GERSON DE SOUZA FARIA

IDENTIFICAÇÃO DAS TECLAS DIGITADAS A PARTIR DA VIBRAÇÃO MECÂNICA

Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do título de Mestre em Engenharia

São Paulo
2012

GERSON DE SOUZA FARIA

IDENTIFICAÇÃO DAS TECLAS DIGITADAS A PARTIR DA VIBRAÇÃO MECÂNICA

Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do título de Mestre em Engenharia

Área de Concentração:
Sistemas Eletrônicos

Orientador:
Prof. Dr. Hae Yong Kim

São Paulo
2012

FICHA CATALOGRÁFICA

Faria, Gerson de Souza
Identificação das teclas digitadas a partir da vibração mecânica / G.S. Faria. – São Paulo, 2012. 42p.

Dissertação (Mestrado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos.

1. Redes de computadores (Segurança) 2. Processamento digital de sinais 3. Reconhecimento de padrões I. Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Sistemas Eletrônicos II. t.

Agradecimentos

Ao professor Hae Yong Kim pela seriedade e exigência no processo de orientação, pelo constante estímulo e pela parceria real de trabalho.

Aos professores Reynaldo Daniel Pinto e Miguel Arjona Ramirez pelas valorosas contribuições na banca de qualificação.

Ao Departamento de Engenharia de Sistemas Eletrônicos da Escola Politécnica pela aprovação da apresentação dos resultados em congresso nacional.

À Capes, pela concessão de bolsa de estudo.

Aos meus irmãos Laercio e Alexandre, e ao Ivan Pagnossin pela paciência nas enfadonhas sessões de tomadas de pressionamentos de teclas. Ao Ivan também pelas valiosas dicas de uso do LaTeX.

Aos meus pais, que, pais que são, raramente sabem ao certo o que seus filhos fazem (e dificilmente conseguimos explicar o que fazemos...) mas torcem para que tudo dê certo.

Ao professor Emilio Del Moral Hernandez, cuja disciplina "Aplicação de Inteligência Computacional e Técnicas de Processamento de Sinais a Sistemas Sensores e Biossensores" ensejou a realização do experimento ATM, e ao Fernando Ginez, colega de pesquisa no mesmo.

Ao Cláudio Bordin pela disponibilização do modelo de dissertação em LaTeX.

Ao CCE pela assistência e suporte operacionais.

À Mimi Carolina (em memória), Ninoca Maria, Tita Tereza (em memória) e Jolie Marie, que sempre estiveram presentes, em todos os momentos.

E *last but not least*, à Ana, pelo apoio constante, dedicação e carinho, sem os quais nada disso teria sido realizado.

They constantly try to escape
From the darkness outside and within
By dreaming of systems so perfect that no one will need to be good
– TS Eliot, citado por R. Anderson

Sumário

Introdução **1**

1 Descrição das Vulnerabilidades Exploradas **6**
1.1 Introdução 6
1.2 Teclados Mecânicos Genéricos 6
1.3 Terminais de Ponto de Venda (POS ou PIN-pad) 8

2 Classificação de Sinais Unidimensionais - Abordagem Adotada **10**
2.1 Introdução 10
2.2 Notações 12
2.3 Características 15
2.4 Algoritmos de Aprendizado de Máquina 16

3 Experimentos Realizados com Teclado Genérico (ATM) **18**
3.1 Montagem Experimental 18
3.2 Acelerômetros e Sistema de Aquisição 18
3.3 Obtenção das Amostras 20
3.4 Características Utilizadas 20
3.5 Resultados Experimentais 21

4 Experimentos Realizados com Terminal POS (PIN-pad) **22**
4.1 Montagem Experimental 22
4.2 Experimento PIN-pad I 23
4.3 Experimento PIN-pad II 26

Conclusão **35**

Lista de Figuras

1.1 Teclado genérico de automação comercial utilizado em um dos ataques efetuados. 7
1.2 Geração atual de teclados mecânicos utilizados na maioria dos terminais bancários de auto atendimento. 7
1.3 Modelo genérico de PIN-pad, ou terminal POS. 8
1.4 Exemplo de selo de detecção de violação utilizado para evidenciar a abertura de equipamentos. 9

2.1 Dois pressionamentos da mesma tecla pela mesma pessoa podem ser bem diferentes. No gráfico, a aceleração da componente $\vec{z}$ de um acelerômetro para a tecla "0". 11

3.1 Montagem do teclado e disposição e posicionamento dos acelerômetros. A base é uma placa acrílica com 5mm de espessura. 19
3.2 Exemplo de amostra da aquisição da tecla "1". Apenas o eixo $\vec{z}$ foi utilizado. 20
3.3 O momento de inércia do sistema ao redor de $\vec{x}$ é menor do que ao redor de $\vec{y}$, facilitando o reconhecimento de linhas. 21

4.1 Layout do teclado do terminal POS utilizado. 22
4.2 Vista da parte inferior do terminal, sem a tampa de acesso aos conectores SAM, com a disposição dos acelerômetros utilizados. 23
4.3 Uma placa da plataforma aberta Arduino foi utilizada como sistema de aquisição. Para acomodar circuitos auxiliares e conectores para os acelerômetros, uma placa suplementar foi montada sobre o Arduino. Para a conversão de níveis (5V$\leftrightarrow$3.3V) do barramento I^2C, dois transistores MOSFET foram utilizados 24

4.4 Uma placa da plataforma aberta Arduino foi utilizada como sistema de aquisição. Para acomodar circuitos auxiliares e conectores para os acelerômetros, uma placa suplementar foi montada sobre o Arduino. Um circuito de conversões de nível (5V$\leftrightarrow$3.3V) com maior *throughput* (MAX3391) foi utilizado para o barramento SPI 26
4.5 Os intervalos de amostragem dos dois sensores para a aquisição de um pressionamento é bastante irregular e somente na média é proxima ao valor nominal. 28
4.6 Distribuição das ocorrências de intervalos de aquisição de um dos sensores. A maior ocorrência se dá em 332μs (aproximadamente 3012 amostras/s) quando a frequência nominal de trabalho é de 3200 amostras/s ($\approx$312μs.) 29
4.7 Estimativas de Densidade Espectral de Potência Média (PSD) para os modos "mesa" e "mão" para o eixo $\vec{z}$. 32
4.8 Eixos principais dos momentos de inércia do PIN-pad. É mais fácil identificar colunas do que linhas porque o momento de inércia no eixo $\mathbf{I_y}$ é menor do que no eixo $\mathbf{I_x}$. Nota: Este esboço não corresponde ao equipamento analisado. 34

Lista de Tabelas

3.1 Taxas de reconhecimento em % obtidas no experimento ATM. 21

4.1 Taxas de reconhecimento em % obtidas no experimento PIN-pad I, modo “mesa”. 25
4.2 Taxas de reconhecimento em % obtidas no experimento PIN-pad II, modo “mesa” sem alinhamento temporal. 30
4.3 Taxas de reconhecimento em % obtidas no experimento PIN-pad II, modo “mesa” com alinhamento temporal. 30
4.4 Taxas de reconhecimento em % obtidas no experimento PIN-pad II, modo “mão” sem alinhamento temporal. 31
4.5 Taxas de reconhecimento em % obtidas no experimento PIN-pad II, modo “mão” com alinhamento temporal. 31

Lista de Símbolos

$*$	Correlação cruzada (CC)
$\otimes$	Correlação cruzada normalizada (NCC)
M	Número de amostras deslocadas em uma operação de correlação
N	Tamanho de um vetor de amostras
T	Período de amostragem

Lista de Abreviaturas e Siglas

ATM	(*Automatic Teller Machine* ou *Automated Teller Machine*) Caixa eletrônico de auto atendimento
CC	(*Cross Correlation*) Correlação cruzada
EMSEC	(*Emission Security*) Segurança de emissões
MLP	(*Multilayer Perceptron*) Perceptron multicamadas
NCC	(*Normalized Cross Correlation*) Correlação cruzada normalizada
NSA	(*National Security Agency*) Agência Nacional de Segurança dos Estados Unidos da América
Open-CV	(*Open Computer Vision*) Biblioteca de código aberto com rotinas para processamento de imagens, visão computacional e aprendizado de máquina
PIN	(*Personal Identification Number*) Número de identificação pessoal
PIN-pad	Terminal de ponto de venda em que o PIN é inserido
POS	(*Point of Sale*) Terminal de ponto de venda
PSD	(*Power Spectral Density*) Densidade Espectral de Potência
RBF	(*Radial Basis Function*) Função de base radial
SVM	(*Support Vector Machine*) Máquina de vetores de suporte

Resumo

Este trabalho descreve um ataque que detecta as teclas pressionadas em teclados mecânicos pela análise das vibrações geradas quando as mesmas são pressionadas. Dois equipamentos foram experimentados no ataque: um teclado genérico de automação comercial e um terminal de ponto de venda (POS / PIN-pad). Acelerômetros são utilizados como sensores de vibração. Propositalmente, o equipamento necessário para a execução do ataque é de baixíssimo custo, de modo a ressaltar o risco das vulnerabilidades encontradas. Obtivemos taxas de sucesso médio de 69% no reconhecimento das teclas pressionadas para o terminal PIN-pad em repouso e 75% para o mesmo sendo segurado na mão. No caso de teclado de automação comercial, as taxas médias de acerto ficaram em torno de 99%.

Palavras-chave: Processamento de sinais. Segurança da informação. Ataque a Canais Secundários. Tempest. PIN-pad. ATM. Acelerômetros. Teclados. Arduino.

Abstract

This work describes an attack that identifies the sequence of keystrokes analyzing mechanical vibrations generated by the act of pressing keys. We use accelerometers as vibration sensors. The apparatus necessary for this attack is inexpensive and can be unobtrusively embedded within the target equipment. We tested the proposed attack on an ATM keypad and a PIN-pad. We achieved the key recognition rates of 99% in ATM keypad, 69% in PIN-pad resting on a hard surface and 75% in PIN-pad hold in hand.

Keywords: Signal Processing. Information Security. Side channel attack. Tempest. PIN-pad. ATM. Accelerometers. Keyboards. Arduino.

Introdução

Considerações Iniciais

Atualmente, teclados mecânicos são a principal interface homem-máquina devido à sua facilidade de operação, eficiência e baixo custo. No mercado de meios de pagamento eletrônico, teclados são a escolha natural para a entrada de dados sigilosos, como senhas em terminais de ponto de venda,[1] caixas eletrônicos etc. Na esfera governamental, os teclados mecânicos são utilizados para inserir os números de candidatos em urnas eletrônicas. Deste modo, a possibilidade de que alguém descubra a sequência de teclas digitadas (sem que o usuário perceba) é uma séria ameaça à segurança de sistemas. Dois tipos de teclado são analisados neste trabalho – teclados de terminais de ponto de venda e teclados originalmente utilizados para entrada de dados em estabelecimentos bancários. Utilizamos o termo "terminal POS" ou "PIN-pad" de forma indistinta, como sendo um equipamento portátil, que recebe o cartão magnético ou *smart card* do cliente e que possui um teclado embutido em seu corpo para entrada de PIN ou senha.

Revisão da Literatura

Não encontramos na literatura ataques a teclados mecânicos pela análise de vibrações capturadas por meio de acelerômetros. Estudos correlatos apresentam apenas ataques que analisam os sons gerados ao pressionar teclas de teclados de computador [2, 3, 4], teclas de terminais de caixas eletrônicos [2] e ataques acústicos em outros dispositivos,

[1] Segundo dados da Associação Brasileira das Empresas de Cartões de Crédito e Serviços (ABECS), as duas maiores credenciadoras operam no Brasil com mais de 4 milhões de terminais, tendo efetuado 3 bilhões de operações no ano de 2010 [1].

tais como impressoras matriciais [5]. Tromer apresenta em [6] uma criptanálise em que afirma ser possível identificar as operações matemáticas de uma assinatura RSA sendo executadas pela CPU, por meio da captura de emanações acústicas de um capacitor eletrolítico da fonte de alimentação, na faixa de 20KHz. Cai e Chen descrevem um ataque que permite inferir os dígitos pressionados no teclado virtual de celulares baseados no sistema Android analisando o movimento do aparelho capturado pelo acelerômetro interno do mesmo [7]. Uma análise geral sobre a vulnerabilidade de sensores de telefones celulares é apresentada em [8].

Objetivos

O principal objetivo deste trabalho é descrever um ataque físico não invasivo a teclados mecânicos. A técnica aqui empregada foi testada em dois experimentos: um teclado genérico de automação comercial e um terminal de ponto de venda *Point Of Sale* (POS) nos quais foi possível detectar as teclas digitadas a partir das vibrações mecânicas geradas nos equipamentos pelo ato de pressioná-las. Tais vibrações são capturadas por acelerômetros instalados na base do teclado para o caso de terminais de automação e no interior do terminal, para o caso dos equipamentos POS. A possibilidade de um ataque similar foi sugerida por Kuhn [9]:

> *Information theft through unconventional side-channels is unlikely to remain restricted to the electromagnetic, optical, and acoustic domain. For example, a mechanical side-channel could be exploited by installing pressure sensors underneath the feet of a keyboard, or the table on which it rests. How the force vector of each keystroke will be split up among these anchor points will depend on the location of the respective key. Two or three attached transducers should suffice to distinguish and record keystroke sequences, an attack that may be of particular concern with trusted PIN-entry devices.*[2]

[2]Tradução livre: "É improvável que roubo de informação através de canais secundários não convencionais permaneça restrito aos domínios eletromagnético, óptico e acústico. Por exemplo, um canal secundário mecânico poderia ser explorado instalando-se sensores de pressão sob os pés de um teclado, ou a mesa em que ele se encontra. O modo como os vetores das forças de cada pressionamento se-

O autor sugere a possibilidade de identificação das teclas pressionadas pela análise vetorial das forças resultantes em determinados pontos do equipamento, como, por exemplo, nos suportes da base (pés). Kuhn afirma ser improvável que o roubo de informação por meio de canais secundários (*side channels*) fique restrito aos domínios eletromagnético, óptico e acústico. Porém, segundo o nosso conhecimento, este ataque nunca foi testado experimentalmente. Diferentemente da proposta de Kuhn, nosso ataque não analisa as forças nas bases, mas sim as vibrações mecânicas geradas pelo ato de pressionar as teclas.

Motivação e Justificativa

Com a crescente generalização do uso de equipamentos eletrônicos em transações comerciais, surge concomitantemente uma nova gama de crimes eletrônicos, evoluindo conjuntamente à tecnologia empregada nos equipamentos. Como forma de conter o avanço de tais delitos, criam-se instituições, normas e padrões de certificação de segurança, baseados em um primeiro momento nos paradigmas, nas doutrinas e nas experiências de campo dos órgãos de segurança nacionais, no âmbito de inteligência e contra-inteligência do período posterior à II Guerra Mundial. Tal cenário – de caráter militar – tinha em vista essencialmente equipamentos eletromecânicos, em que efeitos de emissão eletromagnética são comuns devido ao chaveamento de motores de dispositivos de cifração, equipamentos de fac-símile, copiadoras, terminais de teletipo (teleimpressoras) etc. Tais emissões carregam informação que pode eventualmente ser utilizada, seja por seu conteúdo sigiloso de interesse, seja por expor indevidamente a operação e características do equipamento utilizado [10]. A área militar de EMSEC (*Emission Security*) [11, capítulo 17] é especificamente dedicada à prevenção de ataques pelo uso de "emanações comprometedoras", do inglês *compromising emanations*. O escopo do EMSEC é relativo às ondas eletromagnéticas, principalmente emissão no espectro de RF. Até o momento, tais especificações são de uso estritamente militar e confidencial, sendo que umas poucas partes dos documentos originais são de domínio

rão compostos irá depender da localização da respectiva tecla. Dois ou três transdutores deverão ser suficientes para distinguir e armazenar a sequência de pressionamentos, um ataque que pode ser de preocupação especial em equipamentos de inserção do PIN"

público graças ao *Freedom of Information Act* (FOIA) vigente na legislação norte-americana [11, p. 546],[12, 13].

Embora os processos de certificação de equipamentos para uso comercial não tenham que possuir o mesmo rigor no tocante à emanações, muito de seu perfil parece ter sido emprestado das especificações de caráter militar. Como exemplo, é interessante ressaltar que o principal consórcio responsável pelo desenvolvimento de padrões em segurança de pagamentos com cartão, o *Payment Card Industry - Security Standards Council* (PCI) cite nominalmente emissões de caráter do EMSEC, mas não considere explicitamente as vibrações mecânicas como fonte potencial de ameaça à segurança de informação.[3]

Abordagem Proposta

A abordagem de ataque aqui desenvolvida é a de análise de vibração mecânica de teclados, originada pelo ato de teclar. Consideramos tal ataque como um *side-channel attack*, situação em que a informação vaza por um canal distinto do projetado intencionalmente para comunicação [11]. *Side-channel attack* é normalmente um ataque baseado na informação ganha da implementação física de um criptossistema [15, 16]. Outros exemplos desse tipo de ataque compreendem o uso de informação temporal (*timing analysis*), consumo de energia (*power analysis*), vazamento de emissão eletromagnética ou sonora, que podem prover informação adicional a ser explorada de forma a quebrar o sigilo do sistema. Ataques invasivos[4] não são abordados ou considerados neste trabalho.

[3] *"There is no feasible way to determine any entered and internally transmitted PIN digit by monitoring sound, electro-magnetic emissions, power consumption or any other external characteristic available for monitoring – even with the cooperation of the device operator or sales clerk – without requiring an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation."* [14, p. 9]. Tradução livre: "Não deve haver um modo viável de determinar qualquer dígito do PIN inserido e transmitido internamente pela monitoração de som, emissões eletromagnéticas, consumo de energia ou qualquer outra característica externa disponível para monitoração – mesmo com a cooperação do lojista – sem que o mesmo requeira um potencial de ataque de ao menos 26 para identificação e exploração inicial e um mínimo de 13 para o uso final".

[4] Ataques em que há algum tipo de dano ou modificação do equipamaneto alvo.

Principais Contribuições

A principal contribuição deste trabalho é expor uma vulnerabilidade inerente ao uso de teclados mecânicos, sejam independentes ou sejam embutidos em terminais POS. Apresentamos elementos suficientes mostrando que ataques não invasivos a ambos para acesso indevido à informação são possíveis e podem ser efetuados a um baixíssimo custo.

Organização do texto

O conteúdo deste trabalho está organizado da seguinte maneira:

- O Capítulo 1 apresenta os principais pontos de vulnerabilidade dos equipamentos explorados pelo ataque;
- O Capítulo 2 aborda as técnicas aplicadas na classificação dos sinais;
- O Capítulo 3 apresenta o experimento utilizando o teclado ATM, os resultados obtidos e as discussões;
- O Capítulo 4 apresenta dois experimentos utilizando um terminal PIN-pad, os resultados obtidos e as discussões comparativas entre estes e o experimento ATM;

Por fim, apresentamos as conclusões finais sobre os resultados.

Publicações

O conteúdo desta dissertação deu origem às seguintes publicações:

- O artigo *Identificação das teclas digitadas a partir da vibração mecânica* [**?**], publicado nos Anais do 30º Simpósio Brasileiro de Telecomunicações, (anexado ao final deste trabalho) que consiste em parte do experimento PIN-pad I.
- O artigo *Identification of Pressed Keys From Mechanical Vibrations*, submetido ao periódico IEEE Transactions on Information Forensics and Security, que consiste do conteúdo dos experimentos ATM, PIN-pad I e PIN-pad II desta dissertação.

Capítulo 1

Descrição das Vulnerabilidades Exploradas

1.1 Introdução

Sistemas mecânicos possuem frequências de operação resultantes de várias características intrínsecas a estes, como o material utilizado em sua construção, peso, geometria, composição das partes, dinâmica de movimentação, interação com o meio etc. Tais propriedades fazem com que o sistema apresente características próprias quanto à sua resposta a algum estímulo externo. Essas características constituem uma espécie de "assinatura" física do mesmo para determinado fenômeno. De forma análoga, os instrumentos musicais e suas notas são reconhecíveis pelo som que produzem quando tocados, ainda que por músicos diversos. Sua "assinatura" é composta pelos mesmos elementos citados acima: material, peso, geometria etc. Com base nessa intuição, nos perguntamos sobre a possibilidade de identificar as teclas pressionadas em teclados pela vibração originada pelo pressionamento das mesmas.

1.2 Teclados Mecânicos Genéricos

Caixas eletrônicos de auto atendimento são vítimas constantes de ataques por motivos óbvios. Uma galeria bastante elucidativa de ataques pode ser vista em [18]. Teclados como o da Figura 1.1 foram utilizados em terminais de auto atendimento de bancos por

Figura 1.1: Teclado genérico de automação comercial utilizado em um dos ataques efetuados.

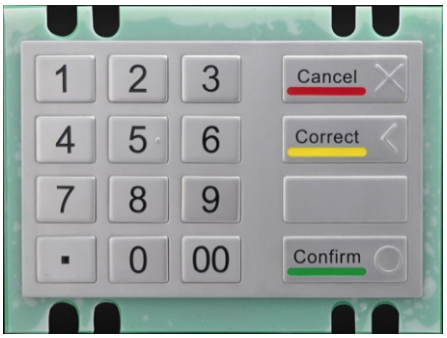

Figura 1.2: Geração atual de teclados mecânicos utilizados na maioria dos terminais bancários de auto atendimento.

longo período de tempo. Aparentemente tal modelo tem sido substituído, não sendo mais utilizado ao menos para este segmento. Hoje, observam-se teclados metálicos de menor curso de tecla, e estas, de altura menor, como o exemplo da Figura 1.2, denominados genericamente de “teclados ATM antivandalismo”. Tal alteração pode ter a capacidade de mitigar ataques de tipo acústico [2], dentre outras qualidades. Os teclados de geração anterior emitem um som bastante característico e de intensidade audível a metros de distância, quando pressionados com intensidade razoável, constatado no experimento aqui realizado com esse modelo de teclado.

Figura 1.3: Modelo genérico de PIN-pad, ou terminal POS.

1.3 Terminais de Ponto de Venda (POS ou PIN-pad)

Assim como ATMs, terminais POS também são alvos constantes de ataques. Equipamentos como os terminais POS (Figura 1.3) possuem mecanismos de detecção de violação física (*tampering*), de modo a destruir informação sensível, como chaves criptográficas, contidas em seu perímetro de segurança. Saar Drimmer *et. al.* [19] evidenciaram de forma contundente que em determinadas circunstâncias esse mecanismo pode ser completamente burlado.

Uma inspeção visual mostrou que terminais POS possuem em sua parte inferior uma tampa removível de serviço e manutenção de modo a oferecer acesso legítimo aos conectores de cartões SAM (*Security Authentication Module*), responsáveis pela segurança da comunicação do sistema bem como pela autenticação com as redes de serviços. De forma a ampliar as opções dos lojistas, fabricantes de terminais POS disponibilizam equipamentos com até quatro conectores, possibilitando a operação de várias prestadoras de serviços de meios de pagamento em um mesmo terminal.

Se por um lado ampliam-se as opções de operação para várias prestadoras, por outro aumenta-se o risco na segurança, pois tal espaço possibilita a implantação de dispositivos de coleta ilegal de informação (*bugs*, que em nosso caso são os acelerômetros). Um mecanismo de detecção de abertura comumente utilizado é o da aplicação de selos do tipo *void seal* (Figura 1.4), no encontro da tampa com o corpo do terminal, indicando visualmente a prévia abertura do compartimento. Mas nos casos de compartimento de acesso legítimo, tais selos são dificilmente encontrados. Porém, ainda que

existam, por várias razões, o consumidor não costuma prestar atenção a tal item no momento anterior ao ato de digitar a sua senha. Além do acesso ao compartimento, outra condição que beneficiaria ainda mais um ataque é a alimentação elétrica disponível nos terminais dos conectores SAM, que poderia ser utilizada para alimentar cartões SAM falsos contendo acelerômetros e possíveis circuitos auxiliares de comunicação. Como consequência, o ataque poderia se tornar não invasivo e não detectável no terminal, sem uso de fios e baterias aparentes.

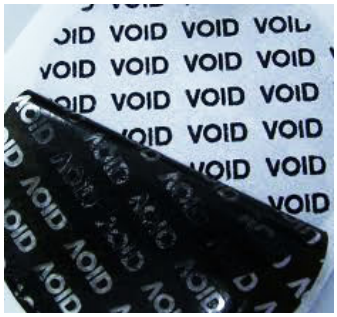

Figura 1.4: Exemplo de selo de detecção de violação utilizado para evidenciar a abertura de equipamentos.

Capítulo 2

Classificação de Sinais Unidimensionais - Abordagem Adotada

2.1 Introdução

Uma mesma pessoa pode apertar uma tecla de várias formas diversas, com maior ou menor intensidade, maior ou menor permanência da pressão na tecla, variação nas componentes de força dadas pelo ângulo do dedo relativo ao teclado etc. Por outro lado, mesmo que ela se esforce para pressionar uma tecla de modo semelhante, a vibração gerada no equipamento pode ainda ser bem variada, como podemos observar na Figura 2.1.

Um outro elemento complicador de uma possível modelagem é o fato de o sistema ser perturbado em posições físicas distintas, correspondentes às diferentes teclas. Observamos ainda que vibrações aparentemente espúrias ocorrem no teclar de algumas teclas específicas, devido à oscilação de partes internas do terminal, que ressonam na presença de energia naquela vizinhança. Este fenômeno não ocorre em todos os pressionamentos, mas em situações em que a pressão exercida ultrapassa algum limiar.

Dada a extensa variabilidade de fenômenos existentes no sistema, optamos por não adotar a abordagem de identificação paramétrica, mas sim, abordamos o problema como um caso de classificação de padrões via aprendizado de máquina.

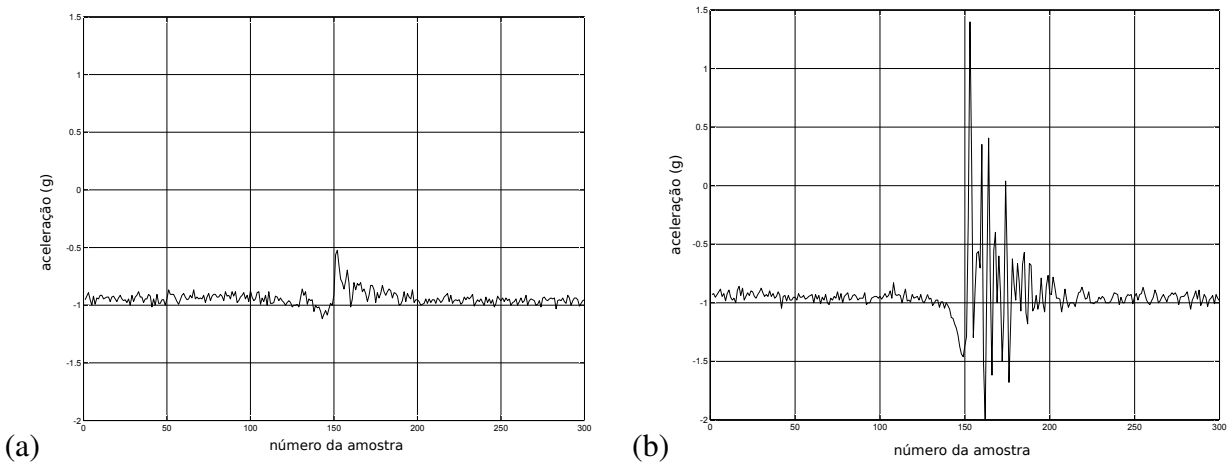

Figura 2.1: Dois pressionamentos da mesma tecla pela mesma pessoa podem ser bem diferentes. No gráfico, a aceleração da componente $\vec{z}$ de um acelerômetro para a tecla "0".

Deste modo, em lugar de uma identificação paramétrica, foram extraídas características do sistema, ou seja, características consideradas relevantes em um processo de aprendizado/discriminação. As características aqui escolhidas não caracterizam variáveis do sistema como um todo, conforme observado em [2] que utiliza espectro de frequência da emissão audível de pressionamentos, ou alguma representação deste, como cepstrum. Também não consideramos o uso de coeficientes de autoregressão, coeficientes de decomposição wavelet etc., pois assim estaríamos no âmbito da representação paramétrica (1º caso) ou espectral (2º caso), e não entendemos aí capacidade de discriminação das teclas, pela vibração gerada. Isto é, entendemos ser uma suposição demasiado forte – incorrendo em possível perda de generalização – a de que as teclas possuam respostas em frequência distintas a ponto de poderem ser caracterizadas por isso. Ademais, bastaria uma alteração em algum componente comum ao sistema (a borracha das teclas, a espessura da placa de circuitos, por exemplo) para que todo o espectro de frequências de vibração mecânica se deslocasse completamente.

Dadas tais suposições, o que se procurou aqui foi tentar obter características que explorassem dependências mútuas entre os sinais de aceleração, como o atraso relativo na propagação destes, muito mais dependente das posições das teclas e acelerômetros do que da frequência de resposta do sistema, de caráter geral. Para isso, as características foram computadas utilizando-se correlações cruzadas e correlações cruzadas

normalizadas pelas variâncias, projetadas de forma a descrever dependências mútuas entre os sinais, estes analisados sempre aos pares.

É importante frisar que, embora consideremos a adoção de características superior neste caso em termos de generalização comparado à análise espectral e paramétrica, os experimentos não foram testados em vários dispositivos, i.e., o equipamento em que o sistema foi treinado é o mesmo em que foi testado.

2.2 Notações

Seja v_i, $0 \leq i < N$, a série temporal de N valores de aceleração adquiridos de um eixo de um acelerômetro, com um período de amostragem fixo T. O valor médio de v é denotado por $\bar{v}$. O vetor de média nula $\tilde{v}$ é definido como $\tilde{v}_i = v_i - \bar{v}$. Utilizamos apenas valores de aceleração com extração da média pois nessa análise não nos interessa a contribuição da aceleração estática da gravidade.

O produto escalar entre os vetores de média nula $\tilde{v}$ e $\tilde{w}$ é:

$$\tilde{v} \cdot \tilde{w} = \sum_{i=0}^{N-1} \tilde{v_i} \tilde{w_i} \tag{2.1}$$

O produto escalar está diretamente relacionado ao cosseno do ângulo entre ambos vetores e pode ser utilizado como medida de "similaridade" dos dois sinais. Ele é invariante a *bias* (porque ambos os vetores são de média nula) mas não é invariante à amplitude (ele é diretamente proporcional à magnitude dos dois vetores).

Suponhamos que os valores de aceleração obtidos quando uma pessoa pressiona a mesma tecla com diferente pressão difiram apenas em amplitude. Neste caso, seria muito desejável o uso de características invariantes à amplitude. O produto escalar torna-se invariante à *bias* e amplitude se o dividirmos pelas normas dos dois vetores, obtendo o coeficiente de correlação:

$$corr(\tilde{v}, \tilde{w}) = \frac{\tilde{v} \cdot \tilde{w}}{\|\tilde{v}\| \|\tilde{w}\|} \tag{2.2}$$

Tal suposição (a energia de um pressionamento altera apenas a amplitude da vibração) é somente parcialmente verdadeira, como pode ser visto na Figura 2.1. Desta

forma, utilizamos ambos, produto escalar e coeficiente de correlação na tentativa de criar características relevantes para a identificação das teclas.

Suponha que a vibração gerada por um pressionamento demore n_1 períodos de amostragem até alcançar o acelerômetro A_1 e demore n_2 períodos para alcançar o acelerômetro A_2. Neste caso, observaremos um pico no produto escalar (ou correlação) entre os valores de aceleração obtidos por A_1 e aqueles obtidos por A_2, quando o último for deslocado para a direita de $n_1 - n_2$ posições, caracterizando a tecla pressionada. As características abaixo foram projetadas para detectar correlações sobre deslocamentos dos sinais.

A correlação cruzada (CC) entre $\tilde{v}$ e $\tilde{w}$ é um vetor cujos elementos são os produtos escalares calculados entre vetores deslocados, ignorando-se os elementos que não possuem o par correspondente:

$$(\tilde{v} * \tilde{w})_n = \begin{cases} \sum_{i=0}^{N-n-1} \tilde{v}_i \tilde{w}_{n+i}, & 0 \leq n < N \quad (2.3) \\ (\tilde{w} * \tilde{v})_{-n}, & -N < n < 0 \quad (2.4) \end{cases}$$

Note que $(\tilde{v} * \tilde{w})_0 = \tilde{v} \cdot \tilde{w}$.

Similarmente, a correlação cruzada normalizada (NCC) é um vetor cujos elementos são coeficientes de correlação calculados entre vetores deslocados, ignorando-se os elementos que não possuem o par correspondente:

$$(\tilde{v} \otimes \tilde{w})_n = \begin{cases} \dfrac{\sum_{i=0}^{N-n-1} \tilde{v}_i \tilde{w}_{n+i}}{\sqrt{\sum_{i=0}^{N-n-1} \tilde{v}_i^2 \sum_{i=0}^{N-n-1} \tilde{w}_{n+i}^2}}, & 0 \leq n < N \quad (2.5) \\ (\tilde{w} \otimes \tilde{v})_{-n}, & -N < n < 0 \quad (2.6) \end{cases}$$

De forma análoga, $(\tilde{v} \otimes \tilde{w})_0 = corr(\tilde{v}, \tilde{w})$. A correlação cruzada normalizada tem sido utilizada há bastante tempo em visão computacional para encontrar modelos padrão em imagens, em uma operação denominada *template matching* [20].

Denotemos o vetor coluna com $2M + 1$ elementos centrais de CC como:

$$(\tilde{v} * \tilde{w})^M = \begin{bmatrix} (\tilde{v} * \tilde{w})_{-M} \\ (\tilde{v} * \tilde{w})_{-M+1} \\ \dots \\ (\tilde{v} * \tilde{w})_{M-1} \\ (\tilde{v} * \tilde{w})_{M} \end{bmatrix} \tag{2.7}$$

Similarmente, denotemos o vetor coluna com $2M + 1$ elementos centrais de NCC como:

$$(\tilde{v} \otimes \tilde{w})^M = \begin{bmatrix} (\tilde{v} \otimes \tilde{w})_{-M} \\ (\tilde{v} \otimes \tilde{w})_{-M+1} \\ \dots \\ (\tilde{v} \otimes \tilde{w})_{M-1} \\ (\tilde{v} \otimes \tilde{w})_{M} \end{bmatrix}. \tag{2.8}$$

Como será descrito nas seções relativas aos experimentos, no caso ATM, utilizamos três acelerômetros e tomamos apenas amostras do eixo $\vec{z}$ de cada sensor, obtendo três sinais. Deste modo, um pressionamento é representado por três vetores coluna, cada um contendo 300 valores de aceleração:

$$\mathbf{V_{ATM}} = (\mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3) \tag{2.9}$$

Nos experimentos com PIN-pad, utilizamos dois acelerômetros e tomamos amostras dos três eixos de cada sensor. Assim, um pressionamento é representado por seis vetores coluna, cada um contendo 300 amostras de aceleração:

$$\mathbf{V_{PIN}} = (\mathbf{x}_1, \mathbf{y}_1, \mathbf{z}_1, \mathbf{x}_2, \mathbf{y}_2, \mathbf{z}_2) \tag{2.10}$$

onde $\mathbf{x}_1$ corresponde aos valores de aceleração do eixo $\vec{x}$ do sensor 1 e assim por diante.

2.3 Características

Algumas das características (ou *features*) listadas abaixo são aplicáveis a todos os experimentos, algumas a um experimento específico.

2.3.1 $\mathbf{cc_{same}}$

O vetor de características $\mathbf{cc_{same}}$ é formado pelo conjunto de $2M + 1$ elementos centrais das correlações cruzadas de pares de vetores de aceleração de mesma coordenada física, tendo a média subtraída, para algum $M \geq 0$, isto é:

$$\mathbf{cc}_{\mathbf{same}}^{\mathbf{ATM}} = \begin{bmatrix} (\tilde{z}_1 * \tilde{z}_2)^M & (\tilde{z}_2 * \tilde{z}_3)^M & (\tilde{z}_1 * \tilde{z}_3)^M \end{bmatrix} \tag{2.11}$$

$$\mathbf{cc}_{\mathbf{same}}^{\mathbf{PIN}} = \begin{bmatrix} (\tilde{x}_1 * \tilde{x}_2)^M & (\tilde{y}_1 * \tilde{y}_2)^M & (\tilde{z}_1 * \tilde{z}_2)^M \end{bmatrix} \tag{2.12}$$

A motivação do uso de produtos escalares de vetores de mesma coordenada física é a de que sensores distintos iriam adquirir vibrações similares mas com atrasos distintos. Essa distinção de atrasos iria auxiliar na discriminação da tecla pressionada.

2.3.2 $\mathbf{cc_{comb}}$

O vetor de características $\mathbf{cc_{comb}}$ é o conjunto de $2M + 1$ elementos centrais das correlações cruzadas de todas as combinações 2 a 2 dos vetores de média extraída. Ele possui $15 \times (2M + 1)$ elementos nos experimentos com PIN-pad. Esta característica não é utilizada nos experimentos com ATM porque $\mathbf{cc}_{\mathbf{comb}}^{\mathbf{ATM}} = \mathbf{cc}_{\mathbf{same}}^{\mathbf{ATM}}$. Aqui utilizamos correlações entre eixos de diferentes coordenadas físicas, inclusive, esperando que, ao prover mais informação ao sistema, o aprendizado de máquina possa aproveitar e generalizar as relações de tridimensionalidade presentes no movimento. Assim como $\mathbf{cc_{same}}$, esta característica não é normalizada, ou seja, a informação de amplitude dos pressionamentos é aqui considerada.

2.3.3 $\mathbf{ncc_{same}}$

O vetor de características $\mathbf{ncc_{same}}$ é obtido substituindo-se as correlações cruzadas $*$ em $\mathbf{cc_{same}}$ por correlações normalizadas $\otimes$. Correlações cruzadas normalizadas são invariantes à *bias* e amplitude, desconsiderando a amplitude das vibrações.

2.3.4 $\mathbf{ncc_{comb}}$

O vetor de características $\mathbf{ncc_{comb}}$ é obtido substituindo-se as correlações cruzadas $*$ em $\mathbf{cc_{comb}}$ por correlações normalizadas $\otimes$. Esta característica não é utilizada no experimento ATM porque $\mathbf{ncc_{comb}^{ATM}} = \mathbf{ncc_{same}^{ATM}}$.

2.3.5 Esquemas de Classificação

Em todos os experimentos, os mesmos dados foram utilizados em três "esquemas" distintos. O primeiro esquema consiste em agrupar o pressionamento pela linha da tecla, o segundo pela sua coluna e o terceiro esquema em identificar a tecla diretamente por seu rótulo. Por exemplo, a tecla "6" recebeu o rótulo "2" no esquema linhas pois está localizada na segunda linha; "3" no esquema colunas pois está localizada na terceira coluna, e "6" no esquema teclas. No experimento ATM, 9 teclas são distribuídas em 3 linhas e 3 colunas (Figura 3.1) e nos experimentos PIN-pad, 12 teclas distribuídas em 4 linhas e 3 colunas foram utilizadas (Figura 4.1). A separação em esquemas linha e coluna se mostrou bastante útil pois possibilita a identificação de um dos aspectos limitantes no reconhecimento das teclas. Dado que a média de acerto no reconhecimento de uma tecla é aproximadamente o produto entre as médias de acertos de linhas e de colunas, tal decomposição indica a deficiência no reconhecimento, se na identificação de linhas ou de colunas.

2.4 Algoritmos de Aprendizado de Máquina

Utilizamos três algoritmos de aprendizado de máquina: Perceptron Multicamadas (MLP), Árvores Aleatórias (RT) e Máquina de Vetores de Suporte (SVM). Nos três casos, usamos implementações providas pela biblioteca C++ OpenCV [21, 22]. Nenhuma

técnica de redução de dimensão de características foi adotada, i.e., não foi utilizado nenhum algoritmo de seleção de variáveis do conjunto de características considerados mais relevantes segundo algum critério.

2.4.1 Perceptron Multicamadas (Multilayer Perceptron)

A configuração do MLP [23] foi composta de uma camada de entrada (as próprias características), duas camadas ocultas de 30 neurônios cada e uma camada de saída. O número de neurônios da camada de saída varia de acordo com o esquema/experimento. Para o esquema de colunas, é igual a 3 para ATM e PIN-pad; para linhas, é igual a 3 para ATM ou 4 para PIN-pad. Para o esquema de teclas, é 9 para ATM ou 12 para PIN-pad. O algoritmo de aprendizado utilizado foi o *error back propagation*. Nenhuma otimização de arquitetura foi efetuada, sendo que a quantidade de neurônios e camadas ocultas foram escolhidas *ad-hoc*.

2.4.2 Árvores Aleatórias (Random Trees)

Árvores aleatórias (algoritmo também conhecido como "florestas aleatórias") é um algoritmo baseado em uma floresta de árvores de decisão [24]. Uma de suas características interessantes é a de poder operar com características de faixa dinâmicas bastante distintas sem a necessidade de normalização.

2.4.3 Máquina de Vetores de Suporte (Support Vector Machine)

Utilizamos SVM com função de base radial (RBF) [25, 26]. Optamos por deixar a implementação OpenCV escolher automaticamente os parâmetros ótimos. Antes de efetuar o treino e teste, as características foram normalizadas na faixa $[-1, +1]$.

Capítulo 3

Experimentos Realizados com Teclado Genérico (ATM)

3.1 Montagem Experimental

Para a abordagem proposta, três acelerômetros foram posicionados em uma placa acrílica em que o teclado também é fixado (Figura 3.1). A fixação é feita mediante o uso de quatro postes metálicos, mantendo o teclado elevado e tendo como contato mecânico com a base apenas estes quatro pontos, por meio dos quais a vibração gerada pelo ato de teclar é transmitida à placa acrílica, na qual quatro pés de borracha foram aplicados nos vértices.

3.2 Acelerômetros e Sistema de Aquisição

Os acelerômetros utilizados são Freescale MMA7260QT, analógicos, do tipo MEMS (*Microelectromechanical Systems*) [27], com sensibilidade ajustável eletronicamente para $\pm$1,5g, $\pm$2g, $\pm$4g e $\pm$6g. Experimentalmente verificamos que a sensibilidade de $\pm$1,5g (800mV/g) é suficiente e a mais adequada para a intensidade de vibrações que serão medidas.

O hardware utilizado para a aquisição e conversão analógico-digital dos sinais dos sensores é um kit de desenvolvimento de software básico, equipado com um microcontrolador LPC2148 de arquitetura ARM7, cujos conversores A/D internos possuem

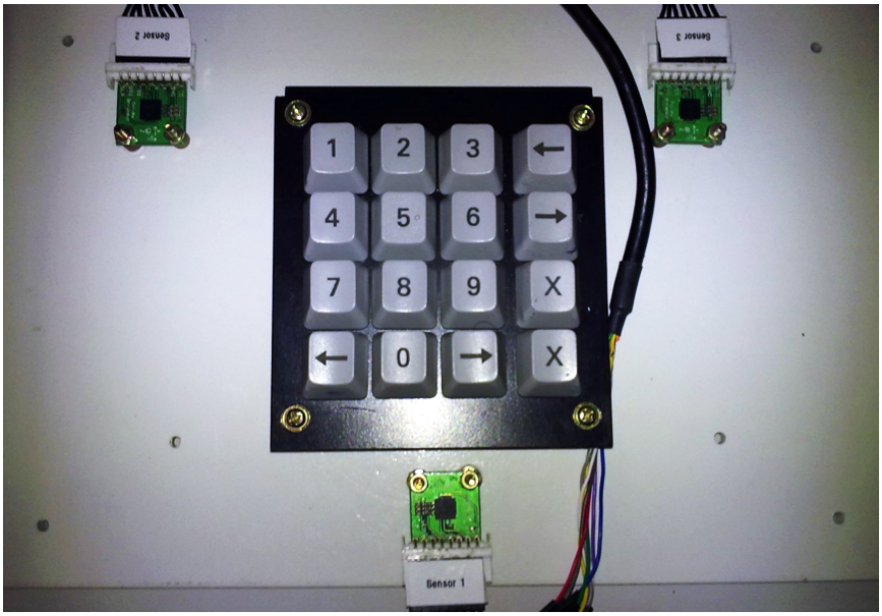

Figura 3.1: Montagem do teclado e disposição e posicionamento dos acelerômetros. A base é uma placa acrílica com 5mm de espessura.

resolução de 10bits.

O software de aquisição foi desenvolvido para trabalhar na frequência de amostragem de 6,666kHz, que se mostrou adequada para amostrar sinais com duração média de 10ms e frequência máxima de 500Hz. Além dos conversores A/D internos, foi utilizada a UART (*Universal Asynchronous Receiver/Transmitter*) do microcontrolador para enviar os dados das amostras pela interface serial no padrão RS232 à uma taxa de 115.200 bits por segundo.

Por questões de simplificação do modelo e limitação do canal de comunicação serial, somente o eixo $\vec{z}$, normal ao pressionamento das teclas, foi amostrado. Foi desenvolvido um software que, ao detectar um evento de pressionamento de tecla, uma janela de 300 amostras de cada sensor é coletada, sendo que são armazenadas 50 amostras anteriores ao evento e outras 250 após. Na frequência de trabalho definida, essa janela de amostragem corresponde a aproximadamente 45ms (Figura 3.2).

A detecção do evento de pressionamento é feita pela análise da magnitude do sinal medido por cada um dos sensores. Uma variação, em módulo, superior a 10% do valor médio calculado durante o repouso do teclado (momento sem nenhum pressionamento de tecla), em qualquer um dos três sensores, corresponde ao evento de início de pressionamento.

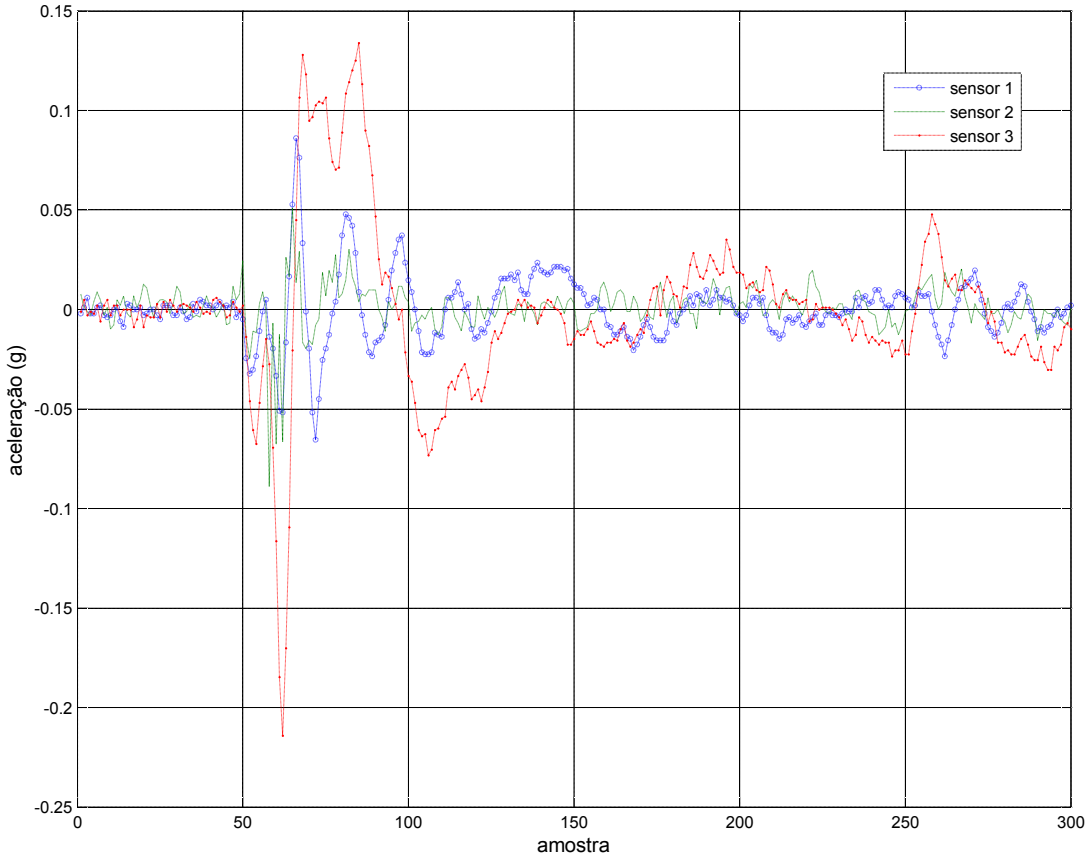

Figura 3.2: Exemplo de amostra da aquisição da tecla "1". Apenas o eixo $\vec{z}$ foi utilizado.

3.3 Obtenção das Amostras

De modo a capturar diferentes formas de teclar cada uma das teclas, o processo de amostragem envolveu cinco pessoas, cada uma pressionando 10 vezes cada uma das teclas da matriz 3×3 que corresponde às teclas de 1 a 9 do teclado utilizado no experimento (Figura 3.1). Notou-se durante o processo de coleta das amostras que cada pessoa possui uma maneira diferente de teclar, que envolve variações na intensidade e na posição de toque na tecla. Dos aproximadamente 450 pressionamentos, 80% foi reservado para treino e 20% para teste.

3.4 Características Utilizadas

As características utilizadas para o experimento ATM foram $\mathbf{cc_{same}}$ e $\mathbf{ncc_{same}}$, com valores de M variáveis.

		Esquema Linhas			Esquema Colunas			Esquema Teclas		
Característica	Dim	MLP	RT	SVM	MLP	RT	SVM	MLP	RT	SVM
$\mathbf{cc_{same}}$	45	100,0	96,7	100,0	97,9	90,4	97,7	95,0	86,1	96,1
	63	100,0	97,9	100,0	97,9	91,7	94,1	95,1	89,3	97,2
$\mathbf{ncc_{same}}$	45	100,0	97,8	100,0	97,9	89,2	97,0	96,9	86,2	97,0
	63	100,0	98,9	100,0	98,3	90,3	97,0	97,3	88,7	99,3

Tabela 3.1: Taxas de reconhecimento em % obtidas no experimento ATM.

3.5 Resultados Experimentais

A Tabela 3.1 apresenta as taxas de acerto de reconhecimento para o experimento ATM para os três esquemas, linhas, colunas e teclas. Os melhores resultados encontram-se destacados. Para o reconhecimento de linhas, todas as características utilizadas forneceram taxas de acerto de 100% para os classificadores MLP e SVM. Já para colunas, a característica $\mathbf{ncc_{same}}$ superou as demais, embora na média as outras também forneceram valores bastante elevados. Note que o esquema "linhas" atinge melhores taxas de reconhecimento do que o esquema "colunas". O oposto será observado nos experimentos com PIN-pad. Este fato pode ser explicado considerando-se que a base do experimento ATM é maior na largura (x) do que na profundidade (y), como pode ser visto na Figura 3.3. Deste modo, o momento de inércia com relação ao eixo $\vec{x}$ é menor que o momento com relação ao eixo $\vec{y}$. Consequentemente, é mais fácil balançar ou rotacionar o equipamento ao redor de $\vec{x}$ do que $\vec{y}$.

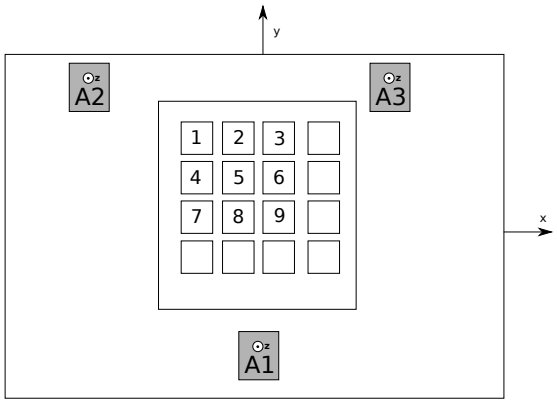

Figura 3.3: O momento de inércia do sistema ao redor de $\vec{x}$ é menor do que ao redor de $\vec{y}$, facilitando o reconhecimento de linhas.

Capítulo 4

Experimentos Realizados com Terminal POS (PIN-pad)

4.1 Montagem Experimental

A abordagem aqui adotada poderia ser aplicada a praticamente qualquer terminal POS que possua teclado mecânico em seu corpo. A matriz de teclas do equipamento utilizado é padrão, como pode ser observada na Figura 4.1. As placas dos acelerômetros foram envolvidas em um pedaço de espaguete termo retrátil e coladas nas posições da Figura 4.2.

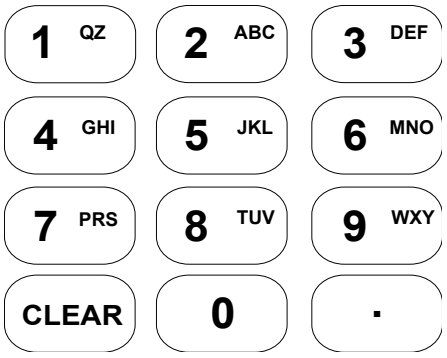

Figura 4.1: Layout do teclado do terminal POS utilizado.

Os acelerômetros não possuem qualquer conexão elétrica com o terminal, sendo que no protótipo foram utilizados cabos de conexão ligando os sensores ao sistema de aquisição. Após acondicionados os sensores e os cabos, a tampa original foi recolocada

no terminal.

Dois experimentos foram realizados com o terminal PIN-pad, aqui denominados de PIN-pad I e PIN-pad II. Os acelerômetros utilizados em ambos os experimentos são distintos, dentre outras características que serão descritas nas seções correspondentes.

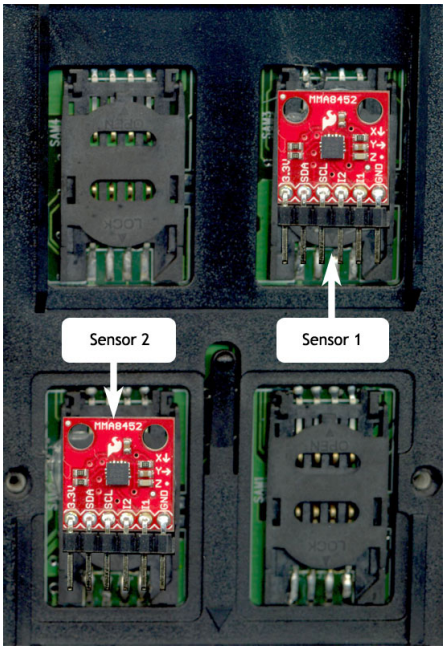

Figura 4.2: Vista da parte inferior do terminal, sem a tampa de acesso aos conectores SAM, com a disposição dos acelerômetros utilizados.

4.2 Experimento PIN-pad I

4.2.1 Acelerômetros e Sistema de Aquisição

Os acelerômetros utilizados são MMA8452, digitais, de 12 bits e três eixos, da família Freescale Xtrinsic [28]. O sistema de aquisição foi desenvolvido na plataforma Arduino Mega 2560 [29], como mostra a Figura 4.3. A comunicação entre o sensor e o Arduino é feita via barramento I^2C [30], utilizando-se conversores de nível. A escala de aceleração adequada foi $\pm 2g$ e a taxa de amostragem adotada foi a máxima para o acelerômetro, 800 amostras/s. Utilizamos as informações de aceleração nos três eixos. Para cada pressionamento de tecla, foram coletadas 300 amostras, para os três eixos dos dois sensores, totalizando 1800 elementos por pressionamento.

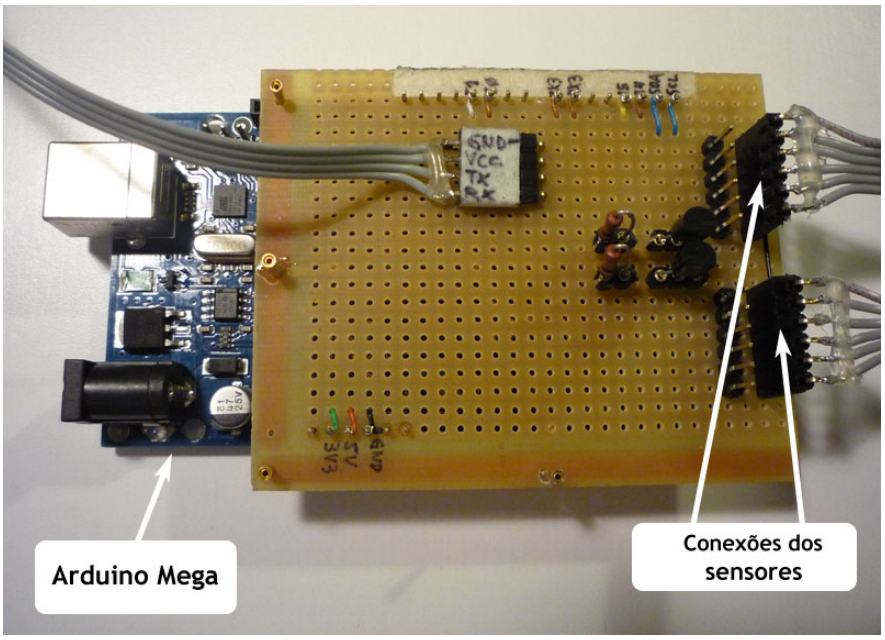

Figura 4.3: Uma placa da plataforma aberta Arduino foi utilizada como sistema de aquisição. Para acomodar circuitos auxiliares e conectores para os acelerômetros, uma placa suplementar foi montada sobre o Arduino. Para a conversão de níveis (5V$\leftrightarrow$3.3V) do barramento I^2C, dois transistores MOSFET foram utilizados

4.2.2 Obtenção das Amostras

De modo a capturar diferentes formas de teclar cada uma das teclas, o processo de obtenção das amostras envolveu duas pessoas em cinco sessões de tomada de pressionamentos. Cada sessão foi composta pelo pressionamento de 40 vezes cada uma das 12 teclas da matriz 4×3 da Figura 4.1.

Um dos testadores executou três sessões e o outro duas sessões. No total, foram adquiridos 2400 pressionamentos, 200 para cada tecla. Durante o processo de coleta das amostras, notamos que cada pessoa possui uma maneira distinta de teclar, envolvendo variações na intensidade, na posição e na permanência do dedo sobre a tecla. Um programa MATLAB foi desenvolvido para a leitura das amostras do sistema de aquisição. Em todas as sessões, o terminal ficou em repouso sobre uma mesa. As amostras foram tomadas sempre com o terminal desligado, pois o fator em análise é a vibração mecânica do mesmo, sendo indiferente o equipamento estar ou não energizado.

Utilizamos os dados de 4 sessões das 5 para treino. Os dados da sessão excluída do treinamento foram utilizados para teste. O procedimento é repetido excluindo-se uma sessão de cada vez e treinando com as 4 restantes. Os resultados apresentados na

Característica	Dim	Esquema Linhas			Esquema Colunas			Esquema Teclas		
		MLP	RT	SVM	MLP	RT	SVM	MLP	RT	SVM
$\mathbf{cc_{same}}$	45	34,7	35,8	35,4	64,1	68,4	55,2	24,3	25,5	21,2
	63	35,3	36,7	30,3	64,4	69,2	56,9	25,3	25,7	21,9
$\mathbf{cc_{comb}}$	45	40,3	42,3	36,8	78,9	79,6	78,1	36,0	35,5	36,1
	75	39,5	42,4	36,8	79,9	80,9	81,1	36,6	37,0	39,0
$\mathbf{ncc_{same}}$	45	33,8	34,7	37,2	64,3	66,8	70,5	24,4	25,1	30,1
	63	32,1	36,4	37,8	64,1	66,9	72,5	24,5	26,5	30,2
$\mathbf{ncc_{comb}}$	45	38,4	42,7	44,5	78,6	80,9	81,6	34,3	36,6	38,5
	75	40,0	44,4	46,5	80,7	83,1	84,2	37,2	38,5	42,1

Tabela 4.1: Taxas de reconhecimento em % obtidas no experimento PIN-pad I, modo "mesa".

tabela correspondem às médias dos 5 resultados de teste.

4.2.3 Características Utilizadas

Para o experimento PIN-pad I, foram utilizadas as características $\mathbf{cc_{same}}$, $\mathbf{ncc_{same}}$, $\mathbf{cc_{comb}}$ e $\mathbf{ncc_{comb}}$, com valores de M variáveis.

4.2.4 Resultados Experimentais

A Tabela 4.1 apresenta as taxas de acerto de reconhecimento para o experimento. Neste caso, diferentemente do experimento ATM, as taxas de reconhecimento de colunas é muito maior do que a de linhas. Em todos os esquemas, a combinação da característica $\mathbf{ncc_{comb}}$ de dimensão 75 com o classificador SVM produziu as melhores taxas de acerto, com 46,5%, 84,2% e 42,1% para os esquemas linhas, colunas e teclas, respectivamente. A taxa de acerto de 42,1% é extremamente baixa comparada com 99,3% obtida no experimento ATM. Assim, um novo experimento foi conduzido, o "Experimento PIN-pad II", descrito na próxima seção, de modo a tentar obter maiores taxas de reconhecimento.

4.3 Experimento PIN-pad II

4.3.1 Acelerômetros e Sistema de Aquisição

A montagem do experimento PIN-pad II é muito similar à montagem do experimento PIN-pad I. No entanto, utilizamos um modelo distinto de acelerômetros: Analog Devices ADXL345, com 10 bits de resolução, três eixos e taxas de amostragem máxima de 3200 amostras/s [31]. Tal acelerômetro possui um barramento de dados com maior *throughput*, o *Serial Peripheral Output* (SPI), exigindo um esquema de conversão de níveis adicional, como pode ser visto na Figura 4.4. Escolhemos esse modelo pois consideramos que a baixa taxa de amostragem do experimento anterior (800 amostras/s em comparação a 6700 amostra/s no experimento ATM) poderia ser responsável pelas baixas taxas de acerto daquele experimento. Deste modo, utilizamos a maior taxa disponível pelos novos acelerômetros, 3200 amostras/s, quatro vezes maior que a do experimento PIN-pad I. Como no experimento anterior, utilizamos as informações de aceleração nos três eixos.

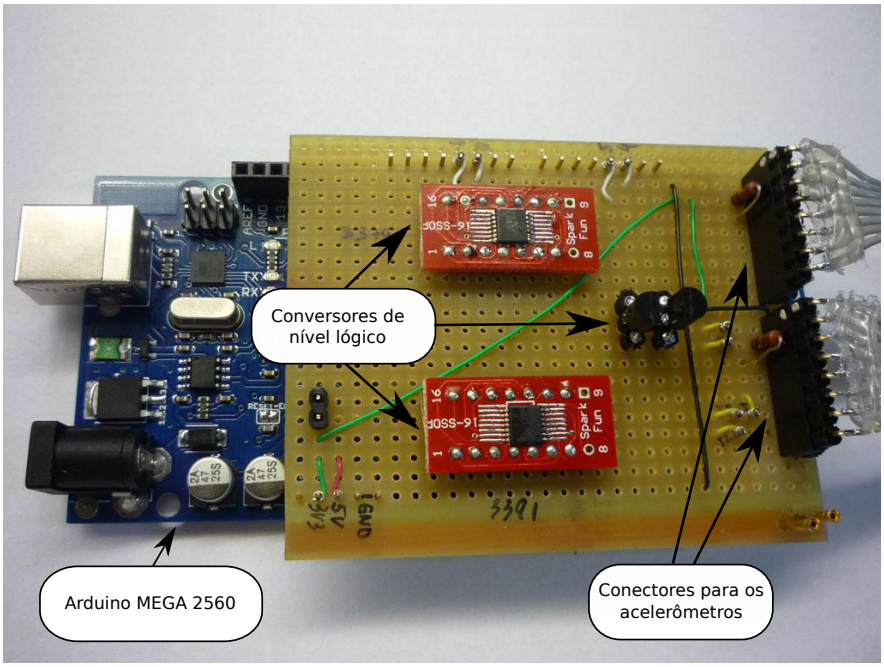

Figura 4.4: Uma placa da plataforma aberta Arduino foi utilizada como sistema de aquisição. Para acomodar circuitos auxiliares e conectores para os acelerômetros, uma placa suplementar foi montada sobre o Arduino. Um circuito de conversões de nível (5V↔3.3V) com maior *throughput* (MAX3391) foi utilizado para o barramento SPI

4.3.2 Obtenção das Amostras

Foram adquiridos pressionamentos de 5 pessoas, cada uma participando de duas sessões. Na primeira sessão, a pessoa pressiona as teclas com o PIN-pad em repouso em uma superfície rígida ("modo mesa"). Na segunda sessão, a pessoa pressiona as teclas segurando o terminal com uma das mãos ("modo mão").

Cada sessão foi composta de 40 pressionamentos para cada uma das 12 teclas do terminal cujo teclado é esboçado na Figura 4.1. Um total de 4800 presionamentos foi adquirido (5 pessoas $\times$ 2 sessões $\times$ 12 teclas $\times$ 40 pressionamentos). Para cada pressionamento, 300 valores de aceleração dos três eixos de ambos os sensores foram adquiridos, totalizando 1800 amostras. Utilizamos os dados da sessão 1 ("modo mesa") independentemente dos dados da sessão 2 ("modo mão").

Utilizamos os dados de 4 pessoas das 5 para treino. Os dados da pessoa que foram excluídos do treinamento são utilizados para teste. O procedimento é repetido separando-se para teste os dados de uma pessoa de cada vez e treinando-se com os dados das 4 restantes. Os resultados apresentados nas tabelas correspondem às médias dos 5 resultados de teste.

4.3.3 Características Utilizadas

Para o experimento PIN-pad II, foram utilizadas as características $\mathbf{cc_{same}}$, $\mathbf{ncc_{same}}$, $\mathbf{cc_{comb}}$ e $\mathbf{ncc_{comb}}$, com valores de M variáveis.

4.3.4 Alinhamento das Amostras

Observamos que as taxas de amostragem dos dois acelerômetros eram ligeiramente distintas, dado que os acelerômetros digitais possuem relógios internos independentes. Outro problema observado é que o sistema de aquisição alterna sequencialmente as leituras das amostras entre os sensores, isto é, amostras dos dois sensores não são adquiridas "simultaneamente" (com atraso negligenciável comparando-se ao período de amostragem), causando um desalinhamento temporal nos dados adquiridos.

A Figura 4.5 apresenta os intervalos de amostragem dos dois sensores para a aquisição de um pressionamento (300 amostras). A média para o sensor 1 é $\approx 312\mu$s ($\approx$3208

amostras/s) e para o sensor 2 é ≈310μs (≈3228 amostras/s).

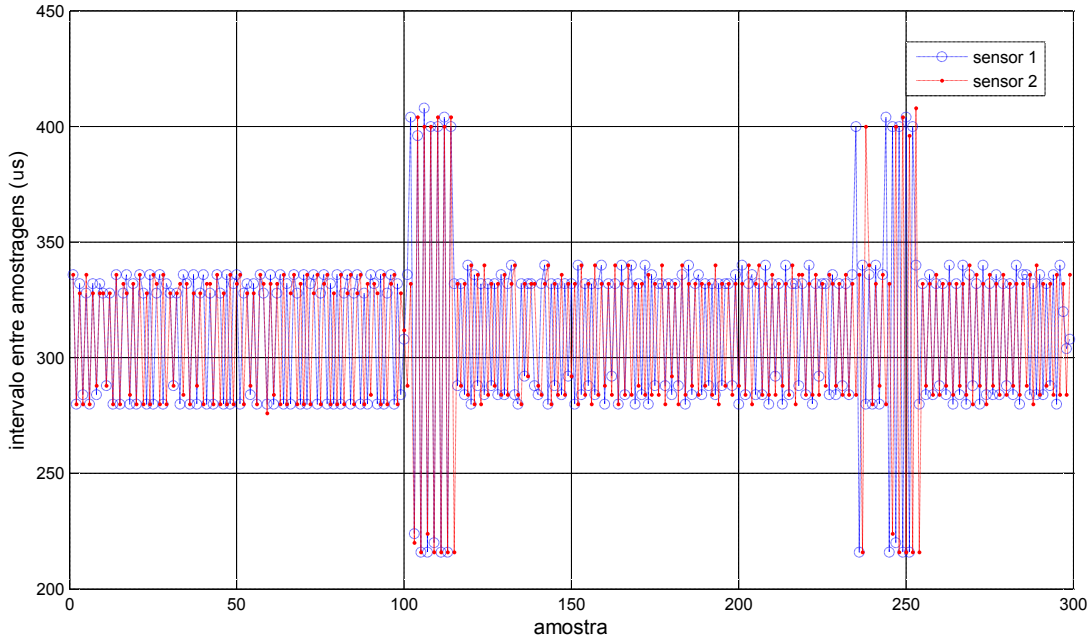

Figura 4.5: Os intervalos de amostragem dos dois sensores para a aquisição de um pressionamento é bastante irregular e somente na média é proxima ao valor nominal.

A Figura 4.6 apresenta o histograma dos intervalos de amostragem para um conjunto inteiro de aquisições. Observamos que o intervalo entre amostragens do sistema torna-se bastante irregular, variando de ≈200μs a ≈400μs.

Assim, de forma a minimizar estes problemas de sincronização, armazenamos juntamente às amostras de aceleração o *timestamp* do momento em que a amostra foi adquirida, com a precisão permitida pelo sistema de aquisição de 4μs. Utilizando-se a informação do instante das amostras, uma interpolação *spline* cúbica foi efetuada nos dados de modo a obter uma aproximação dos valores de amostras para uma sequência de intervalos regulares de tempo. Os valores de reconhecimento foram comparados para os casos sem alinhamento temporal e com alinhamento temporal.

4.3.5 Resultados Experimentais

Modo MESA

A Tabela 4.2 apresenta as taxas de reconhecimento com o PIN-pad em repouso sobre uma superfície rígida (“modo mesa”), sem alinhamento temporal das amostras. As

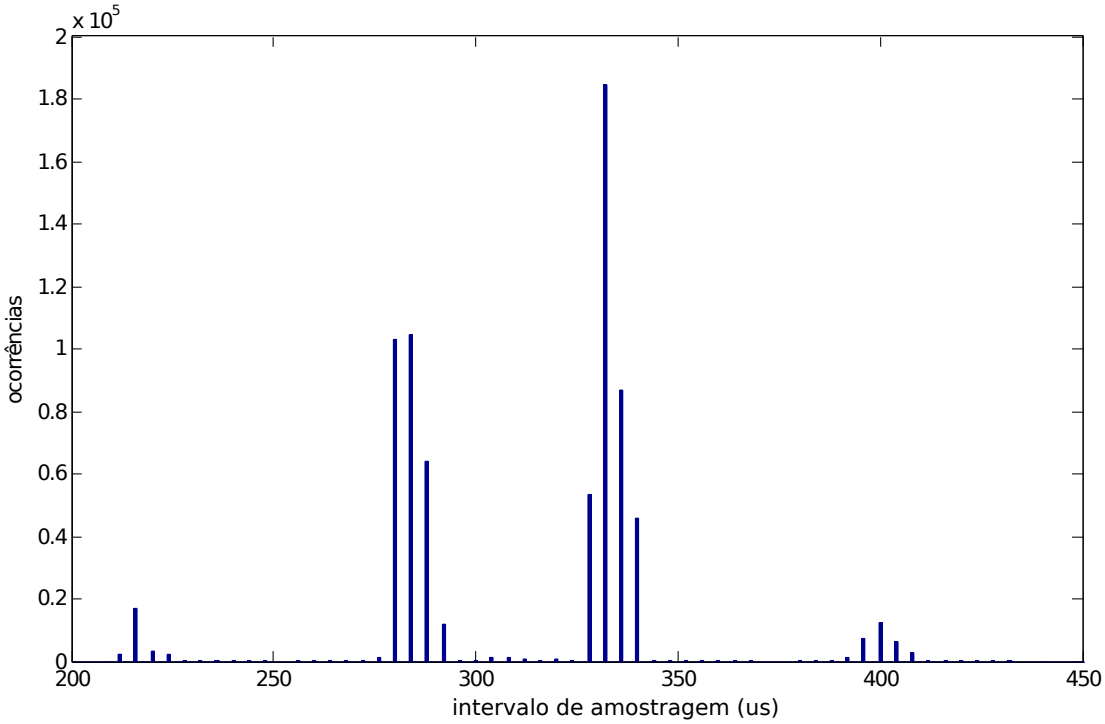

Figura 4.6: Distribuição das ocorrências de intervalos de aquisição de um dos sensores. A maior ocorrência se dá em 332μs (aproximadamente 3012 amostras/s) quando a frequência nominal de trabalho é de 3200 amostras/s ($\approx$312μs.)

taxas de reconhecimento são significativamente maiores do que aquelas obtidas no experimento PIN-pad I (Tabela 4.1), provavelmente devido ao aumento da taxa de amostragem (3200 amostras/s em vez de 800 amostra/s). A melhor taxa de acertos de teclas aumentou de 42,1% (Tabela 4.1) para 63,4% (Tabela 4.2). Assim como no experimento PIN-pad I, a característica $\mathbf{ncc_{comb}}$ com dimensão 75 combinada com o classificador SVM atingiu as melhores taxas de acerto em todos os três esquemas.

A Tabela 4.3 apresenta as taxas de acerto para os mesmos dados submetido ao processo de alinhamento temporal das amostras. As taxas de acerto aumentaram ainda mais. Com alinhamento, a melhor taxa de reconhecimento de teclas foi 68,8%.

A característica $\mathbf{ncc_{comb}}$ com dimensão 75 combinada ao classificador SVM obteve uma das mais altas taxas de acerto em todos os três esquemas.

Característica	Dim	Esquema Linhas			Esquema Colunas			Esquema Teclas		
		MLP	RT	SVM	MLP	RT	SVM	MLP	RT	SVM
$\mathbf{cc_{same}}$	45	53,6	44,5	48,2	79,4	77,5	77,0	51,1	37,7	48,8
	63	56,2	46,4	51,6	80,8	78,7	80,1	50,3	38,7	51,9
$\mathbf{cc_{comb}}$	45	55,8	48,5	51,2	84,5	80,3	80,0	51,8	39,9	52,2
	75	58,7	51,9	56,6	87,8	82,6	83,8	59,2	43,7	57,0
$\mathbf{ncc_{same}}$	45	55,4	50,6	58,0	78,6	75,9	81,9	50,6	44,2	53,5
	63	57,7	52,2	60,8	81,1	78,5	84,1	56,1	45,5	56,7
$\mathbf{ncc_{comb}}$	45	55,4	53,5	59,9	83,7	79,3	85,0	56,1	46,2	55,7
	75	61,4	56,6	63,4	88,0	83,1	88,2	61,0	49,9	63,4

Tabela 4.2: Taxas de reconhecimento em % obtidas no experimento PIN-pad II, modo "mesa" sem alinhamento temporal.

Característica	Dim	Esquema Linhas			Esquema Colunas			Esquema Teclas		
		MLP	RT	SVM	MLP	RT	SVM	MLP	RT	SVM
$\mathbf{cc_{same}}$	45	61,0	51,0	59,4	84,1	80,2	81,0	61,5	44,0	62,8
	63	65,6	53,0	63,9	85,9	80,2	83,4	66,4	45,1	66,1
$\mathbf{cc_{comb}}$	45	62,7	50,6	57,0	86,3	81,2	82,1	59,4	43,3	53,2
	75	65,4	53,4	60,4	89,1	83,6	83,8	64,8	46,9	62,7
$\mathbf{ncc_{same}}$	45	63,4	59,7	66,0	81,7	78,9	85,8	64,2	53,9	65,3
	63	67,0	60,3	68,2	83,7	81,6	87,1	66,5	57,4	66,4
$\mathbf{ncc_{comb}}$	45	62,0	57,5	62,6	83,3	80,9	86,6	61,1	50,3	62,6
	75	66,0	60,5	67,3	89,5	84,8	89,9	68,6	57,5	68,8

Tabela 4.3: Taxas de reconhecimento em % obtidas no experimento PIN-pad II, modo "mesa" com alinhamento temporal.

Modo MÃO

As Tabelas 4.4 e 4.5 apresentam as taxas de acerto com o PIN-pad no modo "mão", sem alinhamento temporal e com alinhamento temporal, respectivamente.

Em geral, as taxas de acerto para o modo "mão" são maiores do que os correspondentes do modo "mesa". Novamente as taxas de acerto com alinhamento de tempo (Tabela 4.5) são maiores do que as correspondentes sem alinhamento (Tabela 4.4). Como era de se esperar, o alinhamento temporal melhora a qualidade dos dados obtidos, sendo assim uma etapa de pré-processamento essencial neste cenário.

A melhor taxa de reconhecimento de todos os experimentos com PIN-pad foi de 75,2%, obtida no modo "mão" com alinhamento temporal, utilizando-se as características $\mathbf{ncc_{same}}$ com dimensão 63 combinada ao classificador MLP (Tabela 4.5).

Levantamos algumas hipóteses para explicar a maior facilidade de reconhecimento no modo "mão". A Figura 4.7 ilustra a estimativa de potência dos sinais de aceleração para os modos "mesa" e "mão" para o eixo $\vec{z}$.

Os gráficos correspondem ao periodograma médio de todos os pressionamentos, para fins de análise qualitativa. É possível observar que para o modo "mão", as maiores energias estão concentradas em regiões de frequência baixa ($\ll$100Hz) ao passo que para o modo "mesa", os picos principais ocorrem na vizinhança de 100Hz. Observamos também que o pico de energia da principal componente ($\vec{z}$) é aproximadamente 3 vezes maior para o modo "mão". Com base nessa observação, é possível concluir que tal faixa de frequências ($\ll$100Hz) traz mais informação sobre o evento de pressionamento. Isto significa que além da vibração de frequência mais alta devida ao

		Esquema Linhas			Esquema Colunas			Esquema Teclas		
Característica	Dim	MLP	RT	SVM	MLP	RT	SVM	MLP	RT	SVM
$\mathbf{cc_{same}}$	45	73,2	61,8	69,5	74,0	72,0	65,3	60,7	43,8	53,5
	63	74,8	61,3	70,8	76,7	75,6	75,4	64,6	46,5	60,0
$\mathbf{cc_{comb}}$	45	61,1	45,3	59,4	87,9	87,8	87,9	58,4	42,4	55,7
	75	67,0	50,9	62,7	86,8	89,0	88,0	65,4	47,0	59,2
$\mathbf{ncc_{same}}$	45	73,9	65,4	73,8	73,3	71,3	74,6	61,6	45,4	59,6
	63	74,9	65,6	72,4	78,8	74,0	77,5	66,0	50,5	63,8
$\mathbf{ncc_{comb}}$	45	60,6	54,7	59,0	88,4	86,6	88,8	60,2	48,6	61,4
	75	69,3	57,9	70,9	88,2	87,5	90,0	66,9	51,9	65,9

Tabela 4.4: Taxas de reconhecimento em % obtidas no experimento PIN-pad II, modo "mão" sem alinhamento temporal.

		Esquema Linhas			Esquema Colunas			Esquema Teclas		
Característica	Dim	MLP	RT	SVM	MLP	RT	SVM	MLP	RT	SVM
$\mathbf{cc_{same}}$	45	82,6	66,6	79,9	75,8	73,2	70,5	69,6	49,2	61,9
	63	82,0	67,0	76,6	81,6	75,1	75,4	72,8	52,3	64,4
$\mathbf{cc_{comb}}$	45	68,3	49,0	63,0	88,3	89,2	89,0	63,1	45,4	58,8
	75	74,7	54,4	69,2	88,6	89,4	88,8	70,8	50,0	66,2
$\mathbf{ncc_{same}}$	45	81,8	71,1	77,6	76,5	72,0	78,0	70,4	51,4	67,2
	63	82,0	71,7	81,1	80,1	75,2	81,1	75,2	55,1	70,5
$\mathbf{ncc_{comb}}$	45	68,1	57,7	65,2	88,8	86,6	89,0	67,9	53,1	65,3
	75	74,8	62,7	75,5	90,4	87,4	91,1	74,3	57,8	70,5

Tabela 4.5: Taxas de reconhecimento em % obtidas no experimento PIN-pad II, modo "mão" com alinhamento temporal.

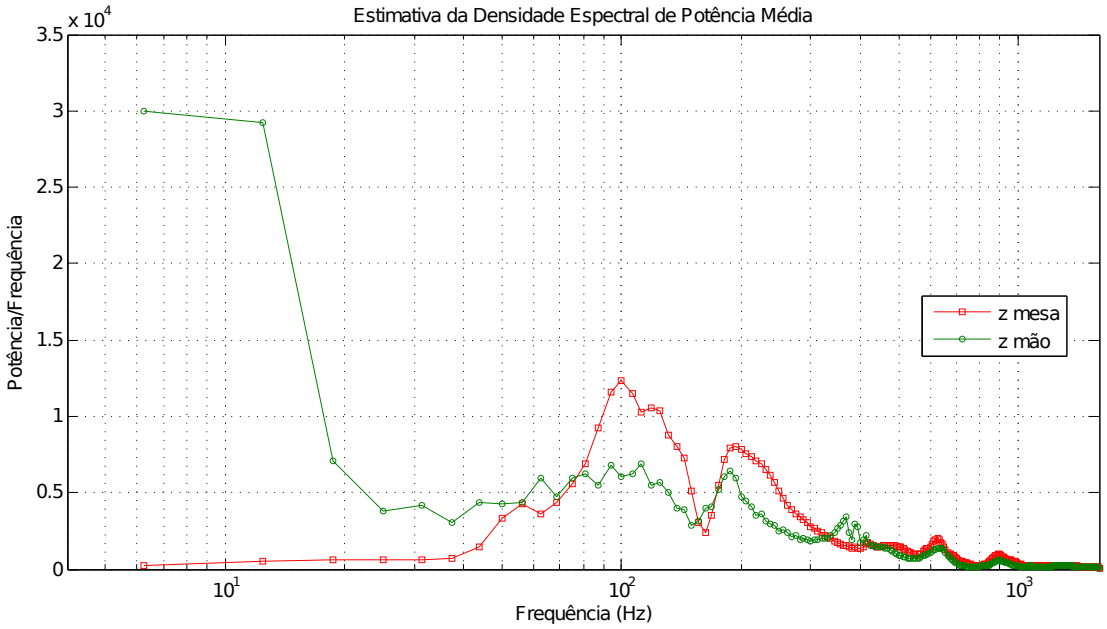

Figura 4.7: Estimativas de Densidade Espectral de Potência Média (PSD) para os modos "mesa" e "mão" para o eixo $\vec{z}$.

pressionamento da tecla, a informação de movimento tridimensional devida às oscilações das mãos pode ter colaborado significativamente com o processo de classificação. Contrariamente, no modo "mesa", a atividade nessa faixa de frequências é inexistente.

4.3.6 Discussão

Os resultados do experimento PIN-pad II foram superiores aos do experimento PIN-pad I pelos seguintes motivos:

1. A taxa de amostragem foi quadruplicada, o que aumenta a capacidade de distinguir atrasos e torna mais preciso o cáculo das características.

2. A interpolação numérica produz características mais robustas.

No entanto, as taxas de reconhecimento do experimento ATM são ainda maiores do que do experimento PIN-pad II. Isso pode ser devido aos fatores:

1. No experimento ATM, três acelerômetros permitem a triangulação do campo de vibração.

2. No experimento ATM, o sistema lê os três valores de aceleração simultaneamente, com atraso irrelevante. A taxa de amostragem é mantida constante e fornecida por um relógio único. Em comparação, nos experimentos PIN-pad, cada sensor possui seu relógio, com taxas de amostragem ligeiramente distintas. Além disso, o instante de cada amostragem depende da disponibilidade do barramento de dados, compartilhado por ambos os sensores (Figuras 4.5 e 4.6).

3. A interpolação numérica melhorou substancialmente os resultados mas ainda assim é uma aproximação.

4. O experimento ATM utilizou taxa de amostragem de aproximadamente 6700 amostras/s, duas vezes a do experimento PIN-pad II e 8 vezes a de PIN-pad I.

5. No experimento ATM, não foram utilizados testadores independentes. Embora os dados de treino e teste sejam segregados, ambos partem dos mesmos treinadores, o que eleva naturalmente as taxas de reconhecimento. Isto não ocorre nos experimentos PIN-pad, em que os dados dos treinadores são utilizados apenas para treino.

4.3.7 Reconhecimento de Linhas e Colunas

Em todos os experimentos com o terminal PIN-pad, as colunas foram sempre mais fáceis de serem identificadas do que as linhas. Este fato pode se explicado utilizando-se a mesma argumentação utilizada na Seção 3.5. O terminal PIN-pad é alongado (Figura 4.8), isto é, ele é maior em profundidade (y) do que em largura (x). Deste modo, o momento de inércia relativo ao eixo $\mathbf{I_y}$ é menor do que o relativo ao eixo $\mathbf{I_x}$, onde $\mathbf{I_y}$ e $\mathbf{I_x}$ são os eixos centrais dos momentos de inércia nas direções $\vec{y}$ e $\vec{x}$. É possível estimar aproximadamente[1] os momentos de inércia centrais relativos ao eixos $\vec{x}$ e $\vec{y}$ utilizando-se as equações:

$$\mathbf{I_x} = \frac{M(b^2 + c^2)}{12} \tag{4.1}$$

[1] As equações 4.1 e 4.2 são exatas apenas para paralelepípedos simétricos de massa uniforme [32].

$$\mathbf{I_y} = \frac{M(a^2 + c^2)}{12} \tag{4.2}$$

Utilizando-se as dimensões reais do equipamento analisado, $a \approx 70$ mm, $b \approx 180$ mm e $c \approx 30$ mm, observamos que $\mathbf{I_y}$ é aproximadamente 6 vezes menor do $\mathbf{I_x}$. Isso significa que é muito mais fácil rotacionar ou vibrar o equipamento sobre $\mathbf{I_y}$ que $\mathbf{I_x}$, resultando em maiores variações de amplitude naquela orientação e, por conseguinte, tornando maior a capacidade de identificação de colunas do que de linhas, ou seja, o sistema responde mais à variações na direção das colunas do que das linhas. Outro aspecto relevante na capacidade de discrimar linhas e colunas é o de as linhas serem mais próximas entre si do que as colunas, como pode ser visto na Figura 4.1. A proporção entre as distâncias entre linhas e entre colunas é 1:2.

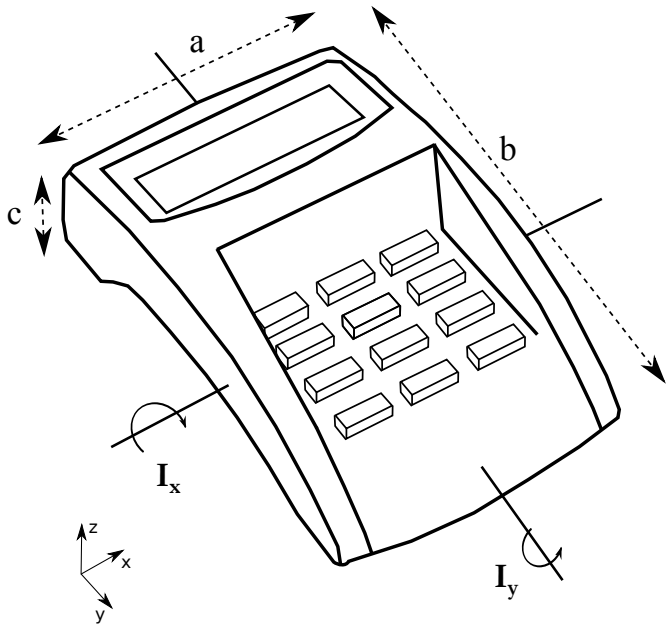

Figura 4.8: Eixos principais dos momentos de inércia do PIN-pad. É mais fácil identificar colunas do que linhas porque o momento de inércia no eixo $\mathbf{I_y}$ é menor do que no eixo $\mathbf{I_x}$. Nota: Este esboço não corresponde ao equipamento analisado.

Conclusão

Este trabalho abordou o problema de identificação de teclas pressionadas em um teclado ATM e em um terminal POS, pela análise das vibrações mecânicas produzidas pelo ato de teclar. Obtivemos taxas de acerto de 99,3% no experimento ATM. Esta taxa é extremamente elevada, mesmo considerando-se que o resultado foi obtido em ambiente de laboratório. Ele mostra quão correlacionados são os pressionamentos e as vibrações, vazando quase que completamente toda a informação.

Também obtivemos taxas de acerto de 68,8% e 75,2% no experimento com terminal POS em repouso em uma superfície rígida e sendo segurado na mão, respectivamente. Estas taxas são igualmente muito elevadas e certamente configuram brechas de segurança. Em segurança da informação, a descoberta de qualquer dado que aumente o conhecimento da informação sigilosa é considerada uma brecha de segurança.

Consideramos também que o fácil acesso ao compartimento de conectores SAM agrava a vulnerabilidade do terminal POS, permitindo uma instalação não detectável de acelerômetros e sistemas de comunicação, ocultando totalmente o dispositivo ilegal. Vale ressaltar que microcontroladores e dispositivos de comunicação sem fio estão disponíveis com dimensões extremamente reduzidas, com capacidade de processamento cada vez maior e na faixa de preço de poucas dezenas de dólares[2].

A sugestão de Kuhn [9] afirmando ser improvável que o roubo de informação por meio de canais secundários (*side channels*) fique apenas restrito aos domínios eletromagnético, óptico e acústico é totalmente procedente, e a sua viabilidade é corroborada pelos resultados aqui obtidos. Não seria, de forma alguma, absurda a hipótese do sur-

[2]Apenas como exemplo, a Texas Instruments lançou em setembro de 2012 uma plataforma de desenvolvimento equipada com processador ARM Cortex M4F de 80MHz com 12 canais de conversão A/D de 12 bits e uma grande variedade de interfaces de comunicação pelo preço promocional de US$4.99. [33]

gimento de uma nova gama de ataques com o uso de sensores, dada a massificação dessa tecnologia em dispositivos móveis ser hoje uma realidade. A crescente facilidade com a qual implementações de software e hardware são efetuadas e o crescente barateamento destes torna ainda mais importante um aprofundamento no estudo das possibilidades dessas tecnologias na elaboração de ataques cada vez mais inusitados. Para comprovar tal possibilidade, todos os experimentos aqui desenvolvidos foram executados com equipamentos de custo extremamente baixo, utilizando técnicas simples e hardware de conhecimento público.

Na realidade, a relação de dependência entre os avanços tecnológicos e suas consequências, tanto gerais como no tocante ao sigilo da informação não constituem novidade teórica. O trecho seguinte sobre o TEMPEST[3], escrito em 1981 de autoria de um oficial da *National Security Agency*, fornece um panorama abrangente do problema:

> *We are being faced with more and more types of sophisticated information processors - including computer-based systems - and these are proliferating at a greater rate we can track. This fact, coupled with more widespread knowledge of the phenomenon, the decline in the availability of trained technical personnel for testing and corrective action in the field (...), and the advent of more potent exploitation devices and techniques place us in a less than satisfactory posture.* [34, p. 39] [4]

Embora o autor deste trecho o tenha elaborado tendo o âmbito militar como preocupação, décadas de informações abundantes sobre a escalada de fraudes efetuadas por meios eletrônicos em todos os domínios da sociedade demonstram que o trecho citado extrapola a esfera para o qual foi originalmente imaginado, tanto no aspecto da evolução tecnológica como no da capacidade de formação de pessoal.

Ainda que o escopo dessa dissertação seja delimitado a apenas um aspecto da segurança de dispositivos, acredito ter demonstrado o potencial de falha de segurança que

[3]Codinome dado pela NSA ao problema de segurança da informação devido às emanações eletromagnéticas (e, em menor escala, acústicas) [10]

[4]Tradução livre: "Estamos sendo confrontados com mais e mais tipos de processadores de informação – incluindo sistemas computacionais – e estes estão se proliferando a uma velocidade maior do que podemos acompanhar. Este fato, juntamente a uma ampla difusão de conhecimento do fenômeno, o declínio na disponibilidade de pessoal técnico treinado para teste e ação corretiva na área (...) e o advento de mais dispositivos e técnicas poderosas de exploração nos coloca em uma posição menos que satisfatória."

acomete projetos de sistemas físicos, que em princípio deveriam possuir excelência em níveis de segurança.

Uma linha argumentativa de defesa recorrente por parte de fabricantes de sistemas quando confrontados com ataques originados de pesquisas acadêmicas, é a de que tal ataque seria inviável nas ruas, por tratar-se de pesquisa de elevado grau de complexidade ou alto custo. Na realidade, tal argumento não se sustenta de forma geral, sendo o trabalho aqui apresentado apenas mais um contraexemplo. Ademais, considerar que recursos sejam fatores limitantes é equivalente a ignorar a existência de grupos criminosos profissionais, estabelecimentos comerciais controlados por máfias etc. cuja disponibilidade de recursos (tempo, dinheiro, acesso à informação privilegiada etc.) não pode ser negligenciada de forma alguma.

Desta forma, é forçoso compreender a segurança como algo além da mera adequação à normas de certificação, que são procedimentos baseados em fatos ocorridos, ou seja, possui os olhos dirigidos ao passado. O conselho de Sun Tzu permanece atual, após 2.500 anos [35, cap. III]:

> "Sobressai-se em resolver as dificuldades quem as resolve antes que apareçam."

Em outras palavras, ataques que outrora poderiam ser considerados tecnologicamente inviáveis, com o tempo passam naturalmente a fazer parte da realidade. A postura psicológica de negação da possibilidade de existência de ataques até então inauditos não deve fazer parte da conduta do profissional de segurança.

Um outro aspecto de risco, que vai além do aqui tratado, reside na adesão apenas tecnológica como a solução para a segurança em sentido amplo, postura analisada de forma extensiva principalmente em [11]. Utilizando nosso caso como exemplo, de pouco vale o algoritmo ou número de bits utilizados na chave de cifração da comunicação do equipamento – orgulhosamente divulgados pelos fabricantes – se a maior parte da informação torna-se disponível externamente.

Durante o processo de realização deste trabalho, observamos muitos estabelecimentos comerciais operando equipamentos com as exatas deficiências aqui expostas. Não obstante, tais equipamentos carregam o rótulo de "Equipamento certificado de

acordo com os padrões PCI", fato que, após os resultados aqui obtidos, merece uma séria reflexão.

Com respeito à contramedidas, é importante considerar que cada novo projeto de equipamento traz em si vulnerabilidades peculiares, bem como mitigação destas, sendo normalmente inaplicável uma única metodologia à solução do problema.

Concluindo, acredito ter contribuído para a ampliação do espaço de possibilidades de ataques, cuja dimensão é problemática e quiçá imensurável.

Referências Bibliográficas

[1] Associação Brasileira das Empresas de Cartões de Crédito e Serviços (ABECS), "Evolução Máquinas POS". Disponível em: http://www.abecs.org.br/site2012/admin/arquivos/estudos/%7BA3E4D2A7-337E-4E88-B180-B40167EC37F5%7D_2249-A-Maquinas_POS_14_04_10.pdf, Acesso em ago., 2011.

[2] D. Asonov and R. Agrawal, "Keyboard acoustic emanations," in *Proc. IEEE Symp. Security and Privacy*, pp. 3, 2004.

[3] L. Zhuang, F. Zhou, and J. D. Tygar, "Keyboard acoustic emanations revisited," *ACM T. Information and System Security*, vol. 13, no. 1, pp. 3:1–3:26, Oct. 2009.

[4] Y. Berger, A. Wool, and A. Yeredor, "Dictionary attacks using keyboard acoustic emanations," in *Proc. 13th ACM Conf. Computer and Communications Security*, pp. 245–254, 2006.

[5] M. Backes, M. Dörmuth, S. Gerling, M. Pinkal, and C. Sporleder, "Acoustic side-channel attacks on printers." in *Proc. USENIX Security Symposium*, pp. 307–322, 2010.

[6] E. Tromer, "Hardware-based Cryptanalysis," Weizmann Institute of Science, Tese de Doutorado, 2007. Disponível em: http://tau.ac.il/~tromer/papers/tromer-phd.pdf, Acesso em set., 2011.

[7] L. Cai and H. Chen, "Touchlogger: inferring keystrokes on touch screen from smartphone motion," in *Proc. 6th USENIX Conf. Hot Topics in Security*, 2011.

[8] L. Cai, S. Machiraju, and H. Chen, "Defending against sensor-sniffing attacks on mobile phones," in *Proc. 1st ACM Workshop on Networking, Systems, and Applications for Mobile Handhelds*, pp. 31–36, 2009.

[9] M. G. Kuhn, "Compromising emanations: eavesdropping risks of computer displays," University of Cambridge, Computer Laboratory, Tech. Rep. UCAM-CL-TR-577, 2003.

[10] J. Friedman, "TEMPEST: A Signal Problem", NSA Cryptologic Spectrum, 1972. Disponível em: http://www.nsa.gov/public_info/_files/cryptologic_spectrum/tempest.pdf, Acesso em jul., 2012.

[11] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley Publishing, 2008.

[12] "NSA - Declassification and Transparency", Disponível em: http://www.nsa.gov/public_info/declass/index.shtml, Acesso em out., 2012.

[13] "NSA Response to FOIA for Tempest-related Documents". Disponível em: http://cryptome.org/nsa-foia-app2.htm, Acesso em set., 2012.

[14] Payment Card Industry - Security Standards Council LLC, *PIN Transaction Security (PTS) Point of Interaction (POI) Derived Test Requirements v3.1*, Disponível em: https://www.pcisecuritystandards.org/documents/PCI_PTS_POI_DTRs_v3_1.pdf, Acesso em jul., 2011.

[15] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM side-channel(s)," in *Cryptographic Hardware and Embedded Systems*, LNCS, vol. 2523, pp. 29–45, 2003.

[16] F. X. Standaert, T. Malkin, and M. Yung, "A unified framework for the analysis of side-channel key recovery attacks," in *Advances in Cryptology - EUROCRYPT*, LNCS, vol. 5479, pp. 443–461, 2009.

[17] G. S. Faria, H. Y. Kim, "Identificação das teclas digitadas a partir da vibração mecânica," in *Anais do XXX Simpósio Brasileiro de Telecomunicações*, 2012.

[18] “Krebs on Security - All About Skimmers”. Disponível em: http://krebsonsecurity.com/all-about-skimmers/ Acesso em ago., 2011.

[19] S. Drimer, S. J. Murdoch and R. Anderson, “Thinking inside the box: system-level failures of tamper proofing,” in *IEEE Symp. on Security and Privacy (Oakland)*, pp. 281–295, May, 2008. Disponível em: http://www.cl.cam.ac.uk/~sd410/papers/ped_attacks.pdf Acesso em set., 2012.

[20] J. P. Lewis, “Fast template matching,” in *Proc. Vision Interface*, pp. 120–123, 1995.

[21] G. Bradski and A. Kaehler, *Learning OpenCV: Computer Vision with the OpenCV Library*, O’Reilly, 2008.

[22] “The OpenCV website”. Disponível em: http://opencv.willowgarage.com/wiki, Acesso em fev., 2011.

[23] R. P. Lippmann, “An introduction to computing with neural nets,” *IEEE ASSP Magazine*, vol. 4, no. 2, pp. 4 –22, Apr. 1987.

[24] L. Breiman, “Random forests,” *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.

[25] J. A. K. Suykens and J. Vandewalle, “Least squares support vector machine classifiers,” *Neural Processing Letters*, vol. 9, pp. 293–300, 1999.

[26] C. J. C. Burges, “A Tutorial on Support Vector Machines for Pattern Recognition”, *Data Min. Knowl. Discov.*, vol. 2, no. 2, pp. 121–167 June, 1998.

[27] Freescale Semiconductor - MMA7260QT: 3-Axis Acceleration Sensor. Disponível em: http://www.freescale.com/webapp/sps/site/prod_summary.jsp?code=MMA7260QT, Acesso em jul., 2011.

[28] Freescale Semiconductor - MMA8452: Xtrinsic 3-Axis, 12 Bit Accelerometer. Disponível em: http://www.freescale.com/webapp/sps/site/prod_summary.jsp?code=MMA8452Q&fr=g, Acesso em set., 2011.

[29] Arduino Board Mega 2560. Disponível em: http://arduino.cc/en/Main/ArduinoBoardMega2560, Acesso em fev., 2011.

[30] NXP Interface Solutions I^2C Bus. Disponível em: http://ics.nxp.com/literature/presentations/interface/pdf/interface.solutions.pdf, Acesso em out., 2011.

[31] Analog Devices - ADXL345 3-Axis, ±2g, ±4g, ±8g, ±16g Digital Accelerometer. Disponível em: http://www.analog.com/static/imported-files/data_sheets/ADXL345.pdf, Acesso em dez., 2011.

[32] R. P. Feynman, R. B. Leighton and M. Sands, *The Feynman Lectures On Physics*, Addison-Wesley Publishing Company, vol. I, ch. 19, 1963.

[33] The Stellaris ARM® Cortex™- M4F LaunchPad Evaluation Platform. Disponível em: http://www.ti.com/ww/en/launchpad_site/stellaris.html?DCMP=stellaris-launchpad&HQS=stellaris-launchpad, Acesso em out., 2011.

[34] A History of U.S. Communications Security (U), *The David G. Boak Lectures - Vol. II*, July, 1981. Disponível em: http://www.nsa.gov/public_info/_files/cryptologic_histories/history_comsec_ii.pdf, Acesso em set., 2012.

[35] S. Tzu, *A Arte da Guerra*, L&PM, 2003.

Identificação das teclas digitadas a partir da vibração mecânica

Gerson de Souza Faria e Hae Yong Kim

***Resumo*— Este artigo descreve um ataque que detecta as teclas pressionadas em um terminal de ponto de venda através da análise das vibrações mecânicas geradas quando as teclas são pressionadas. Usamos acelerômetros como sensores de vibração. O aparelho necessário para este ataque é de baixo custo e pode ser incorporado discretamente dentro do terminal. Obtivemos uma taxa de sucesso que varia de 58% a 82% em reconhecer as teclas pressionadas.**

Palavras-Chave—ataque não invasivo, segurança da informação, acelerômetros, vibração, senha, ponto de venda.

***Abstract*— This paper describes an attack that detects the sequence of keystrokes on a point of sale terminal through the analysis of mechanical vibrations generated when the keys are pressed. We use accelerometers as vibration sensors. The apparatus necessary for this attack is inexpensive and can be unobtrusively embedded within the terminal. We achieved a success rate ranging from 58% to 82% to recognize the keys.**

Keywords—side-channel attack, information security, accelerometer, vibration, password, POS.

I. INTRODUÇÃO

Atualmente, teclados mecânicos são a principal interface homem-máquina devido à sua facilidade de operação, eficiência e baixo custo. No mercado de meios de pagamento eletrônico, teclados são a escolha natural para a entrada de dados sigilosos, como senhas em terminais de ponto de venda, caixas eletrônicos etc. Na esfera governamental, os teclados mecânicos são usados para inserir os números de candidatos em urnas eletrônicas. Assim, a possibilidade de que alguém descubra a sequência de teclas digitadas (sem que o usuário perceba) é uma séria ameaça à segurança de sistemas.

O objetivo deste artigo é descrever um ataque físico não invasivo a terminais de ponto de venda (POS - *Point Of Sale*) que permite detectar as teclas digitadas a partir das vibrações mecânicas geradas no equipamento pelo ato de pressioná-las. Tais vibrações são capturadas por acelerômetros instalados no interior do terminal.

A possibilidade de um ataque similar foi sugerida por Kuhn [1], em que o autor sugere a possibilidade de identificar as teclas pressionadas pela análise vetorial das forças resultantes em determinados pontos do equipamento, por exemplo, nos suportes da base (pés). O autor afirma ser improvável que o roubo de informação por meio de canais secundários (*side-channels*) fique restrito aos domínios eletromagnético, óptico e acústico. Porém, segundo o nosso conhecimento, este ataque nunca foi testado experimentalmente. Nosso ataque não analisa as forças nas bases, mas sim as vibrações mecânicas geradas pelo ato de pressionar as teclas.

A. *Trabalhos relacionados*

Não encontramos na literatura ataques a teclados mecânicos pela análise de vibrações capturadas por meio de acelerômetros. Encontramos apenas ataques que analisam os sons gerados ao pressionar teclas de teclados de computador [2, 3, 4], teclas de terminais de caixas eletrônicos [2] e ataques acústicos em outros dispositivos, tais como impressoras matriciais [5]. Shamir e Tromer apresentam em [14] uma prova de conceito de criptanálise baseada em emanações acústicas de computadores pessoais. Cai e Chen apresentam um ataque que permite inferir os dígitos pressionados no teclado virtual de celulares baseados no sistema Android analisando o movimento do aparelho capturado pelo acelerômetro interno do mesmo [11]. Uma análise geral sobre a vulnerabilidade de sensores de celulares é apresentada em [16].

B. *Contribuição*

A principal contribuição deste artigo é expor uma vulnerabilidade na arquitetura de terminais POS. Apresentamos elementos suficientes que mostram que ataques não invasivos a terminais POS para roubo de senha são possíveis e podem ser efetuados a um baixíssimo custo.

II. DESCRIÇÃO DAS VULNERABILIDADES IDENTIFICADAS

Equipamentos como os terminais POS possuem mecanismos de detecção de violação física

(*tampering*), de modo a auto-destruir informação sensível, como chaves criptográficas contidas em seu perímetro de segurança em caso de detecção de violação. No entanto, uma inspeção visual mostrou que vários terminais POS possuem em sua parte inferior uma tampa removível de serviço e manutenção de modo a oferecer acesso legítimo aos conectores de cartões SAM (*Security Authentication Module*), responsáveis pela segurança da comunicação do sistema bem como pela autenticação com as redes de serviços. Tal espaço possibilita a implantação de dispositivos de coleta ilegal de informação ("*bugs*", que em nosso caso são os acelerômetros). Um mecanismo de detecção de violação comumente utilizado são selos do tipo "*void seal*" (Figura 1), aplicados no encontro da tampa com o corpo do terminal, indicando visualmente a prévia abertura do compartimento. Obviamente, o consumidor não costuma prestar atenção a tal item no momento de digitar a sua senha.

Fig. 1. Exemplo de selo de detecção de violação utilizado para evidenciar a abertura de equipamentos.

Além do acesso ao compartimento, outra condição que beneficiaria ainda mais um ataque é a alimentação elétrica disponível nos terminais dos conectores SAM, que poderia ser utilizada para alimentar cartões SAM falsos contendo acelerômetros e possíveis circuitos auxiliares de comunicação. Como consequência, o ataque poderia se tornar não invasivo e não detectável no terminal, sem uso de fios e baterias aparentes.

III. MONTAGEM DO ATAQUE

A. *Posicionamento dos sensores*

A abordagem aqui adotada pode ser aplicada em praticamente qualquer terminal POS que possua teclado mecânico em seu corpo. A matriz de teclas do equipamento utilizado é padrão, como pode ser observada na Figura 2.

Fig. 2. Formato da matriz de teclas do equipamento utilizado no ataque.

Dois acelerômetros são utilizados no ataque. As placas dos mesmos foram envolvidas em um pedaço de espaguete termo-retrátil e coladas nas posições da Figura 3. Os acelerômetros não possuem qualquer conexão elétrica com o terminal, sendo que no protótipo foram utilizados cabos de conexão ligando os sensores ao sistema de aquisição. Após acondicionados os sensores e os cabos, a tampa original foi recolocada no terminal.

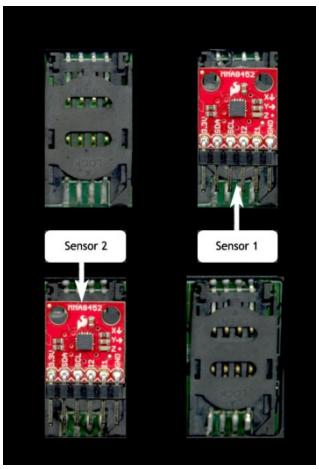

Fig. 3. Vista da parte inferior do terminal, sem a tampa de acesso aos conectores SAM, com a disposição dos acelerômetros utilizados. A máscara preta na imagem foi aplicada para não expor detalhes que pudessem identificar o modelo do equipamento.

B. *Acelerômetros e sistema de aquisição*

Os acelerômetros utilizados são MMA8452 de 12 bits e três eixos, da família Freescale Xtrinsic [6]. O sistema de aquisição foi desenvolvido na plataforma Arduino Mega 2560 [12], como mostra a Figura 4.

A escala de aceleração adequada foi ±2g e a taxa de amostragem adotada foi a máxima para o acelerômetro, 800 amostras/s. Utilizamos as informações de aceleração nos três eixos. Foram coletadas 300 amostras para cada pressionamento de tecla, para os três eixos dos dois sensores, totalizando 1800 elementos por teclagem.

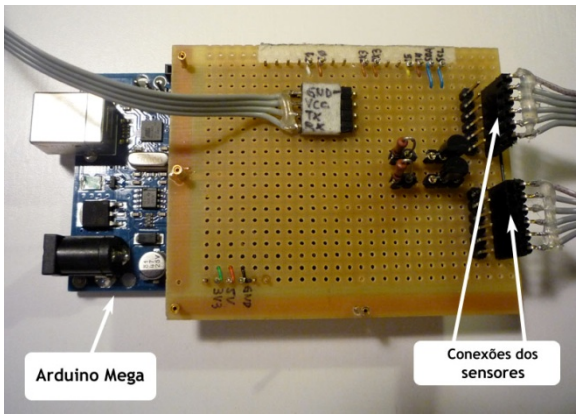

Fig. 4. O hardware do sistema de aquisição de dados consta de um Arduino Mega 2560 e uma placa de montagem sobre este, onde são conectados os cabos dos sensores.

C. *Obtenção das amostras*

De modo a capturar diferentes formas de teclar cada uma das teclas, o processo de obtenção das amostras envolveu 2 pessoas em 5 sessões de teclagens. Cada sessão foi composta pelo pressionamento de 40 vezes cada uma das 12 teclas da matriz 4x3 da Figura 2. Um dos testadores executou três sessões e o outro duas sessões. No total, adquirimos 2400 teclagens, 200 para cada tecla. Durante o processo de coleta das amostras, notamos que cada pessoa possui uma maneira distinta de teclar, envolvendo variações na intensidade, na posição e na permanência do dedo sobre a tecla. Desenvolvemos um programa MATLAB para a leitura das amostras do sistema de aquisição. Em todas as sessões, o terminal ficou em repouso sobre uma mesa, tendo um *mousepad* como base. As amostras foram tomadas com o terminal desligado.

IV. A ABORDAGEM ADOTADA

A. *Propriedades do sistema em análise*

Na teoria clássica de sistemas, a resposta do sistema a uma entrada impulsiva é a sua função de transferência. Se o sistema for linear, a sua saída é dada pela convolução entre a resposta impulsiva e o sinal de entrada [7]. Contudo, o sistema em análise é mecanicamente complexo, havendo acoplamento entre componentes fixos e móveis, amortecedores nas teclas, nos pés etc. Diante disto, não é razoável supor uma hipótese de linearidade para o sistema. Além disso, as pessoas podem apertar uma tecla de várias formas distintas, com maior ou menor intensidade, com maior ou menor permanência da pressão na tecla, com variação nas componentes de força etc. (Figura 5). Dessa forma, não adotamos a abordagem de identificação de sistemas, mas sim, abordamos o problema como um caso de classificação de padrões.

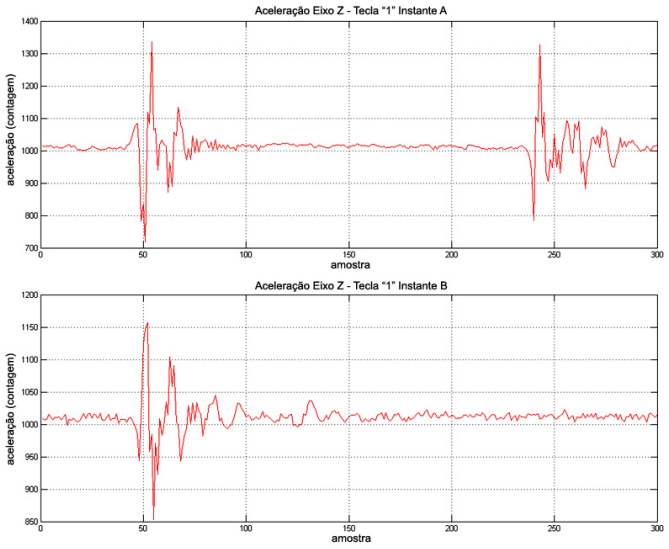

Fig. 5. Exemplos de duas amostras da aceleração do eixo Z (normal ao terminal) do mesmo sensor, da mesma tecla, efetuadas pela mesma pessoa. Os dois gráficos são bastante diferentes: o sentido da aceleração está invertido; o amortecimento e a amplitude são distintos. Além disso, o gráfico superior mostra a vibração de soltura da tecla (o segundo pulso). Este evento não ocorre no gráfico inferior, pois ocorreu fora do intervalo de aquisição.

B. *Características utilizadas*

Cada amostra é representada por um vetor de dimensão 6:

$$\mathbf{v} = (v_x, v_y, v_z, w_x, w_y, w_z)$$

sendo:

- v_x, v_y, v_z = vetores coluna com 300 amostras do sensor 1, eixos *x, y, z*.
- w_x, w_y, w_z = vetores coluna com 300 amostras do sensor 2, eixos *x, y, z*.

O vetor **v** também pode ser considerado como uma matriz 300×6.

As características (*features*) que utilizamos procuram identificar as dependências mútuas entre os sinais do vetor **v** para reconhecer as teclas. Deste modo, não consideramos representações isoladas dos sinais (e.g. espectro de frequência, coeficientes de auto regressão etc.). As seguintes características foram testadas (rótulos adotados em negrito):

- **xcorr**: correlação cruzada entre os sinais de mesma coordenada, i.e., correlação entre (v_x, w_x), (v_y, w_y) e (v_z, w_z), com m *lags,* centrados em zero, para m = ±5. A dimensão do vetor de características resultante é 3×(2|m| + 1) = 33.

- **pca**: vetores normalizados das p componentes principais da *Principal Component Analysis* (PCA) [8, cap.6] de **v,** para p = 3. Dimensão do vetor de características é 6p = 18.
- **cov**: matriz de covariâncias do vetor **v**, dada por:

  $\mathbf{C_v} = (\mathbf{v} - \boldsymbol{\mu_v})^T (\mathbf{v} - \boldsymbol{\mu_v})$

  Sendo $\boldsymbol{\mu_v}$ o vetor de médias das colunas de **v**. A matriz de covariâncias resultante é uma matriz simétrica 6×6. Consideramos apenas o triângulo superior dessa matriz, resultando um vetor de características de dimensão 21.
- **white**: a matriz de *whitening* (ou *sphering*) de um vetor aleatório de média nula $\mathbf{z} = (z_1 \ldots z_n)$ é uma transformação linear calculada sobre **z** de forma a tornar seus elementos $\mathbf{z}_i$ decorrelacionados e com matriz de covariância **I** (matriz identidade). [8, p.140].

  Sejam:

  $\mathbf{E} = (\mathbf{e_1} \ldots \mathbf{e_n})$ a matriz cujas colunas são os autovetores de norma unitária da matriz de covariância $\mathbf{C_z}$;

  $\mathbf{D} = \text{diag}\ (\mathbf{d_1} \ldots \mathbf{d_n})$ a matriz diagonal dos autovalores da matriz de covariância $\mathbf{C_z}$.

  Assim, a matriz de *whitening* é dada por:

  $\mathbf{W} = \mathbf{D}^{-1/2}\mathbf{E}^T$

  O vetor transformado, de média nula e matriz de covariância **I** é então:

  $\mathbf{y} = \mathbf{Wz}.$

  A matriz de transformação **W** é utilizada como característica, possuindo dimensão = n^2, onde n é a dimensão do vetor **z**. Para a característica rotulada de **white**, utilizamos a matriz **W** calculada para os pares (v_x, w_x), (v_y, w_y) e (v_z, w_z), resultando num vetor de características de dimensão $3 \times 2^2 = 12$.
- **whitecruz**: matriz de *whitening* das combinações das 6 componentes do vetor **v** tomadas 2 a 2, resultando num vetor de características de dimensão $15 \times 2^2 = 60$.

Desenvolvemos um programa MATLAB para a geração das características. Para mais informações sobre o cálculo das mesmas, indicamos [8, 15].

C. Classificadores

Para cada conjunto de características do item anterior, testamos os seguintes classificadores (rótulos em negrito):

- **MLP**: rede neural artificial tipo perceptron multicamadas, na configuração fixa entrada-30-30-N, sendo N o número de classes;
- **RTree**: árvores aleatórias;
- **SVM**: máquina de vetores de suporte (apenas o kernel linear foi utilizado).

Utilizamos a implementação dos classificadores da biblioteca OpenCV 2.3 [17]. Todos os classificadores operaram no modo de múltiplas classes. Do total de amostras utilizadas, 80% foram destinadas a treino e 20% a teste, escolhidas de forma aleatória. Para mais informações sobre os classificadores, indicamos [9, 10, 13].

D. Esquemas de classificação dos sinais

O conjunto de dados de treino foi composto a partir de três esquemas de classes. Foram adotadas classes de 'linhas', 'colunas' e 'teclas'. No primeiro e segundo casos, as amostras das teclas foram agrupadas em sua linha/coluna. Para as classes de 'teclas' não há agrupamento.

V. RESULTADOS E DISCUSSÃO

As cinco melhores combinações de características e classificadores podem ser vistas no gráfico da Figura 6, com os três esquemas de classificação: 'linhas', 'colunas' e 'teclas'. O produto das probabilidades de acerto de linhas e colunas é designado no gráfico como 'colunas x linhas'. Observamos que a taxa de acerto de colunas é extremamente elevada e bem superior à taxa de acerto de linhas. A taxa de acerto da classificação 'teclas' é muito próxima ao produto 'colunas x linhas', indicando que o reconhecimento das teclas está limitado pela capacidade de reconhecimento das linhas. Deste modo, a taxa de reconhecimento da melhor combinação (perceptron multicamadas + matriz de covariâncias) ficou em torno de 68% com desvio padrão $\sigma \sim 5\%$. Tabelas I e II mostram as matrizes confusão para o melhor caso.

Notamos que é mais fácil discriminar as colunas do que as linhas, pois a variação da amplitude da vibração no sentido transversal é maior do que na longitudinal, devido à geometria do terminal: o comprimento do terminal é aproximadamente o dobro de sua largura e as linhas estão mais próximas entre si do que as colunas.

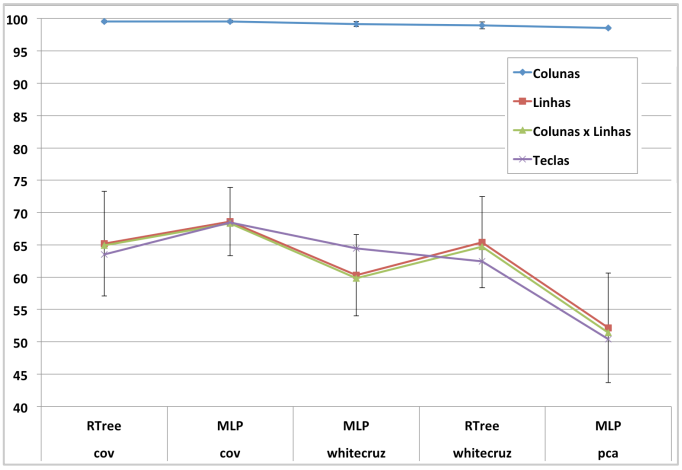

Fig. 6. Taxas de acertos (eixo vertical) obtidos para as cinco melhores combinações de métodos de classificação e características (eixo horizontal). O reconhecimento de colunas é muito superior ao de linhas.

TABELA I. MATRIZ CONFUSÃO DE LINHAS

	1	2	3	4	acerto (%)
1	**95**	21	0	0	81,9
2	24	**80**	19	7	61,5
3	3	20	**70**	26	58,8
4	0	11	21	**83**	72,2

TABELA II. MATRIZ CONFUSÃO DE COLUNAS

	1	2	3	acerto (%)
1	**162**	1	0	99,4
2	0	**159**	0	100,0
3	0	1	**157**	99,4

VI. TRABALHOS FUTUROS

Em todos os nossos testes, utilizamos apenas um tipo de características por vez. Talvez as taxas de reconhecimento possam ser melhoradas alimentando o classificador com uma combinação de vários tipos de características ao mesmo tempo. Pensamos ainda que uma modelagem das dependências entre os eixos de aceleração poderia auxiliar no posicionamento dos acelerômetros e melhorar os resultados. Dado que parte dos usuários opera o terminal segurando-o com uma das mãos, seria importante testar o ataque proposto para este caso.

VII. CONCLUSÕES

A análise das vibrações mecânicas de um terminal POS decorrente do ato de teclar permitiu descobrir os dígitos teclados com taxas de acerto entre 58% e 82% por dígito. O reconhecimento das teclas ficou limitado somente pela capacidade de discriminar linhas, uma vez que o acerto no reconhecimento de colunas foi de 99,6%. A possibilidade de acesso físico ao compartimento de conectores SAM facilita (embora não seja necessária) a instalação discreta de acelerômetros e, eventualmente, de sistemas de comunicação. Isto aumentaria a vulnerabilidade do equipamento.

REFERÊNCIAS

[1] M. G. Kuhn. *Compromising emanations: eavesdropping risks of computer displays* - Technical Report UCAM-CL-TR-577, University of Cambridge, Computer Laboratory, Dec. 2003, p.132.

[2] D. Asonov, R. Agrawal. *Keyboard Acoustic Emanations* – Proceedings IEEE Symposium on Security and Privacy, May 2004.

[3] L. Zhuang et al. *Keyboard Acoustic Emanations Revisited* - Proceedings of the 12th ACM Conference on Computer and Communications Security, Nov. 2005, pp. 373-382

[4] Y. Berger et al. *Dictionary attacks using keyboard acoustic emanations*, Proceedings of the 13th ACM conference on Computer and communications security, 2006, Alexandria, Virginia, USA.

[5] M. Backes. *Acoustic side-channel attack on printers* - USENIX Security'10 Proceedings of the 19th USENIX conference on Security, 2010.

[6] Freescale. MMA 8452: Xtrinsic 3-Axis, 12 bit Accelerometer (http://www.freescale.com/webapp/sps/site/prod_summary.jsp?code=MMA8452Q&fr=g) Acessado em Janeiro 2012.

[7] Oppenheim, Alan V.; Schafer, R. W.; and Buck, J. R. (1999). *Discrete-time signal processing*. Upper Saddle River, N.J.: Prentice Hall

[8] Hyvärinen, Aapo & Karhunen, Juha & Oja, Erkki. *Independent Component Analysis*. John Wiley & Sons, 2001.

[9] C.J.C Burges. *A Tutorial on Support Vector Machines for Pattern Recognition,* 1998 - (http://www.umiacs.umd.edu/%7Ejoseph/support-vector-machines4.pdf). Acessado em Fevereiro 2012.

[10] G. Bradski, A. Kaehler. *Learning OpenCV: Computer Vision with the OpenCV Library*. O'Reilly, 2008

[11] L. Cai and H. Chen. 2011. *TouchLogger: inferring keystrokes on touch screen from smartphone motion.* In *Proceedings of the 6th USENIX conference on Hot topics in security* (HotSec'11). USENIX Association, Berkeley, CA, USA, 9-9.

[12] Arduino homepage: http://www.arduino.cc/. Acessado em Fevereiro 2012.

[13] S. Haykin, *Neural Networks and Learning Machines – Third Edition* – Pearson. 2009.

[14] A. Shamir, E. Tromer. *Acoustic cryptanalysis - On nosy people and noisy machines* (http://www.cs.tau.ac.il/~tromer/acoustic/). Acessado em Dezembro 2012.

[15] D. H. Kil, F. B. Shin. *Pattern Recognition and Prediction with applications to signal characterization*. American Institute of Physics, Woodbury, New York, 1996.

[16] L. Cai, S. Machiraju, H. Chen. *Defending against sensor-sniffing attacks on mobile phones*. In *Proceedings of the 1st ACM workshop on Networking, systems, and applications for mobile handhelds* (MobiHeld '09). ACM, New York, NY, USA, 31-36. 2009

[17] OpenCV homepage: http://opencv.willowgarage.com/wiki. Acessado em Fevereiro 2012.

Gerson de Souza Faria e Hae Yong Kim: Escola Politécnica, Universidade de São Paulo - São Paulo, Brasil. emails: gerson.faria@usp.br, hae@lps.usp.br.
Este trabalho foi financiado parcialmente pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes).