Fraunhofer AISEC

Shedding too much Light on a Microcontroller's Firmware Protection

Proceedings of the 11th USENIX Workshop on Offensive Technologies (WOOT '17) - Vancouver, BC, Canada

CVE number 2017-18347

Almost every microcontroller with integrated flash features firmware readout protection. This is a form of content protection which aims at securing intellectual property (IP) as well as cryptographic keys and algorithms from an adversary. One series of microcontrollers are the STM32 which have recently gained popularity and thus are increasingly under attack. However, no practical experience and information on the resilience of STM32 microcontrollers is publicly available. The paper presents the first investigation of the STM32 security concept, especially targeting the STM32F0 sub-series. Starting with a conceptual analysis, we discover three weaknesses and develop them to vulnerabilities by demonstrating corresponding Proofs-of-Concept. At first, we discover that a common security configuration provides low protection which can be exploited using our Cold-boot Stepping approach to extract critical data or even readout-protected firmware. Secondly, we reveal a design weakness in the security

configuration storage which allows an attacker to downgrade the level of firmware protection, thereby enabling additional attacks. Thirdly, we discover and analyze a hardware flaw in the debug interface, attributed to a race condition, that allows us to directly extract readprotected firmware using an iterative approach. Each attack requires only low-priced equipment, thereby increasing the impact of each weakness and resulting in a severe threat altogether.

DOWNLOAD

DOWNLOAD

DOWNLOAD

Download

DOWNLOAD

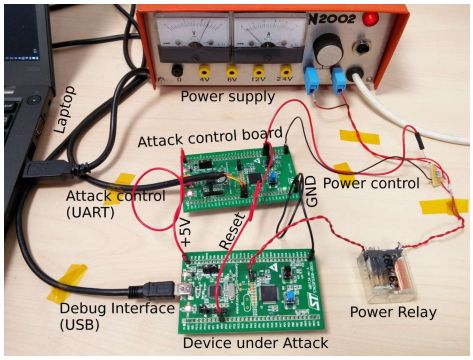
Download

DOWNLOAD

Download

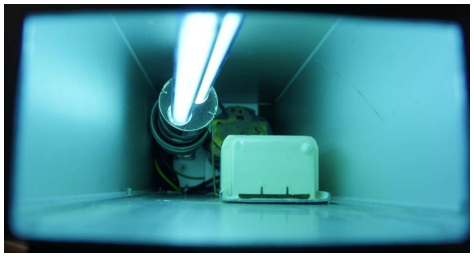
DOWNLOAD

Laboratory setup for Cold Boot Stepping



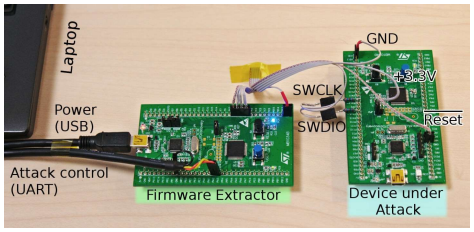
By observing changes in SRAM, one can reverse-engineer the basic control flow, find out the usage of specific addresses and may also discover briefly visible secret data. The system is only allowed to run for a precisely controlled duration and is then stopped. The contents of the SRAM is read out and a snapshot is created. With well chosen and increasing runtime duration this is similar to stepping through the firmware, since only a few instructions are executed between each SRAM snapshot.

UV-C irradiation setup for Security Downgrade



The STM32 Readout Protection Level protection mechanism is based on the RDP and nRDP bytes in the option byte memory region. At the power-on event, the option bytes are loaded from flash memory and the corresponding RDP Level is set. We show by experiment, that a flaw in the implementation evolves to a practical threat. The option byte memory region can be modified specifically by UV-C light performing optical fault injection.

Setup for firmware extraction out of a device using RDP Level 1



The STM32F0 series microcontrollers use the Serial Wire Debug interface for debugging and flash programming. When a debugger becomes attached to this interface in Readout Protection Level 1, the flash protection logic cuts access to flash memory. Due to a race condition in the implementation not only a single access can be performed, but the whole firmware can be extracted from a microcontroller.

Contact

Stefan Tatschner
Security Researcher

Fraunhofer AISEC
Lichtenbergstraße 11
85748 Garching b. München

stefan.tatschner@aisec.fraunhofer.de