LibCrypt Tutorial - (guida a cura di Littlemouse)

Come funziona il LibCrypt

I CD PSX protetti con il LibCrypt hanno dei settori del sottocanale Q modificati. La protezione legge questi settori e ricalcola una chiave a 16 bit (chiamata Magic Word), utilizzata, in seguito, per la decodifica di un insieme di dati.

Il codice LibCrypt può essere diviso in 3 subroutines indipendenti.
La prima ha lo scopo di prevenire l'utilizzo dell'Action Replay (AR).
La seconda calcola la chiave a 16 bit (Magic Word) e scrive il risultato nel registro BPC COP0.
La terza si occupa del check finale, decodificando una serie di dati con la Magic Word e bloccando il gioco se il risultato è diverso da quello atteso. Tale verifica può avvenire immediatamente (es. FF8), oppure soltanto se si arriva ad un certo livello (es. Spyro 2), oppure i dati possono essere controllati periodicamente durante i caricamenti (es. Soul Reaver) o, infine, in specifici momenti (es. Mulan).

Esistono attualmente almeno 4 varianti di LibCrypt chiamate LC1, LC2, LC3, LC4.
La LC1 è utilizzata dal primo gioco PAL protetto con LibCrypt e cioè Medieval. La protezione LC2 è certamente quella più utilizzata. Per dare un'idea, i giochi che utilizzano la variante LC3 sono: Speed Freeks, Formula 1 '99, Tele+ Premier Manager (aka Premier Manager 2000), Ronaldo V-Football, Spyro 2, Spyro 3, Sydney 2000, Men in Black: The Series - Crashdown, Lucky Luke: Western Fever, mentre il gioco F1 2000 utilizza la variante LC4.

Come rimuovere il LibCrypt (LC2)

Per rimuovere il LibCrypt si possono usare approcci diversi.
Si potrebbe modificare la routine del check finale tra dati decodificati tramite Magic Word e risultato atteso dal gioco, ma, come menzionato prima, questa verifica può essere effettuata più volte nel corso di un gioco e non potremmo essere sicuri di aver rimosso tutti i controlli.
Il metodo che useremo, invece, è quello di cambiare la routine che controlla e calcola la Magic Word in modo da inserire sempre il valore corretto nel registro BPC, indipendentemente dal fatto che sia presente il CD originale oppure una copia. Anche in questo caso ci sono delle controindicazioni, perché, per inserire il valore corretto in registro BPC, dobbiamo essere in possesso del CD originale.

Per raggiungere il nostro obbiettivo affronteremo il problema in due fasi. Nella prima fase faremo le modifiche necessarie per determinare la Magic Word (MW), utilizzando il gioco originale, mentre nella seconda, modificheremo la routine che calcola la MW in modo tale che inserisca sempre il valore corretto nel registro BPC del coprocessore.

Fase 1: Ricerca della MW (vecchio metodo)

In passato, questa fase era quella a cui occorreva dedicare la maggior parte del tempo. Infatti, la prima subroutine del Libcrypt non solo impedisce l'utilizzo della Action Replay, ma blocca anche l'utilizzo di un qualsiasi debugger, in quanto la protezione utilizza i registri COP0 usati normalmente dai debuggers per i breakpoint. Pertanto, se si vuole analizzare il codice con un debugger, occorre, per prima cosa, disabilitare questa routine.

Annullare la routine Anti-Par

Probabilmente molti conoscono l'articolo dei BAD pubblicato su GameCopyWorld. In quel articolo viene spiegato il funzionamento della seguente routine Anti-Par, responsabile anche dell'inizializzazione dei registri del coprocessore utilizzati dalla protezione.

[01] 80090818 LUI v0, 0x1F00
[02] 8009081C MTC0 v0, BPC
[03] 80090820 LUI v0, 0x1FFC
[04] 80090824 MTC0 v0, BPCM
[05] 80090828 MTC0 v0, BDA
[06] 8009082C LUI v0, 0x8009
[07] 80090830 ADDIU v0, v0, 0x0848
[08] 80090834 MTC0 v0, BDAM
[09] 80090838 LUI v0, 0xE180
[10] 8009083C MTC0 v0, DCIC
[11] 80090840 JR ra

Per evitare che l'Action Replay mandi in crash la PSX oppure il debugger, abbiamo bisogno di prevenire che un breakpoint venga attivato nei primi 256k della memoria. La soluzione più semplice consiste nel rimuovere l'istruzione (10) con un comando NOP (0x00000000). Con questa semplice patch possiamo usare il debugger per la ricerca della MW, ma, occorre tener presente che tale modifica non sarà necessaria per il crack finale.

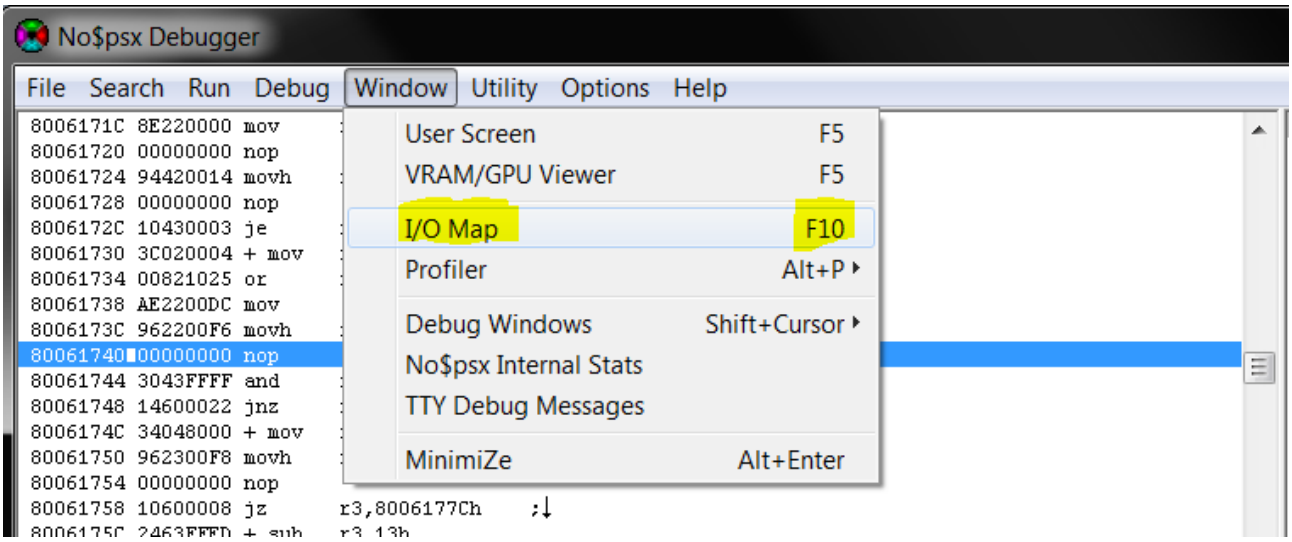
Magic Word

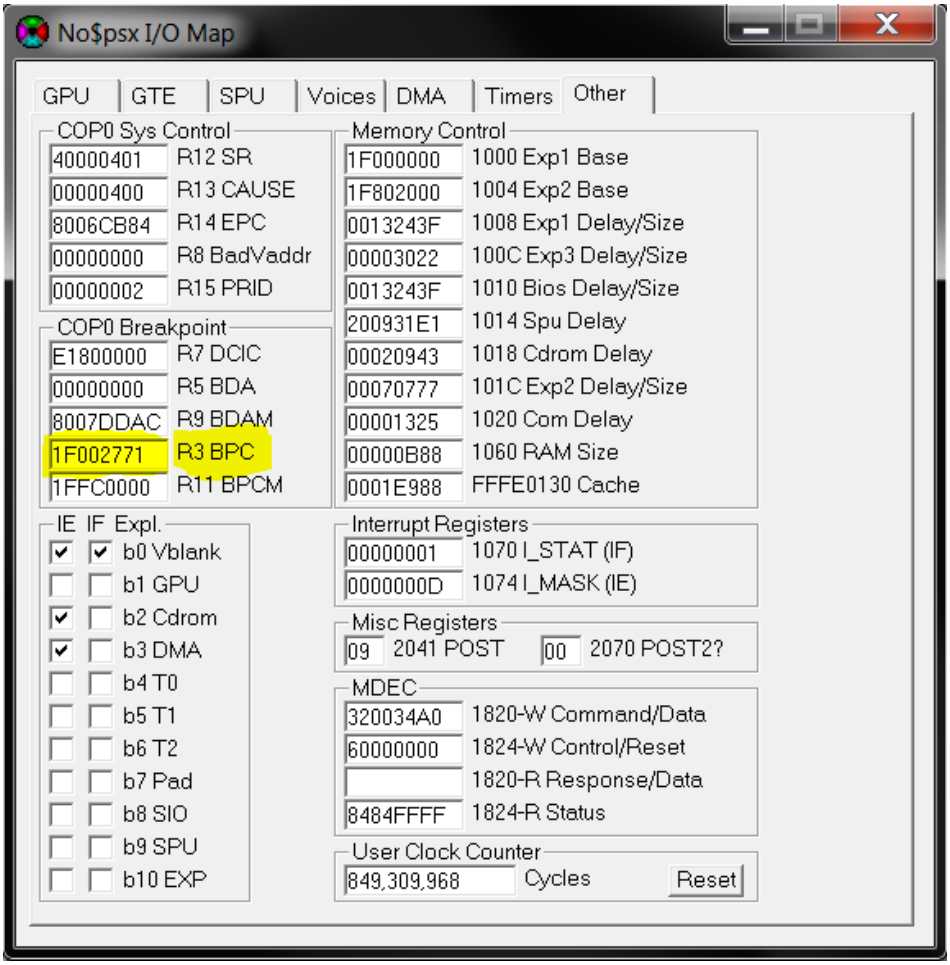
La routine successiva a quella Anti-Par è quella che effettua diversi controlli (CD, ModChip ...) e, poi, calcola la MW. Scorrendo il codice di questa subroutine, il punto 15 è quello in cui la MW è stata calcola ed è possibile leggerla nel registro r2.

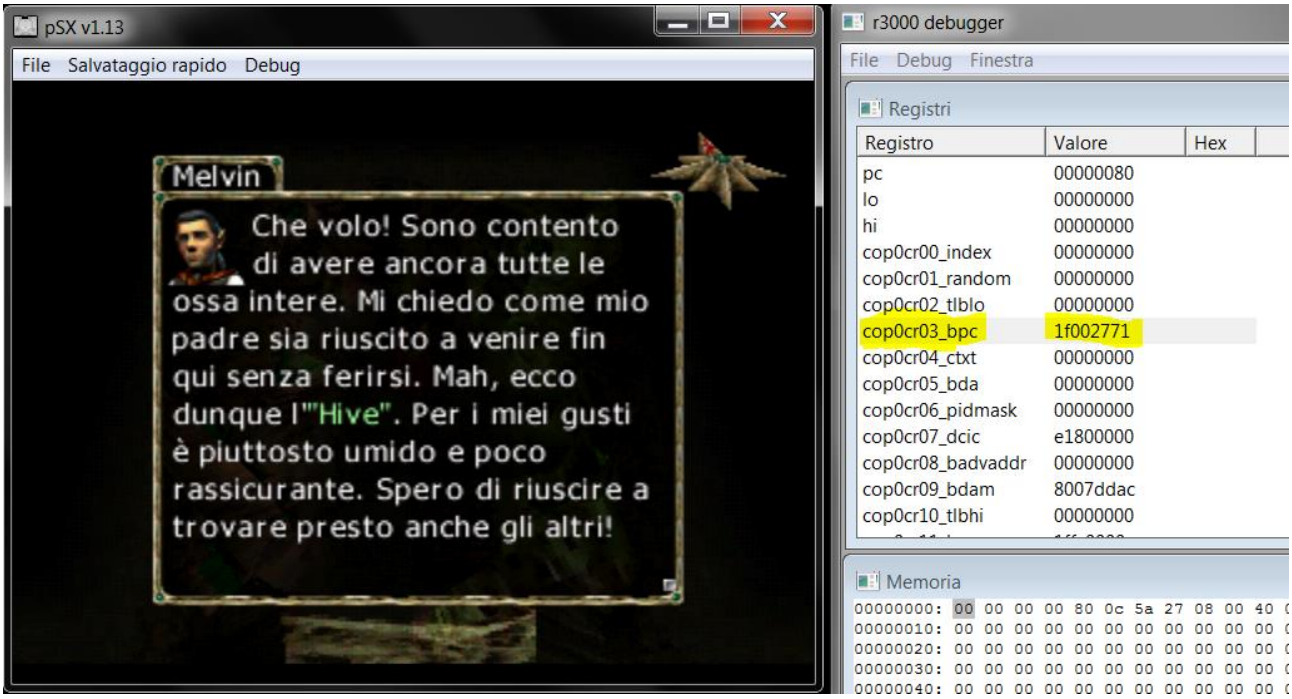
[01] 80090AE0 ADDIU r0, r0, 0x49C4	3813 8424	
[02] 80090AE4 SW zero, 0x0000(a0)	0000 80AC	
[03] 80090AE8 MFC0 r2, BPC	0018 0640	
[04] 80090AEC LB r0, 0x0004(a1)	0400 A480	
[05] 80090AF0 ANDI at, r2, 0xFFFF	FFFF C130	
[06] 80090AF4 BNE at, zero, 0x80090B18	0800 2014	Anti-MOD Check
[07] 80090AF8 ANDI r3, r3, 0x0002	0200 E730	
[08] 80090AFC BEQ r3, zero, 0x80090B18	0600 E010	Anti-MOD Check
[09] 80090B00 ADDI r0, r0, 0xFFAD	ADFF 8420	
[10] 80090B04 BNE r0, zero, 0x80090B18	0400 8014	Anti-MOD Check
[11] 80090B08 NOP	0000 0000	
[12] 80090B0C LB r0, 0x0007(a1)	0700 A480	
[13] 80090B10 LUI r2, 0x1F00	001F 063C	
[14] 80090B14 OR r2, r0, r2	2530 8600	Calculate MW
[15] 80090B18 MTC0 r2, BPC	0018 8640	Add MW in BPC register
[16] 80090B1C JR ra	0800 E003	

Fase 1: Ricerca della MW (nuovo metodo)

Un metodo molto più semplice per trovare la Magic Word di un gioco PSX protetto tramite LibCrypt è quello dell'utilizzo di un emulatore con debugger integrato (ad esempio PsX 1.13 oppure no$psx), in quanto, utilizzando un disco originale oppure una copia con file sub e/o sbi del disco originale, basterà aspettare che la MW venga scritta nel registro BPC del coprocessore.







Fase 2: La patch

Per realizzare la patch dovremo inserire il valore della MW, ora in nostro possesso, nel registro r2 appena prima che venga copiato nel registro BPC del coprocessore. Per fare questo occorrerà cambiare l'istruzione 14 con la seguente OR r2, r2, MW (dove MW nel nostro caso è 2771) che in formato esadecimale corrisponde a 7127 C634 (dal momento che la PSX utilizza il formato Little Endian, i bytes devono essere scritti in modo invertito).
Questi semplici 4 bytes sono sufficienti per rimuovere la protezione LibCrypt. Tuttavia, dal momento che le istruzioni 6, 8 e 10 si riferiscono al controllo Anti-MODchip, normalmente in tutte le patch si procede anche al loro annullamento tramite delle istruzioni NOP.
Pertanto, la subroutine patchata si presenterà nel modo seguente:

[01] 80090AE0 ADDIU r0, r0, 0x49C4	3813 8424	
[02] 80090AE4 SW zero, 0x0000(a0)	0000 80AC	
[03] 80090AE8 MFC0 r2, BPC	0018 0640	
[04] 80090AEC LB a0, 0x0004(a1)	0400 A480	
[05] 80090AF0 ANDI at, r2, 0xFFFF	FFFF C130	
[06] 80090AF4 NOP	0000 0000	NOP anti-MOD check
[07] 80090AF8 ANDI r3, r3, 0x0002	0200 E730	
[08] 80090AF4 NOP	0000 0000	NOP anti-MOD check
[09] 80090B00 ADDI r0, r0, 0xFFAD	ADFF 8420	
[10] 80090AF4 NOP	0000 0000	NOP anti-MOD check
[11] 80090B08 NOP	0000 0000	
[12] 80090B0C LB r0, 0x0007(a1)	0700 A480	
[13] 80090B10 LUI r2, 0x1F00	001F 063C	
[14] 80090B14 OR r2, r2, 0x2771	7127 C634	Patch for LibCrypt
[15] 80090B18 MTC0 r2, BPC	0018 8640	
[16] 80090B1C JR ra	0800 E003	

Applicare la patch

Per applicare la patch finale, occorre estrarre dalla iso l'eseguibile del gioco e, quindi, modificare il file con un editor esadecimale. Infine, tramite il software CDMage importare l'eseguibile modificato nella iso in modo che vengano corretti anche i settori ECC / EDC. Una volta fatto questo si potrà creare una patch in formato PPF confrontando la iso originale con quella modificata.

Considerazioni finali

In pratica, una volta trovata la MW con un emulatore con debugger, per superare la protezione di un gioco protetto con LibCrypt (in versione LC2 non criptata), basterà utilizzare la funzione di Search and Replace di un qualsiasi editor esadecimale secondo lo schema sotto riportato.

```
****************************************
 LibCrypt (LC2) Patch Scheme
****************************************

PAR Check Skip (not needed in final patch)
==========================================

Original - 80E1 023C 0038 8240
Patched  - 80E1 023C 0000 0000


MOD Check Skip
==========================================

Original - 0800 2014 0200 E730 0600 E010 ADFF 8420 0400 8014 0000 0000
Patched  - 0000 0000 0200 E730 0000 0000 ADFF 8420 0000 0000 0000 0000


Add Magic Word in BPC COP0
==========================================

------------------------------------------------------------------
Magic Word stored in BPC COP0 register - 0x1F002771
------------------------------------------------------------------

Original - 2530 8600
Patched  - 7127 C634
```