Experiment 6 Documentation

Bill of Materials(BOM)

A screenshot of a computer

Description automatically generated

A diagram of a microcontroller

Description automatically generated

Schematic of the board

a. Given the BoM and the schematic you created from just looking at the board, can you recreate this board?

- With a complete and accurate Bill of Materials (BoM) and a schematic derived from the board, it is technically possible to recreate the PCB. However, there are challenges, especially with multi-layer PCBs where not all connections are visible. Also, some components may have proprietary firmware or configuration that's not apparent from visual inspection.

b. How would you go about recreating this board?

1. Use the BoM and schematic to create a PCB layout using CAD software.

2. Source the components listed in the BoM.

3. Manufacture the PCB using a PCB fabrication service.

4. Assemble the PCB by soldering the components onto it, either manually or through a PCB assembly service.

5. Program and configure any microcontrollers, FPGAs, or other programmable devices using the correct firmware or design files.

6. Test the newly created board to ensure it functions as intended.

c. What implications does the recreation of this board or other devices entail in the electronics supply chain?

- Recreating boards can lead to counterfeit products entering the market, undermining the intellectual property rights of the original manufacturers. It can also lead to quality control issues, as counterfeit products may not meet the same standards as the original. This can damage a brand's reputation and potentially lead to safety risks if the counterfeit electronics fail.

d. What else can an attacker do with this kind of information?

- An attacker with the BoM and schematic could:

1. Produce counterfeit boards for illicit sale.

2. Analyze the design for vulnerabilities to exploit in the original product.

3. Reverse-engineer proprietary technology for competitive analysis or for creating derivative works without consent.

e. How do you prevent an attacker from performing this visual inspection RE attack?

- To prevent such attacks, companies can:

1. Use security measures such as potting compounds to obscure the PCB.

2. Employ proprietary or custom components that are hard to source.

3. Implement trace routing within inner layers of multi-layer PCBs to prevent easy tracing.

4. Utilize secure boot mechanisms and encryption to protect intellectual property.

5. Control and monitor the distribution of schematics and design files.

f. Besides visual inspection, what are other RE attack techniques (not just on PCB), and why are they dangerous?

- X-Ray Imaging: Used to see through layers on a multi-layer PCB, revealing hidden traces and components.

- Decapsulation of ICs: Physically opening up chips to reveal the die for analysis, potentially allowing for cloning or reverse-engineering of proprietary circuit designs.

- Side-channel Analysis: Exploiting information gained from the physical implementation of a system, such as timing information, power consumption, electromagnetic leaks, etc.

- Firmware Dumping: Extracting code from memory components to analyze the software and algorithms used.

These techniques are dangerous as they can be used to uncover trade secrets, create counterfeit products, or find vulnerabilities that can be exploited in attacks such as IP theft, creating backdoors, or circumventing security measures.