

**ESCOLA SUPERIOR ABERTA DO BRASIL - ESAB
LATO SENSU EM ENGENHARIA DE SISTEMAS**

ERNESTO JORGE COSTA MARTINS

**A FORÇA DAS SENHAS E SUAS IMPLICAÇÕES NA SEGURANÇA
DAS INFORMAÇÕES**

VILA VELHA-ES

2010

ERNESTO JORGE COSTA MARTINS

**A FORÇA DAS SENHAS E SUAS IMPLICAÇÕES NA SEGURANÇA
DAS INFORMAÇÕES**

**Monografia apresentada à ESAB -
Escola Superior Aberta do Brasil, sob
orientação do Prof. Dr. Jaime Roy
Doxsey e da Prof^a Maria Ionara
Barbosa de Andrade Gonçalves.**

VILA VELHA-ES

2010

ERNESTO JORGE COSTA MARTINS

**A FORÇA DAS SENHAS E SUAS IMPLICAÇÕES NA SEGURANÇA
DAS INFORMAÇÕES**

Aprovada em 07 de maio de 2010.

.....

.....

.....

VILA VELHA-ES

2010

À DEUS e à todos que auxiliaram nesta caminhada.

À minha família pelo amor, carinho e compreensão constantes.

AGRADECIMENTOS

Aos meus orientadores, Dr. Jaime Roy Doxsey e Prof^a Maria Ionara Barbosa de Andrade Gonçalves; aos amigos da instituição onde trabalho pelo incentivo e idéias. Um agradecimento especial ao húngaro Péter Török por sua contribuição a este trabalho.

“Quanto mais aumenta nosso conhecimento, mais evidente fica nossa ignorância.”

(John Fitzgerald Kennedy, ex-presidente dos Estados Unidos)

RESUMO

O objetivo deste trabalho foi investigar as causas que levam os usuários a criar senhas fracas sob a visão da Psicologia e da Segurança da Informação, e assim entender o comportamento humano para que se possam aprimorar os meios que levem a sistemas mais seguros, tanto pela conscientização do usuário de suas responsabilidades com sua segurança, como pela necessidade de revisão de políticas de segurança dos sistemas para a condução de soluções através da melhor utilização dos componentes de *hardware*, *software* e *peopleware*. Com esta intenção foi realizada uma pesquisa bibliográfica e um estudo de caso, onde foram analisadas 13815 senhas e a comparação de resultados alcançados em outros estudos. Conclui-se que além da necessidade de educar os usuários para adotar uma postura de responsabilidade com suas senhas, deve haver o compromisso do pessoal da área da segurança da informação em impedir que as senhas criadas sejam frágeis. Partindo do entendimento das limitações humanas sugere-se a necessidade de disseminação de soluções para socorro aos usuários na criação de senhas seguras, utilizando-se de meios diversos para a maximização da segurança de suas informações e dos sistemas em geral.

LISTA DE TABELAS

Tabela 1 - Distribuição do tamanho das senhas.	37
Tabela 2 - Composição das senhas.	38
Tabela 3 - Análise de itens relativos à identidade na formação das senhas.	39
Tabela 4 - Senhas repetidas na base de dados.	40
Tabela 5 - Composição das senhas alfabéticas encontradas no dicionário.	42
Tabela 6 - Composição das senhas que são nomes próprios.	42
Tabela 7 - Levantamento da força das senhas geradas pelo KeePass.	45
Tabela 8 - Tabela comparativa de senhas em diferentes avaliadores de força.	46
Tabela 9 - Tabela das avaliações possíveis em cada tipo de análise.	46
Tabela 10 - Comparação da força das senhas com dicionários inglês e português	47
Tabela 11 - Distribuição dos caracteres nas senhas.	49
Tabela 12 - Distribuição dos caracteres no dicionário utilizado.	51
Tabela 13 - Distribuição dos caracteres nos três levantamentos.	52

SUMÁRIO

INTRODUÇÃO	10
I SEGURANÇA DA INFORMAÇÃO	13
II O SER HUMANO E A SEGURANÇA DA INFORMAÇÃO	15
III SENHAS E A MEMÓRIA HUMANA	17
III.1 EFEITOS VINGANÇA.....	19
IV TRABALHOS RELACIONADOS AO USO DE SENHAS	21
V O DILEMA DAS SENHAS	23
VI PERCEPÇÃO DAS NECESSIDADES DO USUÁRIO	25
VII GOLPES, FRAUDES E ESTATÍSTICAS	26
VIII A NECESSIDADE DA POLÍTICA DE SENHAS	27
IX FERRAMENTAS DE APOIO	31
X ESTUDO DE CASO DA BASE DE DADOS "OBSOLETO" ..	35
X.1 INTENÇÃO.....	35
X.2 OBJETIVOS DA PESQUISA.....	35
X.3 SOBRE O BANCO DE DADOS "OBSOLETO".....	36
X.4 FERRAMENTAS UTILIZADAS NA ANÁLISE DOS DADOS..	36
X.5 A ANÁLISE DAS CARACTERÍSTICAS DAS SENHAS.....	37
X.6 ANÁLISE DA FORÇA DAS SENHAS.....	42
X.7 ANÁLISE DOS CARACTERES USADOS NAS SENHAS....	48
CONCLUSÕES	53
REFERÊNCIAS BIBLIOGRÁFICAS	55

INTRODUÇÃO SEGURANÇA DA INFORMAÇÃO, FORÇA DAS SENHAS, MEMÓRIA HUMANA

A área de Segurança da Informação tem buscado alternativas seguras para que o convívio homem-computador seja facilitado, mas apesar disto o usuário ainda necessita de mais atenção, compreensão e treinamento para que o uso das ferramentas digitais ofereça a tranquilidade e a segurança necessária em qualquer atividade humana.

Com o crescimento das atividades *on-line* tanto a segurança necessita adequar-se aos novos tempos para fornecer facilidades de uso seguro e treinamentos aos usuários, como este também deve assumir o uso mais responsável da tecnologia, comprometendo-se com sua integridade digital.

Sabe-se que o acesso às informações digitais efetiva-se, na maioria absoluta dos casos, pelo uso de senhas que variam em amplitude e estrutura de acordo com cada organização. Este uso frequente de senhas obriga a memória humana a uma sobrecarga que ela não pode suportar, levando o usuário a abrir mão da segurança de senhas fortes em prol de senhas de fácil memorização para seu uso cotidiano.

É necessário, então, buscar o entendimento do comportamento dos usuários, e partindo destas premissas implementar soluções que conduzam ao uso fácil e seguro da tecnologia que nos rodeia.

Motivação

A idéia de estudar este comportamento ocorreu durante um treinamento de usuários, onde estes deveriam criar identificações em dois novos sistemas e suas senhas correspondentes, e a notória dificuldade da memorização de mais duas novas senhas.

A partir daí identificou-se claramente a necessidade de entender o comportamento dos usuários e tentar propor alternativas que permitissem facilitar o processo de criação, memorização e gerenciamento de suas senhas.

Objetivo Geral

Este estudo objetiva revelar o que há por trás do dilema do gerenciamento pessoal das senhas e assim ampliar o conhecimento na área, levando em consideração as características da mente humana.

Objetivo Específico

Realizar um levantamento bibliográfico identificando as origens dos problemas e soluções possíveis de como enfrentá-los.

Elencar propostas de soluções para melhoria dos sistemas nos aspectos de segurança da informação;

Relatar por intermédio de um estudo de caso como é o comportamento dos usuários na criação de uma senha para um sistema, e por meio da medição a força das senhas de um banco de dados identificar quais são as fragilidades presentes no processo de sua criação.

Metodologia da Pesquisa

A primeira providência adotada no desenvolvimento desta pesquisa foi buscar trabalhos científicos na área da memória humana que abordassem o tema e fornecessem pistas sobre o comportamento padrão das pessoas relacionado ao uso de senhas.

A busca de informações atuais na área da Psicologia resultou promissora através da descoberta de uma Tese de Doutorado que foi realizada em Porto Alegre, RS, Brasil, em 2006 e que realizou experimentos sobre a força das senhas e que estava disponível na internet.

Com base nas informações colhidas, seguiu-se uma pesquisa bibliográfica como referencial teórico visando à compreensão dos problemas, a melhoria da segurança dos sistemas, e o levantamento dos prós e contras das opções apontadas como soluções possíveis na área de segurança da informação.

Para fins de análise da qualidade das senhas dos usuários brasileiros foi realizado um estudo de caso com 13815 senhas que foram importadas para a planilha eletrônica MS-Excel 2007, para o software KeePass Password Safe versões 2.08 e 2.09, e para o banco de dados PostgreSQL, foi utilizada também a linguagem de programação Regina REXX, todos no sistema operacional Windows XP. Estes softwares proporcionaram as ferramentas necessárias às análises da composição das senhas e sua força.

I SEGURANÇA DA INFORMAÇÃO

Segundo a ABNT (2005) a informação é um ativo que faz jus à proteção e cuidado, e devido ao aumento da interconexão, ela está cada vez mais exposta às ameaças e vulnerabilidades, e que independente do meio pelo qual ela é compartilhada ou armazenada, recomenda-se que haja sempre uma proteção adequada.

Ainda segundo a ABNT (2005), a segurança da informação é obtida pela prática de um conjunto de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. E estes controles além de estabelecidos, devem ser permanentemente criticados e melhorados para garantir que tanto os objetivos do negócio e da segurança sejam atendidos.

A necessidade de segurança das informações não é algo novo, pois escritas cifradas já eram usadas no Antigo Egito pelo escriba do arquiteto do faraó, aproximadamente em 1900 a.C. Da mesma forma em 50 a.C. Júlio César usava sua cifra de substituição em comunicações governamentais, com a intenção de proteger informações confidenciais que não deveriam cair no domínio público ou na mão de inimigos. (MORENO, E.D.; PEREIRA, F.D.; CHIARAMONTE, R.B., 2005, p.22).

Segundo Russell(1991), há três aspectos distintos na segurança do computador: sigilo ou confidencialidade, exatidão ou integridade e disponibilidade e que devem ser observados para a proteção de sistemas e informações.

O atributo da disponibilidade refere-se que um sistema de computador deve manter a informação disponível aos seus usuários e que tanto o *hardware* como o *software* mantenham-se trabalhando eficientemente e que o sistema esteja apto a se recuperar rápida e completamente se um desastre ocorrer.

O atributo da integridade está diretamente vinculado à contínua integridade das informações armazenadas no computador e significa que o sistema não deve corromper ou permitir qualquer alteração não autorizada, maliciosa ou acidental.

Sendo o atributo de confidencialidade relacionado à autorização de acesso à informação pelo proprietário, tem como sua forma mais comum de autenticação pelo proprietário da informação, ou privilégio de acesso à informação, o uso de senhas.

Muitos são os motivos que levam a este fato. O uso de senhas é uma forma amplamente aceita pelos usuários, sua criação e autenticação demora poucos segundos, o sistema de implantação e manutenção é simples e seu custo é baixo.

Por outro lado, os usuários continuam a esquecer suas senhas ou misturá-las com outras, ou mesmo deixá-las expostas, e isto coloca em risco sua própria finalidade de criação.

Assim, verifica-se que "...a segurança, em geral, e a segurança da informação, em particular, é mais do que um problema social ou humano é também um problema tecnológico." (NORMAN, apud SILVA, 2007), pois quando os códigos de segurança ou procedimentos tornam-se muito complexos e as pessoas não conseguem lembrá-los, utilizam-se de recursos inseguros e óbvios como colá-los em seus monitores, embaixo dos teclados, telefones ou *mouse pad*, colocando em risco a segurança apesar de todo aparato tecnológico desenvolvido para tal.

Ainda segundo Norman (apud SILVA), a segurança da informação é um problema de sistemas, mas um sistema onde o componente humano é o mais importante, então é necessário desenvolver métodos e sistemas que levem em conta este componente humano com todas suas capacidades e limitações.

II O SER HUMANO E A SEGURANÇA DA INFORMAÇÃO

Sasse (apud SILVA, 2007) considera que a fortaleza da corrente está na força de seu elo mais fraco e que este elo mais fraco referenciado na literatura da segurança da informação é o ser humano. Percebe-se a veracidade desta afirmação quando se constata que em muitos casos a segurança é quebrada pela utilização dos conhecimentos adquiridos pela exploração do comportamento humano.

A técnica conhecida como Engenharia Social é a aquisição de privilégios de acesso ou aquisição de informações por alguém que manipula pessoas a realizarem atos que normalmente elas não fariam e está baseada nos atributos da natureza humana, como a tendência de confiar nas pessoas, a vontade de ajudar, ou mesmo o medo.

Um dos maiores desafios na área de Segurança da Informação (SI) é a autenticação, ou seja, o processo em que se distinguem usuários autorizados de usuários não-autorizados. E na mesma medida que se ampliam os serviços *online* cresce também a necessidade de proteção das informações, cuja abordagem mais utilizada é o uso de identificação e senhas textuais.

Problemas de esquecimento, vulnerabilidade no gerenciamento das senhas, escolhas de palavras simples, nomes fáceis de adivinhar, número do telefone, entre tantos outros, evidenciam que as políticas de segurança, quando existentes, não são observadas.

Todos estes fatores levam ao usuário ser considerado como elo mais frágil na corrente da segurança da informação, dentre muitos outros, como *software*, *hardware*, protocolos de comunicação.

Nielsen (2004) considera que as armadilhas da internet não devem ser combatidas colocando a carga sobre os usuários, pois eles precisam de proteção e é a tecnologia que deve modificar-se para fornecer isto. Seu ponto de vista é que a educação do usuário não deve ser a principal iniciativa em relação aos problemas de

segurança, porque esta abordagem não funciona. Ele considera que um usuário médio não está preparado para todas as armadilhas existentes na internet e a sociedade deve agir de um modo pró-ativo para que as fraudes e os crimes cometidos pela internet sejam enfrentados, pois seu impacto na economia e no bem-estar dos cidadãos é maior agora do que muitos outros crimes que absorvem recursos policiais.

O roubo de senhas de bancos tem ocorrido frequentemente, e na busca de ser ressarcido por seu prejuízo, correntistas tem buscado a Justiça para esclarecimento da responsabilidade da operação. Em alguns julgamentos a responsabilidade é colocada justamente sobre os ombros do usuário e este termina arcando com o prejuízo, porém em outros julgamentos a Justiça posiciona-se protegendo a parte mais vulnerável do sistema, que é o correntista, cobrando do sistema bancário a adoção de medidas que diminuam a facilidade de ocorrência de fraudes e desvios.

Informações apresentadas no site internetlegal.com.br em outubro de 2009, mostram decisões conflitantes da Justiça sobre a responsabilidade do correntista; uma decisão cobra do banco a necessária segurança ao acesso possibilitada a seu correntista via internet, já em outra decisão o correntista foi considerado negligente por não se precaver das fraudes que eram anunciadas no site do próprio banco.

De fato causa estranheza que o sistema bancário não tenha adotado senhas com uma maior quantidade de caracteres ou mesmo senhas alfa-numéricas, elevando assim a segurança para ambas as partes.

III SENHAS E A MEMÓRIA HUMANA

Segundo da Silva (2007), há consenso na literatura da Psicologia que os problemas dos sistemas de autenticação baseados em senhas estão relacionados com as condições de funcionamento da memória humana.

Sendo assim, na intenção de administrar suas senhas, muitas pessoas recorrem ao expediente de criar algum registro físico de suas senhas, seja em meio eletrônico ou em papel.

Ainda são raros os estudos que investigam a criação e o uso de senhas, mas em um deles foram encontradas evidências empíricas de que dois terços das senhas observadas haviam sido criadas em torno de características pessoais dos usuários, enquanto a maioria restante das senhas relacionava-se a família, amigos ou relacionamento amorosos, dentre os quais, nomes próprios e aniversários compunham aproximadamente metade de todas as senhas levantadas (BROWN, apud DA SILVA, 2007).

Em outro estudo encontrou-se evidências que pessoas com oito a onze senhas tinham maior probabilidade de não conseguir lembrá-las (CARSTENS, apud DA SILVA, 2007). Com a crescente necessidade de autenticação em *websites*, contas bancárias, *e-mail*, e toda sorte de softwares que requerem autenticação, atualmente é comum que se possua um grande número de senhas.

Estudos foram feitos abordando as deficiências da autenticação por meio de senhas textuais, e criaram algumas opções a seu uso. Entre elas:

- Senhas Cognitivas - por meio de respostas a cinco questões sobre fatos e opiniões pessoais;
- *passphrases* - ou frase secreta, similar a senha, porém mais longa para oferecer mais segurança;
- Senhas Gráficas - visando explorar a capacidade da memória visual;
- Uso de *tokens* - objetos identificadores;

- Biometria - obtenção de dados da fisiologia do usuário.

Apesar destas opções nenhuma delas ainda conseguiu superar a conveniência e baixo custo das senhas textuais tradicionais. Sabendo-se que as memórias não são armazenadas de forma integral, e mesmo quando estabelecidas e consolidadas elas não são permanentes, pois o esquecimento ocorre continuamente enfraquecendo o traço de memória do que foi aprendido, observa-se que muitas das deficiências dos sistemas de autenticação por senhas ocorrem pela função natural do esquecimento humano (SCHACTER, apud DA SILVA, 2007).

Assim sendo, as pessoas acabam utilizando estratégias não seguras no uso das senhas devido às falhas de memória, adotando maus hábitos como anotar ou reutilizar a mesma senha, motivados pela impossibilidade de memorizar suas senhas (SILVA, 2007, p.23-24).

Segundo da Silva (2007, p.23-24):

"Os estudos da Psicologia Cognitiva que têm pesquisado o funcionamento da memória, têm mostrado consistentemente que: guardar informações literais, ou detalhes superficiais como a exata ordem em que os caracteres aparecem em uma senha, é uma tarefa cognitivamente difícil e suscetível a falhas (REYNA & BRAINERD, 1995); as pessoas tendem a ter facilidade de lembrar de informações em que o significado esteve envolvido na codificação, especialmente se combinado com a presença de pistas compatíveis na hora do teste de recordação (S.C. BROWN & CRAIK, 2000) - o que geralmente não é o caso das senhas aleatórias ou geradas pelo sistema; com a falta de uso e a passagem do tempo, traços literais, como a estrutura da senha ou a fonte, tendem a se perder; o fato de processar informações de natureza similar interfere em seu registro mnemônico (F.N. DEMPSTER & BRAINERD, 1995; PERGHER & STEIN, 2003), acarretando perda de parte ou de toda a informação."

Segundo da Silva (2007), estes estudos mostram que as senhas consideradas seguras, que seriam conjuntos de caracteres sem sentido e aleatórios, contendo letras maiúsculas e minúsculas, números e caracteres especiais, são mais difíceis de recordar, pois que lembrar itens sem sentido é mais difícil que recordar itens com significado.

Ainda segundo da Silva (2007), a maior ironia no uso das senhas é que elas deveriam ser fáceis de gerar e lembrar para seu proprietário, mas difíceis de serem adivinhadas por outras pessoas, porém os critérios considerados para gerar senhas fortes ou seguras fazem com que estas sejam difíceis de adivinhar e também difíceis para seres humanos manter na sua memória, principalmente quando se possui diversas senhas para lembrar.

III.1 EFEITOS VINGANÇA

Segundo Tenner (1997), consequências não intencionais da tecnologia induzem a um comportamento que parecem anular o próprio motivo de usá-lo, são chamados de *revenge effects* (i.e., efeitos vingança). Entretanto não é somente a tecnologia a responsável pelos efeitos vingança, é somente quando ela está apoiada em políticas de segurança como leis, regulamentos, costumes e hábitos que ela aparece em sua plenitude.

Na área de segurança das senhas há um exemplo deste efeito quando as diretrizes de segurança entram em conflito com os hábitos e as capacidades cognitivas humanas que torna difícil e frustrante a recordação das senhas. É neste momento que o efeito vingança revela-se por meio dos registros físicos das senhas ou o reuso de uma mesma senha. Este ato anula a intenção de proteção, expondo o usuário a uma vulnerabilidade muito grande.

No começo, para que uma senha fosse considerada uma boa senha era suficiente que ela devesse ser lembrada e mantida secreta, porém hoje ela também tem que ser segura contra ataques de intrusos; assim uma boa senha também tem que ser forte, deste modo ela se tornou algo difícil de recordar.

Esta dificuldade criou maus hábitos entre os usuários que usam senhas curtas consistindo de nomes, apelidos, endereços, datas de aniversário, seus e de seus parentes, ou mesmo palavras simples de dicionário. Dentre estes os dois mais freqüentes e preocupantes maus hábitos são o reuso da mesma senha para múltiplas autenticações e o armazenamento de senhas em papéis ou meio eletrônico (A.S.BROWN; MORRIS & THOMPSON, apud DA SILVA, 2007).

A maioria das soluções propostas para os problemas de senhas pode ser classificada em três categorias:

- Medidas pró-ativas que identificam senhas fracas no momento da geração e rejeitam-na;
- Tecnologia de segurança, como a criptografia;
- Educação e treinamento do usuário.

Nenhuma delas, porém aborda as limitações da memória (DHAMIJA & PERRIG, apud SILVA, 2007) e todos tem suas próprias falhas, assim como as medidas para identificar senhas fracas podem estimular o usuário a copiar ou armazenar suas senhas. Além disto, nenhum usuário está imune a um ataque de engenharia social.

As limitações humanas de uma recordação exata geram um conflito com as exigências de senhas seguras, sendo que os usuários frequentemente preferem diminuir a carga da memória à custa da segurança (WIEDENBECK, apud SILVA, 2007).

IV TRABALHOS RELACIONADOS AO USO DE SENHAS

Em alguns trabalhos relacionados ao uso das senhas, observam-se características que se mantêm ao longo do tempo. Em 1979, Morris e Thompson analisaram um banco com 3289 senhas e observaram tendências das senhas serem curtas ou palavras selecionadas do dicionário. Eles descobriram que um simples ataque de senhas de dicionário quebraria um terço das senhas.

Em 1999, Zviran e Haga pesquisaram entre 860 usuários e relacionaram que uma senha maior não é necessariamente mais difícil de lembrar, mas uma senha complexa, composta de todos os tipos de caracteres é de fato mais difícil de lembrar. Estes autores argumentaram que os usuários ainda escolhem senhas baseadas em detalhes pessoais significativas para o usuário, relativamente curtas, compostas de caracteres alfanuméricos, raramente modificavam-nas e frequentemente escreviam-nas.

Ainda em 1999, Adams e Sasse conduziram uma pesquisa na internet com 139 pesquisados, e foi encontrada uma tendência das senhas escolhidas serem com o mínimo número de caracteres permitidos. Confirmaram também que as pessoas tendem a basear suas senhas em informações com significado pessoal, que podem ser facilmente encontradas, e muitas vezes a mesma senha é reutilizada entre diferentes sistemas.

Já em 2004, Carstens et al conduziram uma pesquisa e um estudo experimental onde seus resultados indicaram que senhas que continham informações que eram significativas ao indivíduo eram mais fáceis de lembrar, mesmo se elas contivessem caracteres adicionais, como símbolos e caracteres de pontuação. Outro comportamento comum observado foi o reuso da senha entre sistemas diferentes e a anotação de uma ou mais senhas.

Também em 2004, Brown e colegas realizaram uma pesquisa entre 218 estudantes onde, para a maioria das senhas observadas, a mais frequente entidade que

aparecia era o participante ou seus parentes, e as informações mais frequentemente usadas como base para as senhas eram nomes e datas e o formato mais comum era a data completa (i.e., dia, mês e ano) e a data parcial (i.e., com dia e mês somente).

Em 2006, Pilar da Silva et al, conduziu um estudo de pesquisa com 263 participantes, onde descobriu-se que a maioria das senhas (62,6%) era somente numérica, seguida pelas somente alfabéticas (24,3%) , alfanuméricas (12,4%) e apenas (0,7%) continham números, letras e outros caracteres.

Nesta pesquisa também se confirmou a tendência de usuários com melhor educação terem um maior número de senhas e conseqüentemente mais problemas de memória com suas senhas. Adicionalmente identificou que mais da metade dos pesquisados (59,2%) que tinham tido problemas de memória admitiram que mantinham um registro físico de no mínimo uma de suas senhas, tendo 52,8 % necessitado restabelecer sua senha no mínimo uma vez, e muitas senhas foram reusadas para mais de uma conta.

Descobriu-se também que 39,5% das senhas examinadas foram baseadas em datas, seguidas por números (17,1%), nomes (12,5%) e misturadas (10,9%).

Contrariamente ao que eram esperados, com base na literatura, os resultados indicaram que a idade e o nível educacional não afetaram a memória para senhas tanto quanto o número de senhas que uma pessoa possui. Tendo várias senhas, como um efeito vingança, as pessoas são levadas a terem problemas de memória, esquecimentos da ordem correta dos caracteres, misturarem suas senhas e colocar a senha correta na conta errada.

Os dados desta pesquisa corroboraram as pesquisas de Adams e colegas (1999, 1997) que já apontavam que o fator que mais impactava no esquecimento de senhas era a quantidade dela que um indivíduo possuía. Eles recomendaram não ter mais do que cinco senhas diferentes.

V O DILEMA DAS SENHAS

Segundo da Silva (2007) as normas de procedimento devem estar disponíveis para auxiliar as pessoas no desenvolvimento de senhas fortes e que sejam aceitáveis para a segurança da informação. Sugere que isto pode ser conseguido com treinamento de usuários, sensibilizando-os sobre os riscos associados à utilização de senhas fracas, bem como sobre as boas práticas, tais como as senhas mnemônicas.

Senhas mnemônicas são aquelas geradas com uma técnica de significado mnemônico, como por exemplo, as primeiras letras de um verso de uma música (i.e., verso da música **Sapato 36** de Raul Seixas "Eu calço é 37, Meu pai me dá 36", cria a senha "Eklç37, Mpmd36!"), que pode ser tão segura como uma sequência de símbolos sem sentido. Este tipo de senha reveste-se das características de facilidade de associação e as características que tornam uma senha forte.

Contudo, Nielsen (2004) diz que o treinamento do usuário não é suficiente para resolver o dilema das senhas, porque mesmo que os usuários estejam conscientes dos perigos e saibam o que eles devem fazer, eles ainda escolherão senhas que eles realmente possam lembrar.

Considera-se então que se é o número de senhas o que torna difícil lidar com elas, parece que a única solução razoável é ter um número aceitável delas, um máximo de quatro ou cinco, como recomendado por Adams e Sasse (1999) e confirmado na pesquisa de Pilar da Silva et al.

Brown (2004) sugere que quando não se possa evitar ter muitas senhas, que se criem categorias de senhas, assim poder-se-ia definir quatro ou cinco categorias de informações de acordo com sua importância (i.e., o valor dos dados armazenados) e sensibilidade (i.e., o grau dos problemas causados se a informação vazasse) e assim criar quatro ou cinco senhas que o usuário pudesse lembrar mas com um nível de força da senha apropriada para cada categoria, e reutilizá-las.

Porém, não há unanimidade neste tipo de pensamento, havendo mesmo aqueles que defendem que as senhas devem ser anotadas, para que se possam ter senhas fortes e fugir também dos riscos do esquecimento.

Para Burnett (2005), escrever sua senha em um papel de recados é uma má idéia, porém não é uma má idéia armazená-la em um local seguro, e que para uma segurança real devem ser usadas práticas de segurança testadas pelo tempo para que se tenha a garantia que algo é seguro.

Observa-se que este tema não está pacificado, há visões discordantes sobre o assunto, porém o número de senhas aumenta incessantemente e não há como depender somente da memória humana para o gerenciamento delas.

VI PERCEPÇÃO DAS NECESSIDADES DO USUÁRIO

Segundo Pressman (1995), a engenharia humana para desenvolvimento de sistemas é reconhecida como uma etapa importante, visto que os sistemas devem ser amigáveis ao usuário quando se tenta a HCI (i.e., interação homem-computador), para isto faz-se necessária a compreensão dos componentes do elemento humano.

Para Pressman (1995) entre os diversos fatores do elemento humano, destacam-se: representação da memória e conhecimento humanos, pensamento e raciocínio, percepção visual, percepção visual e construção do diálogo humano.

Ele afirma ainda que: "A engenharia humana é uma atividade multidisciplinar que aplica conhecimentos derivados da psicologia e da tecnologia para especificar e projetar uma HCI de alta qualidade", (PRESSMAN,1995,p.195-196).

Segundo sua visão a expressão **fatores humanos** assumem diferentes significados: "Em um nível fundamental, devemos entender percepção visual, a psicologia cognitiva de leitura, memória humana e raciocínio dedutivo e indutivo. Em um outro nível, devemos entender o usuário e seu comportamento", (PRESSMAN,1995,p.602-603). Partindo desta premissa considera que se os fatores humanos não tiverem sido observados, o sistema será quase sempre visto como não-amigável.

Todos estes conceitos levam-nos a crer que ainda há a necessidade do pessoal da tecnologia da informação entender os fatores que conduzem os usuários a descuidar de sua segurança no geral, e especificamente no uso das senhas, para que se possam desenvolver soluções sem descuidar dos aspectos humanos buscando resultados que contemplem sistemas amigáveis e seguros.

VII GOLPES, FRAUDES E ESTATÍSTICAS

Em outubro de 2009, tivemos notícias do vazamento de senhas do Hotmail na web. Segundo especialistas que fizeram a análise das senhas de dez mil contas do webmail, o maior problema verificado entre a maioria dos usuários afetados estava no fato das senhas serem simples ou fracas.

Segundo o site idgnow (2009) foi constatado pelo pesquisador de segurança Bogdan Calin que duas senhas fracas – 123456 e 123456789 – eram as duas senhas mais utilizadas pelas vítimas. De 9800 contas legítimas, estavam 82 que usavam uma destas duas senhas, verificou ainda que somente 6% das senhas eram misturas de números, letras e outros caracteres, e 60% eram apenas maiúsculas, minúsculas ou números. O pesquisador conclui dizendo que a maioria dos internautas usa senhas fracas, o que mostra que a mesma situação que ocorria no passado ainda é a mesma.

Porém a pouca preocupação com as senhas atinge também as empresas. Em pesquisa realizada pelo Aberdeen Group, descobriu que 45% das organizações permitem que termos comuns do dicionário sejam usados como senhas e 29% das empresas consultadas não exigem qualquer padrão para o número de dígitos da senha. A pesquisa revelou ainda que 64% delas não exigem a troca regular das senhas e que 88% dos usuários corporativos tem, em média, de 5 a 6 senhas relacionadas ao trabalho.

Segundo o site computerworld (2008), este estudo foi realizado com 150 organizações de um conjunto diversificado de indústrias globais em março de 2008 e evidencia que a mesma situação atinge a todos, pessoas e empresas.

VIII A NECESSIDADE DA POLÍTICA DE SENHAS

A autenticação nos sistemas de informática normalmente é baseada no uso de senhas, ela é um meio muito utilizado por sua facilidade de implantação e manutenção e por seu baixo custo, porém este meio também é o mais inseguro. Para que os usuários tenham uma senha segura não basta somente uma solicitação para que eles criem senhas fortes, pois na maioria dos casos ele não tem idéia do que sejam senhas fortes, deste modo é necessária uma política de senhas que eduque e oriente o usuário como alcançar este objetivo.

Utilizando análise bibliográfica e pesquisas na internet, pode-se compor uma síntese de regras para que as senhas criadas sejam seguras e para evitar vulnerabilidades que os intrusos irão tentar explorar.

O que deve ser feito:

- As senhas devem ter no mínimo 10 caracteres;
- As senhas devem incluir uma mistura de espaços, caracteres alfanuméricos (letras maiúsculas, letras minúsculas e números) e caracteres não-alfabéticos, como "@#\$%^&*";
- As senhas devem incluir o uso de ambos os lados do teclado ou as duas mãos ao digitar. Em outras palavras, não utilize senhas que usem somente a mão esquerda ou somente o lado esquerdo do teclado;
- Para facilitar a memorização das senhas, utilize padrões mnemônicos. Por exemplo: O verso da música "Eu calço é 37, Meu pai me dá 36", cria a senha "Eklç37, Mpm36!";
- As senhas devem ser modificadas regularmente ou com base no número de acessos (convém que senhas de acesso a contas privilegiadas sejam modificadas mais freqüentemente do que senhas normais) e evitar a reutilização do ciclo de senhas antigas;
- As senhas devem ser fáceis de lembrar e difíceis de adivinhar;
- As senhas temporárias devem ser modificadas no primeiro acesso ao sistema;

- Se os usuários necessitam acessar múltiplos serviços, sistemas ou plataformas, e forem requeridos para manter separadamente múltiplas senhas, convém que eles sejam alertados para usar uma única senha de qualidade para todos os serviços, já que o usuário estará assegurado de que um razoável nível de proteção foi estabelecido para o armazenamento da senha em cada serviço, sistema ou plataforma.

O que não deve ser feito:

- Ao criar uma senha nunca utilize palavras que você pode encontrar em dicionários de qualquer idioma (ou estas mesmas palavras soletradas de trás para frente), principalmente a palavra "senha", ou uma palavra com um número associado (rota66);
- Não utilize a mesma senha para todos os seus servidores, roteadores e outros equipamentos. Porque se uma máquina for comprometida o invasor poderia ganhar automaticamente acesso aos seus outros servidores;
- As senhas como nome do usuário ou sua abreviatura, apelidos, combinações simples (abc123), substantivos (casa, meia, cadeira, Brasil), datas (11092001), sequências do teclado numérico (12345,147258), sequências alfabéticas (asdfg, qwerty), ou repetição de números (33333) e outros são extremamente fáceis de um invasor descobrir, portanto não devem ser usadas;
- As senhas não devem ser baseadas em nada que alguém facilmente possa adivinhar ou obter usando informações relativas à pessoa, por exemplo, nomes, números de telefone e datas de aniversário;
- As senhas devem ser isentas de caracteres idênticos consecutivos, todos numéricos ou todos alfabéticos sucessivos, evite também usar um caractere mais de duas vezes;
- As senhas não devem ser incluídas em nenhum processo automático de acesso ao sistema, por exemplo, armazenadas em um macro ou funções-chave;

- A mesma senha não deve ser usada para uso com finalidades profissionais e pessoais;
- Se for usar uma senha baseada em palavra conhecida e quiser fazer alteração de letras por outros códigos, também conhecido por ofuscação, evite substituições do tipo "a" por "@", "5" por "s", "1" por "i", "3" por "e", por serem muito evidentes.

Porém, apesar do consenso em torno de diversas orientações, uma delas não escapa de opiniões divergentes. É a respeito de anotar as senhas. Embora haja uma concordância em evitar manter senhas anotadas ao lado do monitor, teclado, *padmouse*, telefone, ou qualquer suporte físico inseguro, alguns aceitam a idéia que se você achar que não poderá se lembrar de uma senha e deve anotar alguma coisa, que a anotação seja uma palavra ou frase que o fará lembrar-se da senha, mas nunca anote suas senhas, memorize-as. O problema que esta orientação inibe os usuários a criarem senhas suficientemente fortes pelo receio de esquecerem-nas.

Em junho de 2005, durante uma conferência, Jesper Johansson, especialista em segurança da Microsoft pronunciou-se que as políticas de segurança deviam encorajar as pessoas a anotarem suas senhas. Ele relatou que possuía 68 senhas diferentes e que se não pudesse anotar nenhuma delas, terminaria por usar a mesma senha em todas as situações. No seu ponto de vista, as empresas erraram durante anos dizendo que os usuários não deveriam anotá-las.

A opinião de Bruce Schneier, outro especialista em segurança, é a mesma de Johansson, e em seu site deixa um recado bem claro estimulando que os usuários anotem suas senhas.

As afirmações destes especialistas fazem sentido, já que anotando você pode criar senhas fortes e complexas dificultando que as mesmas sejam descobertas e ao mesmo tempo diminuindo o esforço da memória ao recordar senhas. O fator mais importante nesse caso é o suporte onde elas serão anotadas.

Em fevereiro de 2008, Johansson pronunciou-se novamente ratificando o que havia dito anteriormente, agora com 114 senhas para 114 sistemas diferentes, e sugerindo

o emprego de softwares gerenciadores de senhas, a exemplo dele mesmo que utiliza um software *open source*, onde você irá colocar todas suas senhas em uma base de dados criptografada, protegida por uma senha mestre e/ou um arquivo-chave, e que possui métodos de geração de senhas seguras para auxiliar o usuário. Atualmente a própria Microsoft em seu site de segurança ao dar dicas de como criar senhas fortes incentiva a idéia de anotar as senhas para que elas permaneçam seguras e úteis.

Para auxiliar o usuário na verificação e/ou geração de senhas, além de softwares especializados há também este recurso na internet, onde um destes serviços é prestado pela Microsoft, para verificação da força de uma senha. O internauta preenche o campo com sua senha e um texto colorido vai indicando a qualidade da senha que o usuário testou, classificando-a como fraca, média, forte e melhor.

Há também outro site conhecido como *The Password Meter* que faz a medição e mostra em uma tabela qual a atribuição de pontos a cada letra digitada, classificando as senhas em muito fraca, fraca, boa, forte e muito forte.

Para fins de verificação, foi usada a senha mnemônica citada anteriormente como exemplo ("Eklç37, Mpmd36!") nos dois medidores, obtendo nas duas avaliações pontuações máximas de senha muito forte.

Esta forma de medir a força das senhas já está sendo implementada em alguns sites, como o Hotmail, e quando o usuário começa a criar sua senha para autenticação, ele mostra ao usuário a força dela para estimulá-lo a criar uma senha melhor.

IX FERRAMENTAS DE APOIO

Segundo Russel (1991), identificação é a maneira que você diz ao sistema quem você é; autenticação é a maneira que você prova ao sistema que você é quem que você disse que é. Na maioria dos sistemas multiusuário, você deve identificar-se, e o sistema tem que autenticar a sua identidade, antes que você possa usar o sistema.

São usadas três maneiras para você pode provar que é você mesmo; alguma coisa que você sabe; alguma coisa que você tem; e alguma coisa que você é.

O mais comum exemplo daquilo que você sabe é por meio do uso de senhas. Como exemplo de alguma coisa que você tem, algum hardware que se possa carregar, poderia ser uma chave ou *smart cards* (i.e., cartões inteligentes) como os que se usa rotineiramente ao sacar dinheiro no caixa eletrônico do banco.

Já na categoria do que você é, surge o auxílio da biometria com leitura da impressão digital ou análise de padrões de voz ou retina.

Porém, são as senhas as ferramentas de autenticação de uso mais popular, devido as suas características de baixo custo de implementação, manutenção, e facilidade de criação e alteração.

A necessidade de gerenciamento das senhas, fez surgirem diversos gerenciadores *online* de senhas gratuitos que se comprometem a cuidar das senhas. Empresas como a Microsoft são bem claras ao sugerir que se evite a terceirização das senhas, explicando ao usuário que se pessoas mal-intencionadas descobrirem a senha do armazém *online* através de computadores em rede, eles terão acesso a todas suas informações.

Há à disposição na internet softwares para gerenciamento de senhas, que utilizam a criptografia para manter todas as senhas seguras e organizadas. Há soluções para todo tipo de plataforma, sistemas operacionais, pagos e gratuitos. No estudo de caso apresentado a seguir foi usado o software KeePass Password Safe versões 2.08 e 2.09, que é um software *open source*.

Pressman(1995) prescreve que os analistas façam testes de segurança para tentar verificar se todos os mecanismos de proteção embutidos num sistema irão protegê-lo de acessos indevidos. Segundo suas palavras:

"Durante o teste de segurança, o analista desempenha o(s) papel(éis) da pessoa que deseja penetrar no sistema. Qualquer coisa vale! O analista pode tentar adquirir senhas mediante contatos externos; pode atacar o sistema com software customizado projetado para derrubar quaisquer defesas que tenham sido construídas; pode desarmar o sistema, negando serviço a outros; pode intencionalmente provocar erros no sistema, esperando acessá-lo durante a recuperação; pode "folhear" através de dados inseguros, esperando descobrir a chave para a entrada no sistema."

Ou seja, não há meio proibido ao analista ao buscar descobrir as fragilidades do sistema sob análise.

Ele conclui dizendo que se houver tempo e recursos suficientes, um bom teste de segurança irá penetrar no sistema, e caberá ao projetista fazer com que este acesso custe mais do que o valor da informação que será conseguida.

Em função do valor das informações há várias técnicas criadas para o furto de senhas e para a abordagem. As duas técnicas mais comumente usadas para o roubo de senhas são o *phishing* e o *keylogging*.

O envio de e-mails falsos, mais conhecido como *phishing*, é uma fraude eletrônica, onde o fraudador faz se passar por uma pessoa confiável, empresa ou instituição oficial por meio de um *e-mail* ou mensagem instantânea, com a intenção de adquirir informações importantes como senhas e números de cartão de crédito. O termo *phishing* vem em função das artimanhas criadas para pescar (i.e.; do inglês fish) informações sensíveis dos usuários.

Já o *keylogging*, ou armazenar as teclas digitadas em um arquivo, por meio de um *keylogger* tem por finalidade monitorar tudo o que é digitado. Alguns casos de *phishing*, assim como outros tipos de fraudes virtuais, se baseiam no uso de algum tipo de *keylogger*, instalado no computador sem o conhecimento da vítima, que vai

capturando os dados e os envia a um *cracker*, que posteriormente irá utilizá-los com finalidades fraudulentas.

Ciente de que a tentativa de invasão usa meios diversos, há que se pensar também em soluções de hardware que permitam atenuar as vulnerabilidades e trazer mais tranquilidade ao mundo digital.

Uma possibilidade em termos de proteção é o uso de hardware para armazenamento de chaves criptográficas, alguns destes dispositivos são minúsculos computadores chamados *tokens*. Ele pode se parecer como um cartão plástico inteligente, uma chave plástica, um pequeno anexo da porta USB ou mesmo um anel que você usa no dedo.

Um *token* contém um pequeno chip com um processador, um tipo de sistema operacional, e recursos limitados de entrada/saída, memória e espaço de armazenamento. A vantagem de usar os *tokens* é que o invasor não tem acesso a eles, a não ser no breve momento que o *token* está conectado ao computador. Eles podem manter suas senhas fortes, seguras e disponíveis.

Há também um recurso que começa a ganhar força no mercado, que é a biometria que se utiliza de características físicas para verificar sua identidade. Grandes bancos brasileiros já estão adotando esta solução para aumentar a segurança de seus clientes, e contam com a aceitação da maioria da população.

Segundo pesquisa publicada em janeiro de 2009, no site *computerworld*, 71% da população prefere a impressão digital como método biométrico de identificação. Na escala de preferência, a senha pessoal ficou em segundo lugar, com 67%, e em terceiro ficou a leitura de íris, com 60%.

Percebe-se através desta pesquisa que os usuários também estão preocupados com sua segurança digital, e veem com bons olhos a entrada da biometria na sua proteção.

Burnett (2002) cita o caso de uma cidade da Califórnia, Estados Unidos, onde o governo local descobriu que um servidor público tem que estabelecer e memorizar de 6 a 9 senhas para acessar diferentes aplicativos e com isto tinham de administrar o fato das senhas perdidas e esquecidas. A prefeitura em questão percebeu a necessidade da redução do número de senhas e ao mesmo tempo alcançar maior segurança. Após diversas alternativas terminaram optando pela utilização da biometria.

Com o uso da biometria, através de *scanners* de impressão digital, para cada um de seus terminais de computador eliminou a necessidade de múltiplas senhas, aumentou a segurança de seus dados sigilosos e as chamadas para o serviço de suporte caíram substancialmente, gerando economia ao município.

Percebe-se que a biometria ainda não se expandiu ao grande público, mas pela tendência que se observa no comportamento em grandes empresas brevemente ela estará incorporada no dia a dia.

X ESTUDO DE CASO DA BASE DE DADOS "OBSOLETO"

X.1 INTENÇÃO

Com a intenção de colocar em prática as idéias de Pressman sobre os testes de segurança e identificar a força das senhas utilizadas pelos usuários de um sistema, foi realizada uma pesquisa para identificar e quantificar as fraquezas e a partir daí desenvolver estratégias que estimulem a criação de senhas com uma segurança maior.

Simultaneamente, traçar um comparativo com as informações provenientes de outras pesquisas, estudos e informações técnicas.

Alvo do estudo: Um banco de dados de uma organização localizada no Estado do Rio Grande do Sul, Brasil, com um total de 13815 identificações e senhas que foi desativado em dezembro de 2008.

Os dados foram analisados durante o ano de 2009 quando esta base de dados já não estava mais em uso. Durante este relato o banco de dados que será alvo da pesquisa será chamado de **Obsoleto**.

X.2 OBJETIVOS DA PESQUISA

O objetivo desta pesquisa foi examinar as senhas contidas no banco de dados Obsoleto e:

- averiguar as características;
- averiguar a composição;

- determinar o padrão de composição em relação aos dados cadastrais;
- determinar o tipo;
- fazer testes de senhas de dicionário;
- analisar a força das senhas do banco Obsoleto;
- determinar os caracteres mais usados nas senhas do banco Obsoleto;
- comparar os resultados com resultados de outras pesquisas.

X.3 SOBRE O BANCO DE DADOS "OBSOLETO"

Cumprido esclarecer que cada vez que havia a inserção de novos usuários na base de dados ela dava-se por lotes e que o sistema criava uma senha numérica de 6 dígitos, baseada no microssegundo do relógio do sistema operacional, para cada usuário.

Quando o usuário desejava utilizar o sistema pela primeira vez, ele dirigia-se ao setor de atendimento e fazia a confirmação de seu endereço e era entregue a ele sua senha temporária, com a instrução de que ele imediatamente trocasse-a por uma senha de sua escolha.

As restrições que havia na escolha da senha era o tamanho máximo do campo alfanumérico de 8 caracteres e a impossibilidade de serem criadas senhas com letras minúsculas, pois durante o processo as letras eram transformadas em maiúsculas. Desta maneira, havia inúmeros casos de usuários que nunca desejaram utilizar o sistema e não atualizaram seus endereços e senhas e podem gerar distorções nos resultados.

X.4 FERRAMENTAS UTILIZADAS NA ANÁLISE DOS DADOS

Foram utilizadas três ferramentas para análise das informações. Por meio da exportação dos dados dos usuários foram alimentados três softwares diferentes. O mesmo conjunto de dados foi importado para a planilha MS-Excel 2007, banco de dados PostgreSQL, e para o software de gerenciamento de senhas KeePass Password Safe versões 2.08 e 2.09.

X.5 A ANÁLISE DAS CARACTERÍSTICAS DAS SENHAS

A primeira parte da análise dos dados deu-se por meio da utilização da planilha MS-Excel 2007, onde foram observadas as características das senhas.

O número de caracteres das senhas variou entre 1 e 8 dígitos, tendo sua maior concentração em 6 caracteres. A média aritmética simples resultou em 6,38 caracteres por senha.

Observou-se que a maior quantidade de senhas, 60,37%, possuíam 6 caracteres, sendo seguida por senhas de 8 caracteres com 16,82% e senhas de 7 caracteres com 14,74%, (tab.1) .

Como o campo das senhas era inicializado com um número de 6 dígitos em um campo de 8, consegue-se afirmar que 31,56% dos usuários, que é o somatório de casos de senhas com 7 e 8 caracteres, substituíram a senha temporária por uma senha de maior tamanho, e que 8,07%, que é o somatório de casos de senhas com 5 ou menos caracteres, escolheram uma senha de menor tamanho.

Tabela 1 - Distribuição do tamanho das senhas

Número de caracteres	Total de casos	%
1	11	0,08
2	7	0,05
3	32	0,23
4	158	1,14
5	907	6,57
6	8340	60,37
7	2037	14,74
8	2323	16,82
Soma	13815	100

Também se buscou avaliar a composição das senhas, tentando estabelecer a distribuição do critério usado para sua criação. Notou-se que a maioria absoluta, 84,20%, das senhas é composta somente por números, seguida pelas senhas alfabéticas puras (i.e., somente caracteres compreendidos entre A e Z maiúsculos - que era uma das restrições da inserção das senhas no sistema), com 10,78 %, restando para as senhas compostas o percentual de 5,02 %, (tab.2).

Como se pode concluir sobre os dados mostrados na referida tabela, a grande maioria dos usuários ainda usa senhas fracas: 10,78% alfabéticas puras e 84,20% de numéricas, enquanto somente 5,02% de todas as senhas tem uma composição de letras e/ou números e/ou outros caracteres.

Apesar do que se aconselha, que as senhas mais fortes são a composição destes três elementos, isto só ocorre em minúsculos 0,12% de todas ocorrências.

Tabela 2 - Composição das senhas

Composição das senhas	Número de casos	%	Média de caracteres
Numéricas	11632	84,20	6,21
Alfabéticas puras	1490	10,78	7,22
Alfabéticas + números	671	4,86	7,43
Alfabéticas + caracteres especiais + números	16	0,12	7,58
Alfabéticas + caracteres especiais	6	0,04	5,83
Total	13815	100,00	-

Tentando estabelecer algum padrão utilizado pelos usuários para compor suas senhas, elas foram comparadas com diversos itens dos dados cadastrais que tivessem relação com sua identidade.

O item que teve um número de respostas mais significativo foi daqueles usuários que utilizaram parte de seu nome/sobrenome como senha, totalizando 299 ocorrências, 2,16% de todas as senhas pesquisadas.

O somatório dos outros itens analisados, como uso total ou parcial do número da carteira de identidade, número de identificação no sistema, uso do telefone total ou parcialmente, ou uso do CEP totalizaram 138 casos, correspondentes a 1% do total das senhas, conforme tab. 3 .

Tabela 3 - Análise de itens relativos à identidade na formação das senhas

Itens analisados em relação ao total da amostra	Respostas afirmativas	%
Senha é parte do nome	299	2,16
Senha é parte da Carteira de Identidade	48	0,35
Senha igual a Carteira de Identidade	6	0,04
Senha igual ao número de identificação no sistema	33	0,24
Senha é parte do telefone	24	0,17
Senha é igual ao telefone	23	0,17
Senha é igual ao CEP	4	0,03
TOTAL	437	3,16

Investigando a ocorrência de senhas repetidas verificou-se que havia 12708 senhas únicas (91,99%) do total de 13815 senhas. Dos grupos de senhas repetidas foram analisadas aquelas que apareciam 5 vezes ou mais, totalizando 28 palavras, que apareceram 269 vezes como senhas.

Na separação por tipo observou-se que elas dividiam-se em três grupos: o grupo dos nomes próprios, o grupo das senhas numéricas e o grupo das palavras de dicionário, sendo que a senha repetida mais vezes foi a numérica "1234567" com 77 casos, seguida por outra numérica "12345678" com 18 casos.

O grupo que apresentou maior representatividade foi o grupo das senhas provenientes de nomes próprios, com 23 senhas que se repetem 159 vezes, ficando

em segundo lugar o grupo das numéricas com 4 senhas que repetem-se 105 vezes na base de dados.

Constata-se que, apesar da predominância das senhas do grupo dos nomes próprios, as senhas que tiveram mais repetições isoladamente foram as numéricas e que há de se destacar também que, 3 das 4 com maior número de ocorrências eram sequências numéricas crescentes ou decrescentes.

Dentre as senhas de nomes próprios a que individualmente mais ocorre é a senha "JULIANA" com 17 ocorrências seguidas da senha "RODRIGO" com 14 ocorrências.

Observa-se nesta amostra que as palavras provenientes de dicionário tiveram pouca contribuição na análise de senhas repetidas.

Dentre as senhas esperava-se encontrar, a exemplo de outros estudos, a palavra "SENHA" repetida muitas vezes, o que não ocorreu. Ela apareceu entre as repetidas somente duas vezes, portanto não está constando (tab.4), já que considera a partir de 5 repetições.

Tabela 4 - Senhas repetidas na base de dados

Senha	Ocorrências	Grupo
1234567	77	numérica
12345678	18	numérica
JULIANA	17	nome próprio
RODRIGO	14	nome próprio
GABRIEL	11	nome próprio
MARIANA	10	nome próprio
MATHEUS	7	nome próprio
EDUARDO	7	nome próprio
DANIELA	7	nome próprio
VINICIUS	6	nome próprio
PATRICIA	6	nome próprio
LETICIA	6	nome próprio
LEONARDO	6	nome próprio
GUSTAVO	6	nome próprio
FERNANDA	6	nome próprio
VERONICA	5	nome próprio
VANESSA	5	nome próprio
VALERIA	5	nome próprio
RICARDO	5	nome próprio
OLIVEIRA	5	nome próprio
JANAINA	5	nome próprio

CRISTINA	5	nome próprio
CRISTIAN	5	nome próprio
CASSIANO	5	nome próprio
BIOLOGIA	5	dicionário
ANAPAUULA	5	nome próprio
7654321	5	numérica
0	5	numérica

Em 6 de outubro de 2009, no blog do site www.acunetix.com, um artigo postado pelo especialista em segurança Bogdan Calin divulgou um vazamento de senhas do webmail do Hotmail. Segundo o blog mais de dez mil senhas foram examinadas e após serem retiradas entradas sem senhas sobraram 9843 que foram examinadas. A partir daí foi divulgada uma lista das 20 senhas mais usadas e seu número de ocorrências.

Foi feito um comparativo entre as senhas vazadas mais repetidas e as senhas mais repetidas do sistema Obsoleto. A senha mais repetida do Hotmail era a numérica "123456", com 64 ocorrências. Esta mesma senha ocorre repetida no banco Obsoleto apenas 3 vezes.

A segunda senha mais repetida do Hotmail era outra numérica "123456789", com 18 ocorrências e a mesma senha não ocorre no banco Obsoleto, pois o tamanho do campo da senha no banco é limitado em 8 caracteres.

Por sua vez, as senhas que mais ocorrem no banco Obsoleto também são numéricas, e também são sequências numéricas. As senhas "12345678" e "1234567", que foram as que tiveram o maior número de ocorrências no banco Obsoleto, também estão presentes na lista das 20 mais comuns que foi divulgada pelo especialista em segurança Bogdan Calin.

Chamou a atenção o fato da pouca ocorrência de palavras do dicionário entre as senhas mais repetidas, fato que estimulou uma análise confrontando todas as senhas do banco Obsoleto e um dicionário de palavras em português do Brasil/Portugal com mais de 712000 palavras, entre nomes próprios e verbetes comuns de dicionário, para delimitar o número de ocorrências deste grupo de palavras.

Após a busca das senhas do banco Obsoleto no dicionário, identificou-se 454 ocorrências de senhas que constavam no dicionário.

Cumprido esclarecer que este dicionário foi compilado de verbetes do Brasil, Portugal e de nomes próprios totalizando mais de 712000 palavras que foram carregadas no banco de dados PostgreSQL onde foram confrontadas todas as senhas do banco Obsoleto (13815) com as palavras do dicionário (712132).

Descobriu-se que 3,28% (454) das senhas do banco Obsoleto estavam incluídas nas palavras do dicionário. O próximo passo na análise da amostra foi identificar quais senhas que eram nomes próprios e quais não eram.

Descobriu-se que, do total da amostra (454), 142 senhas estavam no dicionário e não eram nomes próprios, representando 31,28% do total.

O restante das 312 senhas, ou seja, 68,72% eram nomes próprios ou apelidos gerados a partir do nome (i.e., senha "BEL" do nome ISABEL).

Observou-se que, apesar da maioria das senhas alfabéticas serem nomes próprios, uma parcela expressiva (45,83%), eram nomes próprios, porém não faziam parte do nome do usuário e não se conseguiu determinar algum vínculo com o usuário. Estes dados estão presentes nas tabelas 5 e 6.

Tabela 5 - Composição das senhas alfabéticas encontradas no dicionário

Situação 1	Casos	%
Senhas que são nomes próprios	312	68,72
Senhas que não são nomes próprios	142	31,28
Total de senhas constando no dicionário	454	100,00

Tabela 6 - Composição das senhas que são nomes próprios

Situação 2	Casos	%
Senhas que são nomes próprios e parte do nome	169	54,17
Senhas que são nomes próprios e não são parte do nome	143	45,83
Total de senhas que são nomes próprios	312	100,00

Constatou-se que, como mostrava a análise das senhas mais vezes repetidas, as senhas que são nomes próprios aparecem de fato em maior quantidade; porém

mesmo sendo menor sua participação no conjunto das senhas alfabéticas, as senhas que não são nomes próprios e estão no dicionário de palavras possuem uma representação significativa com quase um terço das senhas alfabéticas.

X.6 ANÁLISE DA FORÇA DAS SENHAS

Nesta análise foi utilizado o software de gerenciamento de senhas KeePass Password Safe 2.08 (KeePass), que permite a verificação da força das senhas no momento do cadastramento assim como a geração de relatórios da força das senhas que estejam nele armazenadas.

Ele possui diversos *plugins*, e entre eles está o *StrengthReport*, desenvolvido para a criação dos relatórios de força das senhas. Este foi um fator determinante na escolha deste software, pois através dele pode-se analisar um grande conjunto de senhas automaticamente, como era o banco de dados em questão.

O conjunto de 13815 senhas do banco Obsoleto foi importado para o KeePass, e por meio dele foram gerados três relatórios com análises de força das senhas.

A primeira análise, chamada *Basic*, examinou o comprimento da senha e se ela continha caracteres maiúsculos, minúsculos, números e caracteres especiais usando o algoritmo do *plugin StrengthReport*.

A segunda análise, chamada *Advance*, procurou por correspondências com o nome do usuário, o reverso do nome e no dicionário de palavras que está embutido no programa.

Cumprе explicar que o *plugin* que foi utilizado para geração destes relatórios do KeePass é um software *opensource*. Fazendo a análise do código fonte descobriu-se que o dicionário utilizado continha 411135 palavras em inglês com a menor palavras com 3 letras e a maior com 28. O algoritmo usado para esta análise também é do algoritmo do *plugin StrengthReport*.

A terceira análise, chamada *Built-in*, examina a força das senhas usando uma classe embutida no KeePass chamada de *Quality Estimation class*, não se utilizando de qualquer algoritmo do *plugin StrengthReport*.

Segundo o que os resultados mostraram esta é a análise mais rigorosa da força das senhas. Por meio da análise do código fonte desta classe verificou-se que ela examina os tipos dos caracteres usados na senha, como as letras maiúsculas e minúsculas, números e caracteres especiais que foram usados na sua composição.

Portanto, cada tipo de relatório analisa a mesma senha usando diferentes visões e isto pode gerar diferentes resultados, em que uma mesma senha em um tipo de relatório irá ser considerada razoável, enquanto a mesma senha em outro relatório será considerada muito fraca.

Examinando o relatório *Basic* nota-se que a maior concentração de números está contida em senhas fracas com 68,78%, seguido pelas senhas razoáveis com 26,64% e as senhas médias com somente 4,52%.

Apesar de o relatório realizar um teste básico nas senhas somente 0,07% foram classificadas como fortes, não havendo nenhuma que pudesse ser classificada como muito forte, o que já demonstra a fragilidade das senhas em questão.

Modificando-se o tipo de análise, pelo relatório *Advanced*, percebe-se um deslocamento dos percentuais para as senhas com menor força. O percentual de senhas fracas do relatório *Basic* praticamente deslocou-se inteiro, de 68,78% para 68,48% de senhas muito fracas.

Também se observa que a soma das senhas razoáveis e médias do relatório *Basic*, que totalizam 31,15%, deslocaram-se para as senhas fracas e razoáveis do relatório *Advanced*.

Percebe-se também que as senhas que eram consideradas fortes no relatório *Basic* migraram para classificação média do relatório *Advanced*, com isto o percentual de senhas fortes que apareceram no relatório *Basic* deixaram de aparecer no relatório *Advanced*.

Quando a análise é feita pelo relatório *Built-in*, percebe-se a concentração das senhas muito fracas, com 84,44%, e fracas com 15,07%. Estes números fazem-nos crer que as senhas que eram consideradas fracas no relatório *Advanced*, foram consideradas em sua maioria como muito fracas no relatório *Built-in*.

Na avaliação do relatório *Built-in* não resta nenhuma senha média, forte ou muito forte, sendo a maioria absoluta considerada muito fraca, (tab.7) .

Tabela 7 - Levantamento da força das senhas geradas pelo KeePass

Força da senha Dicionário Inglês	<i>Basic</i>	%	<i>Advanced</i>	%	<i>Built-in</i>	%
Muito Fraca-1/6	0	0,00	9460	68,48	11666	84,44
Fraca-2/6	9502	68,78	2497	18,07	67	0,48
Razoável-3/6	3680	26,64	1849	13,38	2082	15,07
Média-4/6	624	4,52	9	0,07	0	0,00
Forte-5/6	9	0,07	0	0,00	0	0,00
Muito Forte-6/6	0	0,00	0	0,00	0	0,00
TOTAL	13815	100,00	13815	100,00	13815	100,00

Além da medição da força das senhas pelo KeePass, foi selecionado um conjunto de senhas para fazer uma comparação entre o algoritmo utilizado pelo gerador de relatórios e os algoritmos usados por outros dois verificadores de força das senhas por meio da internet. Um foi o *The Password Meter*, (<http://www.passwordmeter.com/>) , e o outro foi o verificador da Microsoft (http://www.Microsoft.com/brasil/athome/security/privacy/password_checker.msp) .

Foi usado o critério das senhas que alcançaram melhor avaliação no relatório *Basic* para escolha das que seriam comparadas com outros resultados. Das 9 senhas que se enquadram neste critério somente 8 senhas únicas foram avaliadas.

Pelo comparativo da amostra, é possível a dedução de que cada avaliador da força das senhas usa um algoritmo diferente para medição, e que o fato de um resultado de uma análise de uma senha resultar "Muito Fraca" em uma avaliação, poderá ser considerada "Razoável" em outra, e em outra ainda poderá ser considerada "Forte". Este é o caso ocorrido com a senha "2211_251", que teve avaliações diferentes em todas as avaliações, (tab.8).

Note-se também que cada avaliador usa uma escala diferente, onde a Microsoft divide em somente 4 pontuações, enquanto a avaliação do KeePass divide em 6 possibilidades, (tab.9).

Tabela 8 - Tabela comparativa de senhas em diferentes avaliadores de força

Senhas testadas	<i>KeePass Basic</i>	<i>KeePass Advanced</i>	<i>KeePass Built-in</i>	<i>Password Meter-on line</i>	<i>Microsoft -on line</i>
\$EZLN%32	Forte-5/6	Média-4/6	Razoável-3/6	Forte-4/5	Forte-3/4
2211_251	Forte-5/6	Média-4/6	Razoável-3/6	Muito Fraca-1/5	Média-2/4
271084_	Forte-5/6	Média-4/6	Razoável-3/6	Boa-3/5	Fraca-1/4
3U5IBTM*	Forte-5/6	Média-4/6	Razoável-3/6	Boa-3/5	Forte-3/4
ALEX99%	Forte-5/6	Média-4/6	Razoável-3/6	Boa-3/5	Fraca-1/4
BAL*13LP	Forte-5/6	Média-4/6	Razoável-3/6	Boa-3/5	Forte-3/4
DU@RT373	Forte-5/6	Média-4/6	Razoável-3/6	Forte-4/5	Forte-3/4
M@RT@85	Forte-5/6	Média-4/6	Razoável-3/6	Boa-3/5	Fraca-1/4

Tabela 9 - Tabela das avaliações possíveis em cada tipo de análise

Avaliações Possíveis <i>KeePass Built-in</i>	Avaliações Possíveis <i>Password Meter - on line</i>	Avaliações Possíveis <i>Microsoft - on line</i>
Muito Fraca 1/6	Muito Fraca 1/5	Fraca 1/4
Fraca 2/6	Fraca 2/5	Média 2/4
Razoável 3/6	Boa 3/5	Forte 3/4
Média 4/6	Forte 4/5	Melhor 4/4
Forte 5/6	Muito Forte 5/5	
Muito Forte 6/6		

Acreditando que a análise ficaria melhor se o banco de palavras do dicionário utilizado no relatório *Advanced* fosse um dicionário em português, buscou-se mais informações sobre o *plugin StrengthReport* e o contato com os autores, questionando a possibilidade da inserção de palavras do dicionário português de Brasil e Portugal para uma análise de acordo com a realidade brasileira.

Após descobrir os autores do *plugin*, os húngaros Péter Török, Adam Erdelyi, na Universidade de Szeged, foi tentado o contato com ambos. Após algumas semanas

Péter Török respondeu à solicitação e enviou dois arquivos '.dll', (i.e., *Dynamic-link library* - biblioteca de ligação dinâmica) e as instruções de como fazer para utilizar um outro dicionário que acordo com a conveniência, o que provocou a necessidade de desinstalar a versão do software de gerenciamento de senhas KeePass Password Safe 2.08 e instalar a versão 2.09, por ser mais atual e permitir os testes que serão mostrados a seguir.

Utilizando as novas possibilidades, foi refeita a análise que se baseou em um dicionário de palavras em português do Brasil e de Portugal, compilado a partir de dicionários disponíveis na internet.

Foi utilizado um dicionário contendo 712132 palavras, utilizando os mesmos parâmetros do dicionário inglês existente, com a menor palavras com 3 letras e a maior com 28.

O que se poderia chamar de quarta análise foi elaborada a partir do novo dicionário de palavras em português e que resultou em diferenças, conforme era o resultado esperado da hipótese.

Devido ao fato do dicionário de palavras só ser levado em consideração no relatório *Advanced*, será somente nele que se refletirão as diferenças da força das senhas. A variação das senhas muito fracas elevou somente 0,19 pontos percentuais, ficando a maior modificação sendo observada nas senhas fracas, que de 18,07% elevaram-se 9,76 pontos percentuais alcançando 27,83% do total, (tab.10).

Desta forma fica claro que senhas que eram consideradas razoáveis mudaram de classificação, aumentando o número das senhas fracas e fazendo alterar o percentual das senhas razoáveis de 13,38% para 3,44%.

Estes resultados reforçam a hipótese de que diferentes bancos de palavras irão mostrar diferentes resultados, assim como diferentes algoritmos irão classificar as senhas de modos diferentes.

Tabela 10 - Comparação da força das senhas com dicionários inglês e português

Força da senha	<i>Advanced</i> Dicionário Inglês	%	<i>Advanced</i> Dicionário Português	%
Muito Fraca 1/6	9460	68,48	9487	68,67
Fraca 2/6	2497	18,07	3845	27,83
Razoável 3/6	1849	13,38	475	3,44
Média 4/6	9	0,07	8	0,06
Forte 5/6	0	0,00	0	0,00
Muito Forte 6/6	0	0,00	0	0,00
Totais	13815	100,00	13815	100,00

X.7 ANÁLISE DOS CARACTERES USADOS NAS SENHAS

Segundo Burnett (2005), a segurança da senha baseia-se em uma estratégia básica: criar uma senha que ninguém pode prever (ou adivinhar) dentro de uma quantidade razoável de tempo, e então modificá-la regularmente para melhorar sua força e continuamente tornar difícil sua adivinhação. Para que se possa aumentar a dificuldade da previsão das senhas deve-se aplicar a aleatoriedade dos caracteres usados na formação das senhas.

Segundo a Wikipedia(2009), a palavra aleatoriedade é usada para expressar a falta de ordem ou possibilidade de previsão de um processo, cujo resultado não segue um padrão determinado, mas uma distribuição de probabilidade.

Como a linguagem humana segue um padrão em sua composição é de se esperar que as senhas derivadas também sigam um padrão determinado. Burnett (2005) declara que a maioria das pessoas prefere senhas com letras minúsculas e alguns números, e que se as senhas usassem critérios aleatórios, os caracteres usados nelas não seguiriam um padrão, como o encontrado por ele por meio da análise de 3 milhões de senhas. Segundo sua pesquisa, o número mais usado é o "1", e as 10

principais letras em ordem decrescente de uso são "e","a","r","o","s","i","n","t","l" e "c". Seu estudo, porém não informa valores percentuais de uso de cada letra.

Buscando determinar mais características das senhas usadas no banco Obsoleto, e comparar com os dados levantados por Burnett, foi realizado um levantamento dos caracteres usados na composição das senhas, utilizando a linguagem de programação Regina REXX e após os resultados foram importados para o Excel 2007.

Foram contados 88151 caracteres em 13815 senhas e este levantamento logicamente reafirma que a concentração maior encontra-se nos caracteres numéricos, concentrando 84,72% dos caracteres usados.

Os restantes 16,28% distribuem-se com 15,24% entre as letras e apenas 0,04% em outros caracteres. Observa-se que a distribuição entre as letras não é uniforme, sendo que entre as 10 letras mais usadas, 4 são as vogais "A","I","E" e "O" em ordem decrescente de ocorrências (tab.11).

Examinando a distribuição dos caracteres numéricos verifica-se que há uma pequena preferência para os números "1", "2" e "9", enquanto no estudo americano a preferência é notória para o número "1" com 21%, já o número "2" fica com 13% e o número "0" com 10%.

Considerando-se que no banco Obsoleto só há caracteres maiúsculos, identifica-se a grande semelhança entre os dados encontrados por Burnett e os encontrados neste levantamento, que variam no total de ocorrências, mas onde as vogais "A","E","I" e "O" e a consoante "R" aparecem em maior quantidade de senhas.

Estes números evidenciam a preferência por alguns caracteres em relação a outros, onde alguns aparecem pouquíssimas vezes nas senhas como os caracteres "X","Q","W","Y" e "Z".

Tabela 11 - Distribuição dos caracteres nas senhas

Caráter	Ocorrências	%
1	9164	10,3958
2	8292	9,4066
9	7732	8,7713
3	7328	8,3130
0	7286	8,2654
8	7230	8,2018
4	6957	7,8921
7	6948	7,8819
6	6886	7,8116
5	6856	7,7776
A	2103	2,3857
I	1282	1,4543
E	1160	1,3159
R	996	1,1299
O	934	1,0595
N	852	0,9665
L	821	0,9314
S	664	0,7533
C	578	0,6557
T	525	0,5956
M	523	0,5933
U	454	0,5150
D	440	0,4991
G	340	0,3857
B	292	0,3312
P	290	0,3290
H	229	0,2598
F	199	0,2257
V	191	0,2167
J	147	0,1668
K	114	0,1293
Z	94	0,1066
Y	57	0,0647
W	53	0,0601
Q	51	0,0579
X	49	0,0556
.	12	0,0136
@	4	0,0045
\$	3	0,0034
%	3	0,0034
-	3	0,0034
*	2	0,0023
-	2	0,0023
	2	0,0023
&	1	0,0011
=	1	0,0011
Espaço	1	0,0011
Totais	88151	100,0000

Com a finalidade de identificar a distribuição das letras do dicionário de palavras utilizado para a comparação com as senhas do banco de dados Obsoleto, foi realizado outro levantamento.

Descobriu-se que de um total de 712132 palavras do dicionário foram contados 7.807.908 caracteres e este levantamento mostra que a concentração maior de letras usadas em palavras do dicionário português do Brasil/Portugal são os caracteres "A", "E", "S", "R", "I", "O", "L", "N", "M", "T" em ordem decrescente de ocorrências. Estes 10 caracteres são responsáveis por 77,03% do total das palavras do dicionário, restando para os outros 30 caracteres o total de 22,97% das ocorrências (tab.12).

O levantamento realizado confirmou como sendo as mesmas 10 letras mais utilizadas que o estudo americano apresenta, mudando somente a ordem de ocorrência delas. Quando se compara o estudo americano com o levantamento dos caracteres das palavras do dicionário verifica-se que 9 das 10 letras mais usadas são as mesmas, variando o número de ocorrências (tab.13).

Os resultados revelam que as senhas alfabéticas seguem um padrão de distribuição de letras de palavras do dicionário, e que se confirma tanto no estudo americano como neste, pela semelhança dos resultados encontrados.

Tabela 12 - Distribuição dos caracteres no dicionário utilizado

Caracteres	Ocorrências	%
a	1017800	13,0355
e	899614	11,5218
s	780445	9,9956
r	748049	9,5807
i	633772	8,1171
o	590114	7,5579
l	344192	4,4082
n	337871	4,3273
m	335779	4,3005
t	327048	4,1887
c	272538	3,4905
d	237076	3,0364
u	181345	2,3226
a agudo	154883	1,9837
p	151680	1,9426
v	140250	1,7963

h	125466	1,6069
g	95586	1,2242
b	95142	1,2185
f	84449	1,0816
z	68583	0,8784
i agudo	49289	0,6313
j	24006	0,3075
q	23165	0,2967
a til	22545	0,2887
cedilha	21836	0,2797
x	18856	0,2415
e circunflexo	8823	0,1130
e agudo	5826	0,0746
o agudo	4788	0,0613
o nasalado	2828	0,0362
u agudo	2158	0,0276
a circunflexo	772	0,0099
o circunflexo	554	0,0071
k	270	0,0035
y	175	0,0022
w	169	0,0022
u tremado	149	0,0019
a craseado	11	0,0001
e craseado	6	0,0001
Totais	7807908	100,0000

Cabe explicar que na tabela 12, há a presença do carácter "a craseado" que consta no dicionário de palavras, como na palavra "àquela" e o carácter "e craseado" que também consta no dicionário, como no nome próprio "Lumière".

Tabela 13 - Distribuição dos caracteres nos três levantamentos

Classificação	Caracteres mais usados pelo estudo americano	Caracteres mais usados nas senhas do banco Obsoleto	Caracteres mais usados nas palavras do dicionário
1°	e	a	a
2°	a	i	e
3°	r	e	s
4°	o	r	r
5°	s	o	i
6°	i	n	o
7°	n	l	l
8°	t	s	n
9°	l	c	m
10°	c	t	t

CONCLUSÕES

Através deste estudo evidencia-se que o usuário não está atento de como pode tentar se proteger das ameaças que rondam no mundo digital, pois ele cria senhas muito simples e não possui a cultura da segurança, ao mesmo tempo também é fácil identificar que muitos sistemas permitem o ingresso de senhas que possuem muito pouca força.

A área da segurança da informação pode utilizar-se de levantamentos como os desenvolvidos neste trabalho para estimular que os usuários criem senhas mais fortes, como é o caso dos sistemas que vão mostrando a força da senha assim que ela vai sendo digitada. Isto permite ao usuário ter um retorno imediato sobre a qualidade de sua senha e assim buscar melhorá-la.

Há também sistemas que avisam quando o teclado está travado para escrever somente letras maiúsculas, evitando que se tente acessar o sistema com a senha correta, porém escrita com letras capitais.

Outra possibilidade é mostrar ao usuário, de tempos em tempos, quando foi gerada a senha que ele está usando, para que assim seja estimulado a alterá-la buscando mais segurança.

Os resultados confirmaram as afirmações de que os usuários evitam misturar letras, números e outros caracteres. Ela supõe que isto acontece devido à dificuldade de lembrar as senhas criadas desta maneira.

Examinando os resultados da força das senhas conclui-se que as afirmações de pesquisas anteriores citadas em 1999 continuam válidas quando afirmam que as pessoas tendem escolher as mais fracas senhas permitidas pelo sistema. Estas afirmações são reforçadas quando constatamos que a minoria dos usuários usou caracteres especiais na formação de suas senhas, com somente 0,16% das 13815 senhas analisadas do banco Obsoleto.

Considerando que as pesquisas já haviam indicado que a verdadeira causa do erro humano é devido à sobrecarga das capacidades humanas de processamento de informações, e que lembrar de senhas que são consideradas fortes exigem um esforço muito grande da memória, torna-se notório que não basta culpar os usuários por seus comportamentos.

Conclui-se, portanto que se deve buscar auxílio da tecnologia para projetar sistemas que estimulem o usuário a criar senhas fortes, impedindo-o mesmo de criar senhas fracas, e após sua criação, protegê-las em banco de dados criptografados para senhas como o utilizado neste estudo.

Sugere-se que simultaneamente à criação de sistemas mais seguros deve-se investir em biometria para que o peso da responsabilidade do usuário diminua e ao mesmo tempo ele tenha mais segurança.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 17799: **Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação**. Rio de Janeiro, 2005. 120p.

BAGUETE **Perto e Bradesco: biometria abre contas**. 23 jun. 2009. Disponível em <<http://www.baguete.com.br/noticiasDetalhes.php?id=3508243>>. Acesso em 15 out. 2009.

BAIXAKI **Troque suas senhas: listas de senhas do Gmail e do Hotmail vazaram na internet**. 8 out. 2009. Disponível em: <<http://www.baixaki.com.br/info/2875-troque-suas-senhas-listas-de-senhas-do-gmail-e-do-hotmail-vazaram-na-internet.htm>>. Acesso em 16 out. 2009.

BERNSTEIN, T.; BHIMANI, A; SCHULTZ, E & SIEGEL, C. **Segurança na Internet**. Editora Campus, 1997. 461p.

BURNETT, Mark **Perfect Passwords: selection, protection, authentication**. Syngress Publishing, 2006. 181p.

BURNETT, Steve; PAINE, Stephen **Criptografia e segurança: o guia oficial RSA**. Editora Campus, Rio de Janeiro, 2002. 367p.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL **Cartilha de Segurança para Internet**. 11 jul. 2007. Disponível em: <<http://cartilha.cert.br/>>. Acesso em 13 set. 2009.

CHAMBERLAWS **Top 20: Senhas mais usadas**. 22 jan. 2009. Disponível em <<http://chamberlaws.com/2009/01/top-20-senhas-mais-usadas.html>>. Acesso em 15 out. 2009.

CLUBE DO HARDWARE **Smart Card**. 04 dez. 2002. Disponível em:
<<http://www.clubedohardware.com.br/artigos/665>>. Acesso em 28 out. 2009.

COMPUTERWORLD **Brasileiros confiam na biometria para proteção de dados, diz pesquisa**. 20 jan. 2009. Disponível em:
<<http://computerworld.uol.com.br/negocios/2009/01/20/brasileiros-confiam-na-biometria-para-protecao-de-dados-diz-pesquisa/>>. Acesso em 16 out. 2009.

_____ **Conheça a nova geração de prevenção a fraudes financeiras**. 19 jun. 2009. Disponível em
<<http://computerworld.uol.com.br/seguranca/2009/06/19/conheca-a-nova-geracao-de-prevencao-a-fraudes-financeiras/>>. Acesso em 16 out. 2009.

_____ **Pesquisa: 64% das empresas não exigem troca regular de senhas**. 9 set. 2008. Disponível em:
<<http://computerworld.uol.com.br/seguranca/2008/09/09/pesquisa-64-das-empresas-nao-exigem-troca-regular-de-senhas/>>. Acesso em 16 out. 2009.

DATE, C.J. **Introdução a sistemas de bancos de dados**. Editora Campus, Rio de Janeiro, 2004. 865p.

DECISION REPORT **O paradoxo da segurança**. 13 jul. 2009. Disponível em <
<http://www.decisionreport.com.br/publique/cgi/cgilua.exe/sys/start.htm?infoid=4763&sid=1>>. Acesso em 15 out. 2009.

EBAND **Senha 123456 era a mais comum entre as vazadas**. 7 out. 2009.
Disponível em:
<<http://www.band.com.br/jornalismo/tecnologia/conteudo.asp?ID=200031>>. Acesso em 16 out. 2009.

IDGNOW **Contas do Hotmail que vazaram na web tinham senhas fracas, mostra análise**. São Paulo, 7 out. 2009. Disponível em:
<<http://idgnow.uol.com.br/seguranca/2009/10/07/contas-do-hotmail-que-vazaram-na-web-tinham-senhas-fracas-mostra-analise/>>. Acesso em 16 out. 2009.

_____ **Sistema de biometria analisa padrões cerebrais e batimentos**

cardíacos. São Paulo, 9 mar. 2009. Disponível em:

<<http://idgnow.uol.com.br/seguranca/2009/03/09/sistema-de-biometria-analisa-padroes-cerebrais-e-batimentos-cardiacos/>>. Acesso em 16 out. 2009.

_____ **Roubo de senhas.** São Paulo, 1 jul. 2009. Disponível em:

<http://idgnow.uol.com.br/seguranca/mente_hacker/idgcoluna.2009-06-28.5137710879/>. Acesso em 16 out. 2009.

INFOSERVER **Fim do furto de senhas.** Disponível em:

<<http://www.infoserver.com.br/news/new030608.asp>>. Acesso em 29 out. 2009.

INTERNETLEGAL **Banco deve indenizar correntista que teve conta invadida por**

cracker. 5 out. 2009. Disponível em

<<http://www.internetlegal.com.br/2009/10/banco-deve-indenizar-correntista-que-teve-conta-invadida-por-cracker/>>. Acesso em 29 out. 2009.

_____ **TJRS decide que banco não responde por vazamento de senha no computador do cliente.** 21 out. 2009. Disponível em

<<http://www.internetlegal.com.br/2009/10/tjrs-decide-que-banco-nao-responde-por-vazamento-de-senha-no-computador-do-cliente/>>. Acesso em 29 out. 2009.

JAKOB NIELSEN'S ALERTBOX **User Education Is Not the Answer to Security**

Problems. 25 out. 2004. Disponível em

<<http://www.useit.com/alertbox/20041025.html>>. Acesso em 15 set. 2009.

MICROSOFT **Ajude a proteger suas informações pessoais com senhas fortes.**

22 mar. 2006. Disponível em:

<<http://www.microsoft.com/brasil/athome/security/privacy/password.msp>>. Acesso em 16 out. 2009.

_____ **Verificador de senha**. Disponível em:

<http://www.microsoft.com/brasil/athome/security/privacy/password_checker.msp>.

Acesso em 12 set. 2009.

MORENO, E.D.; PEREIRA, F.D.; CHIARAMONTE, R.B. **Criptografia em Software e Hardware**. Novatec Editora, São Paulo, 2005. 288p.

MOTA, VIKTOR **Senha complicada não impede invasão**. 17 jul. 2009. Disponível em: <<http://www.viktormota.adm.br/v2/2009/07/17/senha-complicada-nao-impede-invasao/>>. Acesso em 27 out. 2009.

PRESSMAN, R.S. **Engenharia de software**. Makron Books do Brasil Editora, São Paulo, 1995. 1056p.

RUSSEL, Deborah; GANGEMI SR, G. T. **Computer Security Basics**. O'Reilly & Associates, USA, 1991. 448p.

SILVA, D. R. P. da. **A memória humana no uso de senhas**. 2007. 105 f. Tese (Doutorado em Psicologia)-Faculdade de Psicologia, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2007.

SUEHRING, Steve **MySQL, a Bíblia**. Editora Campus, Rio de Janeiro, 2002. 674p.

The Password Meter **Password Strength Checker**. Disponível em:

<<http://www.passwordmeter.com>>. Acesso em 13 set. 2009.

WIKIPÉDIA **Aleatoriedade**. Disponível em:

<<http://pt.wikipedia.org/wiki/Aleatoriedade>>. Acesso em 16 out. 2009.