Exploitation Framework for STMicroelectronics DVB chipsets

SRP-2018-02-LEAFLET

I. Description

1. Exploitation framework for ST DVB chipsets	
Description	Software framework making it possible to research security of a SlimCORE and TKD Crypto cores of STi7111 DVB chipset in the environment of a real life digital satellite TV platform (NC+). The framework along accompanied tools already proved its usefulness as they were used for a discovery of the new ST chipset design vulnerability (SRP-2018-02 Issue 7).
Proof of Concept Code Features[1]	▪ administrative access (OS root, JVM root and kernel level access) to STi7111 based set-top-box devices (ITI-2850ST, ITI-2849ST and ITI-2851S) ▪ full read/limited[2] write access to file system ▪ full read/write kernel and ST chipset I/O space access ▪ smart card interface interception (APDU req / resp logging) ▪ runtime firmware interception of STi7111's embedded crypto processor ▪ firewall disabling ▪ java and system level directory tree listing ▪ java and system level file/directory tree transfer ▪ access to information about system configuration (serial number, software version, hardware type, network configuration) ▪ access to information about MPEG services ▪ access to SI MPEG sections (PAT, PMT) ▪ simple MPEG sniffing by PID value ▪ access to information about various cryptographic keys (Conax, hdcp) ▪ access to information about user's subscription's status (Conax card entitlements) ▪ access to Electronic Program Guide (EPG) ▪ DSMCC carousels mounting ▪ MPEG stream capture of arbitrary HD programming

[1] more features could be added to the Proof of Concept code in the future. In such a case, the customer will be notified and will receive a software update.
[2] to `/mnt/flash` directory.

	▪ access to vulnerable STi7111 processor (SlimCORE and TKD crypto core) ▪ inspection of TKD crypto core memory ▪ inspection of chipset security fuses ▪ execution of custom TKD crypto core commands ▪ loading and execution of SlimCORE code (images) produced by SlimCORE assembler tool ▪ Conax CWPK chipset pairing key extraction ▪ plaintext Control Word keys extraction ▪ the possibility to implement custom framework commands (run custom code on a device)
Deliverables	▪ Detailed technical description of a new design vulnerability affecting STi7111 DVB chipset (SRP-2018-02 Issue 7) in a form of a complete SRP-2018-02 report (155+ pages with nearly 30 pages dedicated solely to the new ST issue) ▪ Source and binary codes for a Proof of Concept code exploiting vulnerabilities for set-top-box and STi7111 chipset access (SRP-2018-02 Issues 1-3) ▪ Source and binary codes for a Proof of Concept code exploiting new design vulnerability affecting STi7111 DVB chipset (SRP-2018-02 Issue 7), ▪ Source and binary codes for the 2 tools described in SRP-2018-02 report (Compiler Stubs Generator and SlimCORE assembler)

II. Legal Disclaimer

Beside the SRP license, the following paragraphs describe the legal disclaimer for all Proof of Concept Codes and tools constituting SRP-2018-02 Exploitation Framework (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.

III. SRP pricing

- SRP AO NOT AVAILABLE
- SRP EP NOT AVAILABLE