computer Engineering, Geórgia Institute of Technology, Atlanta – GA, Estados Unidos .

BURNETT, S; PAINE, S. Criptografia e Segurança – O guia oficial RSA, Campus 2002.

INTEL. "Intel Wireless trusted Platform: Security for Mobile Devices".

http://www.intel.com/design/pca/applicationsprocessors/whitepapers/300868.htm , ultima visita em julho de 2006

Java 2 Micro Edition Technology website.

http://www.wireless.jva.sun.com/j2me, ultima visita em julho de 2006

MORENO, E.D. *Criptografia em software e Hardware.* São Paulo, Novatec, 2005.

SZOR, P. Virus Research and Defense, Addison Wesley, 2005.

TRUSTED COMPUTING GROUP

https://www.trustedcomputinggroup.org/, ultima visita em julho de 2006