Radosław Sokół

Jak pozostać anonimowym w sieci

Omijaj natrętów w sieci — chroń swoje dane osobowe!

Helion

Redaktor prowadzący: Michał Mrowiec

Projekt okładki: Studio Gravite / Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/jakpoz
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-246-9847-9

Printed in Poland.

Spis treści

Rozdział 2.

Bezpieczeństwo i prywatność

Niezależnie od tego, czy chce się zapewnić sobie pewien poziom prywatności, czy też wędrować po Internecie całkowicie anonimowo, koniecznie należy zadbać o bezpieczeństwo tych podróży. Dopiero bezpieczne środowisko internetowe — takie, w którym konta usług wykorzystywanych przez użytkownika nie są narażone na włamanie i kradzież danych — pozwala zapewnić jakikolwiek poziom prywatności i anonimowości.

W tym rozdziale przedstawione zostaną już bardziej praktyczne zagadnienia związane z dbaniem o bezpieczeństwo komputera i systemu operacyjnego, zabezpieczaniem usług sieciowych oraz rozsądnym i uważnym korzystaniem z zasobów Internetu.

Hasła

Hasła towarzyszą użytkownikom komputerów prawie od samego początku. Gdy tylko pojawiły się dane, do których dostęp nie powinien być powszechny, starano się uniemożliwić ich odczytanie i modyfikowanie przez stosowanie tajnych haseł. Z kolei gdy coraz szersze możliwości komputerów pozwoliły na korzystanie z nich przez więcej niż jednego użytkownika, a nawet kilku użytkowników jednocześnie, pojawiła się konieczność rozróżniania tożsamości użytkownika. W ten sposób powstały konta użytkowników, do których dowiązano stosowane już wcześniej hasła.

Hasło jest jednym z gorszych sposobów utrudnienia nieautoryzowanego dostępu do komputera, konta użytkownika lub zasobu. Przez lata eksperymentowano ze stosowaniem między innymi kluczy kryptograficznych oraz identyfikacji biometrycznej. Ta ostatnia metoda jest dość kontrowersyjna:

- Techniki rozpoznawania odcisków palców są mało skuteczne w przypadku silnego zabrudzenia, zatłuszczenia lub uszkodzenia opuszków palców (na przykład na skutek oparzenia lub otarcia). Czytniki linii papilarnych są co prawda czasem stosowane jako alternatywne metody uwierzytelniania,

jednak zazwyczaj towarzyszy im bardziej tradycyjne rozwiązanie (na przykład kody cyfrowe lub hasła).

- Rozpoznawanie głosu z jednej strony może uniemożliwić prawidłową identyfikację użytkownika w przypadku choroby lub niedyspozycji, z drugiej zaś fałszywie zaakceptować dostęp niepowołanych osób o podobnym głosie. Urządzenia rozpoznające głos wymagają ponadto idealnych warunków pracy, bez hałasu tła.
- Identyfikację twarzy łatwo uniemożliwić diametralną zmianą fryzury, zarostem lub opatrunkiem. Niektóre systemy rozpoznające użytkowników po twarzy można też było śmiesznie łatwo oszukać, umieszczając przed kamerą odpowiednio ucharakteryzowanego manekina lub wręcz... zdjęcie danego użytkownika.
- Rozpoznawanie tęczówki jest podatne na zafałszowania wynikające ze stosowania okularów, soczewek kontaktowych oraz poddawania oka operacjom chirurgicznym.

Nieco lepszym rozwiązaniem są urządzenia, których obecność jest niezbędna do uzyskania dostępu[1]. Zawierają one generator kluczy kryptograficznych — jego idealna kopia znajduje się w systemie, do którego dostęp jest chroniony. Wprowadzenie (bezpośrednio lub pośrednio) właściwego w danej chwili klucza jest warunkiem uwierzytelnienia użytkownika. Utrudnia to znacznie włamanie osobom, które nie dysponują tym urządzeniem. Mimo to odkryte niedawno w całej rodzinie tokenów luki bezpieczeństwa umożliwiały włamywaczom przewidywanie sekwencji kluczy kryptograficznych i w efekcie unieruchamiały zabezpieczenia.

Wbrew pozorom zatem hasła, choć słabe pod względem bezpieczeństwa i bardzo podatne na ich utratę lub podsłuchanie, mają swoje zalety. Są tworem abstrakcyjnym, więc osoba pamiętająca hasło może go użyć w dowolnym miejscu i czasie. Nawet jeżeli ktoś nie ma fizycznej możliwości wprowadzenia hasła, może poprosić o to w krytycznej chwili zaufaną osobę. Hasła łatwo też przekazywać, na przykład w przypadku przenoszenia odpowiedzialności za serwery lub usługi sieciowe na inną osobę.

Istotne jest jednak, by tworzone hasła były jak najbardziej bezpieczne i jednocześnie jak najłatwiejsze do zapamiętania. Zapisanie hasła likwiduje bowiem jego podstawową zaletę: obecność wyłącznie w pamięci jednej osoby.

Zapisywanie haseł w systemach informatycznych

Wbrew pozorom bardzo niewiele systemów informatycznych zapisuje hasła wprost, to znaczy w formie czytelnej dla człowieka. Taki sposób zapisywania umożliwiałby wykradanie haseł i ich bezpośrednie odczytywanie. W przypadku usług sieciowych dostępnych dla setek tysięcy użytkowników stanowiłoby to katastrofalne naruszenie ich bezpieczeństwa[2].

[1] Tak zwane tokeny.

[2] Nie oznacza to, że takie systemy nie istnieją. W historii bezpieczeństwa sieciowego występowały przypadki wycieku baz danych z hasłami użytkowników zapisanymi czystym tekstem, to znaczy w formie czytelnej bezpośrednio dla człowieka.

Typowo baza danych zawierająca informacje o kontach użytkowników przechowuje tak zwane **skróty haseł**[3]. Skrót jest wartością liczbową o szerokim zakresie[4], uzyskiwaną za pomocą określonego algorytmu[5]. Cechą funkcji skrótu jest to, że jest nieodwracalna. Z jednej strony nie istnieją dwa różne hasła dające tę samą wartość skrótu[6], jednak z drugiej nie jest technicznie możliwe odtworzenie hasła na podstawie samego skrótu, poza czasochłonnym zgadywaniem go[7].

Stosowanie skrótów chroni nie tylko przed wykradzeniem oryginalnej postaci hasła z bazy danych serwisu sieciowego, ale też zapobiega przesyłaniu go przez sieć. Podczas uwierzytelniania się w serwisie, wprowadzone przez użytkownika hasło jest przekształcane na skrót i dopiero w takiej formie przesyłane do serwerów obsługujących usługę. Jeżeli nawet przesyłane informacje zostaną podsłuchane i przechwycone, sam skrót — choć ułatwi nieuprawnione zalogowanie się do serwisu — nie zdradzi postaci hasła.

To samo hasło przekształcone tą samą funkcją skrótu w dwóch różnych serwisach sieciowych skutkowałoby pojawieniem się tego samego skrótu. W takim przypadku wykradnięcie skrótu z jednego serwisu ułatwiałoby włamywaczowi zalogowanie się w drugim serwisie. Z tego powodu skróty wylicza się nie na podstawie samego hasła, lecz hasła połączonego z tak zwaną **solą**[8], czyli dowolnym fragmentem tekstu charakterystycznym dla danego serwisu. Sól, oprócz uniemożliwienia tak prostego włamania się na konta o tym samym haśle, może utrudniać odgadywanie najprostszych haseł użytkowników.

W Internecie znajduje się wiele serwisów umożliwiających eksperymentowanie z przekształcaniem dowolnych zbiorów lub fragmentów tekstu do postaci skrótów[9]. Na przykład hasło alamakota123 po przekształceniu na skrót MD5 i SHA-1 przyjmuje następujące postaci:

```
Hasło:    alamakota1234
MD5:      9ED4ED328CE4568BCB2D5F6F96B177CA
SHA-1:    D954006C1D1F9D4FE74D396426142B673B671B54
```

---

[3] Ang. *password hash*.

[4] Od kilkudziesięciu do kilkuset bitów. Na przykład algorytm MD5 generuje skróty o długości 128 b, a SHA-1 — o długości 160 b.

[5] Dawniej wykorzystywany był algorytm MD5 (ang. *Message Digest, version 5*). Ze względu na znane niedoskonałości tego algorytmu znacząco pogarszające jego bezpieczeństwo, obecnie najczęściej stosowany jest algorytm SHA-1 (ang. *Secure Hash Algorithm, version 1*). Coraz częściej mówi się też o stosowaniu innych algorytmów generowania skrótów haseł, na przykład SHA-2.

[6] W teorii. W praktyce możliwe jest wygenerowanie tak zwanej **wiadomości kolizyjnej**, to znaczy innego fragmentu tekstu (na przykład hasła), którego skrót jest taki sam jak tekstu oryginalnego. Jedną ze wspomnianych wcześniej niedoskonałości algorytmu MD5 jest właśnie względna łatwość generowania wiadomości kolizyjnych.

[7] Patrz niżej, podpunkt dotyczący łamania haseł.

[8] Ang. *salt*.

[9] Przykładowo: *http://onlinemd5.com/*, jednak Autor nie może gwarantować, że po opublikowaniu książki wspomniana strona będzie nadal funkcjonowała i udostępniała tę funkcjonalność.

Łamanie haseł

W filmach hasła łamie się albo przez zgadywanie (przy czym bohater odgaduje właściwe hasło po kilku próbach), albo za pomocą programu, który przegląda kombinacje znaków, a na ekranie pojawiają się na zielono trafienia układające się w kompletne hasło. W praktyce żadna z tych metod nie ma szans zadziałać. Po pierwsze, hasło albo jest całkowicie poprawne, albo całkowicie niepoprawne i na pewno nie ma możliwości dowiedzenia się, że kilka pierwszych liter zostało już odgadniętych. Po drugie, każdy sensowny system po kilku pierwszych nieudanych próbach uwierzytelnienia się w systemie blokuje konto i powiadamia administratora.

Każda poważna próba łamania haseł odbywa się w trybie offline, to znaczy na podstawie wykradzionej bazy danych kont użytkowników zawierającej skróty haseł[10]. W takim przypadku włamywacz nie musi przejmować się mechanizmami monitorującymi błędy uwierzytelnienia ani systemami opóźniającymi kolejne próby zalogowania się do serwisu[11]. Może dokonać tylu prób, ile tylko chce, z maksymalną wydajnością oferowaną przez stosowane komputery[12].

Ogólnie rozpoznaje się trzy podstawowe techniki łamania haseł.

Metoda brutalnej siły

Ta metoda polega na wypróbowywaniu wszystkich kombinacji znaków o coraz to większej długości. Gwarantuje to odgadnięcie hasła, jednak — na szczęście — jest bardzo czasochłonne. Przykładowe czasy odgadnięcia haseł o różnej długości z wykorzystaniem metody brutalnej siły przedstawia tabela 2.1. Należy jednak pamiętać, że czas łamania hasła maleje wraz ze wzrostem mocy obliczeniowej komputerów i z roku na rok ta technika pozwala skutecznie łamać coraz dłuższe hasła.

Szybkość weryfikacji kolejnych kombinacji zależy też od nakładów finansowych poniesionych na łamanie hasła. Można przyjąć, że w przypadku skoordynowanego, dobrze finansowanego projektu tego typu czas łamania hasła skraca się tysiąckrotnie.

W związku z powyższym sensowny poziom bezpieczeństwa w aspekcie możliwości techniki brutalnej siły zapewniają hasła zbudowane co najmniej z małych i wielkich liter, o długości co najmniej 12 znaków. Niestety, łatwe do zapamiętania hasła spełniające te założenia mogą być podatne na atak metodą słownikową.

[10] Niestety, takie bazy danych nagminnie krążą w Internecie. Część z nich jest dostępnych bez problemu w sieciach *peer-to-peer*, inne zaś są udostępniane przez grupy przestępcze za — względnie niewielką w sumie — opłatą.

[11] Większość serwisów internetowych celowo opóźnia kolejne próby uwierzytelnienia w przypadku podania błędnego hasła, by utrudnić i spowolnić włamania.

[12] Masowego łamania haseł dokonuje się często w sposób rozproszony, korzystając albo z setek lub tysięcy komputerów, albo z silnych serwerów wyposażonych w uniwersalne moduły obliczeniowe GPGPU.

Tabela 2.1. *Szacunkowe czasy łamania haseł metodą brutalnej siły*

Długość hasła:	4	5	6	7	8	9	10
Same cyfry	< 1 s	< 1 s	< 10 s	< 90 s	< 17 min	kilka godzin	kilka dni
Same małe litery[13]	kilka sekund	kilka minut	godzina	jeden dzień	kilkanaście dni	kilkanaście miesięcy	kilkanaście lat
Małe i wielkie litery	kilka minut	godzina	kilka dni	kilkadziesiąt dni	kilkanaście lat	kilkaset lat	—
Małe i wielkie litery plus cyfry	kilka minut	kilka godzin	kilkanaście dni	kilka miesięcy	kilkaset lat	—	—
Małe i wielkie litery, cyfry i znaki specjalne	kilkanaście minut	kilkanaście godzin	kilkadziesiąt dni	kilkanaście lat	kilkaset lat	—	—

Metoda słownikowa

Ta metoda polega na sprawdzaniu poprawności haseł pobieranych z przygotowanej wcześniej bazy, tak zwanego **słownika**[14]. Taki słownik zawiera przede wszystkim wszystkie dotychczas odgadnięte hasła, ponieważ istnieje duże prawdopodobieństwo, że inni użytkownicy zastosowali takie same, łatwe do zapamiętania lub wprowadzenia z klawiatury kombinacje znaków. Ponadto tego typu słowniki często uzupełnia się wyrazami ojczystego języka użytkownika, w szczególności imionami, nazwami miast, a nawet przekleństwami.

Korzystanie ze słownika znacząco zmniejsza nakład pracy potrzebnej do złamania hasła. Na przykład złamanie metodą brutalnej siły hasła o długości 10 znaków, składającego się wyłącznie z małych liter alfabetu łacińskiego, wymaga ponad 100 bilionów kolejno przeprowadzanych prób. W przypadku metody słownikowej hasło to może zostać odgadnięte po kilkudziesięciu tysiącach prób, oczywiście jeśli występowało ono w słowniku.

Tabela 2.2 przedstawia 25 haseł najczęściej stosowanych w 2013 roku. Powstała ona na bazie wykradzionych baz danych użytkowników anglojęzycznych i polskojęzycznych serwisów internetowych. Jak widać, wszystkie zamieszczone w tabeli hasła to albo łatwe do wprowadzenia sekwencje sąsiadujących na klawiaturze znaków, lub proste wyrazy (w szczególności imiona). Można być pewnym, że wszystkie one znajdują się wśród pierwszych pozycji wszystkich słowników haseł stosowanych w czasie włamań. Z tego powodu absolutnie należy unikać stosowania haseł choćby podobnych do wymienionych.

[13] Lub same wielkie litery.

[14] Ang. *dictionary*.

Tabela 2.2. *25 haseł najczęściej stosowanych w 2013 roku*[15]

Pozycja	Hasła użytkowników anglojęzycznych	Hasła użytkowników polskojęzycznych
1	123456	123456
2	password	qwerty
3	12345678	12345
4	qwerty	polska
5	abc123	zaq12wsx
6	123456789	456
7	111111	111111
8	1234567	dupa
9	iloveyou	aaaaaa
10	adobe123	podrywacze
11	123123	123123
12	admin	legia
13	1234567890	qwerty1
14	letmein	marcin
15	photoshop	1234
16	1234	qazwsx
17	monkey	mateusz
18	shadow	123qwe
19	sunshine	maciek
20	12345	michal
21	password1	widzew
22	princess	matrix
23	azerty	haslo
24	trustno1	master
25	000000	misiek

Bardziej rozbudowane pakiety oprogramowania służące do łamania haseł metodą słownikową pozwalają dodatkowo określić reguły modyfikacji zawartości słownika. Włamywacz może ustalić, że niektóre litery mają być zamieniane na konkretne symbole, wielkość znaków ma się zmieniać, a na początku lub końcu hasła mają być dodawane dodatkowe symbole lub cyfry. W ten sposób element słownika `katastrofa` może pozwolić włamywaczowi pokonać ustawione przez „sprytnego" użytkownika hasło `K4t4str0f41`: wystarczy, by przewidział reguły zamieniające literę `a` na cyfrę `4` i literę `o` na cyfrę `0`, zmianę pierwszej litery wyrazu na wielką i dodawanie cyfry 1 na końcu wyrazu. Takie modyfikacje znacząco wydłużają czas łamania hasła, jednak wciąż jest on tysiące razy krótszy niż w przypadku metody brutalnej siły.

[15] Źródła: hasła anglojęzyczne: *http://www.cbsnews.com/news/the-25-most-common-passwords-of-2013/*, hasła polskojęzyczne: *http://bs.net.pl/artykuly-nie-tylko-dla-informatykow/najpopularniejsze-hasla-polakow*.

Metoda tęczowych tablic

W przypadku haseł przechowywanych w postaci skrótów, które są dostępne bezpośrednio dla włamywacza, skuteczniejsza z punktu widzenia czasu przeszukiwania może być **metoda tęczowych tablic**[16]. W dużym skrócie: polega ona na wygenerowaniu tablicy, w której dla każdej możliwej wartości skrótu można znaleźć tekst, który doprowadził do powstania tej wartości.

Ponieważ jednak taka tablica miałaby wielki rozmiar, stosuje się pewną sztuczkę. Definiuje się dowolną funkcję (tak zwaną **funkcję redukującą**), która jest w stanie przekształcić wartość skrótu na nowe hasło[17] i wielokrotnie poddaje kolejne hasła na zmianę operacji wyznaczania wartości skrótu oraz redukowania skrótu. W tablicy wyników (nazywanej właśnie **tęczową tablicą**) zapisuje się źródłowe hasło, ostateczną wartość skrótu oraz liczbę operacji, które doprowadziły do powstania tej wartości.

W czasie łamania hasła skróty poddaje się z kolei kolejnym operacjom redukcji, licząc na to, że w pewnym momencie uzyska się wartość zapamiętaną w tęczowej tablicy. Możliwe jest wtedy łatwe skojarzenie wartości skrótu z hasłem.

Metoda tęczowych tablic działa poprawnie jedynie przy przestrzeganiu dwóch ograniczeń:

a) Budowa hasła musi być z góry znana. Tęczowa tablica musi być przygotowana dla haseł spełniających konkretne założenia, na przykład: wszystkie hasła o długości do sześciu znaków, zbudowane wyłącznie z małych liter alfabetu łacińskiego.

b) Wartość skrótu nie może być wygenerowana z uwzględnieniem soli. Jeżeli serwis internetowy zapisuje hasła użytkowników z indywidualną solą, inną dla każdego konta, stosowanie metody tęczowych tablic będzie po prostu nieopłacalne.

Zdobywanie haseł

Nie zawsze hasło musi zostać złamane, by włamywacz mógł skorzystać z obcego konta użytkownika. Istnieją dwie podstawowe techniki pozwalające na uzyskanie hasła obcej osoby, bez konieczności poświęcania na to wielu godzin lub dni.

Metoda psychologiczna

Metoda psychologiczna polega na przekonaniu użytkownika, że powinien przekazać wszystkie swoje dane identyfikacyjne osobie trzeciej. Najczęstszym wytłumaczeniem potrzeby uzyskania czyjegoś hasła są problemy techniczne związane z kontem. Hasło uzyskuje się albo telefonicznie, podając się za pracownika działu obsługi klienta,

[16] Ang. *rainbow tables*.

[17] Nie oznacza to, że tak wygenerowane hasło odpowiada konkretnej wartości skrótu z punktu widzenia algorytmu funkcji skrótu.

działu IT lub działu pomocy technicznej, albo za pośrednictwem poczty elektronicznej lub strony WWW udających oficjalne środki komunikacji danej instytucji. Obecnie tego typu ataki są często przeprowadzane w stosunku do klientów bankowości elektronicznej, a uzasadnieniem potrzeby wprowadzenia hasła na żądanie jest na przykład rzekome zablokowanie konta na skutek wcześniej przeprowadzonych prób włamania.

Najlepszym zabezpieczeniem przed tego typu atakami jest edukacja użytkowników. Jest to szczególnie istotne w przypadku podróbek stron WWW instytucji (na przykład banków), które dla mało doświadczonego użytkownika mogą być trudne lub niemożliwe do odróżnienia od oryginałów. Generalnie jednak poważnym sygnałem ostrzegawczym powinno być samo pytanie o hasło w sytuacji innej niż świadoma próba skorzystania z danej usługi podejmowana przez użytkownika.

Podsłuch hasła

Za pomocą narzędzi służących rejestrowaniu naciskanych klawiszy (programy typu *key-logger*) możliwe jest przechwycenie (podsłuchanie) hasła wprowadzanego przez użytkownika[18]. Podsłuchane sekwencje klawiszy są następnie przesyłane przez sieć do włamywacza lub odczytywane przez niego bezpośrednio w późniejszym terminie.

Użytkownik nie jest w żaden sposób powiadamiany o podsłuchu, a fakt istnienia programu szpiegującego na komputerze może umknąć uwadze nawet doświadczonych administratorów. Programy tego typu najczęściej też nie są wykrywane przez pakiety antywirusowe, są bowiem pisane na zamówienie i używane na ograniczonej liczbie komputerów.

Najlepszym sposobem zabezpieczenia się przed tego typu atakiem jest stosowanie bezpiecznego środowiska programowego[19]. Bezwzględnie należy unikać wprowadzania jakichkolwiek danych wrażliwych (a szczególnie haseł) na komputerach, których bezpieczeństwa nie jesteśmy pewni: komputerach służbowych, należących do znajomych, znajdujących się w miejscach publicznych.

Bezpieczeństwo hasła

Aby zapewnić sensowny poziom bezpieczeństwa hasła, należy:

a) Stosować hasło:

- dłuższe niż 10 znaków;
- składające się co najmniej z małych i wielkich liter, a najlepiej również z cyfr i znaków specjalnych;
- niebędące prostą sekwencją liter leżących blisko siebie na klawiaturze;

[18] I przy okazji wielu innych informacji, które nie są zapisywane lub przesyłane w postaci jawnej.

[19] Techniki umożliwiające zwiększenie poziomu bezpieczeństwa środowiska programowego są opisane w dalszej części tego rozdziału.

- ♦ niebędące wyrazem jakiegokolwiek języka (również z uwzględnieniem prostych, mechanicznych przekształceń wyrazów).

b) Nigdy nie przekazywać nikomu hasła, nawet w sytuacjach, które wydają nam się uzasadnione.

c) Nigdy nie narażać hasła na podsłuchanie, czy to za pomocą oprogramowania typu *key-logger*, czy też podczas przesyłania siecią teleinformatyczną.

Tworzenie bezpiecznych haseł

Istnieje wiele technik tworzenia bezpiecznych haseł. Należy przy tym podkreślić, że sformułowanie „bezpieczne hasło" jest nieco mylące, gdyż nie istnieją całkowicie bezpieczne hasła. Opisane poniżej wybrane techniki pozwalają wymyślić hasła, które są znacznie trudniejsze, jednak nie niemożliwe do złamania.

Technika haseł losowych

Najdoskonalsza z technik, jednak najtrudniejsza w użyciu. Tworzone hasło składa się z całkowicie losowo dobranych liter, cyfr i symboli specjalnych. Najlepiej jest, gdy losowania dokonuje komputer, gdyż ludzie — mimo najlepszych chęci — słabo radzą sobie z generowaniem ciągów losowych i często starają się je przesadnie zróżnicować.

Złamanie hasła losowego jest możliwe przede wszystkim za pomocą metody brutalnej siły. Przy założeniu, że hasło takie będzie miało co najmniej 15 znaków długości, jego odtworzenie — przy obecnym stanie techniki — będzie niemożliwe w skończonym czasie.

Oczywistą wadą haseł losowych jest praktyczny brak możliwości ich zapamiętania. Z kolei zapisanie hasła w wielu przypadkach całkowicie przeczy idei zabezpieczenia dostępu do pewnych zasobów. Ta technika jest jednak stosowana czasem w połączeniu z **bankami haseł** — programami, które przechowują w zaszyfrowanej postaci dane uwierzytelniające w serwisach internetowych i automatycznie wpisują je w odpowiednie pola formularzy logowania się użytkownika. Łączy to wysoki poziom bezpieczeństwa haseł losowych z brakiem konsekwencji wycieku hasła do jednego z używanych serwisów (ponieważ w każdym z nich stosowane jest unikatowe hasło), nie zmniejszając komfortu użytkownika[20].

Przykładowe hasło losowe: `kD7,aUzgfh2_1+A`

Technika pierwszych znaków

Sposobem uzyskania łatwego do zapamiętania, a zarazem względnie losowego ciągu znaków, jest użycie pierwszej litery każdego kolejnego wyrazu długiego zdania lub całego fragmentu tekstu. Na przykład na podstawie fragmentu:

Z matki obcej, krew jego dawne bohatery,

A imię jego czterdzieści i cztery.

[20] Oczywiście wymaga to stosowania bezpiecznego, wiarygodnego programu banku haseł. Źle zaimplementowany bank haseł sam w sobie może zagrozić bezpieczeństwu, ułatwiając wyciek wszystkich danych uwierzytelniających danego użytkownika.

można utworzyć hasło:

```
Zmo,kjdb,Aij4Oi4.
```

mające długość 17 znaków i zawierające małe i wielkie litery oraz cyfry i znaki specjalne. Takie hasło jest bardzo trudne do złamania, lecz można je zapamiętać.

Można stosować odmiany tej techniki lepiej przystosowane do pamiętanego fragmentu tekstu, używając na przykład dwóch pierwszych znaków każdego wyrazu lub ostatniego znaku każdego wyrazu.

Technika całych zdań

Rozwinięciem poprzedniej techniki jest stosowanie jako hasła całego, łatwego do zapamiętania zdania. Na przykład, poprawnym hasłem będzie `SzlaDzieweczkaDoLaseczka DoZielonego`. Co prawda zawiera ono tylko małe i wielkie litery alfabetu łacińskiego, jednak jego długość (35 znaków) w zasadzie wyklucza ataki metodą brutalnej siły. To hasło jest też bardzo trudne do złamania metodą słownikową, gdyż zawiera sześć połączonych elementów słownika. Ze względu na długość trudno również oczekiwać, by poddało się ono atakowi metodą tęczowych tablic.

Ten sposób tworzenia haseł ma jednak dwie podstawowe wady:

a) Niektóre systemy informatyczne nie dopuszczają bardzo długich haseł[21]. Stosowanie opisanej techniki ma sens jedynie w przypadku, gdy hasło składa się co najmniej z czterech lub pięciu wyrazów i 20 znaków.

b) Wpisanie tak długiego hasła zajmuje dużo czasu, zmniejszając produktywność i zwiększając prawdopodobieństwo, że ktoś podglądnie hasło w czasie jego wprowadzania.

Bezpieczne stosowanie haseł

Nawet jeżeli hasło jest trudne do złamania, jego stopień skomplikowania staje się bezwartościowy, jeżeli dobrowolnie lub na skutek pomyłki przekażemy je innej osobie. Należy zatem stosować następujące zasady bezpieczeństwa:

- nie wolno zapisywać haseł w postaci jawnej[22];
- nie wolno przekazywać haseł nikomu, nawet osobom teoretycznie do tego uprawnionym (dział techniczny, szefostwo[23]);

[21] Niechlubnym przykładem są tutaj niektóre usługi internetowe firmy Microsoft, narzucające limit długości hasła wynoszący 16 znaków.

[22] W zasadzie jedynym odstępstwem od reguły niezapisywania haseł jest ich przechowywanie w programach typu bank haseł.

[23] W każdym systemie informatycznym istnieje możliwość utworzenia hierarchii praw dostępu, dającej szefostwu wgląd w używane zasoby bez konieczności znajomości hasła pracownika. Nawet w przypadku kończenia stosunku pracy dział IT ma możliwość skasowania haseł i ustawienia ich od nowa, bez znajomości dotychczasowych. Jedynie w przypadku kont funkcyjnych (a nie indywidualnych) przyjęło się — choć jedynie z wygody — przekazywać hasła administracyjne do urządzeń i serwerów nowym pracownikom na danym stanowisku.

Skorowidz

I

J

K

L

Ł

M

N

O

P

R

S

Ś

T

U

V

W

Z

Ż

Problem ochrony danych osobowych we współczesnym świecie staje się coraz bardziej palący. Dotyczy to także — a może przede wszystkim — Internetu. Zawodne systemy weryfikacji danych w połączeniu z olbrzymimi możliwościami nielegalnego ich gromadzenia i wykorzystywania sprawiają, że każdy z nas może paść ofiarą cyberprzestępców, a przynajmniej codziennie irytować się z powodu nachalnych spersonalizowanych reklam, zalewu sprofilowanego spamu czy innych sygnałów świadczących o tym, że ktoś zbiera nasze dane i próbuje manipulować nami za ich pomocą.

Jeśli chcesz uwolnić się od oglądania czegoś, co atakuje Cię przy każdym otwarciu przeglądarki internetowej, marzysz o tym, by uniknąć natrętnych e-maili od obcych nadawców, które w dodatku wyglądają jak wiadomości od kumpla, i potrzebujesz odrobiny luzu w wirtualnym świecie — ta książka Ci pomoże. Dowiesz się z niej, jak skonfigurować przeglądarkę, by nie zbierała wiadomości o Tobie, i jak korzystać z zaawansowanych systemów ochrony prywatności, takich jak Tor. Zrozumiesz, jak działają internetowi szpiedzy, i nauczysz się ich unikać. Odkryjesz, jak dbać o zawartość swojej poczty i zabezpieczać się przed spamerami. Dla własnego bezpieczeństwa — sprawdź, jak to działa!

- Co to znaczy być anonimowym w sieci?
- Komu może zależeć na śledzeniu użytkownika?
- Techniki zapewnienia bezpieczeństwa wpływającego na anonimowość
- Jak można śledzić i analizować ruch osoby oglądającej strony WWW?
- Co to są ciasteczka i superciasteczka?
- Likwidacja reklam na stronach WWW
- Konfigurowanie przeglądarki WWW pod kątem anonimowości
- Czy można nadać fałszywą wiadomość e-mail?
- Jakie informacje są zawarte w wiadomości e-mail?
- Jak spam pocztowy może naruszać anonimowość i prywatność
- Serwery proxy i VPN: sposób działania, konfiguracja, poziom anonimowości i bezpieczeństwa
- System Tor: sposób działania, sprawdzanie poziomu anonimowości

Zabezpiecz się przed nieproszonymi gośćmi z Internetu!

Helion

25120 numer katalogowy

księgarnia internetowa

http://helion.pl

zamówienia telefoniczne

0 801 339900

0 601 339900

Sprawdź najnowsze promocje:
http://helion.pl/promocje
Książki najchętniej czytane:
http://helion.pl/bestsellery
Zamów informacje o nowościach:
http://helion.pl/nowosci

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
http://helion.pl

ISBN 978-83-246-9847-9

Informatyka w najlepszym wydaniu

cena: 34,90 zł