

Password Safe 1.92b

- Introduzione
- Dettagli tecnici
- Istruzioni d'uso

Egizio Raffaele

Introduzione

- Password Safe 1.92b è stato progettato per mantenere le password in un database criptato protetto da "Safe Combination"
- E' un programma open source per microsoft windows 9x/2000/xp
- Sviluppato dalla [Counterpane internet Security](http://www.counterpane.com)
- E' possibile scaricare l'eseguibile dal sito <http://sourceforge.net/projects/passwordsafe>

Introduzione

- Ad ogni password del database sono associati i seguenti campi:
 - Title
 - UserName
 - Notes (qualsiasi informazione aggiuntiva)
- Supporta un'algoritmo pseudocasuale programmabile per la generazione di password non banali
- Disponibili anche backup e restore per l'archiviazione e il ripristino sicuro del database
- Tramite messaggi di avvertimento cerca di invogliare l'utente a scegliere Safe Combination non banali (dalla Safe Combination dipende la sicurezza del database e di tutte le informazioni in esso contenute)

Dettagli Tecnici Formato Database

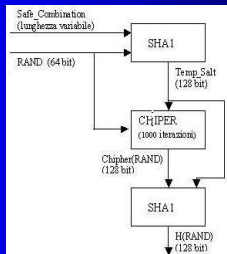
Valore casuale di 8 byte Salt usato da Blowfish Vettore di inizializzazione di CBC-Blowfish

RAND	H(RAND)	SALT	IP
C(Name1)	C>Password1	C(Notes1)	
C(Name2)	C>Password2	C(Notes2)	
.....	
C(NameN)	C>PasswordN	C(NotesN)	

C() è una versione modificata di CBC-Blowfish. C(Name), C>Password) e C(Notes) sono memorizzate come sequenze codificate di blocchi di 8 byte, con il primo blocco di ogni campo che contiene la lunghezza in byte del campo stesso. Il campo Name consiste di due sottocampi, "Title" and "Username", separati da SPLCHR.

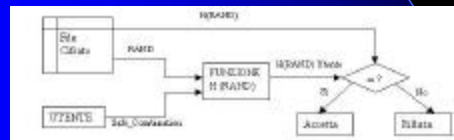
Funzione H(RAND)

- $H(RAND) = \text{SHA1}(\text{tempSalt} | \text{Cipher}(RAND))$
 - tempSalt = $\text{SHA1}(RAND | \text{Safe_Combination})$
 - Cipher(RAND) è ottenuto codificando 1000 volte il valore RAND con uno STREAM CIPHER che usa tempSalt come chiave



Verifica Safe_combination

- Si confronta il valore H (RAND) ottenuto usando la Safe Combination dell'utente con quello memorizzato all'inizio del file cifrato, se i due valori coincidono la Safe Combination viene accettata altrimenti viene rifiutata

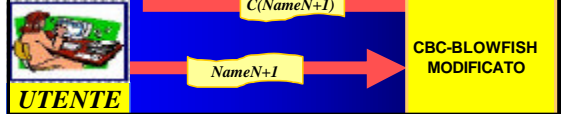


Codifica Nuova Entrata

- Il CBC-Blowfish modificato è applicato separatamente ad ogni campo della sequenza Name|Password|Notes|
- La nuova tripla C(Name)|C>Password)|C(Notes)| viene quindi aggiunta alla fine del database

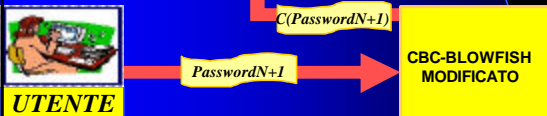
Codifica Nuova Entrata

RAND	H(RAND)	SALT	IP
C(Name1)	C>Password1)	C(Notes1)	
C(Name2)	C>Password2)	C(Notes2)	
.....	
C(NameN)	C>PasswordN)	C(NotesN)	
C(NameN+1)			



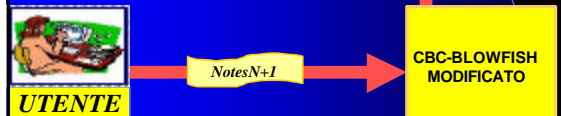
Codifica Nuova Entrata

RAND	H(RAND)	SALT	IP
C(Name1)	C>Password1)	C(Notes1)	
C(Name2)	C>Password2)	C(Notes2)	
.....	
C(NameN)	C>PasswordN)	C(NotesN)	
C(NameN+1)	C>PasswordN+1)		



Codifica Nuova Entrata

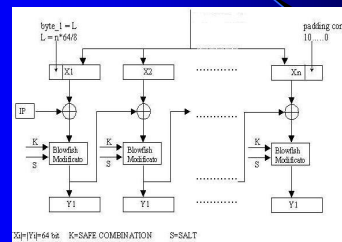
RAND	H(RAND)	SALT	IP
C(Name1)	C>Password1)	C(Notes1)	
C(Name2)	C>Password2)	C(Notes2)	
.....	
C(NameN)	C>PasswordN)	C(NotesN)	
C(NameN+1)	C>PasswordN+1)	C(NotesN+1)	




CBC-Blowfish modificato

- Usa come chiave la Safe Combination
- Il campo salt viene usato per modificare il funzionamento del Blowfish standard
 - Tale accorgimento evita che gli stessi dati vengano cifrati allo stesso modo su due database differenti e toglie all'attaccante la possibilità di usare chip Blowfish disponibili commercialmente (migliore difesa contro attacchi di tipo dizionario)
- Viene aggiunto un byte all'inizio del primo blocco del testo in chiaro contenente la lunghezza in byte del testo stesso comprensiva dell'eventuale padding
 - Tale byte viene usato in fase di decodifica per dividere i campi in modo corretto


CBC-Blowfish modificato



File Menu



- **Save** 
 - Salva le eventuali modifiche effettuate sul corrente database
- **Save As**
 - Salva il corrente database (e le eventuali modifiche effettuate su di esso) con un nome differente. La versione con il vecchio nome non viene modificata
- **Exit**
 - Esce da Password Safe
- E' possibile recuperare una password con un doppio click sulla relativa voce (che copierà la password negli appunti) e con un CTRL+V (che la incollerà dove si vuole) senza comunque mostrarla mai in chiaro

Edit Menu




- **Add entry 1)** 
 - Permette di aggiungere una nuova password al database corrente. Selezionando questa opzione viene visualizzata la seguente finestra:



Edit Menu

- **Add Entry 2)**
 - Title identifica l'accoppiata nome utente/password nell'elenco
 - Notes permette di annotare per ogni coppia di user-id e password ciò che più ci fa comodo
 - Si possono lasciare i campi Username e Notes in bianco ma è necessario riempire i campi Title e Password
 - Generate Random Password permette di generare password in maniera pseudocasuale
- **Edit /View Entry** 
 - Permette di cambiare i dati associati alla password evidenziata nel database corrente. La relativa finestra è molto simile a quella visualizzata da Add Entry
- **Delete Entry** 
 - Permette di cancellare la password selezionata e i relativi campi dal database

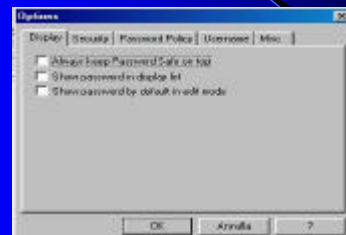
Edit Menu

- **Find Entry**
 - Cerca la prima password che contiene in uno dei campi ad essa associati (eccetto il campo password) il testo digitato nell'apposita casella
- **Copy Password to Clipboard** 
 - Permette di copiare negli appunti la password relativa al voce evidenziata nella finestra principale
- **Copy Username to Clipboard** 
 - Permette di copiare negli appunti l'username relativa al voce evidenziata nella finestra principale
- **Clear Clipboard** 
 - Cancella il contenuto degli appunti. Se un'altra applicazione ha copiato dati negli appunti non sarà possibile cancellarli

Menage Menu

- **Change Safe Combination**
 - Permette di cambiare la Safe Combination del corrente database
- **Make Backup**
 - Permette di creare una copia di backup del corrente database
- **Restore from Backup**
 - Permette di ripristinare l'ultima copia di backup creata
- **Update V1.1 Backups Make Backup**
 - Permette di aggiungere l'estensione .bak alle copie di backup
- **Options Make Backup**
 - Permette di configurare le opzioni

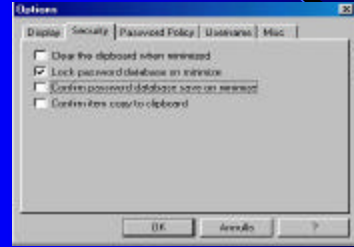
Display Tab



Display Tab

- **Always keep Password Safe on top**
 - Se questa opzione è spuntata le finestre di Password Safe sono poste al di sopra di tutte le altre finestre (opzione disabilitata sui Pocket PC)
- **Show password in display list**
 - Se questa opzione è spuntata la finestra principale contiene una colonna extra che mostra le password
- **Show password by default in edit mode**
 - Se questa opzione è spuntata le password non sono inizialmente oscurate da asterischi nella finestra Edit/View

Security Tab



Security Tab

- **Clear the clipboard when minimized**
 - Se quest'opzione è spuntata gli appunti vengono cancellati quando Password Safe viene ridotto ad icona
- **Lock password database on minimize and prompt on restore**
 - Se quest'opzione è spuntata le informazioni sensibili, come la Safe Combination e gli eventuali cambiamenti nel database non ancora salvati, sono cancellate dalla memoria quando Password Safe viene ridotto ad icona. Quando Password Safe viene ripristinato viene chiesta nuovamente la Safe Combination

Security Tab

- **Confirm password database save on minimize**
 - Se quest'opzione è spuntata Password Safe, quando viene ridotto ad icona, chiede se si desidera salvare gli eventuali cambiamenti effettuati sul database. Se quest'opzione non è spuntata il database viene salvato automaticamente
- **Confirm item copy to clipboard**
 - Se quest'opzione è spuntata Password Safe visualizza un messaggio di notifica quando una password è copiata negli appunti

Password Policy Tab

Le opzioni di questo tabulato servono a personalizzare la politica dell'algoritmo di generazione di password casuali usato nelle finestre di dialogo di **Add Entry** e **Edit/View Entry**.



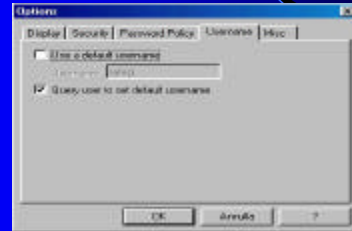
Password Policy Tab

- **Default password length**
 - Con quest'opzione è possibile decidere il numero di caratteri della password
- **Use lowercase letters**
 - Se quest'opzione è spuntata la password generata conterrà delle lettere minuscole
- **Use uppercase letters**
 - Se quest'opzione è spuntata la password generata conterrà delle lettere maiuscole

Password Policy Tab

- **Use digits**
 - Se quest'opzione è spuntata la password generata conterrà dei caratteri numerici
- **Use symbols**
 - Se quest'opzione è spuntata la password generata conterrà dei caratteri simbolici come &, %, \$ ed altri
- **Use only easy-to-read characters**
 - Se quest'opzione è spuntata alcuni caratteri, come ad esempio 0 (zero) che può essere confuso con la lettera o, vengono esclusi dall'algoritmo di generazione delle password

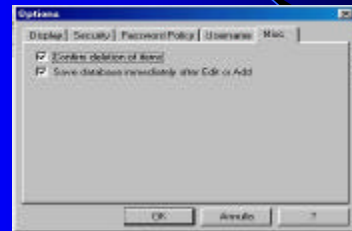
Username Tab



Username Tab

- **Use default username**
 - Permette di specificare un valore di default per il campo Username. Se quest'opzione è spuntata la stringa del campo Username viene inserito automaticamente nel relativo campo della finestra di dialogo di Add Entry (Può comunque essere cambiato)
- **Query user to set default username**
 - Se quest'opzione è spuntata, quando viene inserita una nuova voce nel database con campo Username non vuoto, viene visualizzata una finestra di dialogo che chiede se si desidera impostare il valore del campo Username come username di default

Misc Tab



Misc Tab

- **Confirm deletion of items**
 - Se quest'opzione è spuntata, Password Safe chiede conferma sulla volontà di cancellare una password quando viene usato il comando Delete Entry
- **Save database immediately after Edit or Add**
 - Se quest'opzione è spuntata, Password Safe, salva automaticamente il database ogni qual volta una password viene aggiunta o né vengono modificati i relativi campi (ma non quando la password viene cancellata)