HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza Password Safe programskog paketa

CCERT-PUBDOC-2003-10-43

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.

Sadržaj

1. Uvod

Unatoč postojanju raznih novijih metoda autentikacije kao što su tokeni, pametne kartice, biometrijski uređaji itd., uporaba korisničkih imena i zaporki u današnje vrijeme je još uvijek najraširenija oblik autentikacije. Tipični korisnik danas mora pamtiti od nekoliko pa sve do desetak, ako ne i više, korisničkih imena i zaporki. Zbog velikog broja informacija vrlo često se događa da korisnik zaboravi neki od svojih autentikacijskih podataka, što predstavlja problem. Također, korisnici često imaju tendenciju korištenja istih zaporki za pristup različitim resursima, što sa sigurnosnog stajališta nije dobro. Isto tako, korisničke zaporke često su vrlo jednostavne ili trivijalne, što napadačima potencijalno omogućava lakšu kompromitaciju sustava.
Password Safe je aplikacija koja omogućava korisnicima pohranu informacija o svakom korisničkom računu, zajedno s osnovnim pripadajućim informacijama. Podaci se pohranjuju u sigurnom obliku, korištenjem BlowFish algoritma za šifriranje. Aplikacija je napisana u C++, a radi na svim Windows platformama (9x/ME/2000/XP/CE).

2. Instalacija

Instalacija aplikacije u doslovnom smislu ne postoji, već je dovoljno raspakirati i pokrenuti izvršnu datoteku. Password Safe paket je moguće pronaći na adresi (http://sourceforge.net/projects/passwordsafe) gdje se mogu odabrati `.zip` datoteke za odgovarajuću platformu (Win 9x/ME, 2000, CE). Isto tako, na spomenutoj adresi može se pronaći i izvorni kôd aplikacije. Trenutno je aktualna inačica 1.9.2c.2.
Arhivsku `.zip` datoteku potrebno je raspakirati u željenu mapu na disku i aplikacija je spremna za rad. Osim izvršne datoteke `pwsafe.exe`, u arhivi se nalaze licenca, XML manifest datoteka, te korisnička Help datoteka u uobičajenom `.chm` (engl. *compiled set of HTML files*) formatu. Također postoje README.txt i ReleaseNotes.txt datoteke, u kojima su dane osnovne informacije o paketu, odnosno pregled revizija aplikacije. Kompletan sadržaj .zip arhive je sljedeći:

```
LICENSE
PasswordSafe.exe.manifest
pwsafe.chm
pwsafe.exe
README.txt
ReleaseNotes.txt
```

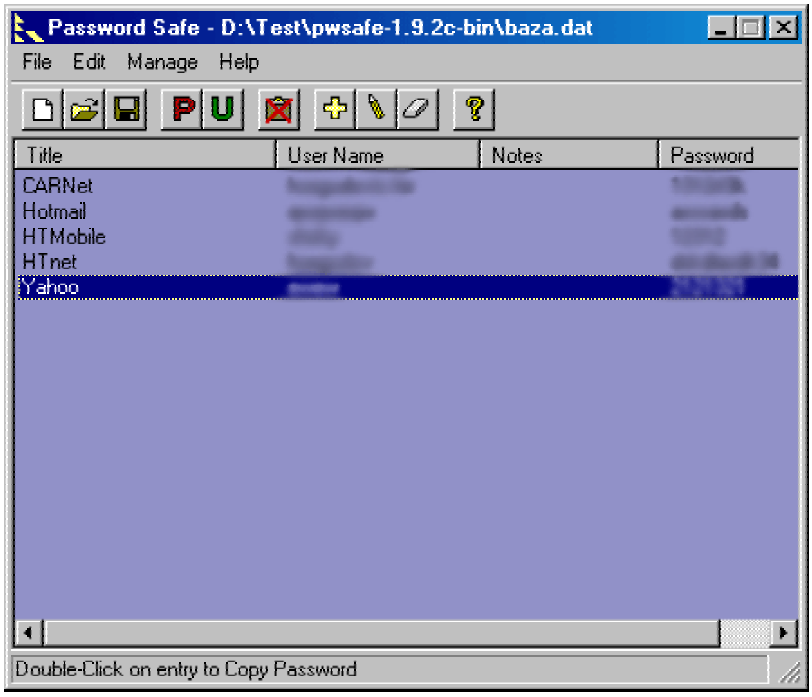
3. Korištenje

Prilikom pokretanja aplikacije korisnik može odabrati rad s postojećom bazom ili otvoriti novu bazu (*Slika 1*). Bazu podataka čini obična .dat datoteka pohranjena na disku i šifrirana BlowFish simetričnim algoritmom. Prilikom otvaranja postojeće datoteke korisnik mora unijeti odgovarajuću zaporku na temelju koje je ranije generiran ključ za šifriranje. Ukoliko se otvara nova datoteka, postupak je sličan, osim što u ovom slučaju korisnik mora odabrati zaporku iz koje se generira ključ kojim se šifrira nova baza. Kod odabira nove zaporke, aplikacija će upozoriti korisnika ukoliko zaporka ne zadovoljava osnovne zahtjeve za složenost (prekratka zaporka, postojanje specijalnih znakova i/ili znamenki), no korisnik je svejedno može potvrditi.

Slika 1: Pokretanje aplikacija i otvaranje baze

Aplikacija posjeduje standardno Windows GUI sučelje, a rad s njom je vrlo jednostavan i intuitivan (*Slika 2*). GUI sučelje se sastoji od tri elementa:

- trake s izbornicima,
- trake s alatima,
- radnog područja.



Slika 2: GUI sučelje

Traka s izbornicima sastoji se od četiri izbornika: *File*, *Edit*, *Manage* i *Help*. Unutar spomenutih izbornika nalaze se opcije kojima se podešava rad aplikacije. Većinu opcija iz izbornika moguće je također dobiti i iz trake s alatima, pritiskom na odgovarajuću ikonu.

Radno područje aplikacije također je vrlo jednostavno i prikazuje sadržaj trenutno otvorene baze. Predefinirano se prikazuje ime odabrano za autentikacijske podatke, korisničko ime, te opis. Korištenjem dodatnih opcija taj pogled je donekle moguće mijenjati.

3.1. Upravljanje

Upravljanje aplikacijom moguće je kroz izbornike ili korištenjem trake s alatima.

Izbornik *File* koristi se za rad s korisničkim bazama, a sadrži sljedeće naredbe:

- *New* – otvara novu bazu,
- *Open* – otvara postojeći bazu,
- *Save/ Save As* – sprema trenutno otvorenu bazu,
- *Exit* – izlaz iz aplikacije.

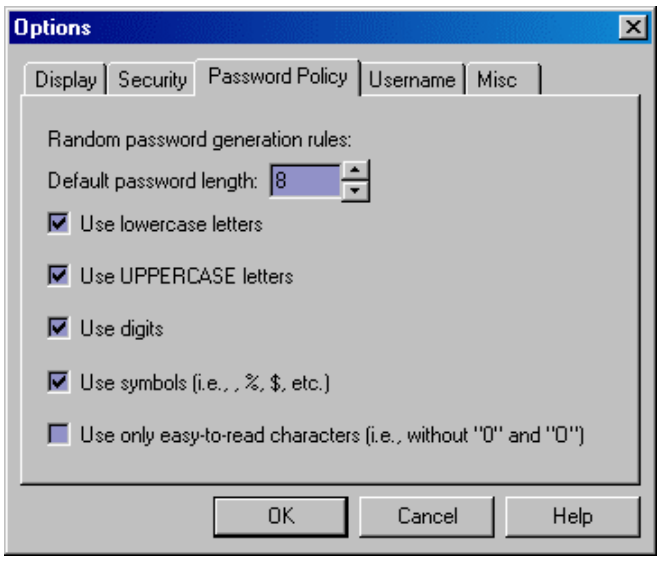
Izbornik *Edit* koristi se za upravljanje zapisima u bazi i kopiranje zaporki, a sadrži sljedeće naredbe:

- *Add Entry* – dodaje novi zapis u bazu. Prilikom dodavanja novog zapisa potrebno je unijeti ime zapisa, korisničko ime, zaporku te opcionalno opis zapisa. Također je moguće i automatsko generiranje sigurne zaporke koja se generira slučajno na temelju trenutno važeće politike.
- *Edit/View Entry* – služi za pregled i/ili uređivanje zapisa u bazi. Ovisno o postavkama zaporke se prikazuju ili su sakrivene, što je korisno u okruženjima gdje korisnik nije siguran od toga da mu netko neće otkriti zaporku pogledom na monitor.
- *Delete Entry* – briše zapis u bazi.
- *Find Entry* – pronalazi zapise u bazi pretražujući sva polja izuzev same zaporke (ime zapisa, korisničko ime i opis).
- *Copy Password to Clipboard* – služi za kopiranje zaporke na *clipboard*. Ova opcija također je korisna za nesigurna okruženja jer korisnik može obaviti bilo koju operaciju sa zaporkom bez njezinog vizualnog otkrivanja.
- *Copy Username to Clipboard* – služi za kopiranje korisničkog imena na *clipboard*.
- *Delete Clipboard* – briše *clipboard*.

Izbornik *Manage* služi za odabir dodatnih opcija i sadrži sljedeće naredbe:

- *Change Safe Combination* – mijenja zaporku trenutno otvorene baze.
- *Make backup* – radi backup trenutno otvorene baze. *Backup* datoteke imaju ekstenziju .bak.
- *Restore from backup* – radi obnovu baze iz odabrane *backup* datoteke.
- Options – omogućava konfiguraciju dodatnih opcija aplikacije kroz sljedeće kartice:
  - *Display* – omogućava podešavanje načina prikaza same aplikacije (*always on top*), prikaza zaporki u glavnom prozoru aplikacije i prikaza zaporki prilikom uređivanja zapisa,
  - *Security* – omogućava postavljanje dodatnih sigurnosnih zaštita; brisanje *clipboarda* nakon korištenja, potvrdu kopiranja, zaključavanje baze prilikom minimizacije aplikacije,
  - *Password Policy* – omogućava definiranje politike za slučajno generiranje zaporki; duljina zaporki, korištenje velikih i malih slova, brojki, specijalnih znakova (*Slika 3*),
  - *Username* – omogućava podešavanje predefiniranog korisničkog imena,
  - *Misc* – omogućava definiciju dodatnih, manje važnih parametara.

Kroz izbornik *Help* moguće je koristiti HTML *Help* podršku za korisnike, te doći do informacija o autoru i inačici aplikacije.



Slika 3: Podešavanje generatora slučajnih zaporki

4. Sigurnost i primjena

Sigurnost baze podataka *Password Safe* programskog paketa temelji se na Blowfish algoritmu. Blowfish je simetrični kriptografski algoritam koji je razvio Bruce Schneier. Algoritam nije patentiran, a njegova uporaba je besplatna. Algoritam kao ulaz uzima 64-bitni otvoreni tekst, nad kojim se u 16 iteracija izvode modulo zbrajanja i XOR operacije. Kao rezultat se pojavljuje šifrirani tekst čija duljina je također 64 bita. Ključ za šifriranje je varijabilne duljine, no maksimalna duljina je ograničena na 448 bita. U ovom trenutku nije poznata niti jedna efikasna kriptoanalitička metoda koja bi kompromitirala ovaj algoritam.

Sam program funkcionira tako da se unesena zaporka koristi za generiranje ključa koji se koristi za šifriranje/dešifriranje datoteke koja sadrži bazu podataka. Ključem se prvo računa *hash* vrijednost te zatim šifrira kratki niz slučajnih podataka pohranjenih na početku datoteke. Dobiveni rezultat se uspoređuje sa šifriranom *hash* vrijednosti pohranjenoj u datoteci. Na taj način se provjerava valjanost zaporke. Ukoliko je zaporka točna, dešifrira se ostatak datoteke. Ostatak datoteke sastoji se od zapisa varijabilne duljine koji sadrže odgovarajuće podatke. Zapisi se čuvaju u memoriji u obliku povezane liste u šifriranom obliku, a dešifriranje se provodi po potrebi.

Aplikacija je sama po sebi zbog opisanog načina implementacije prilično sigurna i predstavlja vrlo koristan alat koji se može primijeniti na nekoliko načina. Korištenjem *Password Safe* programskog paketa korisnicima je na siguran način omogućeno centralizirano upravljanje i pohrana svih relevantnih zaporki. Vrlo korisna je i mogućnost upotrebe generatora slučajnih zaporki. Također, portabilnost je velika jer kompletan paket, zajedno s datotekom koja sadrži bazu podataka stane na jednu disketu. Uporaba je prvenstveno zanimljiva krajnjim korisnicima koji se svakodnevno susreću s mnogim korisničkim imenima koja su im dodijeljena i zaporkama koje moraju pamtiti za poslovne, ali i za osobne potrebe. Naravno, paket može biti zanimljiv kao pomoćni alat mrežnim administratorima koji često veći broj zaporki drže pohranjen negdje na papiru. Korištenjem ovog alata, uz adekvatno odabranu zaporku, odnosno onemogućavanje *brute force* napada, moguće je vrlo dobro zaštititi željene podatke. Pri tome valja imati na umu da se zaporka kojom se zaključava baza ne smije izgubiti ili zaboraviti pošto ne postoji drugi način za dešifriranje pohranjenih podataka ili obnovu zaboravljene zaporke.

5. Zaključak

Analizirani Password Safe programski paket pokazao se kao vrlo koristan alat za pohranu i centralizirano upravljanje višestrukim autentikacijskim podacima korisnika. Korištenje aplikacije je jednostavno i intuitivno, a prilikom analize nisu pronađeni funkcionalni ili logički nedostaci koji bi predstavljali ozbiljni nedostatak.

Kriptografske metode koje aplikacija koristi mogu se smatrati sigurnima za potrebe običnih korisnika, pa i šire od toga. Osim toga, sama aplikacija implementirana je na način da se mogućnost eventualne kompromitacije zaštićenih podataka nakon dešifriranja svede na minimum.

Korištenje alata je preporučeno za korisnike i administratore kojima upravljanje većim brojem autentikacijskih podataka predstavlja dnevni problem. Pri tome ipak valja imati na umu da je za pohranu poslovnih autentikacijskih podataka potrebno proučiti sigurnosnu politiku pojedine organizacije i provjeriti da li se ovaj način pohrane kosi s propisanim pravilima.