Project title: Enhancing Social Media Governance with Policing Bots

Team Members:
- Liam Dumbell ldumbell2021@my.fit.edu
- João Gabriel Silva jsilva2021@my.fit.edu
- Cody Manning cmanning2020@my.fit.edu

Advisor and Client:
- Khaled Slhoub kslhoub@fit.edu
- Affiliation: Florida Institute of Technology

Date(s) of Meeting(s) with the Client for developing this Plan:
- First Meeting - September 1, 2023.
- Future meeting frequency - Bi-Weekly or once every 10 days

Goal and motivation:
We intend to do research on the social media website “X”, formerly known as “Twitter” and analyze “bot” accounts that are active on the website. Using our framework, our client would be able to detect bots of all kinds, but also be able to categorize them into different levels of maliciousness. This is useful because some bots people employ are not made for bad purposes. With our framework, only the one’s deemed negative to the end user's experience will be flagged for reporting (or deletion). Bots have become more and more prevalent on the internet lately, both beneficial and malicious. With the successful completion of our framework, people will be able to detect malicious bots more easily (e.g.: Scam bots or misinformation bots), while still being able to take advantage of the useful bots (e.g.: a bot used to download videos).

Approach:
Key Features:
- Detect Bots
    - Our first feature would allow the client to detect artificial users (bots) in a social media platform. Our first feature would revolutionize the way clients interact with social media platforms by equipping them with a tool designed to detect artificial users, commonly referred to as "bots." By analyzing an account's activity we will detect suspicious behavior that would indicate whether or not the account is run by a bot.
- Distinguish
    - Our second feature will be the ability to distinguish beneficial bots from malicious ones.
      We will need to have more discussions on the ‘ranking’ of the severity of the types of bots. A non-harmful bot is one that is determined to have no negative effects on the social media platform in which it is active. A harmful bot is one that is determined to have some form of negative effect on the social media platform it is active on. This can range from minor negative effects such as spam on a user’s post or profile, to majorly negative effects such as scam bots or bots that maliciously influence political opinions of the social media’s user base on a large scale. By assessing factors such as the bot's origin, its interaction patterns, and its

impact on user experience, we can categorize bots into two distinct classes: non-harmful and malicious.

- Decide
    - Our third feature will be deciding what to do with the account after determining that it is a bot and its level of maliciousness. If we find that the bot account is breaking the terms of service of the platform it is active on, we plan on determining the level of maliciousness, and then determining whether reporting the account to the platform administrators is necessary. If the rule broken is determined to be relatively harmless, the tool will flag the account to collect data from it to improve itself in the future.

Technical Challenges:

- None of the group members currently have any experience using virtual environments for Twitter or using the Twitter API so we will have to take the time to learn the environments in order to develop our proposed tools within them.

- Outside of simple applications in chat rooms like discord, none of the team members have much experience in creating bots, let alone detecting them. We will need to do a lot of research on common methods used in detecting bots, this will entail possibly developing simple bots of our own to understand the inner workings of them.

- None of the group members currently have experience with the libraries or other methods for developing bots for social media platforms which is something we'll have to spend time learning.

- This project will also involve learning a lot of HTML to properly understand and use the different social media APIs.

Milestones for First Semester:

- Milestone 1 (Oct 2):
    - Two technical tools we will be comparing and analyzing are the Tweepy Python library and the OAuth 2.0 Flask Application Approach. Our understanding at the moment is that Tweepy seems to be the more streamlined and simpler approach to creating and using bot accounts on Twitter and The Flask App approach requires a lot more setup but also gives you more control over how the bot stores information as it is directly connected to a database controlled by the user to handle access tokens.
    - Our demos will consist of creating a bot on Twitter that replies to a tweet thought to be posted by a bot account based on if the account has the word "bot" in its username. The bot will be able to read and write messages and have a simple bot detecting system. Two demos will be created using the Tweepy library and Flask App approach in Python separately.
    - Make progress on resolving Technical Challenge 1 by learning how to work with the Twitter API by creating simple bot accounts

    - Compare and select collaboration tools for software development, documents/presentations, communication, task calendar.
    - Create Requirement Document
    - Create Design Document
    - Create Test Plan

- Milestone 2 (Oct 30):
    - Implement, test, and demo the system used to compile data on accounts thought to be bots and store the data locally to be analyzed.
    - Resolve technical challenge 1 for the scope of our project.

- Milestone 3 (Nov 27):
    - Implement, test, and demo the tool to detect whether an account is run by a human or a bot.
    - Resolve technical challenge 2 for the scope of our project.

Task Matrix for Milestone 1:

Task	Liam	Gabriel	Cody
Compare and select Technical Tools	Social media API	Bot creation	Bot detection
"hello world" demos	Social media API	Bot functions	Bot detection
Resolve Technical Challenges	Learn how to create Twitter Bots using the Twitter API, learn relevant HTML	Learn how to create Twitter Bots and learn relevant HTML	Research various methodologies of common known methods of detecting bots, learn HTML, assist with both tools
Compare and select Collaboration Tools	documents/presentations	programs	communication, task calendar
Requirement Document	write 50%	write 25%	write 25%
Design Document	write 25%	write 50%	write 25%
Test Plan	write 25%	write 25%	write 50%

Approval from Faculty Advisor

“I have discussed with the team and approve this project plan, I will evaluate the progress and assign a grade for each of the three milestones.”

Signature_____Date_____