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. Mictrocontrollers are the CPU of a small embedded system and are usually cheap (around £2) and widely available for hobbyists to play or companies to use in their products.

As microcontrollers are used in serious applicationsas well, 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 destroy itself!).

depackaging ways, acids and stuff

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.