Reverse engineering tools for ST DVB chipsets

SRP-2018-01-LEAFLET

I. Description of the reverse engineering tools

1. SlimCORE disassembler	
Description	The tool to disassemble SlimCORE processor instruction streams from various firmwares used by STi7111 DVB chipsets
Features	▪ SlimCORE instruction stream disassembly from a device driver file or input files corresponding to firmware code / data sections ▪ extraction of SlimCORE firmware data / code sections from a device driver file to output files ▪ statistics information regarding the usage of SlimCORE instructions (i.e. unknown, recognized instructions)
Impact	▪ instrumental to analyze the operation of SlimCORE processor firmware and to discover vulnerabilities in STi7111 DVB chipsets (Issues 17-19) ▪ discovery of separate dispatching for DMA and all TKD operations ▪ discovery of a key initialization subroutine
Public reference	▪ HITB talk #2 (slide 50)
Deliverables	▪ source code ▪ a technical document (APPENDIX A) presenting a brief analysis of SlimCORE processor instruction set and operation of the firmware found in ADB STBs (models ITI-2849ST and ITI-2850ST, STTKDMA-REL 3.1.6, 3.5.0 and 3.9.2) that was used as a base material during reverse engineering of TKD core operation ▪ original reverse engineering annotations (APPENDIX B) for SlimCORE firmware 3.1.6, 3.5.0 and 3.9.2 (for use with a SlimCORE disassembler to obtain annotated / commented code)
2. SlimCORE tracer	
Description	The tool to trace execution flow of SlimCORE processor instructions
Features	▪ tracing the execution of SlimCORE processor instructions (single stepping, dump of register contents with proper indication of register changes) ▪ logging of a trace of executed instructions
Impact	▪ reverse engineering of unknown SlimCORE instructions

	▪ location of SLIM Core instruction sequences implementing `DecryptKey` functionality
Public reference	▪ HITB talk #2 (slides 51-53)
Deliverables	▪ source code

II. Notes

1. The tools described above have never been disclosed to any 3rd party. Their existence and usefulness have been known since 2012 though (HITB talk #2).

2. The tools were developed as part of SE-2011-01 project. Their operation was suited to the environment of fully compromised (OS root, JVM root and kernel level access privileges) ITI-2849ST / ITI-2850ST set-top-boxes and SE-2011-01 Proof of Concept code in particular. With the exception of SlimCORE disassembler (standalone tool), successful operation and use of a SlimCORE tracer may require customization and/or porting to the target STi7111 environment (target STB).

III. Legal Disclaimer

Beside the SRP license, the following paragraphs describe the legal disclaimer for the two reverse engineering tools (THE SOFTWARE) offered.

THE SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW NEITHER SECURITY EXPLORATIONS, ITS LICENSORS OR AFFILIATES, NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE SOFTWARE WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS, OR OTHER RIGHTS. THERE IS NO WARRANTY BY SECURITY EXPLORATIONS OR BY ANY OTHER PARTY THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT IT WILL BE ERROR-FREE.

YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION AND USE OF THE SOFTWARE TO ACHIEVE INTENDED RESULTS AND FOR THE INSTALLATION, USE, AND RESULTS OBTAINED FROM IT.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL SECURITY EXPLORATIONS, ITS EMPLOYEES OR LICENSORS OR AFFILIATES BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA, OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION, OR FOR ANY SPECIAL, DIRECT, INDIRECT, INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE, OR OTHER THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE INFORMATION CONTAINED IN THIS DOCUMENT, EVEN IF SECURITY EXPLORATIONS OR ITS LICENSORS OR AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

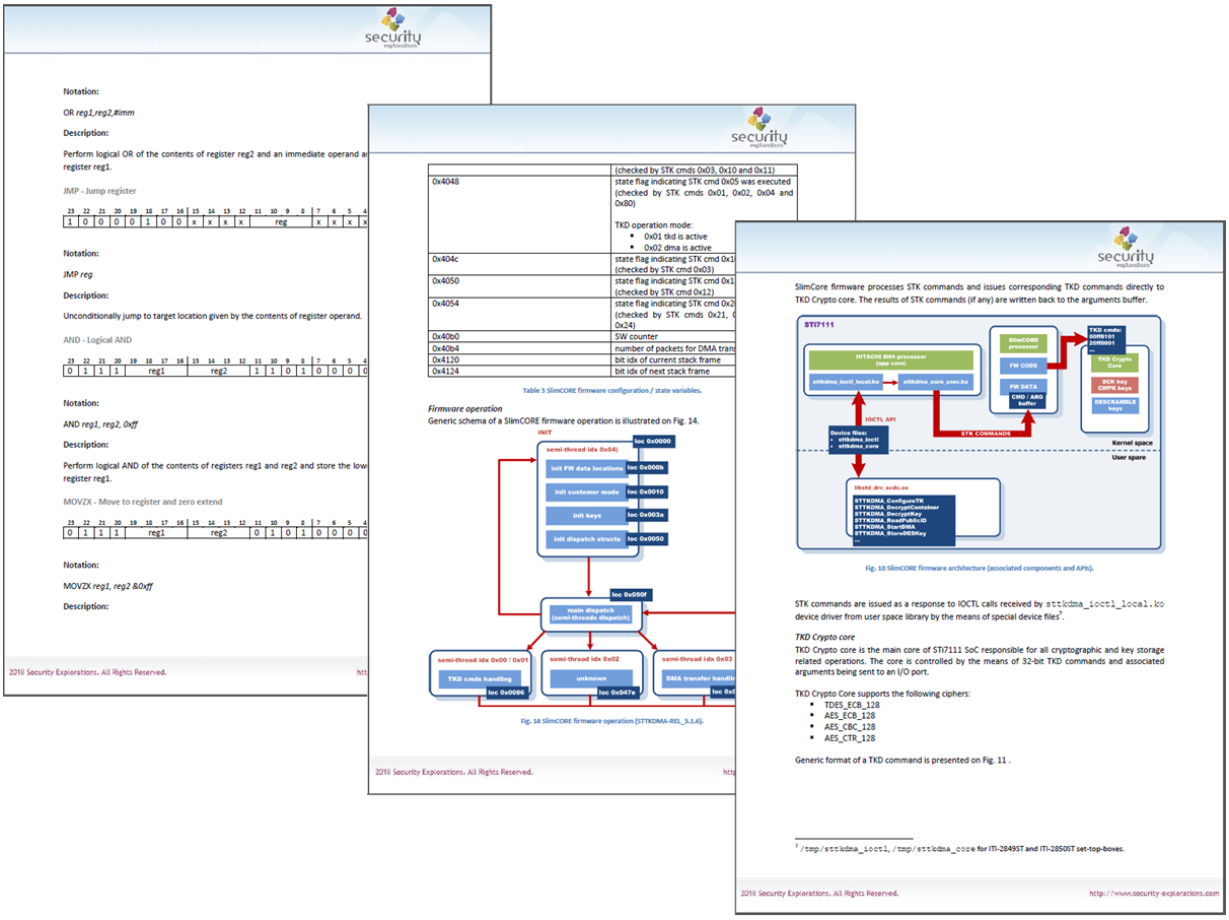
IV. SRP pricing

- SRP AO NOT AVAILABLE
- SRP EP NOT AVAILABLE

APPENDIX A

Table of contents for a technical document included as part of SRP-2018-01 material:

Screenshots of sample pages from a technical document included as part of SRP-2018-01 material:



Document features

- 70+ pages of unpublished and in-depth technical information
- information regarding SlimCORE processor instruction set, their opcodes format and processor operation
- information about reverse engineering approach taken to discover unknown SlimCORE instructions' opcodes and their meaning
- information regarding SlimCORE firmware architecture and operation (threads and their dispatching, STK / TKD commands and their groups, crypto DMA)
- information about locating SlimCORE firmware code and data sections in STTKDMA device driver file and kernel memory
- broad scope of firmwares covered (STTKDMA-REL 3.1.6, 3.5.0 and 3.9.2) making it easy to analyze any other SlimCORE firmware for STi7111 SoC
- detailed explanation of selected code parts (i.e. CWPK and CW keys handling, initialization, crypto DMA)
- information regarding firmware configuration and state variables
- information about changes to most recent firmware 3.9.2 and STMicroelectronics' "addressing" of security issues from 2012
- information about unverified, potential vulnerabilities and further research directions pertaining to TKD crypto core and STi7111 security
- description of SlimCORE disassembler and tracer tools

List of figures from a technical document included as part of SRP-2018-01 material:

List of tables from a technical document included as part of SRP-2018-01 material:

APPENDIX B

A fragment of reverse engineering annotations for STTKDMA-REL_3.1.6:

```
!/*## (c) SECURITY EXPLORATIONS    2011 poland                                  #*/
!/*##     http://www.security-explorations.com                                  #*/
!
!/* RESEARCH MATERIAL:     SRP-2018-01
*/
!/* Reverse engineering annotations                                             */
!/* SlimCORE firmware ver      : STTKDMA-REL_3.1.6                              */
!/*                   code size: 5852 (0x16dc)                                  */
!/*                   sha-1    : afe518789d1b0b1d3c0f8efd2704ac84a69140ed       */
!
!/* THIS SOFTWARE IS PROTECTED BY DOMESTIC AND INTERNATIONAL COPYRIGHT LAWS     */
!/* UNAUTHORISED COPYING OF THIS SOFTWARE IN EITHER SOURCE OR BINARY FORM IS    */
!/* EXPRESSLY FORBIDDEN. ANY USE, INCLUDING THE REPRODUCTION, MODIFICATION,     */
!/* DISTRIBUTION, TRANSMISSION, RE-PUBLICATION, STORAGE OR DISPLAY OF ANY       */
!/* PART OF THE SOFTWARE, FOR COMMERCIAL OR ANY OTHER PURPOSES REQUIRES A       */
!/* VALID LICENSE FROM THE COPYRIGHT HOLDER.                                    */
!
!/* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS     */
!/* OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,*/
!/* FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL     */
!/* SECURITY EXPLORATIONS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, */
!/* WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF   */
!/* OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE      */
!/* SOFTWARE.                                                                   */
0 ########################
0 DISPATCH idx 0x04 -> 0x2000000 (init code)
0 ########################
b ;counter = 0
c ;memory idx of 0x4040 addr
f ;store 0 to [0x4040-0x4060]
10 ;chip customer mode
12 ;low nibble of chip customer mode
14 ;-> chip customer mode == 0x05
16 ;-> chip customer mode == 0x02
18 ;-> chip customer mode == 0x06 (OUR CASE)
1a ;-> chip customer mode == 0x0b
1c ;-> chip customer mode == 0x0f
1e ;-> chip customer mode == 0x03
20 ;-> chip customer mode == 0x07
22 ;-> chip customer mode == 0x08
24 ;-> chip customer mode == 0x0c
26 ;05 -> 0x02 as customer mode
28 ;02 -> 0x04 as customer mode
2a ;06 -> 0x05 as customer mode
2c ;0b -> 0x08 as customer mode
2e ;0f -> 0x09 as customer mode
30 ;03 -> 0x10 as customer mode
32 ;07 -> 0x11 as customer mode
34 ;08 -> 0x20 as customer mode
36 ;0c -> 0x21 as customer mode
38 ;store customer mode =(0x02,0x04,0x05,0x08,0x09,0x10,0x11,0x20,0x21,*0x40)
39 ;subroutine return addr
3a ;init all of the keys (CWPK, CWs)
...
```