P0131 - Electrically conductive adhesives, thermally conductive adhesives and UV adhesives in data extraction forensics

Thibaut Heckmann, Thomas Souvignet, David Naccache

EAFS 2018
8TH EUROPEAN ACADEMY OF FORENSIC SCIENCE CONFERENCE
LYON CONVENTION CENTER - FRANCE
2020 THE FORENSIC ODYSSEY
AUGUST 27TH-31ST 2018

Electrically Conductive Adhesives, Thermally Conductive Adhesives and UV Adhesives in Data Extraction Forensics

Dr Thibaut, Heckmann, IRCGN, PONTOISE, FRANCE
Dr Thomas, Souvignet, IRCGN, PONTOISE, FRANCE
Prof David, Naccache, ENS, PARIS, FRANCE

EAFS 2018
8TH EUROPEAN ACADEMY OF FORENSIC SCIENCE CONFERENCE
LYON CONVENTION CENTER - FRANCE
2020 THE FORENSIC ODYSSEY
AUGUST 27th-31st 2018

Electrically Conductive Adhesives, Thermally Conductive Adhesives and UV Adhesives in Data Extraction Forensics

Dr Thibaut Heckmann[1,2] – Dr Thomas Souvignet[1] and Prof David Naccache[2]
Data Extraction Unit, Forensic Sciences Institute of the French Gendarmerie (IRCGN), PONTOISE[1]
Information Security Group, Ecole Normale Supérieure (ENS), PARIS[2]

Objectives

- Ball Grid Array (BGA) man in the middle platform intends to provide advanced access to all exchanges in real time beetween CPU, memory and crypto components [1]
- Understand or modify the implemented security mechanisms inside secure mobile devices.

Introduction

From a **forensic point of view**, securing embedded systems must be bypassed in order to extract data : proof in court, understanding the disaster (air crash, terrorism) and also ethical challenges (mourning of the victims' families).

With the new secure mobile devices (BlackBerry, iPhone, etc.) it is often necessary for investigators to observe **the CPU-memory's real-time communication** and perform numerous tests on the memory (e.g. by changing some bytes) to **understand or modify the implemented security mechanisms** (manipulate system time, locate password hashes, observe artefacts of implemented security algorithms, etc.).

Important Result

- Man In the Middle Platform on all BGA Components
- Reverse Engineering of Secure Mobile Devices

Main Idea

It is not possible to observe communication bewteen CPU, memory, crypto chips because **signal is transmitted by the internal layers of the Printed Circuit Board (PCB).** Then signals are transmitted through balls located between the component and the board (inaccessible by the investigators). Then the bonding wires are used to make the junction between the BGA balls and silicon die. We decided **to observe/modify protocols directly on the BGA beads** (Fig.1)

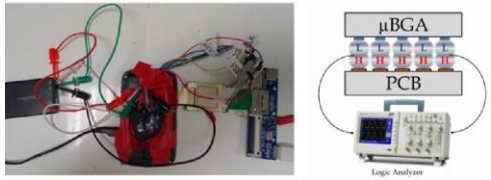

Figure 1: Man In the Middle (MIM) prototype

We observe/modify by reading/writting the memory via the SD protocols of the internal controller of the eMMC (Fig.2).

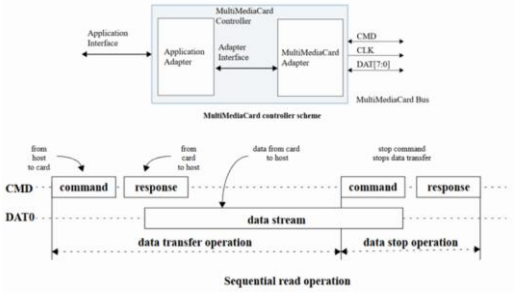

Figure 2: eMMC writting protocol

Methods

- Reballing high temperature (250°C) of the PCB
- Attaching cupper wires (section 30 microns) inside ball we want to observe the signal
- Fixing wires with UV glue and TCA (Fig. 3). The goal here is to prevent the wires from interfering

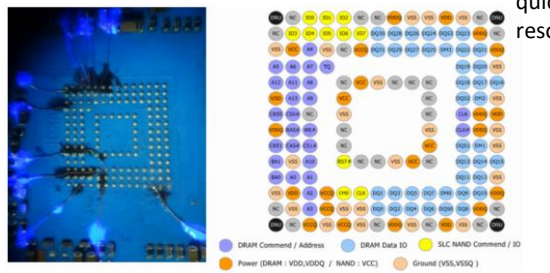

Figure 3: Fixing wires : TCA and UVA

- Reballing low temperature (138°C) the BGA component using technique developed in [2]
- Resoldering using BGA station in low temperature (138°c).

Results

We can understand or modify the implemented security mechanisms inside secure mobile devices (Fig.4).

Figure 4: Reading operation under forensic bridge

Conclusion

This platform developped during this work allows the forensic investigator to realise many tests very quickly without having, each time, to solder and resolder the memory/crypto chips.

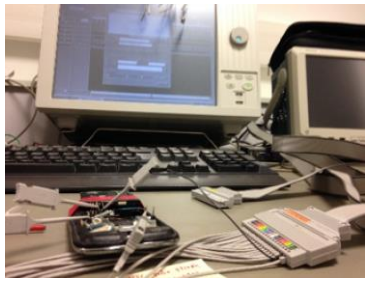

Figure 5: racking signals using a logic analyzer or an FPGA

The techniques using adhesives can enable us to observe/modify the exchange of information between the controller, the memory and crypto chips in real time using FPGA or logic analyser (Fig. 5).

Materials

- Low-temperature Sn42/Bn58 alloy,
- Rewoking technique developed in [2]
- BGA Station
- High-temperature solder ball Sn63/Pb37
- Thermally Conductive Adhesive (TCA)
- Electrically Conductive Adhesives (ECA)
- UV Adhesives (UVA)
- Logical Analyser and FPGA

Contact Information

- **Web:** https://www.gendarmerie.interieur.gouv.fr/ircgn
- **Email:** thibaut.heckmann@gendarmerie.interieur.gouv.fr
- **Phone:** +33 (6)7088 1019

References

[1] Th. Heckmann, Th. Souvignet, and D. Naccache. Electrically conductive adhesives, thermally conductive adhesives and uv adhesives in data extraction forensics. Digital Investigation , 21:53 – 64, 2017.
[2] Th. Heckmann, Th. Souvignet, and D. Naccache. Low-temperature low-cost 58 bismuth/42 tin alloy forensic chip re-balling and re-soldering. Digital Investigation, 19:60 – 68, 2016.