Project 6. Electromagnetic Side Channel for Data Transfer

Motivation

Our team is interested in embedded systems that are related to SDR communication and security. So we decided to choose this project.

“In modern cyber-physical systems, cache and memory accesses by the CPU result in emission of electromagnetic radiation [1].”

By modulating the electromagnetic signals generated by the DRAM clock using only the memory accesses which is a covert channel. There are two sides of the EM covert channel. On the positive side, it can be used as a fast and reliable communication channel even when the main communication channel has been compromised. On the other side, it also can be a security leak where the signals could be decoded from hundreds of meters away without notice.

Design Goals

Develop a covert side channel for data-transfer between the desktop computers by modulating data using memory accesses.

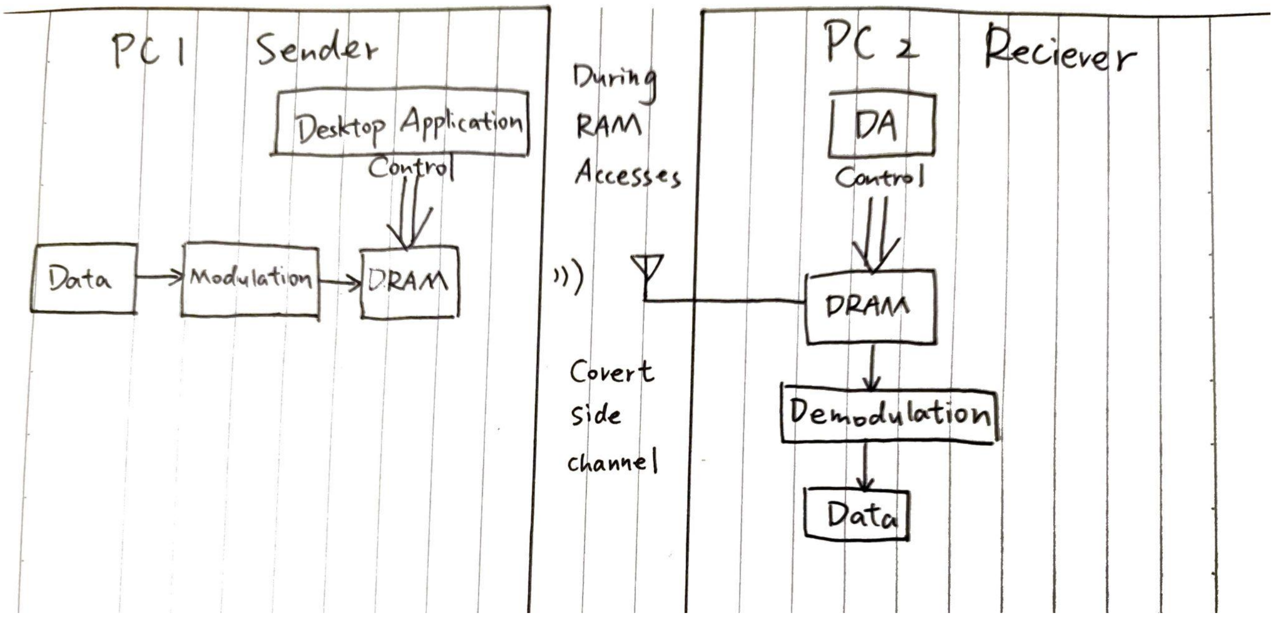
Deliverables

Successfully write a desktop application that uses DRAM accesses to modulate data over EM radiations emitted during RAM accesses.

Perform demonstration of receiving EM radiations emitted by DRAM accesses on another Desktop using SDR and perform demodulation.

Present experimental results to demonstrate a working communication channel between the two PCs.

System Blocks



Software Requirement

Python for desktop application, Matlab for Modulation.

Hardware Requirement

Two PCs (one sender, another receiver), a Software defined radio platform, a Digital Storage Oscilloscope, and a Waveform Generator.

Team Members Responsibilities

Mingrun Zhang: perform SDR implementation and help with writing the desktop application.

Nengxing Shen: perform the signal modulation and demodulation and help with writing the desktop application.

Yaozhong Zhang: write and complete the desktop application and help with performing the signal modulation and demodulation。

Each of the members should help each other with all the processes. Everyone should have the knowledge of how to perform the entire process of this EM side channel data transfer and everyone should participate in the final demonstration and research report..

Project Timeline

Study the materials and references of SDR, set up and implement the SDR device, and knowledge about DSP focusing on modulation and demodulation by Oct 12th.

Design the technological details of covert side channel for data-transfer and operate simulation by software by Oct 26th.

Write and implement the desktop application by Nov 10th.

Implement the channel on SDR and operate experiments to verify the designed method by Nov 24th.

Adjustment week: Nov 25th- Nov 31st. Start to assemble the final research paper.

Final demonstration on Dec 7th. Prepare for slides and presentation until Dec 7th.

Finish project report and research paper by Dec 16th.

References

[1] F. Anwar, ECE 597SD. Class Lecture, Topic:” Projects List “ School of Electrical and Computer Engineering, University of Massachusetts Amherst, Amherst, MA, Sept. 27, 2021.

[2] Z. Zhan, Z.Zhang, X. Koutsoukos. “BitJabber: The World’s Fastest Electromagnetic Covert Channel”.

[3] C. Shen, T. Liu, J. Huang, R. Tan. “When LoRa Meets EMR: Electromagnetic Covert Channels Can Be Super Resilient.”