Attacking Microcontrollers

Author: Dionisio Perez-Mavrogenis (dpm3g10)
Supervisor: Klaus-Peter Zauner (kpz)
Schoold of Electronics and Computer Science, University of Southampton

Microcontroller Introduction

Microcontrollers can be found anywhere, from your cars stereo to missile launch panels and are usually cheap (around £2) and packed with information! They often come with crypto-engines (AES, DES and RSA are common) and hold all sorts of information like private crypto-keys for authentication or propietary algorithm implementations in the firmware or hardware, interesting all sorts of people into the contents of a microcontroller.

insert cool graphic here

Packaging and De-packaging

Typically microcontrollers are too small and fragile to use as they are fabricated (with fabrication lengths shrank to micrometers) and so they are packaged[2]. Packacking material ranges depending on the microcontroller and its intended use, but is usually hard epoxy resin [1] [2]. The packaging tries to protect the microcontroller from its external environment (humidity, radiation, temperature, crashes etc.) and also from prying eyes. Military-grade chips come with a lot of additional circuitry on the packaging whose responsibility is to detect tampering and respond in a suitable manner (even self destruction!) [2].

De-packaging is not always requierd and the methods depend on the packaging used and protective mechanisms in place, but on epoxy-packaged chips one can etch the epoxy away by using HNO_3 or H_2SO_4 and then cleaning the chip in an ultrasonic bath [1] [2]. For other packaging types, e.g. metal ceramic or plastic, one can use similar techniques a... e.g. drills or a blowtorch [2].

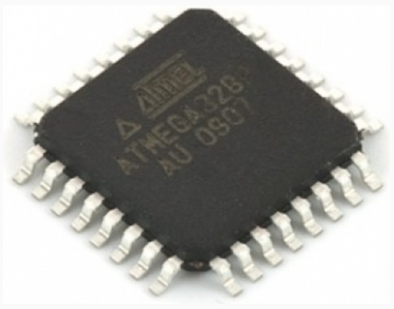

Fig. 1: ATmega328 with epoxy resin packaging.

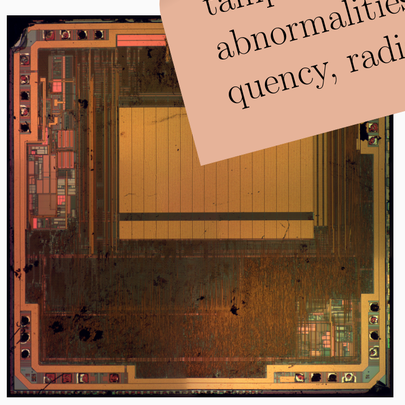

Fig. 2: The exposed die of an ATmega328.

tampering detection means detecting abnormalities in voltage, clock frequency, radiation, tilting etc.

Attack Types

Non-Invasive attacks require no depackaging and are cheap to implement. Popular methods in this category are power analysis and fault injection, where faults may be injected by excessively heating the chip, underclocking or overclocking, using a lot more or a lot less voltage the the chip supports and more. Although these attacks are conceptually easy and do not require expensive hardware to perform, they are tricky to defend from. **Semi-invasive and Invasive** attacks require decapsulation and are a lot more technical, expensive (to perform and repliate) and time consuming with manufacturer-equivalent machinery used.

Sample Attack

provide atmega644 characteristics. set attack scenario, type, setup and exact details

Evaluation

Shit be broken, yo.

qwgfwg

qgwwg

Very sexy, this is.

References

[1] Sergei P. Skorobogatov. Semi-invasive attacks – A new approach to hardware security analysis. Technical Report UCAM-CL-TR-630, University of Cambridge, Computer Laboratory, April 2005.

[2] Bulent Yener and Andrew Zonenberg. CSCI 4,74 / 6974 : Hardware Reverse Engineering. Rensselaer Polytechnic Institute, lecture slides at : `http://security.cs.rpi.edu/courses/hwre-spring2014/`, 2014.