Remarry Syscon

Replacing the Syscon requires you to remarry it to CELL.

Contents

Introduction

The System Controller has different *EEPROM* regions of which two are the NVS (non-volatile storage) and the SNVS (secure NVS).
If CELL wants to access the SNVS it has to be married to the Syscon. The SNVS holds for example the secure product mode information, the lv0/lv1 hash and the SRK/SRH.
This guide will only cover the perconsole section which holds the pairing information and the SNVS section, not the NVS nor the internal (only by Syscon plain accessible) regions.
For easier reading the complete area will be called **SPCR** - Syscon Per Console Region.

Basic Syscon Prerequisites

In order to remarry the Syscon you have to have raw access to the corresponding EEPROM regions.
The SPCR on Mullion (CXR) models is saved at 0x0000-0x2800 while it's at 0x3000-0x5800 on Sherwood (SW) models.
For the NVS regions (and internal regions) please refer to the EEPROM page, this guide will only provide the offsets used by UM.

Procedure

Case #1: A full dump of the original Syscon SPCR is available

If this is the case and you're not switching from Mullion to Sherwood or the other way around you can just copy the SPCR.

Case #2: The original Syscon SPCR is not available

The PS3 needs to run a factory (JIG) firmware in order to remarry the Syscon!
First blank the complete SPCR with hex *FF*. Then for the first 0x30 bytes write this:

```
5E B4 F7 C9 50 62 F1 B2 EC F7 EE 1A 3C E3 D8 D0
C5 C2 73 4B A4 13 3D 2C 9E EE 88 ED 0C A8 15 C7
```

```
8F 59 DC E4 35 A8 11 BD 8B EC 4E 95 09 F1 E7 38
```

And set offset 0x48C07 of the NVS to *00*.

If you start the PS3 you should see this on PS3s with a Mullion Syscon (as part of the bootlog obtainable from the SB UART):

```
[INFO]: sc_init START
[INFO]: 1...o
[INFO]: 2 skip
[INFO]: 3...o
[INFO]: 4.0.1...o    4.0.2...o    4.0.3...o    4.0.4...o
[INFO]: 4.1.1...o    4.1.2...o    4.1.3...o    4.1.4...o
[INFO]: 4.2.1...o    4.2.2...o    4.2.3...o    4.2.4...o
[INFO]: 4.3.1...o    4.3.2...o    4.3.3...o    4.3.4...o
[INFO]: 4.4.1...o    4.4.2...o    4.4.3...o    4.4.4...o
[INFO]: 4.5.1...o    4.5.2...o    4.5.3...o    4.5.4...o
[INFO]: 4.6.1...o    4.6.2...o    4.6.3...o    4.6.4...o
[INFO]: 4.7.1...o    4.7.2...o    4.7.3...o    4.7.4...o
[INFO]: pre5...o
[INFO]: skip 5, 6, 7, 8 (0x31)
[INFO]: sc_init SUCCESS
```

and this on Sherwood models:

```
[INFO]: sc_init START
[INFO]: 1...o
[INFO]: 2 skip
[INFO]: 3...o
[INFO]: 4.0.1...o    4.0.2...o    4.0.3...o    4.0.4...o
[INFO]: 4.1.1...o    4.1.2...o    4.1.3...o    4.1.4...o
[INFO]: pre5...o
[INFO]: skip 5, 6, 7, 8 (0x31)
[INFO]: sc_init SUCCESS
```

(If it instead prints error *80004040C* please refer to the explanation)

After shutting the console down power it up again which causes the Syscon to be remarried a "2nd" time.

It will produce the same output except that the third line changes from "*[INFO]: 2 skip*" to "*[INFO]: 2...o*".

The console will be now in product mode.

To complete the remarrying procedure please install any firmware using the manufacturing updater (launched by *lv2diag*) and set offset 0x48C07 of the NVS back to *FF*.

Explanation

The magic bytes

```
5E B4 F7 C9 50 62 F1 B2 EC F7 EE 1A 3C E3 D8 D0
C5 C2 73 4B A4 13 3D 2C 9E EE 88 ED 0C A8 15 C7
8F 59 DC E4 35 A8 11 BD 8B EC 4E 95 09 F1 E7 38
```

consist of the (uninitialized) Syscon status

```
00000000000000000000000000000001
```

encrypted with Key 0x000

and the Key 0x010

```
5794BC8C2131B1E3E7EC61EF14C32EB5
```

encrypted with Key 0x020.
The last 16 bytes are the CMAC of the previous 16 bytes using Key 0x020.

The Hypervisor uses the Syscon status to determine if it needs to be remarried. 1 means that it needs to be remarried, 2 means it's already married to CELL.
The key saved at offset 0x10 is used to decrypt the second layer of the EID1 stored on the flash.
If this key is wrong, Syscon will return the error *800040C*. The only time this has been observed is on prototype consoles with a Sherwood Syscon. To fix that problem you need to create your own EID1 using the eid_root_key and patch it into the Syscon Firmware.

v · e (https://www.psdevwiki.com/ps3/edit/Template:Reverse_engineering)

Reverse engineering

General	Bluedisk EID0 reDRM · Boot Order · Bugs & Vulnerabilities · Dumping Bootldr · Dumping Metldr · Files on the PS3 · KaKaRoTo_Kind_of_´Jailbreak´ · PS3Cobra Payload Reverse Engineering · PS3UserCheat · QA Flagging · ReDRM / Piracy dongles · Revoke List · RSOD Fix · rtcalarm.dat · Whitelisting · VTRM
Hypervisor	Hypervisor Reverse Engineering · Repository Nodes
Services	Appliance Information Manager · AV Manager · Dispatcher Manager · Factory Data Manager · Indi Info Manager · SB Manager · SC Manager · Secure LPAR Loader · Secure Profile Loader · Secure RTC Manager · Security Policy Manager · Storage Manager · Update Manager · Updater Frontend · USB Dongle Authenticator · User Token Manager · Virtual TRM Manager
Plugin Interfaces	ap_plugin · audioplayer_plugin · audiop_plugin_dummy · audiop_plugin_mini · auth_plugin · autodownload_plugin · autoupdateconf_plugin · avc_plugin · avc_util · avc2_game_plugin · avc2_game_video_plugin · avc2_text_plugin · bdp_disccheck_plugin · bdp_plugin · bdp_storage_plugin · campaign_plugin · category_setting_plugin · comboplay_plugin · custom_render_plugin · data_copy_plugin · deviceconf_plugin · dlna_plugin · download_plugin · dtcpip_util · edy_plugin · esehttp · eseibrd · eseidle · eselock · eula_cddb_plugin · eula_hcopy_plugin · eula_net_plugin · explore_plugin · explore_plugin_ft · explore_plugin_game · explore_plugin_np · filecopy_plugin · friendim_plugin · friendml_plugin · friendtrophy_plugin · game_ext_plugin · game_indicator_plugin · game_plugin · gamedata_plugin · gamelib_plugin · gameupdate_plugin · hknw_plugin · idle_plugin · impose_plugin · kensaku_plugin · msgdialog_plugin · mtpinitiator_plugin · musicbrowser_plugin · nas_plugin · netconf_plugin · newstore_plugin · np_eula_plugin · np_matching_plugin · np_multisignin_plugin · np_sns_plugin · npsignin_plugin · np_trophy_ingame · np_trophy_plugin · osk · oskfullkeypanel · oskpanel · pesm_plugin · photo_network_sharing_plugin · photolist_plugin · photoviewer_plugin · playlist_plugin · poweroff_plugin · premo_plugin · premo_game_plugin · print_plugin · profile_plugin · ps3_savedata_plugin · ps3_savedata_plugin_game · ps3_savedata_plugin_psp · rec_plugin · regcam_plugin · remotedownload_plugin · sacd_plugin · scenefolder_plugin · screenshot_plugin · software_update_plugin · soundvisualizer_plugin · strviewer_plugin · sysconf_plugin · system_plugin · thumthum_plugin · upload_util · user_info_plugin · user_plugin · videodownloader_plugin · videoeditor_plugin · videoplayer_util · videoplayer_plugin · vmc_savedata_plugin · wboard_plugin · webbrowser_plugin · webbrowser_service · webrender_plugin · xai_plugin · xmb_ingame · xmb_plugin
Emulation	PS1 Emulation · PS2 Emulation · PSP Emulation
Extended features	Printer support · Remote Play · String Viewer · Web Browser · XMB In-game background music · PS3 and PSVita Cross Functions · Widgets · Life with PlayStation · PlayView · XMB Manuals
Online	Consoleban · Environments · Online Connections · PSN · PSN Handshake Signup · X-I-5-Ticket
Hardware	**SC** SC Communication · SC EEPROM · Remarry Syscon · Syscon Thermal Configs · Syscon SPI **CELL**

		Cell Configuration Ring · CELL Reset Exploit · CellBE Hardware Implementation Registers · Unlocking the 8th SPE · SPU Isolated Modules Reverse Engineering · SPU LS Overflow Exploit
	RAM	XDR Configuration · Rambus Registers
	SB	ENCDEC Device Reverse Engineering
	HDD	HDD Encryption
	BD	Bluray disc · Basic Bluray disc authentication procedure · BD Drive Reverse Engineering · Disc Identification/Serialization Data · ODE · Remarry Bluray Drive
Tools		IDA pro disassembler and debugger · CCAPI · 0x000EAEB0 · Ps3.xml · Nids.txt · Nids all.txt · Unknown nids.txt · Fnids.idh
Strings	**files**	emer_init · aim spu module · lv1 · hdd_copy · eurus_fw · lv0 · factory data mngr
	dumps	lv2 dump (Rebug 4.46) · lv1 dump (Rebug 4.46) · bootldr dump (2.70) · Network Loading of lv1ldr and above executables
Reference		Archaic · Drk_notes · Canaries
Keys & Seeds		Keys · Per Console Keys · Seeds · ECDSA binaries · AES binaries · DES binaries · Cryptography Tricks