I. Introduction

Hard drives on computers and servers function by controlling a hard drive head that functions to read and store the data on the circular disks, or platters. This hard drive head is controlled by an actuator motor, which includes a permanent magnet. The actuator also includes a coil made from wire that interacts with the magnet when current is passed to produce the force needed to rotate and move the head to the desired position on the disk. This activity produces faint yet measurable magnetic fields that can be exposed via magnetic measurement tools found on many devices such as Arduino sensors, phones, and some smart watches. Although the disks and read/write heads of these hard drives are protected by the hard drive cover and the cover of the machine such as a computer or server, these readings are still perceptible outside of the hard drive. And since the magnetic fields emitted from the hard drive is correlated to the activity happening on the hard drive, whether it be a data read or write, or the boot up sequence of an operating system, this is a way for outside parties to launch side-channel attacks on hard drives.

A side-channel attack, which in this case is more specifically categorized as a non-invasive electromagnetic attack, is a method of gleaning information about a system that does not utilize force or holes in the logic of the implementations but a method that gathers other extraneous information emitted by the system to launch an attack. In addition to inspecting the emitted magnetic fields, scrutinizing the power levels used by the system or the sounds emitted by the keystrokes on a keyboard are also examples of methods of initiating side-channel attacks. With the information gained from the emitted magnetic fields one can determine patterns that come out from tests and distinguish between various hard drive functions. These functions include writing data to the disk (with variations from the size of the data written), reading data from the disk (with variations from both the size of the data being read and the sector from which the data is found), booting up the operating system (which may differ between different operating systems), and many more. Learning how the granularity of these kinds of attacks and what kinds of information malicious attackers can glean from magnetic side-channel attacks can tell us much about how to better protect and maintain the safety our data.

II. Background & Previous Work

Magnetic side-channel attacks have been studied in devices such as CMOS chips and smart cards but hard drive attacks have not yet been thoroughly explored. Last year, I explored another option for magnetic side-channel attacks by using Arduino magnetic field sensors to measure the emitted magnetic fields. In this set up, the Arduino sensors were placed on top of the hard drive, locked into place over the read/write head in a 3D printed hard drive cover, (which ensured that the sensors were in the exact same position for each test), to take
measurements of the fields. In this project, we collected and graphed the results of the data for data write, data read, and OS boot-ups. Some patterns emerged from these tests but the high variation in the resulting patterns and graphs, seemed to show that the Arduino sensors were not as accurate and precise as they needed to be in order to create a reliable data map of the magnetic field levels for the various activities.

Graduate students in Professor Szefer’s lab have also done work in this area, with a project the explored the efficacy of a smart phone magnetometer’s, or digital compass, ability to accurately record the changes in the magnetic fields to produce clear patterns. This approach proved to be more precise and gave clearer patterns for the various activities on the drive. It focused on starting various operating systems, virtual machine activity, server network traffic, and file caching.

III. Project Overview

This project is built upon my last project with the Arduino sensors however, this project will utilize the Android wearable platform to measure and record the emitted magnetic fields. The Android wearable device chosen is the Sony SmartWatch 3 SWR50, which has a magnetometer, or a digital compass. With the ability to detect magnetic fields, this watch can be placed on top of the hard drive, as before with the Arduino sensors, to collect the data. The setup of the project requires the communication between three parts: the Android watch, the server/hard drive that will be measured, and a computer for overall control of the system.

An application will be written for the Android watch that will access the magnetometer in the watch to measure the magnetic fields emitted from the hard drive, display those readings on the screen of the app, and also save the readings into a text file on the watch. This file will then be transferred via server communication to the computer to be processed by a Matlab data processing program, explained later in this proposal. The position of the watch on top of the hard drive will need to be considered and tested as small shifts in the position of the watch will greatly affect the readings of the magnetic fields emitted. Tests will also be done to determine the most effective orientation for the watch. The watch can be laid flat against the top of the hard drive or it may even be more realistic to have it at an angle, similar to that formed by a person wearing the watch and placing his or her wrist on the hard drive.

On the server/hard drive side, various activities must be identified and tested. The activities that we plan to explore include data writes (with various sizes of data), data reads (with readings from various sectors of the disk), and operating system boot-ups (testing both the Windows and Linux operating systems). The variations in these tests will be used to help determine the granularity of this side-channel attack: whether the size of the data creates a differentiable field pattern, whether the sector of the data read affects the pattern, and whether the difference in field patterns emitted by different operating systems as they are booted-up can be exploited to identify the specific operating system being run. By running tests on these activities and variations on these activities, we can determine a pattern for the emitted magnetic fields and establish the efficacy of gleaning the specific hard drive activity from the field patterns emitted.
The computer mediator between these two devices will create a central control center for the watch and hard drive. A TCP server system will be set up to establish communication between the computer and the watch and separately between the computer and test server containing the hard drive for various purposes. One of these purposes is to synchronize and automate the start of the hard drive activity and the start of the data recording on the Android watch. The server work will be done via a python server script and a Matlab script that will trigger both the app to begin recording and the hard drive to begin the process of writing, reading, or booting-up accordingly. The recording time of the app will also be determined by this script as the runtime of different processes differs and the recording time must differ accordingly. The Matlab script will also implement a method to automatically receive the data files from the Android watch that contain the recorded magnetic field readings. Then, these data files will be automatically aggregated and plotted on graphs to allow for better pattern determination between the various hard drive activities. With these graphed patterns for the write, read, and boot-ups, we can attempt to differentiate the highlight the differences between the various activities.

In addition, using the data collected from both the previous Android sensor project, and the Android phone project, we can compare the data with that collected from the Android watch and see if there are overlaps and similar patterns that can be deciphered. Finding similar patterns would help signal the effectiveness and accuracy of the watch method for launching these kinds of side-channel attacks.

IV. Deliverables

- Android watch set up
  - Application that is triggered by Matlab script that measures, displays, stores file of magnetic readings, and sends these files via server connection back to the computer
  - Physical placement and orientation layout for the watch on the hard drive that gives the most accurate and precise magnetic field data
- Control code
  - Matlab code
    - Simultaneously triggers the start of recording in the Android watch app and the start of the hard drive activity
    - Automate a loop test so that multiple courses and data files are generated at the start of each run
    - Receive data files from the app and automatically aggregate and graph data (to show patterns in field level changes)
  - Python server code
    - Establish TCP server communication between the control code and the server/hard drive to allow the control code to send messages to the hard drive and trigger specific activity on the hard drive
- Data Analysis
  - Determine the best graphing method to find patterns in the emitted fields (factors to consider include the angle of the watch and the watch position on the hard drive)
  - Determine the overlap and compatibility between data collected from Arduino sensor and Android phone tests and the Android watch data, which will help determine the efficacy of using Android watches to launch side-channel attacks