

Abre-te Sésamo! A password como representação do sujeito

Rosa Lúcia Coimbra e Urbana Pereira Bendiha

Universidade de Aveiro

1. Introdução

A escolha de uma password revela muito do utilizador das novas tecnologias, já que, para ser facilmente memorizável, deve vir ao encontro de uma motivação pessoal. Esta ligação ao sujeito, que se verifica quando se escolhe como password, por exemplo, nomes de familiares ou de animais de estimação ou datas significativas, é feita em detrimento da segurança. De facto, o risco de terceiros descobrirem e virem a utilizar indevidamente a password aumenta em proporção directa com a transparência em relação ao sujeito. Este acesso indevido poderá ser perpetrado, quer directamente por um conhecimento pessoal, quer por *hackers* através da chamada “engenharia social”.

Tal como no conto de *As Mil e Uma Noites*, os perigos de perda de exclusividade deste conhecimento são reais. Os quarenta ladrões tinham como objectivo proteger o seu saque de ser roubado. Para isso, confiaram num mecanismo de segurança protegido por uma password. Por um dispositivo mágico, a porta da gruta obedecia às palavras, independentemente da voz. A intenção era a de permitir o acesso apenas aos membros do bando, mas o mecanismo não podia evitar que outros usassem esta password (Smith, 2001, p. 5), o que veio a acontecer com Ali Babá. Um segundo perigo é o do esquecimento da password, que, na história, é ilustrado com o episódio de Cacim, que fica preso na gruta.

Nesta comunicação, pretendemos abordar a questão da password como representação do sujeito, quer no aspecto cultural, quer linguístico. Para tal, efectuámos o estudo e a análise dos resultados de um inquérito feito a utilizadores das novas tecnologias, no qual foram aferidos diversos aspectos relacionados com a construção de passwords e com a consciência ou não da dicotomia segurança-memorização.

Como ponto de partida, estabelecemos uma analogia com a história de Ali Babá e os quarenta ladrões.

2. Enquadramento teórico

2.1. O sujeito na linguagem

Qualquer ser humano, no acto de comunicar, não abdica da sua subjectividade. Esta característica do sujeito falante é tão vincada que está presente mesmo na interacção homem-máquina, até quando o sujeito tem consciência de estar perante um objecto incapaz do mesmo tipo de comportamento. Benveniste (1966: 259) aborda esta realidade nos seguintes termos:

É na e pela linguagem que o homem se constitui como *sujeito*; porque só a linguagem funda na realidade, na *sua* realidade que é a do ser, o conceito de “ego”./ A “subjectividade” de que tratamos aqui é a capacidade do locutor se colocar como “sujeito”.

Colocado de outro modo:

As marcas de subjectividade são atravessadas pelas relações sociais, reflexo de exterioridades lingüísticas, projetadas a partir de potencialidades internas advindas das ações dos sujeitos na/da linguagem (Santos, 2004).

Neste sentido, decidimos verificar até que ponto uma comunicação aparentemente neutra e completamente impessoal como é o caso da utilização de passwords para acesso a sistemas informáticos apresenta essas mesmas características.

2.2. O que é uma password?

Mesmo antes da existência de computadores, fez-se sentir a necessidade de factores de autenticação do utilizador legítimo de determinados sistemas (cofres por exemplo). Actualmente, é usual dividirem-se estes factores em três grandes categorias: o que conhecemos (password, código PIN, combinação...); o que temos (ficha, cartão

magnético, chave mecânica...); e o que somos (características biométricas tais como impressão digital, scan do olho, reconhecimento de voz, fotografia...). Cada um destes tipos de autenticação apresenta vantagens e inconvenientes, e podem surgir combinados uns com os outros (por exemplo, um cartão bancário com fotografia e código PIN). Na história de *As Mil e Uma Noites*, a frase senha “Abre-te, Sésamo!” é evidentemente do primeiro tipo; aliás, é pelo facto de não conter características biométricas de reconhecimento de voz, que as personagens Ali Babá e Kasim puderam entrar na gruta, depois terem ilicitamente obtido conhecimento das palavras mágicas.

A palavra password, de origem inglesa e mantendo a grafia original, constitui uma entrada no *Dicionário da Língua Portuguesa Contemporânea da Academia das Ciências de Lisboa*. Aí surge como sinónimo de senha, que, por sua vez, remete para palavra-chave, a qual é definida como “palavra, fórmula ou série de caracteres alfanuméricos, privativa e sigilosa, que permite aceder a uma área de trabalho, uma rede..., vedando o acesso a estranhos”. É precisamente esta a função de “Abre-te, Sésamo!” na história de Ali Babá: “e ele pronunciou estas estranhas palavras: ‘Abre-te, Sésamo!’ e imediatamente apareceu uma larga passagem à superfície da rocha” (ver nota 1).

Na escolha de uma password, devem ser respeitados alguns critérios, por razões de segurança, entre os quais podemos destacar os seguintes:

- o número de caracteres (quantos mais, maior é a segurança garantida pela password);
- alternância de letras (maiúsculas e minúsculas), algarismos e símbolos não alfabéticos;
- evitar qualquer sequência que possa ser facilmente relacionada com a pessoa.

Tendo em mente estes critérios, criámos, para o nosso inquérito (ponto III.4) uma password segura, embora linguisticamente opaca e dificilmente memorizável.

3. O inquérito

Na nossa pesquisa, elaborámos e passámos o seguinte inquérito de modo a caracterizar as escolhas que utilizadores de novas tecnologias fazem em relação a passwords:

Inquérito

Este inquérito é anónimo e os seus resultados e tratamento estatístico destinam-se a uma pesquisa científica. As autoras agradecem a colaboração e disponibilidade.

I. Dados do informante

Sexo: Feminino ☐ Masculino ☐

Idade: Até aos 19 ☐ Dos 20 aos 39 ☐ Dos 40 aos 59 ☐ 60 ou mais ☐

II. É utilizador da Internet?

Nunca ☐ 1 ou 2 vezes por mês ☐ 1 ou 2 vezes por semana ☐ Diariamente ☐

III. Imagine que pretende ser utilizador de um site na Internet que lhe pede para definir uma *password* (senha de acesso). A sua escolha recairia sobre:

1. nome do foro pessoal:

- 1.1. o meu nome ou outra forma de tratamento que me designe ☐
- 1.2. o nome de um familiar ☐
- 1.3. o nome do/a meu/minha companheiro/a ☐
- 1.4. o nome de um/a amigo/a ☐
- 1.5. o nome do meu animal de estimação ☐
- 1.6. o nome de um lugar significativo ☐
- 1.7. outro nome significativo ☐

2. data significativa do foro pessoal:

- 2.1. nascimento ☐
- 2.2. relacionamento amoroso ☐
- 2.3. casamento ☐
- 2.4. divórcio ☐
- 2.5. morte ☐
- 2.6. acontecimento religioso ☐
- 2.7. outro ☐

3. personalidades, datas, factos etc. relacionados com:

- 3.1. Literatura ☐
- 3.2. Música ☐
- 3.3. Desporto ☐
- 3.4. Cinema ☐
- 3.5. Ciência ☐
- 3.6. Artes Plásticas ☐
- 3.7. História ☐
- 3.8. outro domínio ☐

4. uma senha sem significado (por exemplo fTg54k&M8) ☐

IV. A quantas pessoas confiaria a sua password?

Nenhuma ☐ 1 ou 2 ☐ 3 ☐ Mais de 3 ☐

Assim, foram inquiridos 70 informantes, dos quais 45 do sexo feminino e 25 do sexo masculino e de idades agrupadas em quatro escalões: até aos 19 anos (14 mulheres e 12 homens); dos 20 aos 39 anos (25 mulheres e 13 homens); dos 40 aos 59 anos (5 mulheres e 1 homem). No escalão de 60 ou mais anos, não tivemos informantes.

Na primeira questão do inquérito, aborda-se a frequência de utilização da internet (ver figura 1). Os resultados obtidos dividem-se em: nunca (1 homem); 1 ou duas vezes por mês (4 mulheres e 4 homens); 1 ou 2 vezes por semana (18 mulheres e 2 homens); diariamente (20 mulheres e 18 homens). Ou seja, os nossos informantes são, globalmente, utilizadores frequentes da internet e, consequentemente, habituados a lidar com as novas tecnologias da informação.

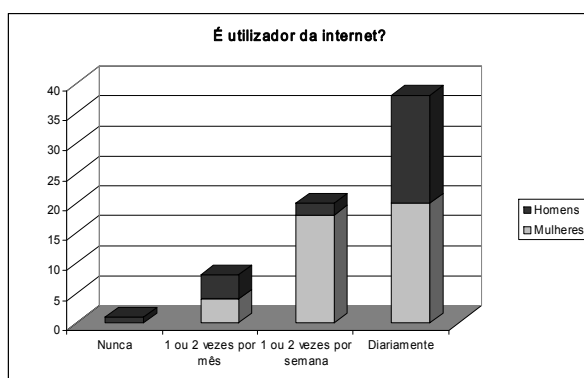


Figura 1

4. Apresentação e interpretação dos resultados

A parte fulcral do inquérito consiste na apresentação de uma situação hipotética em que o informante se encontra perante a necessidade de escolher uma password, a fim de se tornar utilizador de um site na internet. Depois da apresentação desta situação, fornece-se uma lista de domínios conceptuais possíveis de origem dessa hipotética password, divididos em três grandes áreas (ver figura 2). As duas primeiras áreas dizem mais directamente respeito ao foro pessoal do utilizador. A primeira inclui nomes relacionados com ele próprio, lugares, animais e pessoas das suas relações; a segunda abarca datas relacionadas com marcos e acontecimentos da vida do próprio. A terceira categoria, embora não directamente ligada ao sujeito, reflecte, no entanto, as suas escolhas nos sectores sócio-culturais sugeridos. Por fim, foi fornecida a hipótese de

optar por uma password sem significado, mas construída de acordo com as normas de segurança que referimos no ponto 2.2. No inquérito, era pedida uma escolha de entre este elenco de possibilidades. No entanto, vários informantes escolheram mais do que uma hipótese, frequentemente uma de cada um dos grupos apresentados.

A selecção dos itens constantes desta parte do inquérito não é, obviamente, exaustiva, reflectindo um universo de possibilidades que considerámos como possível ponto de partida. Conscientes destas limitações, tivemos o cuidado de deixar em aberto a opção por qualquer outra possibilidade (pontos 1.7, 2.7 e 3.8 do inquérito).

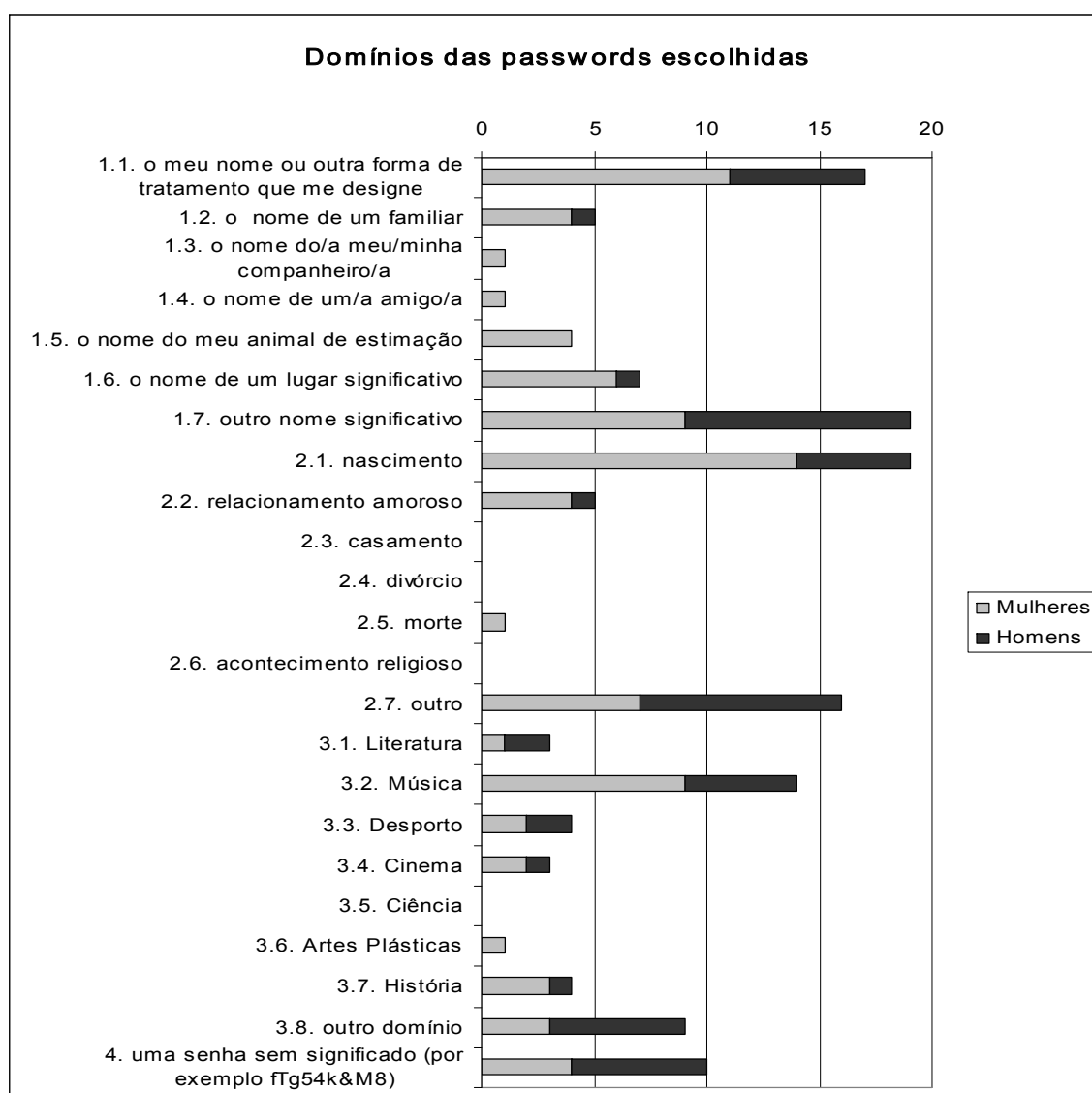


Figura 2

Dos resultados obtidos, podemos constatar que há nítidas preferências por determinadas áreas conceptuais da escolha de password, em detrimento de outras, sendo

algumas até completamente ignoradas: datas de casamento, divórcio e de acontecimento religioso e palavra ligada ao domínio da ciência. Outras áreas foram apenas escolhidas por informantes do sexo feminino: nome de companheiro(a), de amigo(a), animal de estimação, data de morte e palavra da área das Artes Plásticas. Nos restantes casos, foram escolhidas, por mulheres e homens, todo o tipo de passwords. Quantitativamente, predomina o primeiro grupo, que diz mais directamente respeito ao foro pessoal do informante, seguindo-se o segundo grupo, embora também bastante escolhido. Mais abaixo situam-se as preferências de tipo sócio-cultural. Finalmente, o grupo menos escolhido é aquele que engloba apenas a password sem sentido.

Esta password – fTg54k&M8 – foi construída, como já referido, segundo as regras de segurança preconizadas. Constatamos que foi sobretudo escolhida pelos informantes do sexo masculino: 24,0% dos homens escolheram esta password, enquanto que apenas 8,9% das mulheres optaram por ela. Inversamente, sobre as passwords mais pessoais, embora menos seguras, recaíram as escolhas femininas. As passwords, como esta, embora mais seguras, são de mais difícil memorização. Daí o risco do esquecimento da senha e consequente impossibilidade de novo acesso ao sistema. Foi o que aconteceu, na nossa história, com o personagem Kasim: “ele esqueceu-se completamente das palavras cabalísticas e gritou: ‘Abre-te, Cevada!’. Ao que a porta recusou mover-se. Totalmente aturdido e confuso, ele nomeou todos os nomes de grãos, excepto sésamo, o qual se tinha varrido da sua memória, como se ele nunca tivesse ouvido tal palavra” (ver nota 1).

No corpus em análise, com mais de 15 escolhas, apenas encontramos as possibilidades nome do próprio, outro nome significativo, data de nascimento e outra data do foro pessoal. Ou seja, tudo elementos relacionados com o sujeito e a representação que ele faz de si próprio, das suas prioridades, daquilo que considera mais importante e que o define como indivíduo. Estes são precisamente os elementos mais susceptíveis de serem captados através de “engenharia social” (Smith, 2001: 19-23), a qual consiste em investigar indevidamente o sujeito, a fim de obter a password, frequentemente aproveitando a sua boa fé ou ingenuidade. Para além dos chamados “guessing attacks”, outras formas ilícitas de obtenção desta informação consistem na intercepção da password durante a sua transmissão (foi o que fez Ali Babá ao escutar, escondido, o chefe dos ladrões), processo conhecido pela expressão “sniffing attack” e

que pode ir desde o simples espreitar por cima do ombro (daí os caracteres, por precaução, surgirem na forma de asteriscos, p. ex.), até a programas informáticos desenvolvidos com esse fim; ou ainda através de “logins troianos”, i.e., programas que tentam captar uma cópia da password mimetizando o login normal do sistema (Smith, 12001: 23-28).

Finalmente, o questionário termina com a problemática da confiança. Pergunta-se o número de pessoas a quem o sujeito confiaria a sua password.

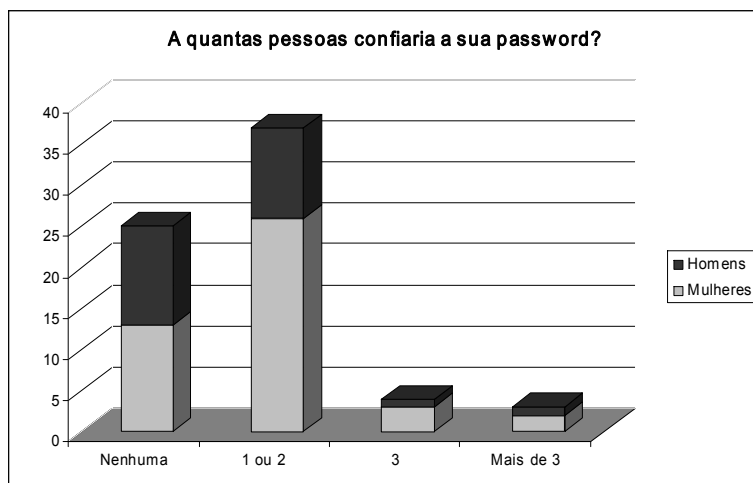


Figura 3

Dos resultados obtidos nesta questão (ver figura 3), observa-se que, apesar de um número significativo de inquiridos, tanto homens como mulheres, não confiar em ninguém a partilha da respectiva password, a maioria das respostas aponta para a existência de uma ou mais pessoas em que esta confiança é depositada. Os resultados percentuais são, no entanto, muito diferentes, nos dois grupos: 48,0% dos homens não confiariam a sua password a ninguém, contra apenas 28,9% no caso das mulheres.

5. Conclusão

Partindo de uma analogia com a história de Ali Babá e os quarenta ladrões, fizemos um estudo sobre a utilização de passwords em sistemas informatizados. Com o inquérito que serviu de suporte à pesquisa, pretendemos abarcar uma ampla gama de domínios conceptuais onde as palavras senha se inserem. No entanto, um estudo mais

aprofundado e linguisticamente mais elucidativo só seria possível se se tivessem solicitado passwords reais, o que, obviamente, traria problemas éticos inultrapassáveis.

Assim, perante os dados obtidos, procurámos caracterizar o tipo de password mais escolhido, de acordo com o sujeito utilizador das novas tecnologias e da sua própria representação. O aspecto mais relevante parece-nos ser o facto de que as pessoas, principalmente as mulheres, parecem privilegiar a identidade em detrimento da segurança.

Um alargamento e aprofundamento desta investigação seria possível, por exemplo, estendendo o inquérito a mais informantes, pedindo mais dados caracterizadores, para além das variáveis sexo e idade. De acordo com as variáveis escolhidas – que poderiam incluir, por exemplo, nacionalidade e local de residência, nível de escolaridade, profissão, etc. – poder-se-ia proceder ao cruzamento de dados, de modo a testar possíveis co-relações caracterizadoras de determinados grupos de sujeitos.

Tal como qualquer pesquisa científica, esta é, portanto, também um campo aberto de possibilidades exploratórias.

6. Referências

Benveniste, Émile, *Problèmes de Linguistique Générale*, Paris, Gallimard, 1966.

Burton, Francis, “Ali Baba And The Forty Thieves”, http://mfx.dasburo.com/an/a_night_30.html

Santos, João Bôsko Cabral, apresentação de: Fernandes C. A et al. (orgs.), *Sujeito, Identidade e Memória*, Uberlândia, EDUFU, 2004.

Casteleiro, Malaca João (coord.), *Dicionário da Língua Portuguesa Contemporânea da Academia das Ciências de Lisboa*, Lisboa, Academia das Ciências de Lisboa e Editorial Verbo, 2001.

ISECOM, *Hacker highschool. Security awareness for teens*, 2004

http://www.hackerhighschool.org/lessons/HHS_en11_Passwords.pdf

Smith, Richard E., *Authentication. From Passwords to Public Keys*, Addison-Wesley, 2001.