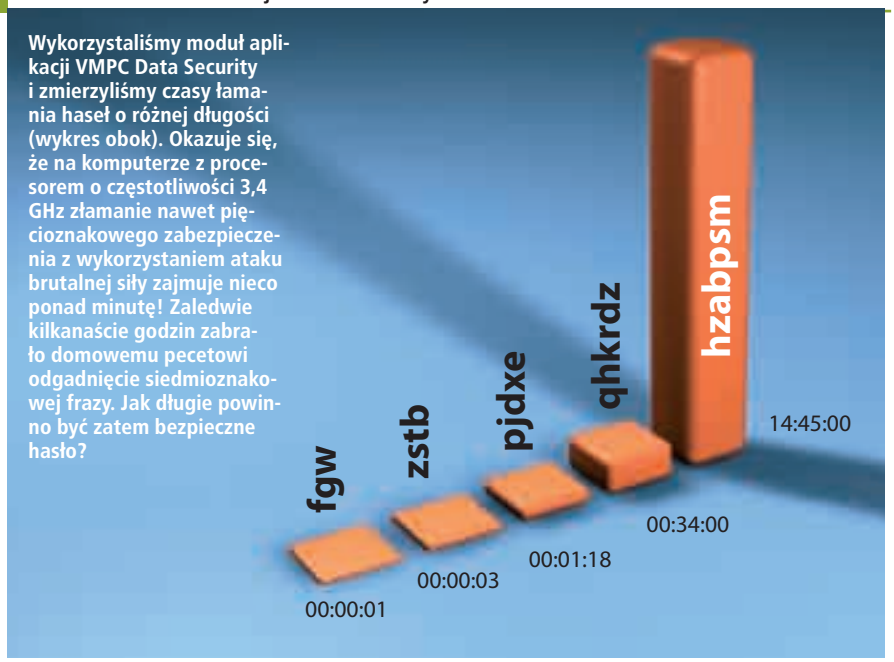


Wykorzystaliśmy moduł aplikacji VMPC Data Security i zmierzyliśmy czasy łamania haseł o różnej długości (wykres obok). Okazuje się, że na komputerze z procesorem o częstotliwości 3,4 GHz złamanie nawet pięcioznakowego zabezpieczenia z wykorzystaniem ataku brutalnej siły zajmuje nieco ponad minutę! Zaledwie kilkanaście godzin zabrało domowemu pecetowi odgadnięcie siedmioznakowej frazy. Jak długie powinno być zatem bezpieczne hasło?

Jakość haseł ma duży wpływ na bezpieczeństwo danych

Nie do złamania?

Podczas użytkowania komputera hasła towarzyszą nam niemal na każdym kroku. Poczta elektroniczna, serwisy internetowe, konto bankowe, szyfrowanie – wszędzie tam jako zabezpieczenia używamy tylko nam znanej frazy. Aby spać spokojnie, trzeba ją jednak odpowiednio dobrać.

Bartosz Żółtak

Najlepszą metodą zabezpieczenia cyfrowych danych przed nieuprawnionym do nich dostępem jest szyfrowanie. Okazuje się jednak, że nie wystarczy użyć sprawdzonego algorytmu i odpowiednio długiego klucza szyfrującego, by nasze zbiory były właściwie chronione. Jeśli do zakodowania poufnych informacji użyjemy prostych (krótkich lub regularnych) haseł, na nic się zdadzą nawet najbardziej wyrafinowane metody kryptograficzne.

W mgnieniu oka

Spójrzmy na prosty przykład. Użytkownik trzymający pliki na zaszyfrowanej partycji, zakodowanej bezpiecznym algorytmem szyfrującym AES i 128-bitowym kluczem, zastosował jednocześnie praktyczne i łatwe do zapamiętania hasło „asd". Czy atakujący, który chce wykraść jego zbiory, musi złamać chroniący je algorytm? Nie! Może pójść na skróty i odgadnąć chroniącą je frazę. Wszystkich liter w alfabecie angielskim jest 26. Trójliterowe wyrażenie może mieć zatem 26*26*26, a więc 17 576 możliwych postaci. Wystarczy, że intruz sprawdzi je wszystkie po kolei (tj. spróbuje otworzyć szyfrowaną partycję, używając każdego z nich), a za którymś razem na pewno trafi na to prawidłowe – o ile system ochrony pozwoli na taką liczbę prób dostępu (np. wiele serwisów WWW blokuje możliwość logowania po trzeciej nieudanej próbie).

Opisana metoda nosi nazwę ataku brutalnej siły (ang. brute-force attack) i jest jednym z najpopularniejszych sposobów łamania zabezpieczeń. Zauważmy, że jeśli włamywacz do znalezienia prawidłowego trójliterowego hasła użyje programu komputerowego i nowoczesnego, domowego peceta, to zajmie mu to dosłownie ułamek sekundy.

Dobrym pomysłem, utrudniającym szybkie złamanie zabezpieczeń, jest rozszerzenie zestawu znaków i stosowanie nie tylko małych, ale i wielkich liter, a także cyfr oraz znaków specjalnych (tzw. krzaczków, np. #$%&@). Już tylko poszerzenie „abecadła" o wielkie litery spowoduje, że czas potrzebny na złamanie ochrony wzrośnie 2^n-krotnie (gdzie „n" jest długością hasła). Znalezienie czteroznakowej frazy zajmie więc nie ok. 3 sekund, ale $3x2^4$, a więc mniej więcej 48 sekund. Trzeba jednak pamiętać, że nie jest to rozwiązanie problemu, a tylko zmniejszenie jego skali.

Długość bezpiecznego hasła

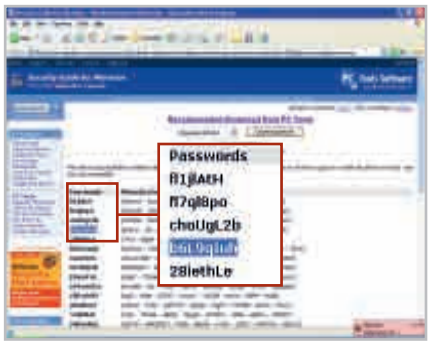
Zadajmy więc sobie pytanie: ile znaków powinno mieć stosowane przez nas hasło do logowania, dostępu do zakodowanej partycji czy szyfrowanego archiwum plików?

Obecnie standardowa długość symetrycznego klucza kryptograficznego wynosi 128 bitów. Zwróćmy uwagę, że gdybyśmy chcieli uzyskać taki sam poziom bezpieczeństwa za pomocą hasła, musiałoby ono mieć – przy założeniu, że składa się z dużych i małych liter oraz cyfr – 22 znaki, ponieważ $(26+26+10)^{22} \approx 2^{128}$. Co więcej, hasło takie nie powinno zawierać ułatwiających zapamiętanie regularności, gdyż atakujący mógłby rozpatrzyć wyrażenia regularne przed innymi. Przykładowo mógłby ciąg znaków: „abcabcabcabcabcabcabca" sprawdzić przed „bexmdndrdavthfvevmxnbk".

Pomocny generator

Należy zatem stosować hasła wygenerowane przez komputer, a nie wymyślone przez człowieka, który z natury szuka regularności. Możemy do tego celu użyć zarówno prostych aplikacji, umieszczonych na stronach WWW (patrz: ramka „Więcej informacji"), lub zaawansowanych narzędzi do tworzenia bezpiecznych haseł (piszemy o nich w dalszej części artykułu).

Fraz utworzonych przez najprostsze narzędzia nie powinniśmy jednak stosować do zabezpieczania bardzo poufnych danych. „Wymyślone" przez nie wyrażenia są stosunkowo łatwe do złamania, ponieważ zostały utworzone za pomocą generatora liczb pseudolosowych. Oprogramowanie to odczytuje pewne zmienne systemowe (np. godzinę) i na tej podstawie tworzy hasła o pożądanej przez użytkownika długości. Zastosowanie tego typu algorytmu oznacza, że potencjalnych fraz może być tyle, ile jest możliwych wartości początkowych licznika czasu. W praktyce będzie to ok. 4 miliardów (2^{32}), bez względu na wybraną długość hasła.



Hasła utworzone za pomocą generatora liczb pseudolosowych trudno odgadnąć. Nie są one jednak najbezpieczniejsze.

O autorze

Bartosz Żółtak jest absolwentem Wydziału Informatyki i Zarządzania Politechniki Wrocławskiej oraz autorem jednokierunkowej funkcji szyfrującej VMPC. Była ona prezentowana m.in. na międzynarodowej konferencji kryptograficznej FSE 2004 w Indiach, gdzie spotkała się z uznaniem specjalistów. Na funkcji VMPC bazuje także stworzona przez autora aplikacja VMPC Data Security. Więcej informacji o Bartoszu Żółtaku i VMPC można znaleźć pod adresem www.szyfrowanie.com.

OPIS	BRIEF	KATEGORIA
Tajemnice dobrych haseł.	Bezpieczeństwo danych w dużej mierze zależy od wymyślonego przez nas hasła dostępu. Utworzenie trudnej do złamania frazy nie jest jednak zadaniem łatwym – powinna być ona odpowiednio długa i nieregularna.	Software | Bezpieczeństwo danych

Łamanie haseł do plików

Bardzo często padamy ofiarą własnej przezorności i zapomniawszy hasła, nie potrafimy otworzyć zabezpieczonego zbioru. Nie oznacza to wcale, że nasze dane przepadły na zawsze – musimy się jednak zabawić we włamywacza i skorzystać z odpowiedniego programu.

Jednym z najpopularniejszych zestawów tego typu narzędzi jest Passware Kit (**www.lostpassword.com**), kosztujący ok. 350 USD. Odzyskuje on hasła do dokumentów, stosując zarówno metodę brutalnej siły, jak i wykorzystując luki w zabezpieczeniach dokumentów niektórych typów. Na tej ostatniej metodzie opiera się także serwis **www.decryptum.com**, umożliwiający złamanie w kilka minut zabezpieczeń plików Worda i Excela. Z kolei by obejrzeć zawartość chronionego archiwum (np. RAR, ZIP), trzeba sprawdzić wszystkie możliwe wyrażenia – tu zatem obowiązuje zasada, że im hasło dłuższe i bardziej skomplikowane, tym więcej czasu potrzeba na jego znalezienie.

Jeśli zatem w ten sposób wygenerujemy nawet 20-znakowe wyrażenie, to i tak czas jego złamania będzie taki sam jak dla hasła 32-bitowego (czyli mniej więcej siedmioznakowego, złożonego z małych liter).

Zgaduj-zgadula

Rozwiązaniem tego problemu jest używanie programów, które generują hasła prawdziwie losowe na podstawie danych dostarczonych przez użytkownika. Mogą to być chwilowe parametry wskaźnika myszki lub losowo wciskane przez użytkownika przyciski na klawiaturze. Utworzenie w ten sposób hasła zajmuje znacznie więcej czasu, ale gwarantuje nam wysoki poziom bezpieczeństwa. Atakujący, by je złamać, będzie miał tylko dwa wyjścia: użyć metody brutalnej siły (nieskutecznej dla odpowiednio długich haseł) lub powtórzyć wykonywane przez nas chaotyczne ruchy myszką (co jest po prostu niemożliwe).

Oczywiście klawiatura i myszka nie wyczerpują wszystkich możliwych źródeł „losowości" – możemy poszukać narzędzi, które do generowania hasła wykorzystają np. nasz głos. Istotne jest, by wyrażenie powstało w wyniku dostarczenia przez użytkownika unikatowych, chaotycznych informacji. A jaki jest efekt? Przykładowa, 128-bitowa fraza, wygenerowana za pomocą programu VMPC Data Security, to... „d8PmZMWy140zVabRBqTHQNX".

Jak to zapamiętać?

Hasło takiej jakości jest kryptograficznie bezpieczne, ale z drugiej strony jego zapamiętanie z pewnością nie jest łatwe. Możemy je przykładowo zapisać na nośniku wymiennym, najlepiej w wielu kopiach. Wówczas jednak istnieje ryzyko kradzieży lub zgubienia nośnika z hasłem, co jest jednoznaczne z utratą zaszyfrowanych danych czy dostaniem się ich w niepowołane ręce.

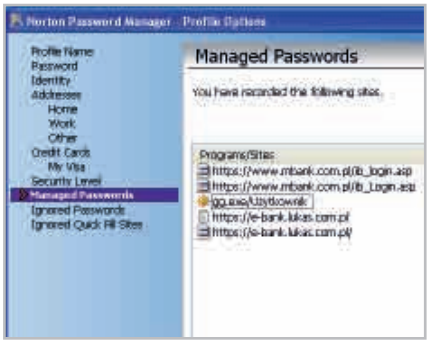
Posługiwanie się trudnymi do zapamiętania frazami ułatwiają tzw. menedżery haseł (patrz: **CHIP 11/2004,** 92). Pozwalają one przechowywać wiele wyrażeń, a niektóre dodatkowo automatyzują proces ich wpisywania (np. na zabezpieczonych stronach WWW). Przykładami takich programów są Roboform (**www.roboform.com**) oraz Norton Password Manager (**www.symantec.com**). Przed wyborem takiej aplikacji warto sprawdzić bezpieczeństwo informacji przetrzymywanych w bazie danych (czy są zaszyfrowane) oraz co się z nimi dzieje po użyciu (czy nie są zapisywane w plikach tymczasowych i czy zostały wymazane z pamięci RAM).

Używanie tego typu aplikacji ma jednak małą wadę. Nawet jeśli program jest bezpieczny, to i tak ochrona wielu fraz – stosowanych przez nas do różnych celów – sprowadza się do poufności hasła dostępu do menedżera. Jeśli zatem ktoś złamie nasze główne zabezpieczenie, to będzie miał dostęp do wszystkich danych znajdujących się w bazie. Hasło dostępu do takiej aplikacji należy więc dobrać szczególnie uważnie – powinno być długie i nieregularne oraz odpowiednio chronione.

Indywidualizacja hasła

Użycie tego samego hasła dla dostępu do forum dyskusyjnego i e-banku jest bardzo niebezpieczne. Wiele osób jednak stosuje tę samą frazę do logowania się w różnych serwisach internetowych. Dzięki takim przyzwyczajeniom włamywacz nie musi obchodzić skomplikowanych zabezpieczeń bankowości elektronicznej – wystarczy, że przechwyci tajne dane na gorzej zabezpieczonej witrynie.

Ciekawą aplikacją eliminującą to zagrożenie jest stworzona przez naukowców uniwersytetu Stanford wtyczka PwdHash (**http://crypto.stanford.edu/PwdHash**). Pozwala ona stosować jedno wyrażenie do logowania się w różnych serwisach bez narażania go na podsłuch przez



Menedżery haseł ułatwiają zapamiętanie danych koniecznych do zalogowania się na stronach internetowych i do aplikacji.

niepowołane osoby. Narzędzie działa w prosty sposób: przepuszcza wpisane przez nas hasło przez tzw. funkcję hashującą (patrz: **CHIP 6/2005,** 100) i dopiero tak „przemielone" przekazuje do właściwego logowania. Jeśli ktoś je przechwyci w trakcie przesyłania, to i tak zobaczy jedynie nic nieznaczący ciąg znaków.

Aby to samo hasło „wyglądało" inaczej na różnych stronach WWW, jest ono dodatkowo hashowane razem z adresem serwisu, w którym się logujemy. Własności funkcji hashujących zapewniają nam, że to samo wyrażenie wpisane nawet na stronach o bardzo podobnym URL zawsze będzie wyglądało inaczej.

Ułomna konieczność

Hasła z całą pewnością nie są doskonałym narzędziem uwierzytelniania dostępu do danych. Te zbyt krótkie i regularne łatwo złamać uniwersalną metodą brutalnej siły. Te bezpieczne natomiast – długie, nieregularne i stworzone przez generator losowy – bardzo trudno zapamiętać. Problemu tego nie rozwiązują (acz w wielu wypadkach ułatwiają życie) także aplikacje do zarządzania hasłami, ponieważ do ochrony głównej bazy danych także stosowana jest jakaś sekretna fraza.

Być może w przyszłości będziemy na masową skalę chronić dane znanymi już dziś metodami biometrycznymi. Na razie jednak pozostają nam stare dobre hasła. ■

Więcej informacji

Generatory haseł online
http://www.winguides.com/security/password.php
http://www.angel.net/~nic/passwd.html
http://passwd.thebugs.ws/