Problemy tworzenia i używania haseł

Międzynarodowa norma ISO/IEC 9594-8 "Information technology - Open Systems Interconnection - The Directory" wydana 15 grudnia 1990 roku wyróżnia dwa poziomy uwierzytelnienia: proste uwierzytelnienie przy pomocy hasła (password) do weryfikacji tożsamości użytkownika; oraz silne uwierzytelnienie uwzględniające dossier uwierzytelniające utworzone z wykorzystaniem technik kryptograficznych. Proste uwierzytelnienie oferuje pewne ograniczone zabezpieczenie przeciwko nieautoryzowanemu dostępowi, natomiast silne uwierzytelnienie powinno być używane jako podstawa gwarantowanej bezpiecznej obsługi.

Proste uwierzytelnienie ma na celu uwierzytelnienie lokalne oparte na unikalnej nazwie (Distinguished Name) użytkownika, ewentualnie dwustronnie uzgodnionym haśle (Password) i obustronnym zrozumieniu środków używania i posługiwania się hasłem wewnątrz pojedynczej dziedziny. Proste uwierzytelnienie może być osiągnięte paroma sposobami:

a) transfer unikalnej nazwy użytkownika i (opcjonalnie) jego hasła w jawnej postaci do odbiorcy dla sprawdzenia;
b) transfer unikalnej nazwy użytkownika, jego hasła oraz liczby przypadkowej i/lub stempla czasowego, przy czym wszystko to zabezpieczone poprzez zastosowanie funkcji jednokierunkowej;
c) transfer zabezpieczonej informacji opisanej w b) łącznie z liczbą przypadkową i/lub stemplem czasowym, przy czym wszystko to zabezpieczone poprzez zastosowanie funkcji jednokierunkowej.

Hasło (password) jest ciągiem znaków, które mogą być użyte w niektórych przypadkach uwierzytelniania. Hasła są często używane do uwierzytelniania tożsamości użytkownika systemu automatycznego przetwarzania danych i w niektórych przypadkach do udzielania lub odrzucenia dostępu do prywatnych lub wielodostępnych danych. Amerykański standard (Federal Information Processing Standard) nr 112 "Password Usage" specyfikuje podstawowe kryteria bezpieczeństwa dla dwóch różnych użyć haseł w systemach przetwarzania danych: (1) osobiste uwierzytelnienie tożsamości użytkownika, nazywane dalej hasłem osobistym (personal password) i (2) autoryzacja dostępu do danych, nazywane hasłem dostępu (access password). Zaleca się, aby hasło osobiste nie było używane jako hasło dostępu.

Oprócz hasła może też być używana tzw. **fraza hasłowa** (Passphrase). Jest to ciąg znaków dłuższy niż akceptowana długość hasła przekształcany przez system haseł w wirtualne hasło akceptowanej długości.

W instytucji, która powinna kontrolować stan bezpieczeństwa swojej sieci komputerowej powinni być dwaj pracownicy odpowiedzialni za ten stan: Zarządzający Siecią (SM - System Manager) oraz Odpowiedzialny za Bezpieczeństwo (SO - Security Officer). Obaj oni powinni przygotować Dokument Wymagań Typowych Haseł (Password Standard Compliance Document), uwzględniając też 10 podstawowych czynników proponowanych przez wspomniany FIPS 112. Czynnikami tymi są:

1) **Zestaw** (Composition). Hasła powinny składać się z podzbioru znaków wybranych przez SM i SO ze zbioru 95 znaków graficznych alfabetu ASCII. Podzbiór ten nie może się składać z mniej niż 10 znaków (tzn. z cyfr 0-9). System hasłowy powinien sprawdzać, czy przy generacji lub zmianie hasła znaki zostały wybrane z ustalonego zestawu.

Uwagi:

Zestaw hasła częściowo zależy od urządzenia z którego hasło ma być wprowadzane. Zależy też od tego jak i gdzie hasło ma być pamiętane i jak zapamiętane hasło będzie porównywane z wprowadzonym hasłem. Minimalny zestaw zawiera 10 znaków ponieważ pewne systemy (np. systemy finansowych transakcji) używają 10 cyfrowy tzw. PIN PAD (Personal Identification Number entry device) do wprowadzania hasła nazywanego PIN. PIN PAD wygląda bardzo podobnie jak klawiatura telefoniczna z klawiszami naciskowymi. Lepszy zestaw składa się z 16 znaków który uwzględnia 10 cyfr plus (A,B,C,D,E,F). Ten zbiór może reprezentować znaki hexadecymalne. Wiele haseł składa się tylko z 26 małych liter (a - z) lub z 26 dużych liter (A - Z). Jednak użycie tylko tych podzbiorów często zachęca do wybierania inicjałów, imion, przezwisk, krewnych, miasta rodzinnego lub powszednich słów łatwych do powiązania z właścicielem hasła.

2) **Przedział długości** (Length Range). Hasła powinny mieć przedział długości ustalony przez SM i SO, nie krótszy niż 4, o maksymalnej długości wynikającej z dalszych rozważań. Wybrany zestaw i przedział długości hasła powinien gwarantować minimum 10^4 możliwych haseł. Wybrany przedział długości haseł powinien zapewniać poziom protekcji proporcjonalny do wartości lub możliwości

chronionych zasobów lub danych. System hasłowy powinien sprawdzać czy generowane lub zmieniane hasło znajduje się w przewidywanym zakresie.

Uwagi:

Długość hasła jest ściśle związana z zestawem dla zapewnienia potencjalnego bezpieczeństwa systemu haseł przeciwko intruzowi chcącemu spróbować wyczerpującego przeglądnięcia wszystkich możliwych haseł. PINy są typowo czterema cyframi z powodu wymaganego niskiego bezpieczeństwa, dla łatwości pamiętania przez wielu podstawowych klientów i dla prędkości i dokładności wprowadzania. System weryfikacji PIN ogólnie zapobiega przed szybkim wypróbowaniem wszystkich 10.000 możliwych PINów dla konkretnego dostępu w celu znalezienia ważnego PINa. Jeśli wszystkie inne czynniki tymczasowo zaniedbamy, bezpieczeństwo zapewniane przez hasło jest wprost proporcjonalne do dopuszczalnej długości hasła. Długie frazy hasłowe można łatwo zapamiętać ale dłużej trzeba wprowadzać.

3) **Okres ważności** (Lifetime). Hasła powinny być ważne nie dłużej niż rok. Ich najkrótszy okres ważności wybrany przez SO w porozumieniu z SM powinien zapewniać wymagany poziom ochrony przy najniższym możliwym koszcie. Hasła w przypadku zawieszenia go lub kompromitacji powinny być zastąpione tak szybko jak to możliwe ale nie później niż w ciągu jednego dnia pracy od chwili zawieszenia lub kompromitacji. Hasła powinny być usunięte lub zaznaczone jako hasła nieważne tak szybko jak to możliwe ale nie później niż w ciągu trzech dni roboczych od chwili gdy właściciel przestał być autoryzowanym użytkownikiem systemu lub którykolwiek ze zbiorów właścicieli przestał mieć autoryzowany dostęp do danych. Hasła zapomniane przez właścicieli muszą być zmienione a nie ponownie wprowadzone. System haseł powinien umożliwiać SO usuwanie lub zmienianie hasła z jednoczesną możliwością przechowywania zapisu o tym fakcie.

Uwagi:

Bezpieczeństwo dostarczane przez hasło zależy od jego składu, długości i jego zabezpieczenia przed ujawnieniem i podstawieniem. Ryzyko związane z niewykrytą kompromitacją hasła może być zminimalizowane przez częstą zmianę hasła. Jeśli hasło zostało w jakiś sposób skompromitowane i jeśli nowe hasło jest utworzone całkowicie niezależnie od starego hasła wówczas dalsze ryzyko związane ze starym hasłem redukuje się do zera. A więc hasła powinny być zmieniane okresowo i muszą być zmienione gdy kompromitacja jest przypuszczana lub potwierdzona. Użyteczny okres ważności hasła zależy od paru zmiennych, wśród nich: (a) koszt zmiany hasła; (b) ryzyko związane z kompromitacją; (c) ryzyko związane z dystrybucją; (d) prawdopodobieństwo "przewidzenia" hasła; (e) liczba użyć hasła; (f) praca znalezienia hasła przez wyczerpującą metodę prób i błędów. Przedział może być okresem czasu lub zależeć od liczby użyć. System haseł powinien mieć zautomatyzowane możliwości wymuszające procedurę zmiany hasła. System powinien sprawdzać czy nowe hasło nie jest takie samo jak poprzednie. Bardzo czułe aplikacje wymagają aby nowe hasło nie było takie samo jak N poprzednich haseł. Taki system wymaga pamiętania N haseł dla każdego użytkownika.

4) **Źródło** (Source). Źródło jest zbiorem dopuszczalnych jednostek które mogą tworzyć lub wybierać ważne hasło spośród wszystkich dopuszczalnych haseł. źródło powinno być ustalone przez SO i SM i powinno być jednym lub paroma z następujących: użytkownik, SO lub zautomatyzowany generator haseł. Wszystkie hasła w momencie dostarczenia, przetransferowania lub zainstalowania nowego systemu (tzn. hasła operatora, programisty systemu, personelu utrzymania lub SO) powinny być natychmiast zmienione przez SO na: (a) hasła które są nieważne, (b) przypadkowe hasła które można następnie zmienić, lub (c) ważne hasła które będą własnością autoryzowanych użytkowników systemu i utworzone zgodnie z dokumentem wymagań typowych haseł. Hasła utworzone przez SO dla nowych użytkowników systemu dla pierwszego wejścia do systemu powinny być wybrane przypadkowo ze wszystkich akceptowalnych haseł (tzn. defaultowe hasła lub hasła sformatowane odniesione do nowych użytkowników lub im przypisane nie mogą być używane). Użytkownicy, którzy tworzą lub wybierają swoje własne hasła osobiste powinni być poinstruowani, że należy używać hasła wybranego przypadkowo ze wszystkich dopuszczalnych haseł lub wybrać takie aby nie miało związku z ich osobistą tożsamością, historią lub środowiskiem. Hasła wybrane lub utworzone przez użytkowników lub SO powinny być przetestowane przez automatyczny system haseł dla upewnienia, że są one zgodne ze specyfikacjami i długością ustaloną dla systemu zanim zostaną zaakceptowane jako hasła ważne.

Uwagi:

Hasła tworzone lub wybierane przez użytkownika powinny być sprawdzane przez zautomatyzowany system haseł na zgodność wszystkich kryteriów systemu haseł. Jeśli hasła są generowane przez system, metoda generacji nie powinna być przewidywalna. Może tu być użyty algorytm DESa łącznie z nie-

deterministycznym parametrem takim jakim są najmniej znaczące bity zegara systemu komputerowego wysokiej rozdzielczości.

5. **Własność** (Ownership). Hasła osobiste wykorzystywane do uwierzytelnienia tożsamości powinny być własnością (tzn. znane) tylko osoby mającej tę tożsamość. Hasła dostępu wykorzystywane do ochrony prywatnych danych powinny być własnością tylko tego, kto utworzył prywatne dane. Hasła dostępu wykorzystywane do danych dzielonych powinny być własnością tylko zbioru tych osób które mają autoryzację z tymi samymi przywilejami dostępu do tych danych. Hasło osobiste każdej osoby która ma autoryzowany dostęp do danych dzielonych i hasło dostępu do tych danych dzielonych nie może być intencjonalnie wybrane lub ustanowione jako identyczne. Każda osoba powinna być odpowiedzialna za zapewnienie ochrony przed utratą lub zdemaskowaniem haseł jakie posiada.

Uwagi:

Osobiste hasło powinno być własnością indywidualną bardziej niż własnością wspólną grupy użytkowników z powodu gwarancji indywidualnej odpowiedzialności w systemie komputerowym. Jest to postulowane nawet wtedy, gdy cała grupa osób ma wspólne przywileje dostępu do tych samych zasobów czy danych. Indywidualna własność osobistych haseł jest wymagana ponieważ: (a) można zakładać indywidualną odpowiedzialność dla określenia kto ma dostęp, do jakich zasobów i dla jakich celów; (b) można zakładać niedozwolone użycie hasła lub utratę hasła; (c) może to być użyte do śledzenia przebiegu aktywności użytkownika; (d) unika się konieczności zmiany hasła całej grupy gdy pojedynczy członek grupy pozostawi lub utraci autoryzowane przywileje.

6. **Dystrybucja** (Distribution) jest zbiorem dopuszczalnych metod dostarczania (transportowania) nowego hasła do jego właściciela i do wszystkich miejsc gdzie ono będzie potrzebne w systemie hasłowym. Osobiste hasła powinny być dystrybuowane ze Źródła hasła w taki sposób, żeby tylko zainteresowany właściciel mógł zobaczyć lub otrzymać hasło. Hasła powinny być dystrybuowane w taki sposób, żeby rekord kontrolny zawierający datę i czas zmiany hasła i identyfikator związany z hasłem (ale nie stare lub nowe hasło) mógł być dostępny dla SO. Hasła powinny być dystrybuowane ze Źródła hasła w taki sposób aby tymczasowo zapamiętane hasło (temporary storage of the password) było wymazywane a długoterminowa pamięć hasła była dostępna tylko dla właściciela(li) i chronionego systemu haseł. Zautomatyzowany system haseł który generuje i dystrybuuje hasła powinien utrzymywać zautomatyzowany rekord z datą i czasem generacji hasła i komu został wysłany (ale nie samo hasło).

Uwagi:

Inicjacyjne hasło (initial password) jest tworzone i dostarczane bezpośrednio albo ustnie albo pisemnie podczas spotkania na którym użytkownik inicjalizuje autoryzowane użycie systemu komputerowego lub dostęp do zbioru danych. Może to być jednorazowe hasło które musi być zmienione po inauguracyjnym wejściu. Hasła dostarczane pisemnie powinny być zawarte w zapieczętowanej kopercie oznakowanej "do otwarcia tylko przez adresata". Instrukcja dla użytkownika powinna być: (a) zniszczyć zapisane hasło po zapamiętaniu go; lub (b) zwrócić zapisane hasło do SO po podpisaniu pokwitowania odbioru hasła i po zapieczętowaniu go w zwrotnej poczcie; (c) użyć hasła jak najszybciej i jeśli hasło może być zmienione przez użytkownika, zmienić je. Niektóre systemy dystrybuują hasła w zapieczętowanych przesyłkach wydrukowanych przez komputer. Przesyłka jest tak skonstruowana, że nie może być wysłana ponownie po otwarciu. Hasło jest drukowane tylko wewnątrz przesyłki na drugiej stronie z wykorzystaniem kalki przyłożonej do tyłu frontowej strony przesyłki. Instrukcja mówi, żeby usunąć front przesyłki który pokazuje nazwisko docelowego odbiorcy, zniszczyć front i zachować hasło (w chronionym miejscu łatwo dostępnym tylko dla docelowego odbiorcy). Część przesyłki która zawiera hasło nie ma żadnych innych identyfikatorów które pozwalałyby na skojarzenie hasła albo z systemem albo z właścicielem. A więc nikt kto znalazłby zgubione hasło nie byłby w stanie posłużyć się nim.

7. **Pamiętanie** (Storage) jest zbiorem dopuszczalnych metod pamiętania ważnego hasła w okresie jego ważności. Zapamiętane hasła powinny być chronione w taki sposób aby tylko system haseł miał autoryzowany dostęp do hasła. Hasła szyfrowane przed ich zapamiętaniem powinny być chronione przed podstawieniem (tzn. ochrona powinna zapewniać to aby jedno zaszyfrowane hasło nie mogło być zamienione na inne jeśli zamiana nie jest autoryzowana).

Uwagi:

Hasła powinny być pamiętane w systemie uwierzytelniania w sposób który minimalizuje jego narażenie na odkrycie lub nieautoryzowaną zmianę. Większość systemów ma zbiór haseł (a password file) tak ustawiony, że może być legalnie czytany tylko przez program "LOGON" (lub jego odmiany). Zbiór jest zabezpieczony przez mechanizm dostępu do zbiorów który sprawdza bit protekcji w tablicy dostępu do

zbioru (FAT). Niektóre systemy oddzielają zbiór z hasłami od zbioru autoryzowanych użytkowników. Indeksowany zbiór jest używany do zapewnienia odpowiedniości między użytkownikiem i hasłem użytkownika. Niektóre systemy szyfrują hasła albo odwracalnie (two-way) albo nieodwracalnie (one-way) korzystając z "klucza szyfrującego dane" (Data Encrypting Key) albo z samego hasła jako klucza. Oczywiście każdy klucz pozostający w pamięci wymaga również protekcji przez szyfrowanie przy pomocy "klucza szyfrującego klucz" (Key Encrypting Key). Typ protekcji zastosowany do haseł powinien być proporcjonalny do protekcji wymaganej dla systemu lub danych. System szyfrowania "one-way" zabezpiecza oryginalne hasło przed każdym, włącznie z SO i programistami systemu.

8. **Wejście** (Entry) jest zbiorem dopuszczalnych metod przy pomocy których hasło może być wprowadzone przez użytkownika systemu dla celów uwierzytelnienia lub autoryzacji. Hasła powinny być wprowadzane przez właściciela gdy tego żąda system haseł w taki sposób aby hasło było chronione przed ujawnieniem jakiemukolwiek obserwatorowi procesu wprowadzania. Liczba dopuszczalnych prób wprowadzania hasła (ponowne wprowadzenie po niepoprawnym wprowadzeniu hasła) powinno być ograniczone do liczby wybranej przez SO. Reakcja na przekroczenie maksymalnej liczby ponownych prób powinna być określona przez SO.

Uwagi:

Użytkownik, który nie ma wprawy w pisaniu na maszynie, często wprowadza hasło jednym palcem. Długie przypadkowe hasło które jest trudne do wprowadzenia, może być bardziej wrażliwe na obserwację aniżeli krótkie łatwo wprowadzalne hasło. W żadnym przypadku żadna drukowana czy wyświetlana kopia hasła nie powinna istnieć po wprowadzeniu hasła. Gdy hasło jest dostarczane jako część w procesie odległego wprowadzania, hasło powinno być dołączane do "przesyłki" w ostatnim możliwym momencie i fizycznie chronione. Użytkownik powinien mieć możność na więcej niż jedną próbę poprawnego wprowadzenia hasła z powodu błędów nieuwagi. Jednakże powinna być jakaś maksymalna liczba prób dla poprawnego wprowadzenia hasła. Dla przeciętnego użytkownika systemu komputerowego maksymalnie trzy próby są odpowiednie. System powinien zapobiegać szybkiemu ponownemu wprowadzeniu hasła po niepoprawnym wprowadzeniu. Powinno upłynąć parę sekund zanim pojawi się ponownie zapytanie o hasło. Zapobiega to zautomatyzowanemu z dużą prędkością pracującemu atakowi prób-i-błędów na system haseł. Rekord bezpieczeństwa powinien zanotować fakt wprowadzania niepoprawnego hasła ale te niepoprawne hasła nie powinny być przechowywane w rekordzie. Alarm bezpieczeństwa powinien być generowany jeśli: (1) maksymalna liczba dopuszczalnych wprowadzeń hasła została przekroczona; (2) maksymalna liczba dopuszczalnych niepoprawnych prób połączenia się z systemem z jednego terminala została przekroczona; (3) maksymalna liczba dopuszczalnych prób połączenia się z systemem dla określonego okresu czasu została przekroczona. Te parametry muszą być ustawione odpowiednio do czułości danych jakie są protegowane, profilu przeciętnego użytkownika systemu i polityki organizacji. Niektóre organizacje będą sobie życzyły aby ustawić parametry wysoko aby zapobiec niezadowoleniu klienta, podczas gdy inna organizacja będzie ustawiała parametry nisko dla zapewnienia kompromisowego bezpieczeństwa. Terminale powinny być odłączone a użytkownicy pozbawieni obsługi jeśli te parametry zostaną przekroczone. SO powinien być jedynym, który może uruchomić terminal i wznowić obsługę użytkownika po takich zdarzeniach. System powinien informować użytkownika po efektywnej procedurze połączenia się z systemem o ostatnim pozytywnym dostępie użytkownika i o każdej negatywnej próbie dostępu. Użytkownik może podjąć parę akcji aby uniemożliwić obserwatorowi nauczenie się hasła przez patrzenie na proces wprowadzania hasła. Pierwsze, wprowadzać hasło tak aby mogło być wprowadzane szybko przy pomocy paru palców. Drugie, ciało może posłużyć do zasłonięcia obserwatorowi procesu naciskania klawiszy w czasie wprowadzania hasła. Trzecie, użytkownik może zażądać aby gość nie patrzył na proces wprowadzania hasła. Czasem użytkownik może wprowadzić hasło przed demonstracją użycia systemu.

9. **Transmisja** (Transmision) jest zbiorem dopuszczalnych metod dla komunikacji haseł od punktu jego wprowadzenia do punktu jego porównania z zapamiętanym, ważnym hasłem. Transmitowane hasła powinny być chronione w stopniu określonym przez SO i conajmniej w stopniu równoważnym ochronie wymaganej przez jednostkę (system lub dane) którą chroni hasło. Transmitowane hasła powinny być szyfrowane w miejscu wprowadzania jeśli dane chronione hasłem są szyfrowane w miejscu wprowadzania danych. Hasła używane jako klucze szyfrowania powinny być wybierane przypadkowo ze zbioru wszystkich możliwych kluczy (tzn. 2^{56} kluczy dla DESa) i powinny być użyte albo jako Klucze Szyfrujące Dane albo jako Klucze Szyfrujące Klucze ale nie razem. Zdeszyfrowane hasła powinny być transmitowane jako znaki ASCII jeśli są wymieniane pomiędzy systemami; szyfrowane hasła i wirtualne hasła powinny być transmitowane jako 64-bitowe pola binarne w komunikacji bitowo-zorientowanej, lub jako

reprezentacje ASCII znaków hexadecymalnych (tzn. 16 znaków ze zbioru [0-9,A-F] w komunikacji znakowo-zorientowanej.

Uwagi:

Większość linii komunikacyjnych między terminalami i komputerami nie zapewnia protekcji przed ujawnieniem hasła. Dlatego użytkownicy powinni być świadomi, że ich hasła mogą łatwo być ujawnione przez pasywny podsłuch. Systemy komputerowe mogą też być łatwo oszukane. Może to wystąpić jeśli intruz wstawi aktywny podsłuch między terminal i komputer. Aktywny podsłuch można zrobić obecnie za kilkaset dolarów przez domowego hobbistę komputerowego. Podsłuch może być zbudowany w teczce i składać się z amatorskiego komputera z chipem komunikacyjnym receive/transmit który odbiera dane z terminala i komputera a następnie retransmituje dane do komputera i terminala dokonując przeglądu ewentualnie modyfikując je wcześniej. Aktywny podsłuch może podstawić jedno hasło użytkownika w miejsce hasła innego użytkownika nawet jeśli hasła są szyfrowane w terminalu. Oszustwo występuje wtedy gdy zbałamucony system "wierzy", że jeden użytkownik jest na terminalu podczas gdy na prawdę jest tam kto inny. Odwrotne oszustwo występuje gdy zbałamucony użytkownik "wierzy", że komunikacja odbywa się z zażyczonym komputerem podczas gdy na prawdę tam jest inny komputer. W ostatnim przypadku autoryzowany użytkownik może być oszukany aby podał ważne hasło przez symulację żądania "LOGON". Po otrzymaniu hasła intruz kontrolujący oszukujący komputer informuje użytkownika, że wymagana usługa jest czasowo nieosiągalna. W czasie tej wymiany intruz otrzymuje ważne hasło bez wiedzy użytkownika. Te zagrożenia mogą być zneutralizowane przez jedną lub dwie metody szyfrowania. Pierwsza, linia komunikacyjna między terminalem i komputerem może być protegowana przez urządzenie szyfrujące które używa tajnego klucza dla szyfrowania całej komunikacji między terminalem i komputerem. Ponadto każda transmisja może być numerowana, dzięki czemu poprzednia transmisja nie może zastąpić późniejszej (tzn. poprzednio użyte ważne hasło nie może być zapamiętane i użyte dla podstawienia nieważnego hasła nawet jeśli oba są szyfrowane). Hasło może być użyte jako klucz szyfrujący lub jako część klucza szyfrującego. Załóżmy, że użytkownik wprowadza hasło które ma być użyte jako klucz szyfrujący w terminalu (tzn. nigdy nie będzie transmitowane do komputera) a hasło użytkownika jest otrzymywane z pamięci komputera a używane jako klucz szyfrujący w komputerze (tzn. nigdy nie jest transmitowane do terminala). Wówczas terminal i komputer są dwustronnie uwierzytelniane jeśli występuje normalna komunikacja używająca procesu szyfrowania i deszyfrowania w terminalu i komputerze, w obu przypadkach używając hasła jako klucza (lub jako części klucza). Hasła używane jako klucze do szyfrowania danych nie mogą być używane jako klucze do szyfrowania kluczy i vice versa. Ma to na celu minimalizację jakiejkolwiek możliwości prób zdobycia klucza (a więc hasła) przy pomocy technik kryptoanalitycznych.

10. **Okres uwierzytelniania** (Authentication Period) jest maksymalnym dopuszczalnym okresem pomiędzy jakimkolwiek początkowym procesem uwierzytelnienia a kolejnym nowym procesem uwierzytelnienia podczas pojedynczej sesji terminalowej lub podczas okresu gdy dane są dostępne. Hasła osobiste powinny być uwierzytelniane każdorazowo gdy jest wykonywane przedstawienie tożsamości, tzn. przy "loginowaniu się" do interaktywnego systemu. Hasła dostępu powinny być uwierzytelniane podczas inicjacyjnej prośby dostępu do chronionych danych.

Uwagi:

Interaktywne "sesje" między użytkownikiem i komputerem poprzez odległy terminal często trwają parę godzin. Podczas gdy polityka bezpieczeństwa powinna stanowić, że terminal który jest zalogowany do komputera nie powinien pozostawać bez opieki użytkownika, w praktyce tak jednak często nie jest. Wiele systemów ma możliwości które automatycznie logoutują użytkownika z systemu jeśli terminal jest nieaktywny przez pewien okres czasu. Ma to na celu zapobieżenie przed użyciem niepilnowanego terminala przez kogoś obcego. Niektóre systemy kontroli dostępu wymagają aby użytkownik re-uwierzytelniał się okresowo oprócz procesu uwierzytelnienia wstępnego. Te systemy często antagonizują użytkownika jeśli częstość uwierzytelniania jest ustawiona wysoko. Re-uwierzytelnianie powinno być wymagane tylko dla spełnienia wysokich wymagań bezpieczeństwa a też gdy terminal był przez pewien czas nieaktywny.

Automatyczny Generator Haseł

5 października 1993 r. National Institute of Standard and Technology w swojej publikacji (nr 181) Federal Information Processing Standards przedstawił algorytm do generacji haseł zabezpieczających zasoby komputerowe.

Algorytm korzysta z liczb losowych do wybierania znaków tworzących przypadkowe wymawialne hasła. Liczby przypadkowe są generowane przed podprogram liczb losowych oparty na trybie elektronicznej książki kodowej szyfru DES. Przedtawiony w standardzie program zawiera następujące opcje: hasła wymawialne, hasła pseudowymawialne, hasła składające się z liter i hasła utworzone z przypadkowego ciągu znaków spośród 95 znaków graficznych ASCII. Poza tym można generować hasła z dowolnego przedziału długości. Program pozwala na wygenerowanie zadanej ilości haseł z określonymi parametrami.

Przykład Dokumentu Wymagań Typowych Haseł
Średni poziom bezpieczeństwa

ORGANIZACJA: Dział Tajny
TYP SYSTEMU: Dane personalne
PRACOWNIK PRZYGOTOWUJ¥CY: Konstancja Janek
DATA: 7 lipiec 1994

1. Przedział długości: 4-8.
   Uzasadnienie: Pozwala to na szeroki zakres wyboru haseł.
2. Zestaw: (A-Z), (a-z) i (0-9).
   Uzasadnienie: £atwość tworzenia haseł i ich pamiętania. Uwzględniając długość, pozwala to na wybór z $62^8+62^7+62^6+62^5+62^4$ możliwych haseł, jeśli znaki są wybierane przypadkowo.
3. Okres ważności: 6 miesięcy.
   Uzasadnienie: Poufność analizowanych danych.
4. □ródło: Automatyczny generator haseł wewnątrz systemu. Użytkownik może odrzucić wygenerowane hasło i zażądać wygenerowania innego.
   Uzasadnienie: Ma to na celu wyeliminowanie możliwości wyboru przez użytkownika znaczącego dla niego hasła i przez to łatwego do przewidzenia dla innych.
5. Własność: Indywidualna.
   Uzasadnienie: Każda osoba ma być uwierzytelniana indywidualnie.
6. Dystrybucja: Hasło inicjacyjne od SO; następne hasła z terminala poprzedzone autoryzowanym dostępem.
   Uzasadnienie: Wszystkie wejścia i wyszukanie są realizowane przez terminale video.
7. Pamiętanie: Szyfrowane hasła z dostępem tylko dla systemu haseł.
   Uzasadnienie: Poufność danych. Hasła są używane jako klucze szyfrowania do szyfrowania identyfikatorów a wynik jest zapamiętywany w centralnym systemie.
8. Wejście: Terminale video, nie-wyświetlające.
   Uzasadnienie: Wszystkie wejścia i operacje wyszukiwania są realizowane z takich terminali. Hasła nie są wyświetlane na terminalu w czasie wprowadzania.
9. Transmisja: Komunikacja tekstu otwartego (jawnego).
   Uzasadnienie: Podczas gdy dane osobowe są poufne, nie jest konieczne szyfrowanie danych podczas transmisji wewnątrz urządzenia.
10. Okres uwierzytelniania: Podczas logowania i po 10 minutach nieaktywności terminala.
    Uzasadnienie: Celem jest uniknięcie wykorzystania przez nieautoryzowanych osobników pozostawionych bez opieki terminali.

Wyznaczanie długości hasła

Bezpieczeństwo gwarantowane przez hasła jest określone przez prawdopodobieństwo z jakim hasło może być przewidziane w okresie jego ważności. Im mniejsze prawdopodobieństwo, tym większe bezpieczeństwo zapewniane przez hasło. Przy wszytkich innych parametrach stałych im dłuższe hasło, tym większe bezpieczeństwo zapewniane przez hasło.

Podstawowe parametry które mają wpływ na długość hasła niezbędne do zapewnienia odpowiedniego stopnia bezpieczeństwa to:

L - maksymalny okres ważności w którym hasło może być używane do logowania się do sytemu.
P - prawdopodobieństwo, że hasło zostanie przewidziane w ciągu okresu ważności, przy założeniu ciągłego tworzenia przewidywań w tym okresie.

R - liczba prób przewidywań na jednostkę czasu jaką można wykonać.
S - przestrzeń haseł, tzn. całkowita liczba unikalnych haseł które mogą być wygenerowane przez algorytm generacji haseł.
A - liczba znaków w alfabecie.

Przyjmując tylko przypadki gdy S jest większe niż L*R a stąd P jest mnijsze od 1, zależność między tymi

P = {L*R}over S

parametrami ma postać:

Parę czynników ma wpływ na prędkość z jaką mogą być wykonane próby wejścia do systemu gdy nie jest znane ważne hasło. Przede wszystkim trzeba tu wziąć pod uwagę protekcję zbioru z hasłami. Jeśli zbiór z hasłami nie jest protegowany (tzn. każdy może go przeczytać jak zwykłe dane), wówczas "przewidywanie" nie jest konieczne.

Jeśli zbiór z hasłami może być czytany ale hasła są szyfrowane, można osiągnąć bardzo dużą prędkość przewidywań stosując specjalny program komputerowy do próbowania słów ze słownika jako możliwe hasła szyfrując je i porównując z szyfrowanymi hasłami ze zbioru haseł. Podobna sytuacja zachodzi gdy do ochrony zbiorów są używane tylko hasła.

Jeśli zbiór z hasłami ma efektywną kontrolę dostępu i procedura logowania nie da się obejść, prędkość przewidywań może być kontrolowana poprzez ustawienie limitów ma liczbę logowań lub innych prób jakie mogą być podjęte zanim zostanie przerwane połączenie lub proces.

Jeśli wszystkie inne czynniki są ustalone to im krótszy jest okres ważności hasła, tym mniejszą liczbę prób przewidywania można wykonać i dla tego większy jest stopień bezpieczeństwa hasła.

Długość hasła i wielkość alfabetu są czynnikami wpływającymi na rozmiar maksymalnej przestrzeni haseł.

S = A^M

Następująca zależność wyraża długość hasła M:

Przykład:

Hasła nazywane "user-friendly" (nazywane również frazami hasłowymi) mogą być generowane używając np. 3 symboli z alfabetu (słownika) spośród 2000 symboli, gdzie każdy symbol jest wymawialnym słowem składającym się z 4, 5 lub 6 znaków. A więc:

A = 2000 symboli (słów)
M = 3
więc $S = 2000^3 = 8*10^9$ unikalnych haseł.

M = {log({L*R}over{P})}over{log (A)}

Przekształcając powyższe wzory otrzymamy oszacowanie na M:

Zwykle otrzymujemy dla M wartość niecałkowitą którą musimy zaokrąglić do najbliższej liczby całkowitej.