Contributos para a criação de uma password segura

Nuno Casteleiro de Goes

ncgoes@gmail.com

Resumo

Hoje em dia é bastante fácil de obter passwords alheias devido à quantidade de software que podemos encontrar na internet para os mais variados casos. As passwords são a chave de acesso a informações pessoais armazenadas num computador ou a contas online. A integridade dos dados depende da sua protecção e, na maior parte dos casos, depende duma password que se quer pessoal e intransmissível. Este artigo explica os erros mais comuns e as regras que deve respeitar para a criação duma password segura e de como a defender de ataques externos.

Palavras-chave: password, palavra-chave, password, *cracker*, *cracking*, protecção da informação, segurança

1. Introdução

No presente, quase todos os serviços da internet que contêm informação do utilizador são protegidos com uma password. Se alguns intrusos ou outros utilizadores mal-intencionados roubarem estas informações, poderão usá-las no seu nome para abrir novas contas de cartão de crédito, solicitar crédito imobiliário ou passar-se por si em transacções online. Na maioria dos casos, só perceberia os ataques quando fosse tarde demais. É muito importante ter alguns cuidados quando escolher uma password.

Escolher uma password fraca eleva muito o risco de ter o seu site ou seu e-mail invadido por terceiros. Na posse da sua password uma pessoa mal intencionada pode retirar o seu site do ar, ler e apagar mails e realizar crimes na internet utilizando o seu nome. Neste artigo abordam-se os erros mais comuns a criar passwords, bem como as regras e as técnicas para criar passwords seguras. Por fim apresentam-se algumas conclusões.

2. Segurança

2.1. Métodos de quebra de passwords

A maior ameaça no que toca à quebra de passwords são os *crackers. Cracker* é o termo usado para designar quem pratica a quebra (ou *cracking*) de um sistema de segurança, de forma ilegal ou sem ética (Wikipédia 2010). Existem *crakers* de software, os programadores, que desenvolvem vírus, trojans e outras aplicações mal intencionadas e os *crackers* criptográficos. Os últimos dedicam-se à quebra de criptografia (*cracking codes*). Este é um procedimento que pode ser executado de várias formas, tanto com lápis e papel, como com o uso de computadores, dependendo da fonte do problema a ser solucionado. *Cracking* define-se como o acto de quebrar uma password ou criptografia através de vários métodos tais como: *brute force*, dicionários, dedução, engenharia social, *exploits*, engenharia inversa, *phishing*, *fake shells* entre outros.

As abordagens são muito variadas podendo ir do teste de todas as combinações possíveis de escrever num teclado, como é o caso do *brute force*, até à utilização da lista de palavras constantes num dicionário.

O problema é que ao fazerem isto estão a dar os seus dados ao *craker* que agora tem livre acesso à sua informação. Existem vários métodos de ataque para quebrar passwords ou forjar mecanismos de autenticação (Penedo 2006):

- *Brute force attacks* – teste de passwords, que normalmente percorre o alfabeto de forma sequencial, até que a autenticação seja bem sucedida. Um mecanismo simples para evitar este tipo de ataque passa por limitar o número de tentativas falhadas, bloqueando as credenciais;
- *Dictionary attacks* – teste de passwords, com recurso a uma lista de palavras bem conhecidas e com grande probabilidade de sucesso. A prevenção para este tipo de ataques, para além do exemplo anterior, é a não utilização de palavras do dicionário como password;
- *Key loggers* – são pequenos programas, inadvertidamente instalados no computador, que registam a actividade de um utilizador no teclado, enviando posteriormente a informação pela Internet.

O método de ataque mais bem sucedido, no entanto, é a chamada Engenharia Social, que se resume a convencer o dono de uma palavra passe a divulgá-la de forma consciente. Regra geral, são estas as abordagens mais utilizadas para apanhar e quebrar passwords.

2.2. Erros mais comuns

2.2.1. Criar passwords baseadas em sequências

Quando um indivíduo mal-intencionado quer descobrir a password de alguém, geralmente tenta primeiro sequências como 123456, abcdef, 1020304050, qwerty (sequência do teclado), entre outros. As passwords sequenciais podem ser decoradas com grande facilidade. Por outro lado, podem ser descobertas com poucas tentativas. Embora possa parecer uma orientação óbvia, muitos problemas de segurança nas empresas e nos serviços da internet ocorrem devido ao uso de passwords deste tipo. Podem ser descobertas com tanta facilidade que são cada vez mais comuns mecanismos que impedem o uso de sequências quando o utilizador vai criar uma password.

2.2.2. Usar datas especiais, número da matrícula do carro, nomes ou termos óbvios

Muitos utilizadores usam dias especiais, como a data de aniversário de um familiar ou a data de casamento, como password. Da mesma maneira, há quem utilize o número da matrícula do carro, o número da sua residência, o número do telefone, o número dum documento, o nome de um filho, o apelido invertido, entre outros. Esta prática é mais segura que o uso de sequências. Por outro lado, uma pessoa mal-intencionada pode descobrir que uma data tem muito significado para o utilizador e levar isso em consideração quando tentar descobrir a

sua password. Além disso, alguém pode ver o utilizador a olhar para um documento antes de escrever a password. Portanto, evitar o uso dessas informações é uma maneira eficiente de reforçar a sua segurança.

2.2.3. Utilizar passwords relacionadas com os seus gostos

Evite utilizar o nome do clube como password. Evite utilizar o nome da banda ou de seus músicos como password. Adora os livros de um determinado escritor? Evite utilizar o nome dele ou de personagens das obras como password. Geralmente quando alguém gosta muito de alguma coisa deixa isso claro perante todos à sua volta, esquecendo-se que todos os que estão ao seu lado também ouvem. Logo, as hipóteses de uma pessoa criar uma password com base nos seus gostos são grandes e um indivíduo mal-intencionado sabe disso. Não crie perguntas que podem ser respondidas facilmente, como por exemplo, "Qual o maior clube de Portugal?" (Benfica). Use perguntas cujas respostas só você conhece, como "Qual o nome da rapariga que me deu o primeiro não?".

2.2.4. Utilizar palavras que estão ao seu redor

A marca do computador do gabinete, o modelo do monitor na sua mesa, o nome da loja que vê da sua janela, enfim, qualquer nome à sua volta pode parecer uma boa ideia para uma password, especialmente quando se trata de uma termo longo e difícil de ser assimilado à primeira tentativa. O problema é que se olhar para algum desses nomes antes de digitar a password, alguém próximo poderá perceber. Portanto, evite usar como passwords termos que são facilmente visíveis no seu ambiente.

2.2.5. Criar passwords parecidas com as anteriores

Muitos sistemas exigem ou recomendam a troca periódica das passwords. Quando o fizer, tenha o cuidado de não utilizar sequências de caracteres semelhantes às anteriores (que apenas diferem num ou noutro caracter, por exemplo) ou mesmo passwords que já tenham sido utilizadas.

2.2.6. A opção "Password em branco"

Uma password em branco (sem password) é mais segura do que uma password fraca, como "1234" (Carmona 2006). Os criminosos podem adivinhar facilmente uma password simples, mas nos computadores com Windows XP, uma conta sem password não pode ser acedida remotamente por meio duma rede ou da Internet. O utilizador pode preferir usar uma password em branco na sua conta de utilizador do computador se forem respeitados os seguintes critérios:

- Tem apenas um computador ou vários computadores, mas não precisa aceder às informações de um deles a partir do outro;
- O computador está fisicamente protegido (confia em todos que têm acesso físico ao computador)

Nem sempre usar uma password em branco é uma boa ideia. Por exemplo, um portátil que costume transportar provavelmente não é fisicamente seguro pois pode ser roubado e comprometer a informação que lá estiver. Assim, neste caso deve ter uma password a proteger os seus dados.

3. Contra-Medidas

3.1. Recomendações para uma password forte

Para o intruso, uma password forte deve parecer uma sequência aleatória de caracteres. Os seguintes critérios podem ajudar uma password a tornar-se forte:

3.1.1. Use uma password longa

Cada caracter adicionado à password aumenta bastante a sua protecção. As suas passwords devem ter 8 ou mais caracteres sendo o ideal que tenham no mínimo 14 caracteres (Assunção 2002). Muitos sistemas também aceitam o uso da barra de espaços nas passwords, para que o utilizador possa criar uma frase composta por várias palavras. Uma frase secreta costuma ser mais fácil de lembrar do que uma simples password, além de ser mais longa e difícil de adivinhar. De seguida apresentam-se algumas considerações quanto ao tamanho da password:

- **Combine letras, números e símbolos:** quanto maior a variedade de caracteres da password, mais difícil será adivinhá-la.
- **Quanto menos tipos de caracteres houver na password, mais longa deverá ser**: Uma password de 15 caracteres, composta somente de letras e números aleatórios é cerca de 33.000 vezes mais forte do que uma password de 8 caracteres composta de elementos de todo o teclado. Desta forma, se não puder criar uma password que contenha símbolos, deverá torná-la consideravelmente mais longa para obter o mesmo grau de protecção. Uma password ideal combina tamanho e tipos de símbolos diferentes;
- **Use todo o teclado**: não use apenas os caracteres mais comuns. Os símbolos escritos com a tecla "Shift" pressionada enquanto o número é digitado são muito comuns nas passwords sendo considerados especiais. A sua password será muito mais forte se escolher entre todos os símbolos do teclado, incluindo sinais de pontuação que não estejam na linha superior do teclado;
- **Use palavras e frases que se possa lembrar com facilidade, mas que outras pessoas tenham dificuldade em adivinhar**: a forma mais fácil de lembrar as suas passwords e frases secretas é anotá-las.

Em geral, as passwords anotadas no papel são mais difíceis de serem comprometidas na Internet do que num gestor de passwords, site ou outra ferramenta de armazenamento baseada em software.

Muitos utilizadores ficam com a sensação que muitas das passwords roubadas são conseguidas devido a uma vulnerabilidade ou falha dos sistemas informáticos. Não deixa de ser verdade, mas a maioria das invasões bem sucedidas ocorrem devido a uma má escolha de passwords.

Uma password segura é aquela que não tem por base nenhuma palavra dum dicionário, tem caracteres especiais e principalmente, que é apenas do conhecimento do próprio

utilizador (Microsoft 2006). Para ter uma password segura é aconselhável seguir as seguintes indicações:

- Nunca usar nomes ou números que possam ser descobertos por um estranho. Isto inclui o login, o seu nome, o nome do animal de estimação, de familiares, datas importantes na família, matrícula do carro, número de telefone, entre outras;
- Nunca use palavras de dicionários, incluindo estrangeiros ou as mesmas palavras por ordem inversa;
- Não use concatenação de palavras, palavras duplicadas ou palavras conhecidas trocando letras minúsculas por maiúsculas;
- A norma ISO 17799 recomenda passwords com o mínimo de 6 caracteres. Com 4 ou menos caracteres podem ser descobertas em poucas horas. No mínimo deve usar 8 caracteres (Fraser 2002);
- Nunca use a mesma palavra em dois lugares diferentes. Se a password for descoberta apenas o local onde usa a mesma fica aberto, estando todos os outros salvaguardados;
- Nunca escreva a password num papel. Memorize-a;
- Evite passwords que utilizem apenas letras e números. Use os caracteres especiais;
- Evite reutilizar ou reciclar passwords antigas;
- Altere a password periodicamente, por exemplo de dois em dois meses;
- Não guarde as passwords em ficheiros do OFFICE ou em TXT no computador. Utilize programas próprios para gerir e guardar passwords mas de preferência memorize-as;
- Tenha cuidado quando estiver a digitar a sua password. Se sentir que está a ser observado pode optar por olhar directamente para a pessoa, ou escrever outra coisa e ir apagando menos uma letra do que escreveu até construir a sua password. Com tantas teclas tentará desta forma distrair o observador;
- Se utilizar uma palavra simples e conhecida, evite a substituição por caracteres óbvios, como por exemplo o a por @ ou o 5 por s;
- Nunca utilize a sua password em computadores que não conhece. Computadores com acesso público podem ter aplicações lá colocadas propositadamente para copiar os seus dados ou simplesmente registar tudo o que escrever no teclado.

Este conjunto de recomendações visam a criação de passwords seguras para que os seus dados estejam protegidos. Seguidamente abordaremos algumas técnicas para criar passwords.

3.2. Métodos para a criação da password

3.2.1. Passwords baseadas na geometria do teclado

É um dos métodos mais utilizados para criar passwords. Consiste em olhar para o teclado e imaginar uma forma ou figura geométrica. Escolhe-se o ponto de partida e os pontos por onde passa a ligação entre eles, escolhida por si. Por exemplo, pode-se imaginar um triângulo com as letras GYJH ou inversamente com as letras GHJN. Deve ter cuidado e evitar linhas rectas, dado que as ferramentas existentes conhecem este procedimento e tentarão descobrir a sequência.

Outro cuidado que deve ter é ocultar qual a figura geométrica em que se está a basear, pois é bem mais fácil apanhar a sua password. Poderão ver em que zona do teclado esta a escrever ou pior, descobrir qual a tecla onde começa. Se usar esta técnica aconselhamos a utilização de caracteres especiais entre as sequências escolhidas. Usando os exemplos acima poderia ser criada uma password do tipo GyJH+gHjN#.

3.2.2. Concatenação de palavras existentes

Este método consiste na união de duas ou mais palavras e pode ser muito interessante por ser fácil de memorizar. Pegando por exemplo na palavra "teclado" e "cinzeiro", são palavras que constam no dicionário mas se juntarmos as duas teremos tecladocinzeiro, que não existe. Se usarmos um caracter especial no meio mais forte será, ficando por exemplo teclado$cinzeiro, onde o $ pode ser !, #, %, &, etc. Se usasse-mos apenas uma palavra com um caracter especial seria fácil para os softwares testar uma palavra usando apenas o teste no caracter diferente, neste caso para um exemplo possível: !teclado ou &teclado. Outra possibilidade é compor as palavras numa só, misturando os caracteres que a compõem, ficando &teclacinzeirodo#. Deve ter aproximadamente dez caracteres para ser segura. Para a tornar mais forte podemos intercalar letras maiúsculas com minúsculas. Poderia ficar então: &TecCinlazeiroDo#.

3.2.3. Letras de frases

Os métodos que a seguir se apresentam são muito eficiente e relativamente fáceis de decorar. É um dos métodos preferidos pois ajuda a memorizar, sendo construído a partir de algo que o utilizador gosta e com alguma complexidade. Para construir uma password só tem que imaginar uma frase fácil de decorar. Uma frase duma letra de uma música conhecida, poema, ditado popular, expressão de trabalho, entre outras. Se pegarmos na primeira letra de cada palavra dessa frase já tem a sua password formada. Para a melhorar basta juntar caracteres especiais e números. Por exemplo, para a frase "Deus quer, o homem sonha, a obra nasce", a password seria: Dq:Hs:aOn que poderia ser melhorada ou reforçada substituindo o a por @ e pondo o algarismo 1 antes do H para 1 homem. Ficaria então: Dq:1Hs:@On.

3.2.4. Construções lógicas

Para criar passwords segundo este método é preciso criar um algoritmo que gere a password de acordo com uma palavra relacionada com o local onde vai utilizar a password. A vantagem deste tipo de password é que apenas é necessário saber o algoritmo e aplicá-lo em função do local onde irá ser utilizada. Por exemplo, podemos considerar as consoantes da password e substitui-las pela letra seguinte na ordem alfabética intercalando letra grande com letra pequena. Pegamos nas vogais e criamos uma correspondência: "a" passa a ser !, "e" passa a @, "i" passa a #, "o" passa a $ e o "u" passa a %. Se nos estivermos a registar no site da Academia a nossa password passaria a ser: !C!d@M#!. Se fossa na loja Zé das Iscas a password seria Z@d!S#sC!s.

As passwords geradas por esta construção são muito eficientes, embora tenham alguns problemas. Se alguém descobrir o seu algoritmo terá acesso a todas as suas passwords e, consequentemente, a todos os sites em que estiver registado. Outra desvantagem é que, devido à complexidade do algoritmo, quando quiser aceder ao site e chegar à altura de escrever a password irá levar muito tempo a construi-la mentalmente.

4. Na prática

O utilizador é livre de escolher a maneira como vai compor a sua password. É aconselhável que utilize um dos métodos apresentados, tendo em conta que o desejável é ter uma password que garanta de forma efectiva a segurança da informação que guarda. Nenhum sistema é infalível mas cabe-nos a nós dificultar a vida daqueles que tentam por meios ilícitos aceder indevidamente à nossa informação.

Existe um conjunto de medidas que pode utilizar e que fazem parte da segurança da sua password. Se a deixar acessível a terceiros pode ter a melhor password possível que a sua vulnerabilidade será tanta quanto a facilidade de a mesma ser acedida (Zúquete 2008). De seguida apresentam-se alguns conselhos para proteger a sua password.

4.1. Não use a opção de "lembrar password"

Os computadores públicos ou do escritório nunca estão protegidos fisicamente, por isso não utilize a opção de "inserir passwords automaticamente", "lembrar password", ou equivalente que muitos sites e navegadores oferecerem. Evite fazer isso inclusive no seu portátil, caso costume utilizá-lo fora de casa com frequência.

4.2. Clique sempre em Sair, Logoff ou equivalente

Muitos de nós fechamos apenas o navegador ao sair de um determinado site. Isto é seguro na maioria das vezes, no entanto, nalguns casos, a simples reabertura da página pode fazer com que o conteúdo privado a que acedeu (a sua conta de e-mail, por exemplo) esteja acessível novamente. Se tiver passwords armazenadas nas mensagens de e-mail, o problema torna-se ainda mais sério. Uma maneira de garantir que isto não acontece é clicar nos *links* ou botões de "Sair", "Logoff", "Sign out", ou equivalente.

4.3. Ao escrever a sua password, verifique se o faz no campo correcto

Tome cuidado para não escrever a sua password no campo errado, por exemplo, no campo "Nome". Se fizer isso, alguém próximo consegue ler o que você escreveu, já que só o campo da password é protegido pela ocultação com asteriscos. Uma boa maneira de evitar isto é não olhar apenas para o teclado enquanto escreve. Olhe constantemente para o monitor e garanta que a sua password está oculta e que o número de dígitos corresponde ao que escreve.

4.4. Cuidado com e-mails ou sites falsos que pedem a sua password

Uns dos ataques mais frequentes na internet são e-mails que nos direccionam para sites falsos que se fazem passar por páginas de bancos, correio electrónico, redes sociais, entre outros, imitando inclusive o visual dos serviços originais, a que se dá o nome de *phishing*. Se o utilizador não perceber que está a aceder a um site falso, vai acabar por entregar a sua password e outros dados ao infractor. Por isso, tenha muita atenção aos detalhes que permitem identificar e-mails ou sites falsos, como endereços não relacionados com o serviço, erros ortográficos grosseiros provocados por traduções online e solicitações suspeitas.

5. Conclusões

A escolha de passwords fáceis e simples é um dos maiores problemas no que toca à segurança da informação. Da lista das vinte maiores vulnerabilidades informáticas a falha na escolha das passwords surge em segundo lugar, constituindo-se num foco de problemas para os administradores de redes e para o próprio utilizador.

Criar passwords eficientes deve ser um ponto crítico no que toca à segurança da informação. Assim, devem ser escolhidas passwords complexas que garantam um elevado grau de dificuldade no que toca à sua quebra. Para as criar devem ser seguidas as recomendações que foram expostas ao longo deste artigo. Por fim, protegê-las é tão ou mais importante como proteger-se a si. A perda de passwords pessoais para outros utilizadores pode ser causa de graves dissabores.

6. Referências

Assunção, M. *Guia do hacker brasileiro.* S. Paulo, 2002.

Carmona, T. *Universo H4CK3R.* S. Paulo: Digerati Books, 2006.

Fraser, R. "ISO 1779 A minimum standard for maximum security." *BCHIMPS - British Columbia Health Information Management Professionals' Society Website.* 2002. http://www.bchimps.bc.ca/pptfiles/Spring 02 Ross Fraser.ppt (acedido em 11 de Fev de 2010).

Microsoft. *Senhas fortes: como criá-las e usá-las.* 22 de Mar de 2006. http://www.microsoft.com/brasil/athome/security/privacy/password.mspx (acedido em 11 de Fev de 2010).

Penedo, D. "Como criar e Utilizar Palavras-Chave." *CERT.PT - Computer Emergency Response Team.* 05 de Jun de 2006. http://www.cert.pt/index.php/pt/recomendacoes/1232-como-criar-e-utilizar-palavras-chave (acedido em 11 de Fev de 2010).

Wikipédia. *Cracker - Wikipédia, a Enciclopédia Livre.* 26 de Jan de 2010. http://pt.wikipedia.org/wiki/Cracker (acedido em 11 de Fev de 2010).

Zúquete, A. *Segurança em redes informáticas.* Lisboa: FCA-Editora de Informática, 2008.