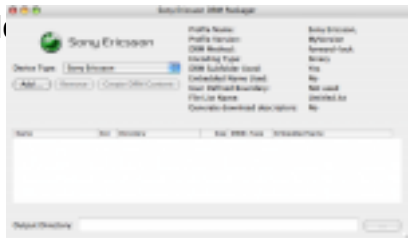
18/01/2009 - DRM per MP3

Il **Il DRM Digital Rights Management (DRM),** come molti di voi sapranno, è un controverso sistema di protezione di contenuti digitali a chiave crittografica.Il meccanismo è semplice: nel file, suoneria o altro,vengono inserite delle informazioni solo chi è in possesso della chiave di cifratura, in genere spedita col file stesso, può accedere a quel contenuto.
In genere attraverso una serie di impostazioni il DRM può essere convenientemente profilato per impedire, ad esempio, il trasferimento via bluetooth di una suoneria da un cellulare all'altro, ma si può anche limitarne la durata d'uso del contenuto nel tempo e via dicendo.
In genere basta compilare un file xml in cui vengono inseriti sia il profilo del cellulare che tutte le limitazioni d'uso.
Detto questo vi vogliamo mostrare un reverse engineering al contrario, ovvero **vi mostreremo non come scardinare la protezione di una suoneria per cellulare, ma come proteggerla attraverso l'uso del DRM**, del resto per combattere il "nemico" bisogna conoscerl



Lo strumento

CED s.r.l. *- Cod.Fisc., P.IVA, n.iscrizione Reg.Imprese CCIAA Venezia: 03529610275 - R.E.A.: 316199*
Sede Legale: *via Po, 3 - frazione Mellaredo - 30030 Pianiga (Venezia) - Tel.041.868.5150 - Fax 041.964.1109*
Sede Operativa: *via Ruffilli, 2 - 65016 Montesilvano Spiaggia (Pescara) - Tel.085.868.1020 - Fax 085.868.1029*
http://www.ced.it/ - E-Mail: amministrazione@ced.it

Esistono diversi strumenti per applicare il DRM a file MP3 o video 3GP, tanto per rimanere su formati multimediali molto diffusi, personalmente ho sempre trovato molto interessante **DRMPackager**, uno strumento di sviluppo messo a disposizione da Sony Ericsson gratuitamente e disponibile per una grande varietà di piattaforme.

In particolare DRM Packager può essere scaricato, nella versione 1.35, all'indirizzo http://developer.sonyericsson.com/site/global/docstools/misc/p_misc.jsp per quattro piattaforme differenti:- Microsoft Windows 2000/XP Disponibile sia con interfaccia grafica che da linea di comando
- Mac OS X Disponibile sia con interfaccia grafica che da linea di comando
- Linux Disponibile solo da linea di comando
- Solaris Disponibile solo da linea di comando

Per la nostra prova abbiamo scelto una versione con GUI, più semplice da utilizzare.
Il programma è piuttosto spartano, nella cartella scaricata troviamo la licenza d'uso, l'applicativo, DRM Packager GUI, e un file main .dpr che è, in sintesi un file XML che può essere modificato, un editor testuale per adattare il DRM ad altri cellulari diversi da modelli Sony Ericsson.

I passaggi per impostare la nostra protezione sono piuttosto semplici.

1) Effettuiamo un doppio clic sull'icona DRM Packager GUI per lanciare il programma. L'interfaccia grafica mostra pochi comandi essenziali. Innanzitutto un menu a tendina con il tipo di device (Device Type) settato su Sony Ericsson sulla base dell'xml di riferimento già compilato. Se vogliamo inserire un altro tipo di cellulare dobbiamo modificare il file xml di impostazione andando ad agire tra i vari Tag con un editor di testo.
Il file xml sarà di questo tipo:

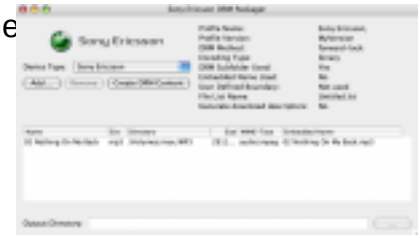
```
<profile>
<profile_name>Sony Ericsson, May 2005</profile_name>
<profile_version>Sample</profile_version>
<min_drm_tool_version>1.32</min_drm_tool_version>
<special_configurations>
```

<do_not_add_preamble_crlf></do_not_add_preamble_crlf>
<do_not_add_epilogue_crlf></do_not_add_epilogue_crlf>
<!?do_not_add_wbxml_byte></do_not_add_wbxml_byte?>
<!?default_non_user_defined_boundary>boundary_1</default_non_user_defined_boundary?>
<!?static_CID>cid:static-CID-$id@custom.com</static_CID?>
<!?static_CEK>abcdefghijklnopqrstuvw==</static_CEK?>
</special_configurations>
<device_type>
<name>Sony Ericsson</name>
<drm_method>forward-lock</drm_method>
<drm_method>combined delivery</drm_method>
<drm_method>separate delivery</drm_method>
<drm_method>Sony Ericsson</drm_method>
<!? allowed values: "forward-lock", "combined delivery", "separate delivery", ""Sony Ericsson" -
->
<transfer_encoding>binary</transfer_encoding>
<transfer_encoding>7bit</transfer_encoding>
<transfer_encoding>8bit</transfer_encoding>
<transfer_encoding>base64</transfer_encoding>
<!? Application?>
<media_type>
<mime_name>application/vnd.eri.thm</mime_name>
<file_extension>thm</file_extension>
<compatible_rights>
<display/>
</compatible_rights>
</media_type>
<!? Images?>
<media_type>
<mime_name>image/jpeg</mime_name>
<file_extension>jpg</file_extension>
<file_extension>jpeg</file_extension>
<compatible_rights>
<display/>
<print/>
</compatible_rights>
</media_type>
</device_type>

CED s.r.l. *- Cod.Fisc., P.IVA, n.iscrizione Reg.Imprese CCIAA Venezia: 03529610275 - R.E.A.: 316199*
Sede Legale*: via Po, 3 - frazione Mellaredo - 30030 Pianiga (Venezia) - Tel.041.868.5150 - Fax 041.964.1109*
Sede Operativa*: via Ruffilli, 2 - 65016 Montesilvano Spiaggia (Pescara) - Tel.085.868.1020 - Fax 085.868.1029*
http://www.ced.it/ - E-Mail: amministrazione@ced.it

2) Per inserire il file da "proteggere" basta cliccare sul pulsante Add. In questo modo si apre l'interfaccia grafica che consente di selezionare il file, nel nostro caso una canzone in formato MP3.
Di default il programma è impostato per applicare un DRM di tipo Forward Lock. In questo modo si crea un documento di MIME con estensione .dm. Il contenuto viaggia in chiaro ma il software del cellulare lo memorizza in modalità protetta impedendo che possa essere inoltrato a terzi.
In pratica risulta impossibile trasferirlo da un cellulare ad un altro.

3) Clicchiamo su Create DRM Content. Nel giro di pochi secondi verrà creata una cartella DRM posizionata ne



directory in cui si trova il file che abbiamo selezionato.
Cliccando all'interno della cartella troviamo un file .dm che è la nostra suoneria protetta e un file .dd che è un file xml di distribuzione. In pratica è un file disgiunto dal file .dm che può essere usato nel caso di distribuzione da server web. E' il caso tipico di una suoneria a pagamento scaricata da un server, in questo caso non si scarica solo il contenuto protetto ma anche i file di specifica e profilazione che sono tutti contenuti nel pacchetto.4) Noterete, all'interno della cartella DRM, una cartellina Right vuota. Qui dovrebbe e

n le

limitazioni d'uso se fosse stato impostato, ovvero la famosa chiave cifrata che ne regola i diritti. Se vogliamo impostare la nostra suoneria dobbiamo andare su Option>Configuration e dal menu a tendina selezionare combined delivery. Così facendo si apre l'interfaccia Separated e Combined delivery Settino in cui si possono impostare tutte le limitazioni d'uso che si desidera.
In questo caso il contenuto viaggia ancora in chiaro ma insieme ad esso è associata una chiave, contenuta nella cartella right, che ne regola i diritti e che consente, ad esempio, di utilizzare il contenuto un numero limitato di volte. In questo caso il pacchetto, chiave + contenuto, vengono scaricati contemporaneamente dal server.
5) L'altra impostazione residua è separate delivery. In questo caso il contenuto e la chiave viaggiano separati: il contenuto è cifrato si può utilizzare solo dopo aver acquisito la chiave, in genere ricevuta separatamente tramite SMS.

CED s.r.l. *- Cod.Fisc., P.IVA, n.iscrizione Reg.Imprese CCIAA Venezia: 03529610275 - R.E.A.: 316199*
Sede Legale: *via Po, 3 - frazione Mellaredo - 30030 Pianiga (Venezia) - Tel.041.868.5150 - Fax 041.964.1109*
Sede Operativa: *via Ruffilli, 2 - 65016 Montesilvano Spiaggia (Pescara) - Tel.085.868.1020 - Fax 085.868.1029*
http://www.ced.it/ - E-Mail: amministrazione@ced.it

CED s.r.l. *- Cod.Fisc., P.IVA, n.iscrizione Reg.Imprese CCIAA Venezia: 03529610275 - R.E.A.:* 316199
Sede Legale*: via Po, 3 - frazione Mellaredo - 30030 Pianiga (Venezia) - Tel.041.868.5150 - Fax 041.964.1109*
Sede Operativa*: via Ruffilli, 2 - 65016 Montesilvano Spiaggia (Pescara) - Tel.085.868.1020 - Fax 085.868.1029*
http://www.ced.it/ - E-Mail: amministrazione@ced.it