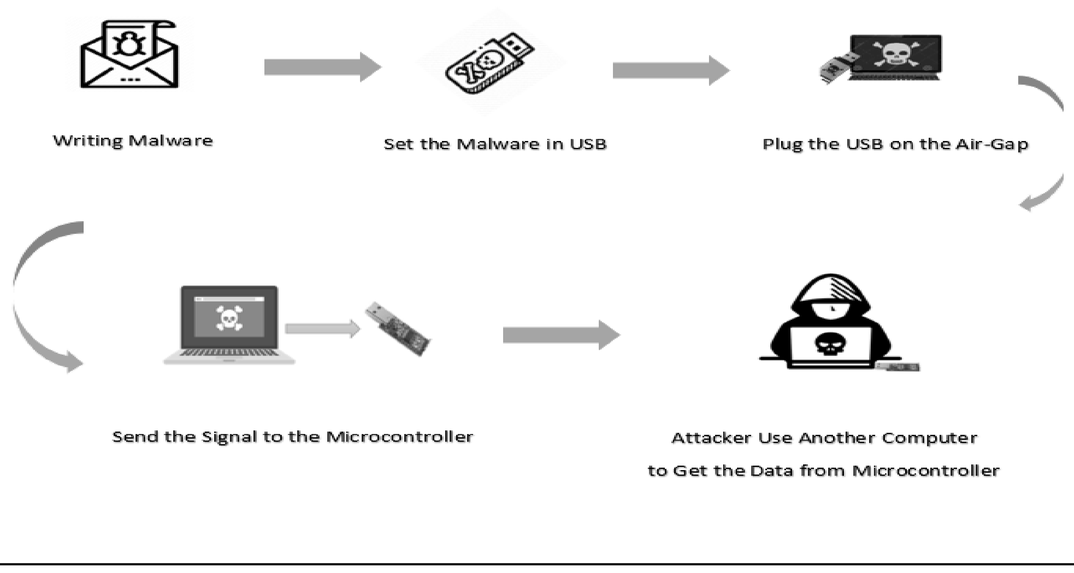
## Overview

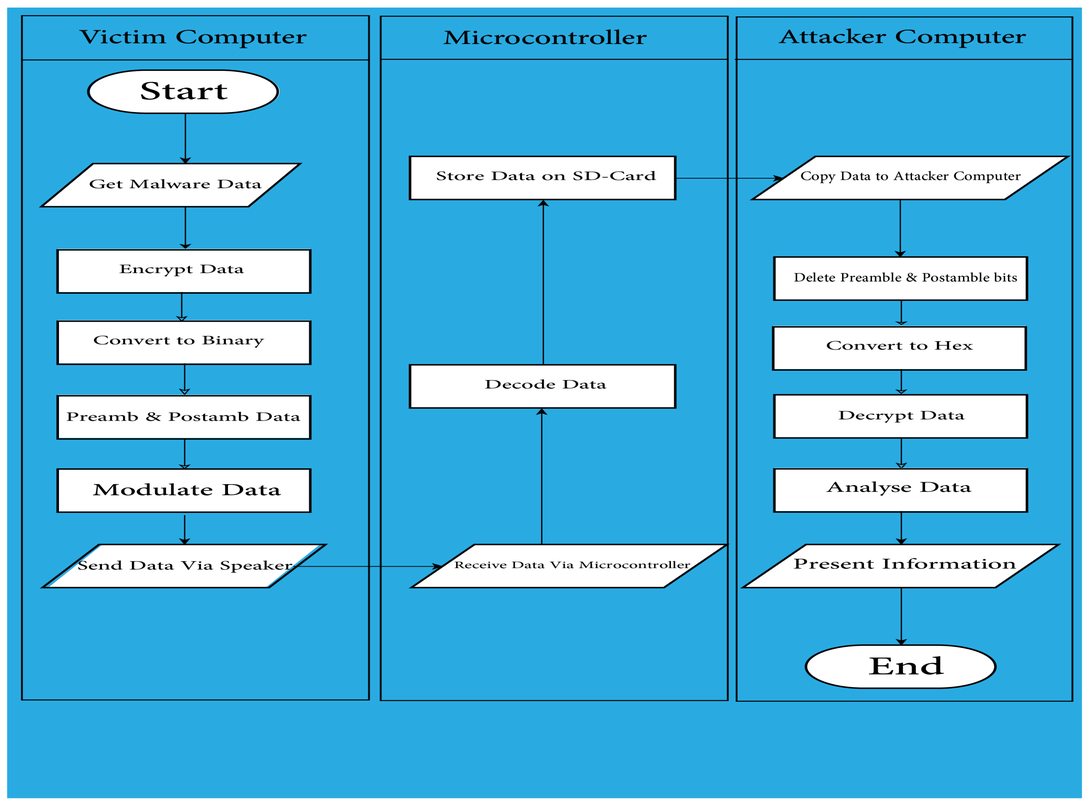
Air gapping means physically isolating a machine from all networks to ensure no information exchange between computers. This is done for security purposes.
In 2010 the Irani nuclear power plant, Natanz, was attacked by the Stuxnet computer malware. Stuxnet was suspected to have been introduced to the target environment through infected USB flash drives. The attack used a covert channel that spied on the power plant's activity and controlled the plant's centrifuges.
Air-gapped devices are thought to be impenetrable. This project will attempt to prove that such attacks are possible, by using a sound covert channels to successfully retrieve information from the victim's machine. Potential covert channels include: microphones, speakers, fan speed, LEDs and component temperatures.

## Objective

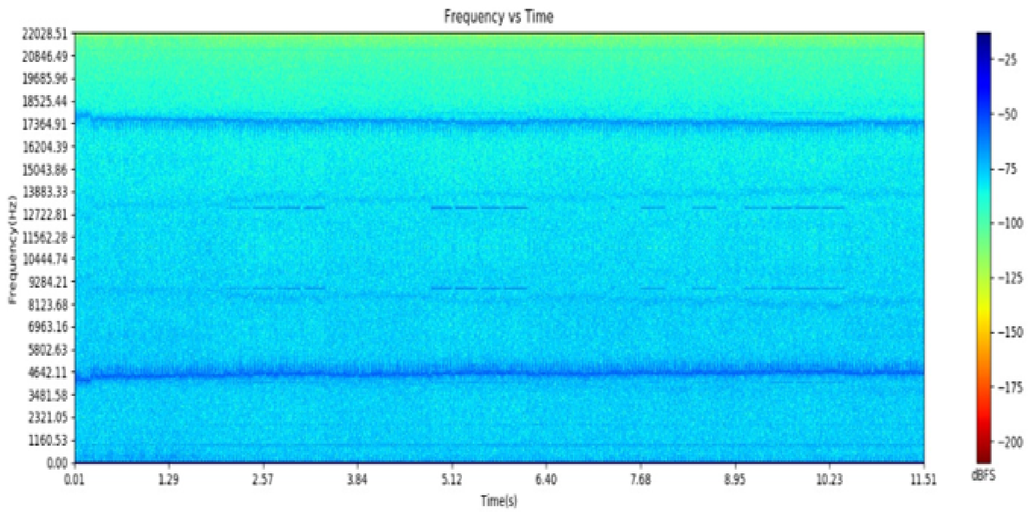
- Demonstrate the transfer of data, using an ultrsound covert channel.
- Optimize the utilization of this covert channel to attack air-gapped computers.
- Spread general awareness about cyber security of air-gapped computers.
- Provide suitable security recommendations based on the research findings.



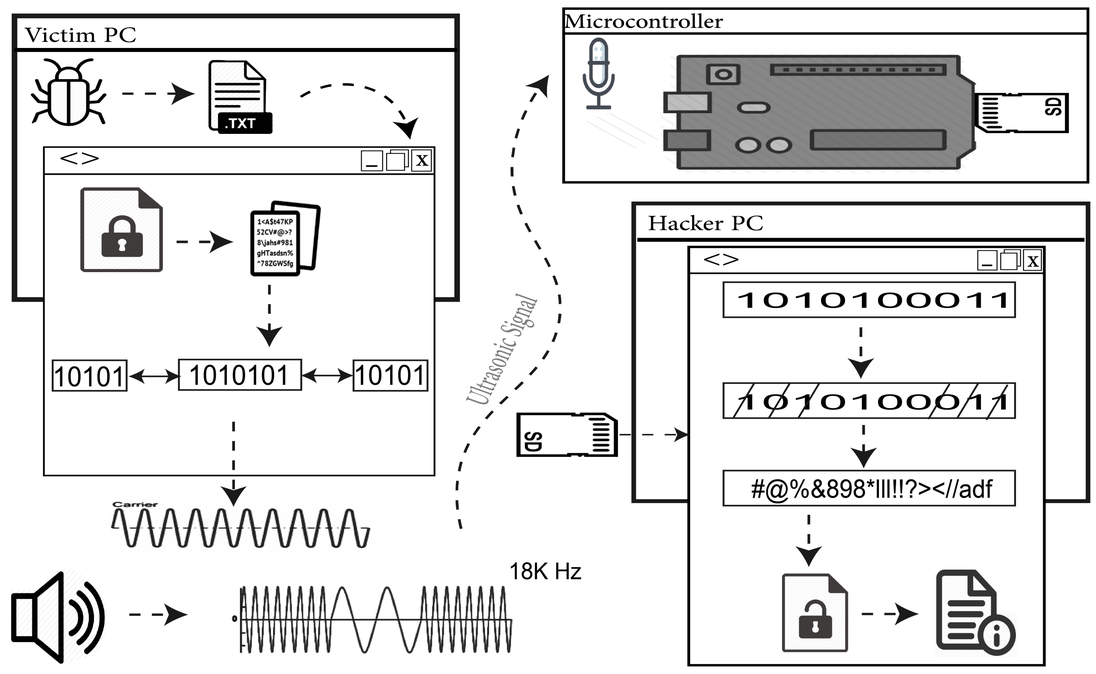

## System Work-Flow



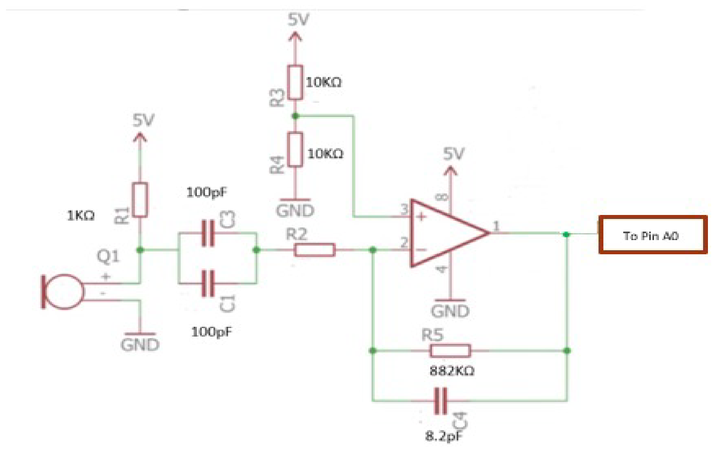

## Frequency vs. Time

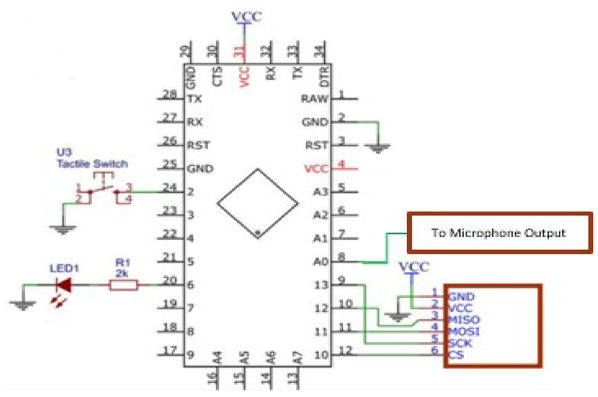


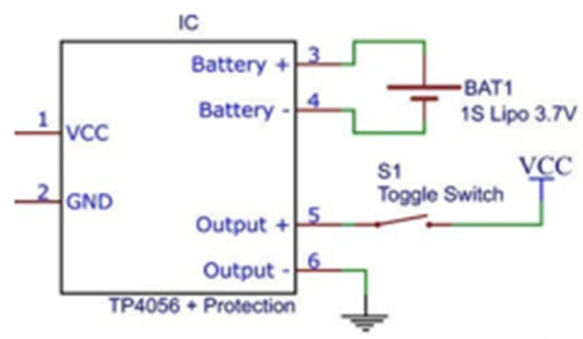

## High Level Archtecture




## Connection Diagram




This work is supported in part by grant No.UREP 25-049-2-019 from the Qatar National Research Fund.