**FYP Project Plan**

**Done By:** Ng Shi Kai

**Brief**

The purpose of this report is to provide a plan for the Final Year Project (FYP). The report would include the aims of the FYP and phases in which the FYP would be conducted.

**Aims**

This FYP aims to help identify non-Day-0 vulnerabilities in current proprietary software distributed by technology firms such as Microsoft and Apple.

**Introduction**

With the introduction of open source libraries, developers are finding it easier to develop software by utilising such open source libraries to avoid recoding existing functionalities. Popular open source libraries include the Linux OS and OpenSSL for data encryption. Technology firms have been known to utilize such open source libraries to develop proprietary software. However, such utilization of open source libraries also leaves these proprietary software vulnerable if left unpatched.

The FYP would identify such vulnerabilities by attempting to identify the open source libraries being used in each proprietary software. Once identified, we would then identify the version of the open source library used. If the version of the library is not the latest, we would then review the GitHub commits for known bugs and vulnerabilities present that were unpatched in that version. These bugs and vulnerabilities would thus then be identified to be present in the proprietary software.

**Project Plan**

Open source libraries would be identified in proprietary software by examining the binaries of the proprietary software. Strings and comments in the software would be identified and matched with known unique strings and comments of the specific version of the open source libraries. In that manner, the version of open source library used in the software would also be made known to us.

The FYP would be conducted over phases:

* Phase 1 would include extraction of strings and comments from current version of an open source library.
* Phase 2 would then increase the scope of data extraction by automating the git functions to obtain all released versions of a library across all known open source libraries.
* Phase 3 would then commence once the database of strings and comments of libraries is setup. In Phase 3, we would analyse the data and try to identify unique strings and comments that would verify the exact version of an open source library.
* Phase 4 would then commence once data analyse is done on the libraries. Phase 4 would include analysing of proprietary software to identify strings and comments before attempting to match them with the unique strings and comments in our built database.

Once all 4 phases are completed, the FYP can be said to be completed too.