# CySec-Game

DESIGN DOCUMENT V1

**sdmay21-50**

**Client**: Manimaran Govindarasu

**Team Members**: Harrison Majerus,

Nicholas Battani, Hayden Sellars,

Jonathan Greazel, Joseph Strobel, Stefan Peng

https://sdmay21-50.sd.ece.iastate.edu/

10/04/2020

# Executive Summary

## Development Standards & Practices Used

- Agile development
- CVSS
- NVD

## Summary of Requirements

- The software shall be remotely accessible through a web application
- The software shall run use-cases of risk assessment scenarios using PowerCyber test bed
- The software shall be integrated with existing testbed and simulation tools
- The software shall utilize Game Theory algorithms for risk assessment of cyber physical systems like the smart grid and provide best strategies to mitigate the risk.
- The software's UI design shall encourage ease of use and work to minimize clicks per action
- Different environments (Windows, Linux, etc.) shall have no effect on software usability
- The software shall cost no more than $0
- A working proof of concept and completed documentation shall be delivered by the end of Spring 2021 semester
- Any sensitive user information shall be stored in a safe and secure manner
- All work shall be original for our development team with credit given to proper sources

## Applicable Courses from Iowa State University Curriculum

- Com S 228
- Com S 309
- Com S 319
- CPRE 530
- SE 329
- SE 339

## New Skills/Knowledge acquired that was not taught in courses

- Game theory
- Cybersecurity for critical infrastructure
- Network modeling

# Table of Contents

## List of figures/tables/symbols/definitions (This should be the similar to the project plan)

# 1 Introduction

## 1.1 Acknowledgement

We would like to thank our project advisor/client Dr. Manimaran Govindarasu and graduate students Burhan Hyder and Kush Khanna for assisting us in our understanding and design of this project.

## 1.2 Problem and Project Statement

Critical infrastructure like power and energy systems are often vulnerable to cyber attacks. Mitigating cyber risk to critical infrastructure is an important part of the design and maintenance of these systems. These power and energy systems commonly use legacy devices where complete upgrades are uneconomical, therefore, risk assessment plays an important role in selectively securing vulnerable or high-risk assets.

The goal of this project is to develop a software tool that helps the critical infrastructure industry to assess cyber risks to power and energy systems and to optimally allocate cybersecurity investments to mitigate the risks. This tool will use game theory models to identify high-risk targets and will directly interface with the PowerCyber testbed for cyber-physical risk assessment and mitigation.

## 1.3 Operational Environment

The operational environment for this product will be dependent on the user. The end user is targeted to be a system administrator who is responsible for network security. The operational environment will involve the user accessing a front-facing user interface and then using that user interface to run network security analysis on their network. There will be a back end that contains a game theory model as well as an optimization engine. They will be able to use this tool to optimize their cyber security investments. This tool will need to be able to work on all modern operating systems (Windows, macOS, Linux) and be easily accessible over the internet.

## 1.4 Requirements

**Functional Requirements**

- The software shall be remotely accessible through a web application
- The software shall run use-cases of risk assessment scenarios using PowerCyber test bed
- The software shall be integrated with existing testbed and simulation tools
- The software shall utilize Game Theory algorithms for risk assessment of cyber physical systems like the smart grid and provide best strategies to mitigate the risk.
- The software's UI design shall encourage ease of use and work to minimize clicks per action

**Non-Functional Requirements**

- Different environments (Windows, Linux, etc.) shall have no effect on software usability
- The software shall cost no more than $0
- A working proof of concept and completed documentation shall be delivered by the end of Spring 2021 semester
- Any sensitive user information shall be stored in a safe and secure manner

- All work shall be original for our development team with credit given to proper sources

## 1.5 Intended Users and Uses

**Users and Uses**

- Cyber Security Analyst - This tool will be used by a member of a company who analyzes risk of cyber attacks and what kinds of damage attackers can do to infrastructures (ie. Electrical Power Grids, advanced manufacturing environments, etc.)
- Cybersecurity Investment scenarios will also be produced by the tool

## 1.6 Assumptions and Limitations

**Assumptions**

- Cyber vulnerability assessment for the possible cyber-attacks targets must be done offline by the user before submitting.
- User input will be in the form of .csv and selection of nodes later on.
- Algorithms will be provided by client and Graduate students.
- Server infrastructure will be provided by Iowa State University.
- The tool will be available via a web application.

**Limitations**

- Game Theory knowledge of the team is minimal.
- There will be no financial resources provided to the team.
- Project will be developed entirely remotely.

## 1.7 Expected End Product and Deliverables

User interface (3/19/2021)

- The user interface (UI) shall be in the form of a web application that can be accessed from any desktop web browser. Users will be able to enter parameters for attackers, defenders, and the network model. These parameters can be either created from scratch or edited from presets. The UI shall display the assessment results to the user.

Backend (4/1/2021)

- The backend will receive parameters and models from the UI and will analyze the given parameters and models using optimization algorithms. It shall support the existing cyber security simulation tool and shall utilize one or more game theory algorithms. The backend will send the results of the analysis back to the UI.

# 2. Project Plan

## 2.1 Task Decomposition

**User Interface**

- Network model
  - View network model
  - Create network model
  - Edit network model, possibly from presets
- Attack and defense parameters
  - View parameters
  - Create parameters
  - Edit parameters, possibly from presets
- API
  - Send data to backend
    - Data from CSV file with model and/or parameter data
  - Receive data from backend
  - Display data from backend
  - Standard user and admin user login

**Backend**

- API
  - Receive data from UI
    - Imported data from CSV file
  - Send data to UI
  - Integrate with simulator tool
  - Authorize user logins
- Optimization
  - Select appropriate optimization algorithm(s)
  - Implement optimization algorithm(s)
  - Analyze model and parameters using optimization algorithm
- Database
  - Construct required tables to store model and parameter data
  - Create required queries to load model and parameter data

See Section 2.4 for details on dependencies and timelines.

## 2.2 Risks And Risk Management/Mitigation

- Requirements change while development is already underway .............................................. 2
  - A team meeting will be conducted to debate the best path forward. Considerations will be made in attempt to save already completed work and avoid backtracking
  - New requirements must be assessed for clarity and conflicts with our time budget

- Project deliverables aren't complete upon due date ................................................................. 8

    - Must be avoided since delaying the due date isn't an option. The team will work diligently to meet intermittent deadlines, ensuring our work is completed on time.
    - The team hopes to be well out of development and into testing by this time, so if a time constraint is met testing will face cuts rather than development

- User data is stolen and used to execute a cyber attack .......................................................... 10
    - We plan to store sensitive data separately and in a safe manner in order to mitigate this risk
    - In the case of a data breach we must first assess what was stolen, alert those who may be compromised, and patch the exploited vulnerability in a timely manner

- The software's predictions are flawed/insufficient to prevent attacks .................................. 6
    - Our application is meant to serve as a proof of concept, so further improvements may be made by other teams
    - The software will include data recording features to assess its failures/successes so our team may catch shortcomings quickly and act fast

- Lack of team communication ......................................................................................... 8
    - This could result in any number of problems and must be avoided at all costs
    - Team members are actively engaged in channels of discourse such as Discord, Git, and semi-weekly meetings to mitigate this risk

## 2.3 Project Proposed Milestones

- Oct 4th - Design Document v1 including chapter 1 and preliminary chapter 2.
- Oct 25th - Design Document v2 including chapters 1, 2 and preliminary chapter 3.
- Nov 15th - Final Design Document including chapters 1, 2, 3, 4, 5 and 6.
- Feb 5th - UI Design and UML Diagram complete.
- Feb 19th – Rough implementation of frontend and backend with simple requests between each side.
- Mar 5th - Testable backend game theory algorithm, front end can handle basic user input in the form of csv.
- Mar 19th - Frontend sends diagram to server's game theory algorithm, backend can communicate with simulator and respond with data in JSON format.
- April 2nd - Optimization of UI and better/more in-depth analysis of diagram and vulnerabilities. This includes full implementation of an algorithm provided by the client.
- April 16th - Full functionality: Frontend can receive diagrams and send them to the server via an API for analysis. Backend will run algorithms and in turn respond to the frontend with analysis.

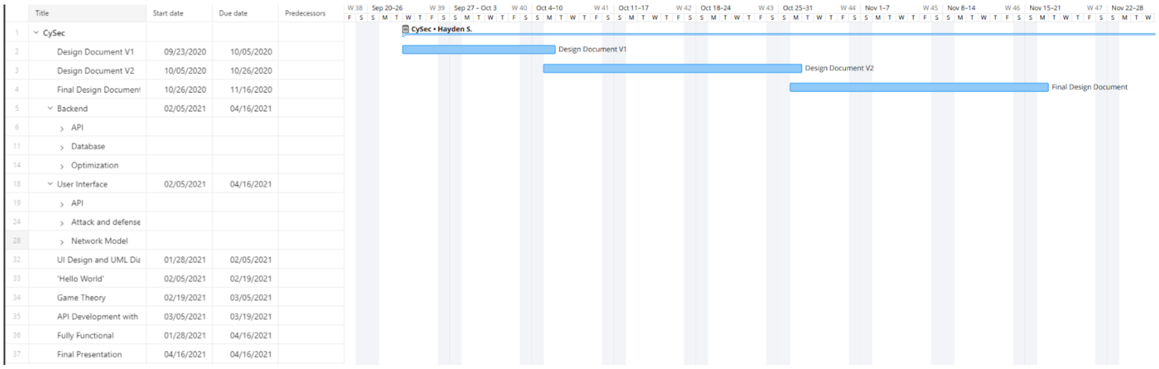
- April 23rd - Presentation and visual displays regarding progress and/or completion of the project.

## 2.4 Project Timeline/Schedule

As mentioned above in the ‘Project Proposed Milestones’ the dates and planned objectives are scheduled into a Gantt chart, as documented here:

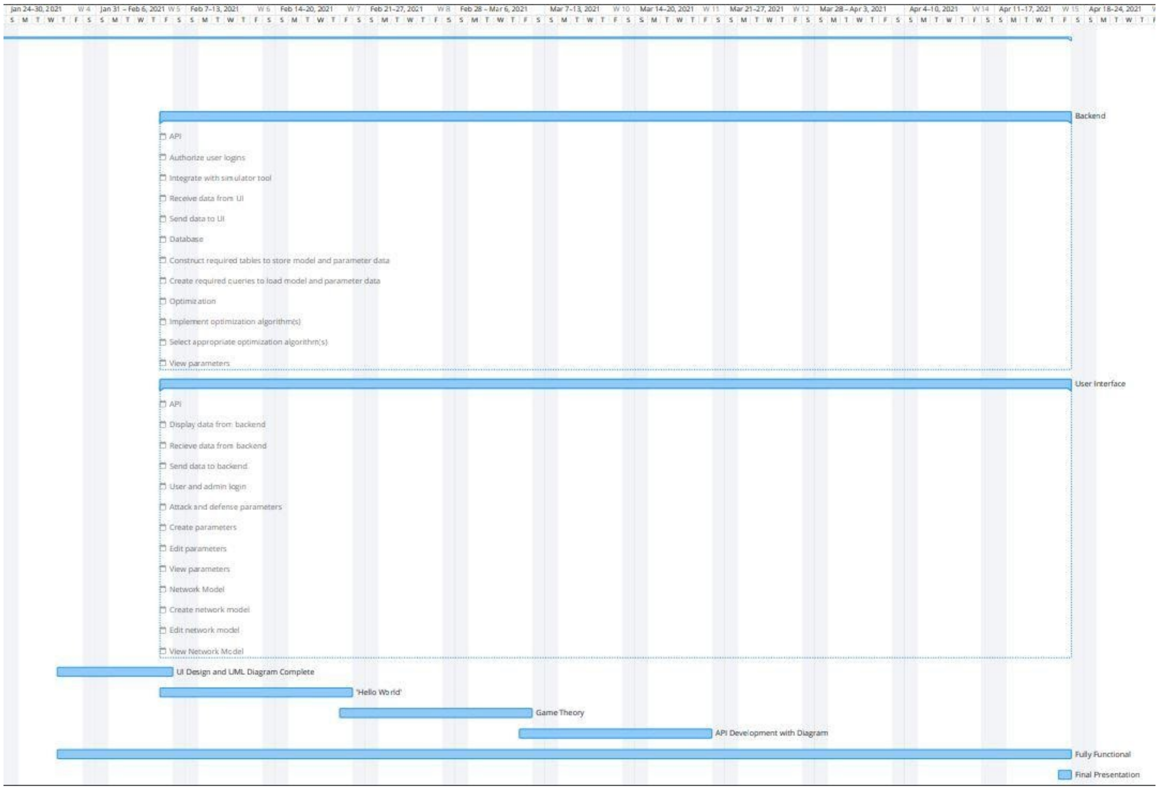
https://www.wrike.com/workspace.htm?acc=4089522#path=folder&id=573735000&c=timeline3&vid=8633423&a=4089522&so=10&bso=10&sd=0&st=space-573734921

This URL link will take the team to see the progress of our project throughout the 2 semester period of Senior Design.



| | Title | Start date | Due date | Predecessors |
|---|---|---|---|---|
| 1 | ⌄ CySec | | | |
| 2 | Design Document V1 | 09/23/2020 | 10/05/2020 | |
| 3 | Design Document V2 | 10/05/2020 | 10/26/2020 | |
| 4 | Final Design Documen | 10/26/2020 | 11/16/2020 | |
| 5 | ⌄ Backend | 02/05/2021 | 04/16/2021 | |
| 6 | › API | | | |
| 11 | › Database | | | |
| 14 | › Optimization | | | |
| 18 | ⌄ User Interface | 02/05/2021 | 04/16/2021 | |
| 19 | › API | | | |
| 24 | › Attack and defense | | | |
| 28 | › Network Model | | | |
| 32 | UI Design and UML Dia | 01/28/2021 | 02/05/2021 | |
| 33 | 'Hello World' | 02/05/2021 | 02/19/2021 | |
| 34 | Game Theory | 02/19/2021 | 03/05/2021 | |
| 35 | API Development with | 03/05/2021 | 03/19/2021 | |
| 36 | Fully Functional | 01/28/2021 | 04/16/2021 | |
| 37 | Final Presentation | 04/16/2021 | 04/16/2021 | |

*Above Figure 2.4.1 shows Gantt Chart for months August - November*



*Above Figure 2.4.2 shows Gantt Chart for months January - April*

## 2.5 Project Tracking Procedures

Our group will be using GitLab to track and manage our project. Within GitLab we will be using Issue Boards to create cards and track tasks that are being worked on and that need to be worked on. For non-technical communication we will be using a Discord server created specifically for our group. For all task specific communication, we will be writing our information within cards, commits, merge requests, and milestones within GitLab. All other technical information or designs will be within our shared folder on Google Drive.

## 2.6 Personnel Effort Requirements

| Task | Hours |
|---|---|
| Design Doc V1 | 10 |
| Design Doc V2 | 10 |
| Final Design Doc | 20 |
| UI Design | 20 |
| “Hello world” front end | 10 |

| | |
|---|---|
| Game theory algorithm | 30 |
| Integration | 50 |
| Optimization | 20 |

The tasks above are estimated based on the teams previous work experience. They are subject to adjustment as the team begins to meet checkpoints and begin tasks.

### 2.7 Other Resource Requirements

This project will require a server to host the service on. Our client and his research group will provide the server needed to host this service. This server will require a game theory model and a cyber optimization engine. The optimization engine will be obtained from our client.