

Agenda

1. Introductions
2. Review of your design from CPRE/EE/SE 491
3. Discussion of any changes or improvements to the design
4. Discussion of the objectives and requirements for CPRE/EE/SE 492
5. Discussion of the schedule and milestones for the project
6. Q&A session

Meeting Minutes

Notes on discussion:

1. We first discussed where we left off last semester. We have implemented the scraper and designed the inputs and outputs for components in the system.
2. Some progress was made between our last meeting in first semester and this meeting. This includes a foundation/initial draft of our frontend and performing rudimentary NER using spaCy.
3. Our previously annotated articles need to be migrated to being annotated with BRAT. Someone will need to complete this during this sprint so we may train our model.
4. We will look into weak supervised learning by gathering a list of companies and attack groups to supply to our NER model.
5. The functionality of our implementation of the scraper component needs to be validated.
6. We need to think further into our testing metrics and strategies for components and the system.
7. We discussed our schedule for this semester and decided that we'd have a better idea at our next bi-weekly meeting. We will complete our action items for this sprint and define the semester timeline at our next meeting. We also discussed milestones of the project. The main milestones are:
 - a. Rudimentary parser implementation using pretrained NER model, basic RE, and storing the results in the database
 - b. Producing our first trained NER model
 - c. Performing rudimentary RE
 - d. Frontend querying the database

Decisions made:

- We will supply the parser with a list of companies and a list of attack groups instead of training it from scratch.
- Use BRAT instead of previous online annotation tool.

Summary

- Project Title: Knowledge Graphs for Cybersecurity Reasoning
- Team members present:
 - Alice Cheatum

- Micah Gwin
- Nicklas Cahill
- Carter Kitelinger
- Brandon Richards
- Michael Watkins (*absent – work conflict*)
- Benjamin Blakely (*advisor / client*)
- Summary of the main points discussed
 - Last semester's design, progress made on implementation, and sharing work done over winter break.
 - Using BRAT as annotation tool instead of previous tool.
 - Training our own NER model / access to HPC cluster.
 - Existing implementation needs to be verified.
 - Testing metrics and strategies need to be revisited.
 - Project timetable and milestones.
- List of any decisions made
 - Supply parser with list of companies and list of attack groups.
 - Use BRAT instead of previous online annotation tool.
- List of any actions to be taken
 - Brandon – Convert old annotations to BRAT format
 - Brandon/Micah – Validate scraper/MongoDB functionality
 - Brandon/Carter – Find list of companies / list of attack groups
 - All – Review test plan, consider testing metrics and strategies
 - All – Consider timetable for this semester
- Next steps for the project
 - Functioning parser using cybersecurity-domain NER and RE.
 - Inserting parsed entities and relationships into knowledge graph (Neo4J database).
 - Querying database from frontend.