HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Upravljanje zaporkama

CCERT-PUBDOC-2004-06-78

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument predstavlja vlasništvo CARNet-a (CARNet CERT-a). Namijenjen je za javnu objavu, njime se može svatko koristiti, na njega se pozivati, ali samo u originalnom obliku, bez ikakvih izmjena, uz obavezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima, povreda je autorskih prava CARNet-a, sukladno Zakonu o autorskim pravima. Počinitelj takve aktivnosti podliježe kaznenoj odgovornosti koja je regulirana Kaznenim zakonom RH.

Sadržaj

1. Uvod

Sigurnost informacijskih sustava jedan je od primarnih ciljeva i zaduženja svake organizacije. Upravljanje sigurnošću informacijskih sustava (engl. ***I**nformation **S**ecurity **M**anagement **S**ystem*) sastoji se od nekoliko modula od kojih svaki ima za cilj opisati razvoj, dokumentiranje i implementaciju određenih sigurnosnih procedura i kontrola koje će ostvarivati zahtijevanu razinu zaštite. Jedan od modula kojem se ne pridaje dovoljno pažnje jest upravljanje zaporkama. Upravljanje zaporkama (engl. *password management*) u prvom redu odnosi se na sam način čuvanja zaporki, međutim, u ovom dokumentu pod tim nazivom obuhvaćen je proces od kreiranja zaporki pa do njihova otkrivanja. Pri spominjanju zaporki potrebno je također objasniti pojmove autentikacije i autorizacije. Autentikacija (engl. *authentication*) je proces provjere identiteta osobe ili procesa (entiteta) koji ima za cilj potvrditi da je entitet upravo onaj za koji se isti izdaje. Autorizacija (engl. *authorization*) je proces u kojem se entitetu odobrava pristup resursima nakon što je uspješno završen proces autentikacije. Postoji nekoliko metoda autentikacije, a jedna od njih je korištenje zaporke (engl. *password*).

Zbog činjenice da zaporke nisu najbolji način provođenja autentikacije zato što mogu biti lako otkrivene, ukradene ili dijeljene između više korisnika, u području sigurnosti informacijskog sustava razvija se modul specijaliziran za upravljanje zaporkama. Upravljanje zaporkama obuhvaća procedure koje se odnose na razvijanje, dokumentiranje i efektivno implementiranje zaporki kako bi se osiguralo zadovoljavanje sigurnosnih zahtjeva definiranih od strane organizacijske sigurnosne politike. Cilj upravljanja zaporkama je podići svjesnost korisnika, definirati razloge korištenja zaporki, savjetovati pri kreiranju zaporke, iznijeti prednosti i nedostatke alata za generiranje zaporki, opisati načine čuvanja zaporki te opisivati alate koji služe za otkrivanje zaporki. Ovaj dokument bavi se upravo osnovama upravljanja zaporkama kako bi se taj modul sigurnosti informacijskih sustava što više pojasnio te da bi se postigli prije navedeni ciljevi.

2. Općenita razmatranja

U većini slučajeva u informatičkom okruženju, autentikacija predstavlja posljednju prepreku između korisnika i računala. Autentikacija putem zaporke je široko rasprostranjena metoda. Zaporka je definirana kao zaštićeni skup znakova koji se koristi kao autentikacija identiteta korisnika ili kao autorizacija pristupa resursu te bi, zbog tog razloga, ona trebala biti jedinstvena za svaki entitet. Zaporku koriste svi korisnici, bez obzira na privilegije i informatičku pismenost. Upravljanje zaporkama započinje odabirom tzv. jake zaporke koja je karakterizirana kao zaporka koja nije predvidljiva te zadovoljava kriterije izbora jake zaporke, a koji su navedeni dalje u dokumentu. Unatoč preporukama koje se daju za odabir jake zaporke, preostaje ljudski faktor koji dodatno umanjuje sigurnosnu razinu koje omogućuju zaporke. Korisnici pomoću zaporki pristupaju informacijskim resursima na radnom mjestu, koriste ih na kućnim računalima, koriste razne servise (informatičke, bankarske, itd.) i pri tome moraju pamtiti nekoliko zaporki ili drugih identifikacijskih podataka odjednom. Ograničenje ljudske memorije uzrokuje pojavu nemalog broja slučajeva u kojima korisnici zapisuju zaporke na papir te ih stavljaju na vidljiva mjesta (stol, zaslon) ili ih pokušavaju prikriti spremajući ih u ladice stola te lijepljenjem s donje strane tipkovnice. Drugi primjer neprimjerenog upravljanja zaporkama je što korisnici biraju zaporke koje su izuzetno lako pamtljive i predvidljive kako bi uspjeli zapamtiti nekoliko zaporki koje su aktualne. Primjer takvih zaporki su imena članova obitelji, kućnih ljubimaca, datumi rođenja ili slični podaci osobne prirode. Administratori, s druge strane, moraju brinuti o zaporkama koje oni koriste pri obavljanju svog posla te o zaporkama korisnika informacijskog sustava. Nije neuobičajena pojava da administratori biraju jednu zaporku za pristup svim resursima s kojima rade ili da koriste predefinirane zaporke (engl. *default passwords*) programskih proizvoda i sklopovlja kako bi sami sebi olakšali pamćenje velikog broja zaporki, no pri tome zaboravljaju da istovremeno ugrožavaju informacijski sustav.

Upravljanje zaporkama ima specifičnosti, a svaka od njih ima dvojako značenje. Primjer jedne specifičnosti je vrijeme trajanja zaporke. Unutar svakog sustava administrator ima mogućnost postavljanja vremenskog perioda unutar kojega se zaporka mora mijenjati, uz različite dodatne opcije, ili postavljanja neograničenog perioda valjanosti zaporke. U slučaju neograničenog korištenja jedne

zaporke povećan je rizik da se, u slučaju otkrivanja zaporke, ona može zlouporabiti i nakon dužeg vremenskog perioda, jer neće biti zamijenjena. Drugi slučaj ima nedostatak što iznenadno upozorava korisnika na promjenu zaporke pri čemu korisnik nema dovoljno vremena odabrati jaku zaporku, a time se povećava mogućnost otkrivanja zaporke.
Odobrenje ulaza u sustav predstavlja prvi prodor u sustav te svakako zaslužuje ozbiljno razmatranje tog sigurnosnog problema. Ozbiljnost još više ističe činjenica da je ophođenje s zaporkama među prvih deset sigurnosnih problema u svijetu.

3. Odabir zaporke

Korištenje zaporki vrlo je dobro uhodan način sigurnosne kontrole, premda nedovoljno siguran. Upravljanje zaporkama, stoga, za svoj prvi cilj ima definiranje preporuka po kojima se odabiru jake zaporke. Jaka zaporka definira se kao zaporka koja nije laka za otkrivanje bilo kojem programskom alatu u razumnom vremenskom periodu (otprilike sedam dana), koja je lako pamtljiva, koja je privatna (koristi ju samo jedan korisnik) i koja je tajna. Samim isticanjem važnosti odabira zaporke, apsolutno se odbacuje mogućnost korištenja praznih zaporki (engl. *null passwords*) tj. zaporki koje uopće ne postoje, što znači da je korisnik, prilikom kreiranja zaporke, umjesto upisa zaporke pritisnuo tipku `Enter`. Osim odabira jake zaporke, aktualno je i pitanje broja zaporki koje se koriste. Ukoliko se koristi jedna zaporka za sve pristupe, u slučaju otkrivanja zaporke napadač ima pristup svim korisničkim resursima. U slučaju korištenja zaporke za pojedine pristupe povećana je mogućnost zaboravljanja ili njihova zapisivanja pri čemu je neizbježno lako otkrivanje zaporki. Kao kompromisno rješenje među navedenim slučajevima preporučljiv je odabir zaporki prema domenama korisničkih pristupa (elektronička pošta, aplikacije, mrežni pristup, web servisi, itd.). Pri odabiru zaporke aktualna su dva načina. Prvi način je samostalan odabir zaporke, a drugi način je korištenje programskih proizvoda za generiranje zaporki. Oba načina odabira zaporki imaju svoje prednosti i mane koje su navedene dalje u dokumentu.

3.1. Samostalan odabir zaporke

Samostalan odabir zaporke je za većinu korisnika najjednostavniji način. Sigurno je da će korisnik takvu zaporku lako zapamtiti, ali je isto tako sigurno da će ona biti lako otkrivena jer je u većini slučajeva sastavljena od osobnih podataka. Kako bi se kod korisnika promijenio ustaljen način odabiranja zaporki, navesti će se preporuke koje upućuju na način odabira jake zaporke koja će korisniku biti pamtljiva.
Zaporka koja će zadovoljiti prethodno navedene karakteristike da neće biti laka za otkrivanje, da je lako pamtljiva, privatna i tajna treba biti odabrana slijedom i kombinacijom ovih preporuka:

1. minimalna dužina zaporke je 6 znakova,
2. treba sadržavati kombinaciju malih i velikih slova,
3. treba sadržavati slova i brojke,
4. treba sadržavati znakove interpunkcije,
5. treba sadržavati minimalno jedan specijalan znak,
6. treba imati minimalno četiri različita znaka (koja se ne ponavljaju),
7. treba izgledati kao niz slučajno odabranih znakova,
8. treba se mijenjati određenom frekvencijom,
9. treba biti različita od prethodno korištene zaporke,
10. treba biti lako pamtljiva samo korisniku.

Primjeri takvih zaporki su: `9#hGfM4`, `hU!4y0k`, `tI1nKu2.` ...
Također postoje i preporuke koje upućuju na to kakva zaporka ne smije biti. To su:

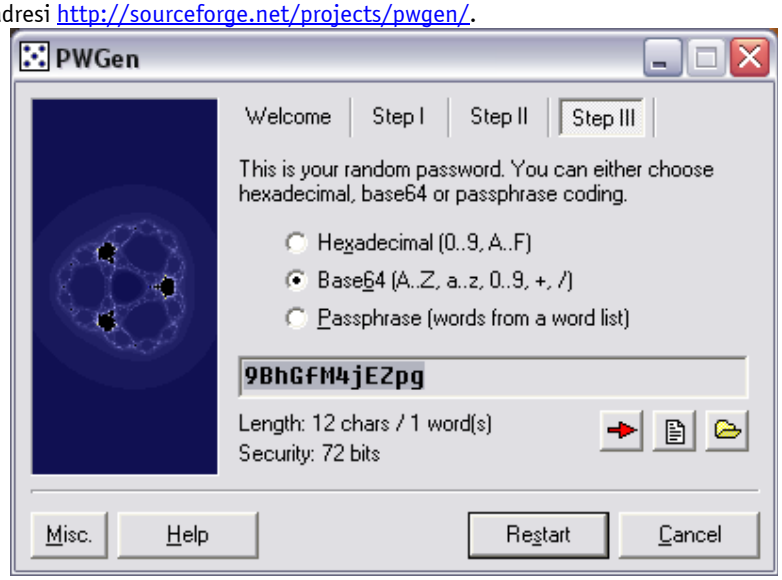
1. ne koristiti korisničko ime ili bilo koji njegov dio,
2. ne koristiti osobne podatke,
3. ne koristiti smislene riječi bilo kojeg jezika,
4. ne koristiti prethodne zaporke ili bilo koji njihov dio,
5. ne koristiti slijedna slova ili brojeve (npr. abcdefg ili 234567),
6. ne koristiti susjedna slova na tipkovnici (npr. asdfghjk).

Primjeri takvih zaporki su: `tigrica`, `aaa555`, `marko23`...

Kako bi se korisnicima olakšao odabir zaporki koje zadovoljavaju prethodno navedene stavke koriste se različite metode. Jedna od metoda je korištenje mnemotehnike. Od rečenice koja ima određeno značenje za korisnika uzmu se prva slova svake riječi koja će činiti zaporku. Npr. od rečenice "Biti ili ne biti, pitanje je sad" kreira se zaporka `BiNb,pjS`.

3.2. Programski proizvodi za generiranje zaporki

Korištenje programskih proizvoda za generiranje slučajne zaporke (engl. *password generator*) oslobađa korisnike od slijeda prethodno navedenih preporuka. Programski proizvodi baziraju se na generiranju zaporki koje su jake, no njihov nedostatak je što se vrlo teško pamte. Dok u prethodno opisanom načinu korisnik ima mogućnost odabrati zaporku koja će njemu biti lako pamtljiva, slučajno generiranje zaporki za rezultat daje nelogičan skup znakova. Time se izaziva mogućnost da korisnik zaporku zapiše na list papira čime sigurnost pada na najmanju moguću razinu jer postoji veliki rizik od lakog otkrivanja zapisane zaporke. Djelomično rješenje problema zapisivanja slučajno generiranih zaporki jest da se korisniku preporuči zapisivanje zaporke, ali s proširenjem stvarne zaporke. U slučaju da je generirana zaporka oblika `9BhGfM4`, korisnik ju može zapisati u obliku `-9BhGfM4-4`.
Jedan od besplatnih alata koji služi za generiranje zaporke je i PWGen 1.40 za Windows operacijske sustave te PWGen 2.03 za Unix platforme koji kreira kriptografski jaku zaporku baziranu na AES enkripcijskom algoritmu. Na slici 1 prikazano je sučelje programa za Windows platformu koji se može pronaći na adresi http://sourceforge.net/projects/pwgen-win/, a alat za Unix platformu može se pronaći na adresi http://sourceforge.net/projects/pwgen/.



Slika 1: *Prozor alata PWGen 1.40 koji generira zaporku*

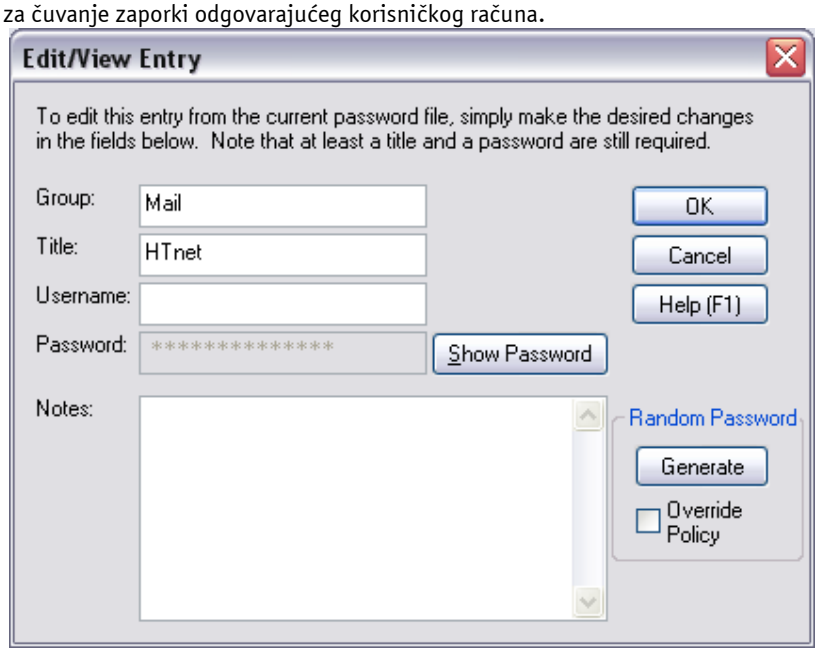
4. Čuvanje zaporki

Svaki korisnik informacijskog sustava susreće se s nekoliko zaporki koje mora koristiti, svakodnevno ili povremeno. U svrhu promicanja korištenja jakih zaporki korisnicima se savjetuje i način čuvanja zaporki:

1. zaporke pamtiti ili koristiti programski proizvod za čuvanje,
2. ne zapisivati ih,
3. ne govoriti ih niti dijeliti bilo kojoj drugoj osobi,
4. ne koristiti (uključivati) opciju "zapamti zaporku" (engl. *remember my password*),
5. odabirati različite zaporke za različite domene,
6. mijenjati zaporke barem svakih 6 mjeseci,
7. ukoliko se zaporka iz opravdanih razloga otkrije trećoj osobi, ona mora biti zamijenjena novom prvom prilikom.

Također postoji i veliki broj programskih proizvoda čija je osnovna namjena upravljanje zaporkama. Čuvanje zaporki, međutim, krši osnovno pravilo upravljanja zaporkama koja definira da se zaporka ne smije zapisivati. U slučaju čuvanja više zaporki u jednoj bazi povećava se sigurnosni rizik. Kompromitiranjem baze s zaporkama napadač ima pristup svim zaporkama. Postoji nekoliko opravdanih razloga koji upućuju na nečuvanje zaporki. Pri razlog je što baza s zaporkama predstavlja tzv. *single point of failure*, a drugi razlog je što takvo čuvanje predstavlja rizik otkrivanja zaporki dok korisnik sam pregledava zaporke (korisnik u njegovo blizini ima pregled sadržaja na zaslonu, korisnik ostavi sadržaj zaslona nezaštićen te bazu s zaporkama otvorenu, itd.). Unatoč opravdanosti navedenih razloga, postoje i razlozi koji upućuju na potrebu čuvanja zaporki korištenjem programskih proizvoda. Prvi razlog je što korištenje baza s zaporkama, koja je zaštićena enkripcijskom zaporkom, predstavlja bolju razinu zaštite od zaporki zapisanih na papirima. Za čuvanje zaporki koriste se programski proizvodi koji se uglavnom dijele na dvije kategorije. Prvu kategoriju čine alati koji služe za spremanje zaporke (engl. *password stores*), koji se koriste uglavnom za spremanje korisničkih imena i zaporki. Drugu kategoriju čine alati za upravljanje zaporkama (engl. *password managers*) koji uključuju i upravljanje pristupom korisnicima i grupama korisnika.

Jedan od programskih proizvoda koji ima zadaću čuvanja zaporki je alat Passwordsafe koji se može pronaći na web adresi http://sourceforge.net/projects/passwordsafe/. Passwordsafe je alat koji čuva zaporke na računalu korištenjem *Blowfish* enkripcije. Slika 2 prikazuje dijaloški okvir u kojem se kreira novi zapis za čuvanje zaporki odgovarajućeg korisničkog računa.



Slika 2: *Prozor alata Passwordsafe u kojem se kreira novi zapis*

Svi programski alati koji su namijenjeni čuvanju i upravljanju zaporkama moraju zadovoljiti tehničke karakteristike te lakoću rada. Tehničke karakteristike odnose se na tehnologiju koja se koristi (enkripcija, implementacija, itd.) dok lakoća rada u alatu obuhvaća intuitivno korisničko sučelje. Također, alati korišteni u ovu svrhu trebaju zadovoljiti određene kriterije kojima se osigurava:

1. tajnost datoteke s zaporkama,
2. integritet datoteke s zaporkama,
3. dostupnost datoteci s zaporkama,
4. skalabilnost,
5. jednostavna implementacija,
6. lakoća korištenja, te
7. opravdanost troškova implementacije.

5. Otkrivanje zaporki

Neki od načina otkrivanja zaporki spomenuti su kroz ovaj dokument (zapisane zaporke na vidljivom mjestu, dijeljenje među korisnicima koji su odsutni s radnog mjesta, itd.) no bitno je napomenuti da nema svako otkrivanje zaporke jednako značenje i jednake posljedice. Otkrivanje administratorskih zaporki rezultira velikim posljedicama za sustav i podatke. Zaporke korisnika koji imaju pristup financijskim podacima te bankarskim ili bolničkim servisima i podacima također spadaju pod jako osjetljive te moraju imati bolju razinu zaštite od zaporki za pristup elektroničkoj pošti.
Otkrivanje zaporki izvodi se na više načina. U ovom dokumentu ukratko su opisana dva osnovna načina za otkrivanje zaporke. Prvi način je pogađanje zaporke ili tzv. "pokušaj – pogreška" način, a drugi je probijanje zaporke. Postoji i nekoliko specifičnih načina koji iskorištavaju razne ranjivosti sustava od kojih će se ovdje spomenuti samo čitanje zaporke iz memorije računala.

5.1. Pogađanje zaporke

Ovaj način otkrivanja zaporki uspješniji je ukoliko napadač pozna osobu čiju zaporku pogađa jer će upisivanjem osobnih podataka ili drugih poznatih karakteristika u većini slučajeva pogoditi pravu zaporku. Ukoliko napadač ne poznaje korisnika, tada se primjenjuju razne tehnike socijalnog inženjeringa koje omogućuju napadaču da otkrije potrebne informacije. Pogađanje zaporke ima nedostatak, a to je veliki broj permutacija poznatih podataka pri čemu se povećava broj pokušaja. Međutim, rizik od mogućnosti pogađanja zaporke moguće je svesti na minimum ograničavanjem dopuštenog broja krivog upisivanja zaporke (uobičajeno je tri pokušaja). Kod ovog načina otkrivanja zaporki, napadač može biti i udaljen od resursa za koji izvodi pogađanje zaporke.

5.2. Probijanje zaporke

Drugi način otkrivanja zaporke je probijanje (engl. *cracking*). Probijanje zaporke znači pokretanje programskih proizvoda koji pogađaju veliki broj zaporki nad datotekama koje sadrže korisnička imena i zaporke. Koriste rječnik i/ili popis uobičajenih zaporki, izvode permutacije riječi unutar rječnika (popisa) te koriste nasilnu metodu (engl. *brute force*) generiranja potencijalne zaporke. Prilikom probijanja zaporki napadač mora biti fizički lociran gdje je i sam resurs za koji se otkriva zaporka.
Ovaj način otkrivanja iziskuje korištenje nekog od mnoštva programskih proizvoda za probijanje zaporke.

5.3. Čitanje zaporke iz memorije računala

Poslužitelji i aplikacije čuvaju zaporke u enkriptiranom obliku na disku, no postoji nekoliko slučajeva kada zaporke, prilikom spremanja u memoriji, nisu enkriptirane. Ta ranjivost sustava može biti iskorištena od strane korisnika jer pristup memoriji nema restrikcije koje se baziraju na privilegiji korisnika. To znači da korisnik – napadač može pristupiti memoriji te iz nje pročitati zaporke. Pri izvođenju tog procesa korisnik mora koristiti programski proizvod koji omogućuje pregled memorije sustava (engl. *memory viewer*). Za lociranje zaporke unutar memorije sustava koriste se dva pristupa, a to su traženje zaporke prema fiksnoj adresi u memoriji te traženjem određenog uzorka unutar memorije.

6. Zaključak

U sigurnosti informacijskog sustava nema mjesta za mit o savršenoj sigurnosti. Bitna je procjena rizika za određeni informacijski resurs te njegovo smanjivanje uvođenjem odgovarajuće sigurnosne procedure. Korištenje zaporki je, koliko jednostavan, toliko i nesiguran način sigurnosne kontrole. Iako je najrasprostranjenija metoda autentikacije, predložena su i implementirana te se i dalje razvijaju razna druga rješenja koja će jednako jednostavno, ali s većom razinom sigurnosti nuditi istu uslugu. Za korisnike na svim razinama preporučljiv je odabir zaporke koja je jaka, po samostalno odabranoj metodi, te pokušaj probijanja zaporke s ciljem provjere njezine efikasnosti. Pravnim osobama se preporučuje provođenje procesa podizanja svjesnosti korisnika te njihovo obrazovanje o sigurnosnim problemima, a preporučljivo je i uvođenje sigurnosne politike upravljanja zaporkama u kojoj će biti propisan postupak odabiranja te čuvanja zaporki, kao i uvjeti koji omogućuju probijanje

zaporke. Takva sigurnosna politika mora se temeljiti na poslovnim procesima, identificiranim resursima te procijenjenom riziku jer cilj politike nije ometati kontinuitet poslovnih procesa, već osigurati odgovarajuću razinu zaštite.

7. Reference

Bishop, M.: Password Management
http://seclab.cs.ucdavis.edu/papers/pdfs/mb-91.pdf

Enterprise Password Management
http://psynch.com/docs/enterprise-password-management.html

Geodsoft - Good and Bad Password How-To
http://geodsoft.com/howto/password/

Kumar, A.: Discovering passwords in the memory
http://www.paladion.net/papers/index.htm

Ranalli, T. H.: Options for Secure Personal Password Management
http://www.giac.org/practical/GSEC/Hugh_Ranalli_GSEC.pdf

SANS Password Policy
http://www.sans.org/resources/policies/Password_Policy.pdf

Shelby, R. Secure password storage
http://www.sans.org/rr/papers/9/693.pdf

Sonnenberg, A.: SSO: Enabling an effective password policy
http://itresearch.forbes.com/detail/RES/1056723362_370.html&src=KA