Universidade Federal de Ouro Preto - UFOP

Instituto de Ciências Exatas e Biológicas - ICEB

Departamento de Computação - DECOM

UMA AUTENTICAÇÃO SEGURA USANDO BLUETOOTH PARA A PLATAFORMA ANDROID

Aluno: Bruno Cerqueira Hott
Matricula: 08.1.4133

Orientador: Ricardo Augusto Rabelo Oliveira
Co-orientador: Jeroen Antonius Maria van der Graaf

Ouro Preto
1 de julho de 2011

Universidade Federal de Ouro Preto - UFOP

Instituto de Ciências Exatas e Biológicas - ICEB

Departamento de Computação - DECOM

COLETA DE CONTEXTO USANDO ACELEROMETRO PARA AUTENTICACAO SEGURA

Relatório de atividades desenvolvidas apresentado ao curso de Bacharelado em Ciência da Computação, Universidade Federal de Ouro Preto, como requisito parcial para a conclusão da disciplina Monografia I (BCC390).

Aluno: Bruno Cerqueira Hott
Matricula: 08.1.4133

Orientador: Ricardo Augusto Rabelo Oliveira
Co-orientador: Jeroen Antonius Maria van der Graaf

Ouro Preto
1 de julho de 2011

Resumo

A expansão da utilização de dispositivos móveis no dia a dia e a troca de informações que se dá entre estes dispositivos é cada vez maior. Pensando na quantidade de dados sigilosos que são transmitidos entre esses aparelhos propomos um método de segurança para a transmissão de dados via bluetooth. A chave de segurança aqui utilizada é gerada a partir do movimento de dois dispositivos móveis, movimento este capturado pelos acelerômetros que estes aparelhos possuem integrados. O método requer então que os celulares pelos quais os dados serão transmitidos estejam fisicamente próximos um do outro.

Este trabalho começa com a captura dos dados referente ao movimento do acelerômetro do celular. Após a captura uma checagem de viabilização será feita considerando o nível de segurança da chave gerada e o tempo em que o usuário terá de balançar os dispositivos. Algum método de transmissão de dados segura será escolhido como o melhor para essa aplicação e a implementação de todo o sistema se dará na plataforma Andoid.

Palavras-chave: Protocolo de comunicação. Dispositivos móveis. Android.

Sumário

Lista de Figuras

Lista de Tabelas

1 Introdução

Celulares, PDAs ou smartphones (que são laptops, PDAs e celulares em um só dispositivo) tornaram-se acessórios essenciais para o agitado estilo de vida moderno. Os celulares e PDAs são convenientes, portáteis e estão cada vez mais sofisticados. Eles podem ser levados a praticamente todos os lugares, junto com anotações e informações importantes, o que o torna disponível a qualquer momento e em qualquer lugar. É provável que haja algumas informações muito importantes armazenadas nesses dispositivos. É provavel também que os usuáros necessitem de compartilhar essas informações com outros aparelhos.

Documentos importantes são transmitidos entre esses dispositivos. Documentos esses que se interceptados por outras pessoas que não estejam autorizadas podem acarretar em grandes dores de cabeça. Pensando nisso apresentamos um método de transferência segura entre dois dispositivos móveis.

Esse método utiliza o princípio de que esses dois dispositivos estão no mesmo espaço e que ambos possuam um acelerômetro embutido. O usuário deverá segurar os dois aparelhos com uma mão e sacudi-los um pouco, esse movimento capturado pelo acelerômetro criará uma chave de segurança que será utilizada na encriptação dos dados à serem enviados e na decriptação desses mesmos dados pelo dispositivo receptor.

2 Justificativa

Os smartphones nunca foram tão baratos, acessíveis e fácil de usar. Por serem multifunção e possuírem uma grande capacidade de memória estes aparelhos podem armazenar muitas informações privadas como agenda de contatos, compromissos, arquivos e planilhas. Todas estas informações quando em mãos erradas podem causar muitas dores de cabeça.

O objetivo deste trabalho é utilizar algum método conhecido e eficaz de criptografia que funcione bem para dispositivos móveis, levando em consideração poder de processamento e vida útil da bateria. As perguntas téoricas que devem ser respondidas no trabalho são:

1. Como qualificar e quantificar a quantidade de bits necessária para eliminar possíveis ataques de um adversário?

2. Como extrair os bits aleatório?

3. Quanto tempo é necessário balançar o dispositivo até conseguir uma quantidade de dados necessário para criar uma chave e eliminar possíveis ataques de um adversário?

O foco inicial deste trabalho é para arquivos de texto, mas a técnica desenvolvida pode ser estendida para outros tipos de arquivos, por exemplo, multimídia. Além do método, ainda existe o objetivo de desenvolver uma aplicação em Android que faça o uso desse método, para testar e validar a implementação do trabalho.

3 Objetivos

A principal contribuição desse artigo vem a ser o estudo de viabilidade que será feito levando em consideração a troca de informação via um protocolo proposto usando bluetooth para a plataforma android. Qual é a viabilidade em balançar dois dispositivos móveis e utilizar a informação do acelerômetro para gerar uma chave aleatória suficientemente grande e confiável que elimine possíveis ataques de um adversário. Quanto tempo é necessário balançar os dispositivos para gerar uma chave aleatória suficientemente aleatória e que satisfaça o método de encriptação.

3.1 Objetivo geral

Este trabalho tem como principal objetivo, a obtenção de bits gerados pelos acelerômetros de ambos os smartphones, para serem utilizados na criação de um protocolo de comunicação seguro. Este protocolo de comunicação visa o compartilhamento seguro de arquivos entre smartphones.

3.2 Objetivos especficos

- Identificar nos trabalhos relacionados as vantagens e desvantagens de cada abordagem;
- Verificar os algoritmos de encriptação na plataforma Android;
- Desenvolver o modelo de coleta de dados que prevê quando o dispositivo está pronto para transmissão;
- Testar o modelo em dispositivos reais, em diferentes situações.

4 Metodologia

As principais atividades previstas para esse projeto são:

- Pesquisa de técnicas para obtenção dos dados gerados pelo acelerômetro de um smartphone;
- Caracterização e classificação dos métodos pesquisados;
- Implementa das técnicas pesquisadas;
- Pesquisa de simuladores android para testes;
- Teste, em simuladores, da coleta de dados do acelerômetro;
- Pesquisa de técnicas para protocolos de comunicação;
- Caracterização e classificação dos protocolos pesquisados;
- Implementação dos protocolos pesquisados;
- Testes em simuladores e por fim testes em dispositivos móveis.

Considerando as atividades descritas, a metodologia prevista para cada atividade será:

- Inicialmente será feita um estudo das diversas técnicas de obtenção de dados de um acelerômetro. Estes métodos serão implementados e testados em simuladores.
- Com os dados dos acelerômetros em mãos, será feito um estudo das técnicas de protocolo seguro para comunicação entre smartphones. Tais métodos serão implementados e passarão por diversos testes em simuladores.
- Na etapa final o produto desenvolvido será implantado em smartphones e os testes finais serão feitos.

5 Desenvolvimento

Na primeira etapa do projeto houve um foco em pesquisar métodos e trabalhos correlatos que pudesses auxiliar na extração de dados do acelerômetro.

Em [1] foi apresentado um método de obtenção de dados de um acelerômetro. Este método leva em conta a orientação dos diversos tipos de dispositivos, cada Smartphone utiliza a sua base de coordenadas própria foi apresentada uma maneira de transformar os dados nessas coordenadas em uma base canônica.

Outros pontos estudados foram o consumo de energia, a precisão dos dados e a seguranca obtida. Um balanceamento entre essas três medidas é fundamental e suas respectivas importâncias são:

- O consumo de energia assim como o consumo de recursos do dispositivo móvel devem ser minimizados, já que dispomos de pouca infra-estrutura.
- A leitura de um movimento feito necessita de uma precisão que o torne único, ou seja, que nos permita tirar uma entropia razoável. Em contrapartida temos de ter em mente que os dados dos acelerômetros de ambos os dispositivos não serão iguais, portanto se a precisão da leitura utilizada for elevada, mais dados desiguais serão capturados.
- A segurança obtida vai depender da aleatoriedade dos dados obtidos e do tamanho da chave que será obtida desses dados. Um movimento do aparelho demasiado longo, com o fim de se obter uma chave altamente segura, pode inviablizar o uso do protocolo.

5.1 Acelerômetro

Foi proposto um modelo para tratamento dos dados obtidos pelo acelerômetro [5]. Este tratamento é dividido em três tarefas: aquisicao de dados do sensor, alinhamento temporal e alinhamento espacial.

- A tarefa de aquisição de dados não apenas consiste em coletar os dados, mas também definir a taxa de amostragem. Estes dados devem ser coletados localmente e, por questões de seguranca, não deve ser trafegado pela rede sem fio. No trabalho de [5], uma taxa de 100 a 600 Hz foi identificada como apropriada.
- A segunda tarefa diz respeito a sincronização temporal para comparação. Como as chaves precisam ser correlatas, e necessário que haja um consenso sobre o início da medicao. Então existem dois problemas: o gatilho (disparo) do evento e a sincronização dos dados. O primeiro pode ser resolvido a partir de um botão pressionado pelo usuário (explícito) ou a deteccao de uma movimentacao brusca (implícito). A sincronizacao pode utilizar a troca de parte dos dados obtidos para ambos os dispositivos marcarem o início da medição ou simplesmente utilizar o disparo evento. Para este trabalho vamos utilizar a deteccao de movimentacao como gatilho e também para sincronização. Existem diversos modelos na literatura para identificar esses movimentos [4] [6].

- A última tarefa de tratamento é responsável por normalizar as informações de cada dimensão considerando que os aparelhos não estão dispostos com os eixos alinhados. Para eliminar o efeito provocado pela rotação do eixo, [5] propôs utilizar o vetor resultante das 3 dimensões. Neste trabalho serão considerados todos os eixos de forma independente para aumentar a entropia da chave. Uma possíel solucao para este caso seria a troca de informacoes a respeito do direcionamento do aparelho no início da medição.

Por fim, depois de tratados os dados deve-se aplicar um dos protocolos de reconciliacao, vistos na próxima subseção.

5.2 Reconciliação de chaves

Informações obtidas através de sensores como acelerômetro, temperatura, câmeras entre outros não são muito precisas e estão sujeitas a interferências, intencionais ou não. Mesmo que dois aparelhos, A e B, fiquem emparelhados corretamente, e o movimento dos dois simultaneamente seja perfeito, a medição em cada um deles será diferente.

Assim, tem-se duas chaves diferentes: K_A e K_B. Para que ambos possam trocar informacoes encriptadas, e necessário encontrar uma chave comum entre eles. O processo de reconciliação de chaves consiste em transformar as duas chaves criptográficas correlatas K_A e K_B em uma única chave K_{AB}.

Essa reconciliação é baseada na troca de informações. Considerando que o canal para essa troca seja público (adversário têm acesso à rede), é preciso que o protocolo utilize o mínimo de informações a respeito da chave.

Neste trabalho serão abordados 3 desses protocolos: BBBSS, Shell e Cascade. Antes de entrar nos detalhes dos protocolos, é importante detalhar algumas primitivas comuns a vários deles.

5.2.1 Primitivas

Uma das primitivas adotadas pelos protocolos é a BINARY [2]. Se A e B possuem Strings X e Y com número ímpar de erros, A envia a B a paridade da primeira metade de X. B compara com a paridade da mesma metade de Y para identificar se o erro ocorreu na primeira ou segunda metade e avisa a A. O processo e repetido tomando-se a metade com erro como String até que o erro seja encontrado.

CONFIRM [2] é outra primitiva que indica, com probabilidade 1/2, quando X e Y são diferentes. Caso elas sejam iguais, a primitiva o informa com probabilidade 1. Para realizá-lo, A e B escolhem um subconjunto de bits. Então comparam as suas paridades. Este processo pode ser repetido k vezes para assegurar com probabilidade de erro de 2^{-k} que A e B são iguais. O tamanho do subconjunto deve ser escolhido adequadamente de forma que a probabilidade de haver um número par ou ímpar de erros no intervalo seja alta.

BICONF [2] é uma combinação das primitivas anteriores. Toda vez que for verificado com CONFIRM que as Strings são diferentes, então executa-se BINARY para encontrar e corrigir o erro.

5.2.2 BBBSS

Inicialmente, o BBBSS aplica a Tansformação de Uniformização[3] a toda string X e Y. Ela permite distribuir os erros igualmente por toda a chave. Para isso,A escolhe uma funcao de permutacao $\pi : 0,1^N \leftarrow 0,1^N$ e envia a descricao a B. Ambos aplicam a função de permutação π nas suas chaves K_A e K_B gerando chaves K'_A e K'_B . Deve-se observar que o número de erros (bits diferentes) continua o mesmo. Essa primitiva ajuda a evitar problemas de erros em rajada.

Após esse processo, X e Y são divididos em blocos de tamanho k. Para cada bloco, BICONF é executado para busca e correção de erros. Como esta primitiva está sujeita a falhas quando o número de erros é par, o procedimento e repetido várias vezes aumentando-se o tamanho do bloco.

5.2.3 Shell

O protocolo Shell [2] divide inicialmente as chaves K_A e K_B em blocos de tamanho k. Aplica-se então BICONF. Se for detectado um erro, todos os bits do bloco errado de B são sobrescritos com os correspondentes de A. No passo seguinte, concatena-se pares de blocos adjacentes e BICONF é aplicado. Novamente, caso um erro seja detectado, os bits do bloco problemático de B são substituídos pelos de A. Repete-se o processo até que o tamanho do bloco seja igual ao tamanho inicial das chaves.

5.2.4 Cascade

Neste protocolo [7], A e B devem decidir antecipadamente o número de passos p. Em cada passo i, ambos permutam randomicamente as chaves K_A e K_B e dividem em blocos de tamanho k(i). Após calcular as paridades de cada bloco, A as envia a B para que o mesmo faca uma busca do tipo BINARY para encontrar e corrigir possíveis erros. Nesse ponto, o número de erros em cada bloco se torna par.

Então, para cada passo $i \geq 2$, aumenta-se o tamanho do bloco para $k(i) = 2k(i-1)$[2]. Deve-se armazenar todos os blocos de bits em cada passo, com suas devidas permutações. Agora seja l o bit corrigido no passo i. E seja X o conjunto de todos os blocos de passos $[1..i-1]$ que contém o bit l. Deve-se corrigir todos os blocos X. Sabe-se então que agora todos esses blocos contém um número ímpar de erros. Então A e B escolhem o menor desses blocos e usam BINARY novamente para encontrar outro erro no bit l.

Seja Y o conjunto de todos os blocos de passos $[1..i]$ contendo l . Corrige-se Y com BINARY. Todos os blocos em $(Y \cup X)/(Y \cap X)$ tem um número ímpar de erros. Então atualiza-se X com $X \leftarrow (Y \cup X)/(Y \cap X)$ e repete-se o processo até que X fique vazio. Neste ponto, o passo i terminou. O protocolo encerra de acordo com o número de passos determinado inicialmente.

6 Trabalhos Futuros

O próximo passo deste projeto será implementar e testar os diversos meios de obtenção de chaves aleatórias a partir do acelerômetro de um smartphone.

Deverá ser implementados e testados os métodos de reconciliação de chaves propostos discutidos neste trabalho. De posse então das chaves obtidas, deveremos estudar e implementar alguns protocolos de comunicação entre estes dispositivos.

O produto final deverá ser testado visando consumo de energia, segurança e praticidade para os usuários.

7 Cronograma de atividades

Na Tabela 1, temos o cronograma de atividades previsto para o próximo semestre.

Atividades	**Ago**	**Set**	**Out**	**Nov**	**Dez**
Implementação do software	X				
Testes e correções	X	X			
Análise de resultados			X		
Redigir a Monografia			X	X	X
Apresentação do Trabalho					X

Tabela 1: Cronograma de Atividades.

Referências

[1] NVIDIA Corporation. Tegra android accelerometer whitepaper. November 2010.

[2] Brassard G. and Salvail L. Secret-key reconciliation by public discussion. 1994.

[3] Bennett C. H., Brassard G., and Robert J.M. Privacy amplification by public discussion. 1988.

[4] Lester J., Hannaford B., and Borriello G. Are you with me? - using accelerometers to determine if two devices are carried by the same person. 2004.

[5] Mayrhofer, R., Gellersen, and H. Shake well before use: authentication based on accelerometer data. 2007.

[6] Huynh T. and Schiele B. Analyzing features for activity recognition. 2005.

[7] Shimizu T., Iwai H., and Sasaoka H. Information reconciliation using reliability in secret key agreement scheme with espar antenna. 2009.