Protezione con Chiave Software

by

“A Strange Site”

http://astrangesite.altervista.org

powered by

dott. Alessandro Strano

CREAZIONE DELLA CHIAVE

Supponiamo di voler realizzare un sistema di protezione del software tramite una “chiave” che ne abiliti appieno le funzionalità.

La “chiave” dovrà avere le seguenti caratteristiche:

- **validità limitata nel tempo;**
- **validità limitata al computer per il quale è stata calcolata.**

Per creare la “chiave” utilizzeremo sia i valori numerici (caratteri dal codice ASCII 30h[1] al codice ASCII 39h) che le lettere maiuscole (caratteri dal codice ASCII 41h al codice ASCII 5Ah); in tutto 36 caratteri, di cui 10 numerici e 26 alfabetici. Indichiamo con “stringa_car” l’insieme di questi caratteri, ovvero la stringa:
“0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ”.

Innanzi tutto, calcoliamo un valore casuale[2] compreso tra 1 e 5 (la sintassi utilizzata nelle formule è quella del Visual Basic[3]).

val_cas = INT(RND(TIMER) * 4) + 1

Questo valore ci servirà per rendere la nostra chiave meno comprensibile; supponiamo di avere ottenuto il valore 3.

Consideriamo poi la data di scadenza che per comodità possiamo indicare con gg/mm/aaaa (gg=giorno, mm=mese, aaaa=anno). Supponiamo sia 31/12/2002.

---

[1] con il simbolo “h” si intende un valore espresso nel formato esadecimale.
[2] gli estremi sono stati fissati in modo tale da far sì che nei conteggi successivi tutti i valori siano compresi tra 1 e 36, il numero di caratteri che abbiamo a disposizione.
[3] Visual Basic è ©Microsoft Corporation.

Convertiamo il giorno in un carattere alfanumerico utilizzando le seguenti formule:
puntatore = 32 – gg + val_cas
carattere = MID(stringa_car, puntatore, 1)
Nel nostro caso puntatore vale 4 e pertanto il carattere sarà "3".

Facciamo altrettanto con il mese, utilizzando possibilmente una formula diversa per il calcolo del puntatore.
puntatore = 10 + mm – val_cas
carattere = MID(stringa_car, puntatore, 1)
Nella fattispecie il puntatore è 19, mentre il carattere è "I".

Per rappresentare le 4 cifre dell'anno possiamo procedere come indicato:
strAnno = STR(aaaa)
'nella formula che segue "i" andrà sostituito con 1 per la prima cifra, 2 per la seconda
'e così via dicendo sino alla quarta cifra
puntatore = CINT(MID(strAnno, i, 1)) + 2^i + val_cas
carattere = MID(stringa_car, puntatore, 1)
Nel nostro caso otteniamo i seguenti puntatori 7, 7, 11, 21 ed, ovviamente, i caratteri "6", "6", "A", "K"

Dobbiamo infine ricavare il numero seriale del disco su cui è installato il software e possiamo farlo tramite le "API" di Windows.

```
'dichiarazione della funzione (ci si rifà alla documentazione della Microsoft)
Private Declare Function GetVolumeInformation Lib "kernel32.dll" Alias "GetVolumeInformationA" (ByVal _
 lpRootPathName As String, ByVal lpVolumeNameBuffer As String, ByVal nVolumeNameSize As Long, _
 lpVolumeSerialNumber As Long, lpMaximumComponentLength As Long, lpFileSystemFlags As Long, ByVal _
 lpFileSystemNameBuffer As String, ByVal nFileSystemNameSize As Long) As Long

'dichiarazione delle variabili e richiamo della funzione (ci si rifà alla documentazione della Microsoft)
Dim strDrive As String
Dim VolName As String
Dim VolSN As Long
Dim nRet As Long
Dim MaxCompLen As Long
Dim VolFlags As Long
Dim VolFileSys As String
VolName = Space(256)
VolFileSys = Space(256)
strDrive="C:\"
nRet = GetVolumeInformation(strDrive, VolName, Len(VolName), VolSN, MaxCompLen, VolFlags, _
        VolFileSys, Len(VolFileSys))
```

Se "nRet" è 0 la funzione ha restituito un errore, altrimenti VolSN contiene il numero seriale. Convertiamo VolSN in una stringa esadecimale di lunghezza fissa e pari a 8 caratteri, premettendo eventualmente degli zeri.
strVolSN = HEX(VolSN)
lun = LEN(strVolSN)
If lun < 8 Then strVolSN = String(8 - lun, "0") & strVolSN

Ricaviamo quindi i nostri caratteri per la chiave:
'nella formula che segue "i" andrà sostituito con 1 per il primo carattere, 2 per il
'secondo e così via dicendo sino all'ottavo carattere.

puntatore = ASC(MID(strVolSN, i, 1)) – 47 + val_cas
carattere = MID(stringa_car, puntatore, 1)

Se, ad esempio, strVolSN è "252811EF" otteniamo i puntatori 4, 6, 9, 6, 12, 5, 5, 25 e pertanto i seguenti caratteri "3", "5", "8", "5", "B", "4", "4", "O".

Aggiungiamo anche un carattere di controllo:
puntatore = ABS(gg + mm + aaaa + val_cas + VolSN) MOD 36 + 1
carattere = MID(stringa_car, puntatore, 1)
Nella fattispecie otteniamo 36 e quindi il carattere di controllo è "Z".

Componiamo infine la nostra chiave disponendo i caratteri secondo un ordine prestabilito ad esempio valore casuale, aaaa, numero seriale, carattere di controllo, gg, mm.
Ecco la chiave: 366AK3585B44OZ3I

Si badi che l'ordine dei caratteri all'interno di stringa_car, ma anche le formule e l'ordine dei caratteri possono essere opportunamente variati ottenendo molteplici soluzioni. Inoltre, è possibile includere nella chiave ulteriori caratteri che serviranno per individuare i moduli da abilitare. Del resto è possibile escludere taluni parametri come, ad esempio, la data di scadenza, qualora non si voglia fissare un limite temporale.

VERIFICA DELLA CHIAVE

Ad ogni esecuzione il software dovrà verificare se la chiave è corretta confrontando la data di scadenza ed il numero di serie codificati in essa con la data di sistema ed il numero seriale del disco fisso del computer. Per recuperare i dati codificati nella chiave bisogna innanzi tutto ricavare il numero casuale che nel nostro caso è il primo carattere, cioè "3". Adesso possiamo ricavare gli altri dati utilizzando le formule impiegate prima.

Ad esempio per quanto riguarda il giorno, esso è codificato nel quindicesimo carattere della chiave. Ricaviamo il puntatore con la seguente formula:
puntatore = instr(stringa_car, MID(chiave, 15, 1))
e quindi risaliamo a "gg" tramite l'equazione "puntatore = 32 – gg + val_cas"
gg = 32 – puntatore + val_cas
otteniamo 31.

Faremo lo stesso anche per gli altri dati eccetto che per il carattere di controllo. Per la verifica di quest'ultimo occorre eseguirne nuovamente il calcolo in base ai dati estratti (data scadenza e numero seriale) e confrontare il carattere così ottenuto con quello riportato nella chiave.

NOTE

Per evitare che tramite la modifica della data si possa aggirare la validità temporale della chiave è possibile ricorrere a due particolari accorgimenti.

Il primo consiste nell'impedire all'utente di inserire nel software date future (cioè date successive a quella corrente) allorquando ciò non sia giustificato dalla natura del tipo di funzionalità che sta adoperando. In questo modo, anche se viene modificata la data e si riesce ad aggirare il controllo di validità della "chiave", è precluso l'utilizzo di date (ovvero registrazioni con date) successive all'effettiva scadenza del software.

Il secondo consiste nel confrontare la data di un file che è aggiornato dal software (per reperire la data del file si può ricorrere alla funzione FileDateTime) con la data odierna, se la data del file è successiva a quella restituita dall'orologio del sistema, evidentemente la data è stata portata indietro e pertanto si può impedire l'uso del software (ovviamente l'accesso in I/O al file di cui si diceva sopra non dovrà aver luogo in questo caso perché, se si tentasse immediatamente un ulteriore accesso, la sua data, modificata nel primo tentativo, sarebbe nel secondo accesso uguale a quella corrente).