Hardware Reverse-engineering: Extracting a Bill of Materials (BOM) from an Embedded System

Tauhidur Rahman, Florida International University

Full points: 100 (see rubric)

Introduction: Reverse engineering (RE) is the process of extracting information related to a design or its functionality. It usually involves various structural and functional analyses of target hardware or its design. RE can be used to perform verification of intellectual property (IP) infringement and detection of malicious circuits and security-critical components in IP and integrated circuit (IC).

The process of RE varies significantly depending on the target abstraction and end goal. For instance, Trojan detection in IC may require decapsulation of the IC, followed by deprocessing of the exposed die to extract the layout of each layer. Conversely, RE of gate-level design is a non-invasive process that extracts a high-level representation of the underlying functionality (e.g., state transition graph) \cite{meade2016gate}. RE of the PCB is commonly observed in practice and usually performed for cloning a system or identifying vulnerabilities in it. RE effort can be automated by applying image processing techniques on high-resolution images of each PCB layer and constructing the layout, schematic, and bill of materials from that. RE of simple two-layer PCB can be done manually by visual inspection and probing the traces and pins on the board with a digital multimeter in continuity test mode. If the probes are placed in two areas of the same trace, it will cause an audible response (beep).

Objectives: You are tasked with extracting a comprehensive Bill of Materials (BOM) for an embedded system*, which is a handheld electronic device used for monitoring environmental data. The device is no longer in production, and there is a need to understand its components for maintenance and potential upgrades.

Task for Students:

- **Device Inspection:** Begin by inspecting the external and internal components of the embedded system:
    - Examine the device's external casing and identify any labels, markings, or serial numbers that may provide clues about the components used.
    - Open the device carefully and document all internal components, including microcontrollers, sensors, connectors, and any custom or off-the-shelf modules.
- **Component Identification:** For each internal component, identify its make and model. In cases where the components have obscured or missing markings, provide educated guesses based on your observations and any available documentation.

- **Microcontroller Analysis:** Focus on the microcontroller or main processing unit:
    - Identify the type and model of the microcontroller.
    - Describe its key features and specifications.
    - If possible, determine the programming interface (e.g., JTAG, SWD) for the microcontroller.
- **Sensor and Module Inventory:** Create a detailed inventory of all sensors, modules, and peripheral components present in the embedded system:
    - Specify the purpose and functionality of each component (e.g., temperature sensor, GPS module).
    - Identify any communication protocols (e.g., I2C, SPI) used by these components.
- **Power Supply and Connectivity:** Document the power supply components and connectivity options of the device:
    - Identify the voltage regulators, batteries, or power sources used.
    - Describe the types of connectors (e.g., USB, Ethernet) and their functions.
- **Additional Components:** If there are any custom or proprietary components in the system, describe them to the best of your ability.
- **BOM Compilation:** Compile all the information you've gathered into a structured Bill of Materials (BOM) document. The BOM should include:
    - Component names.
    - Make and model numbers.
    - Quantities used.
    - Description of component functions.
    - Any relevant notes or observations.
- **Challenges and Assumptions:** Discuss any challenges you encountered during the BOM extraction process, such as missing markings or components that are difficult to identify. Explain any assumptions you have to make and justify them.
- **Documentation:** Summarize your findings in a clear and organized BOM report suitable for maintenance and future development purposes.

*We will provide several unused embedded systems to the students.