Police Bot
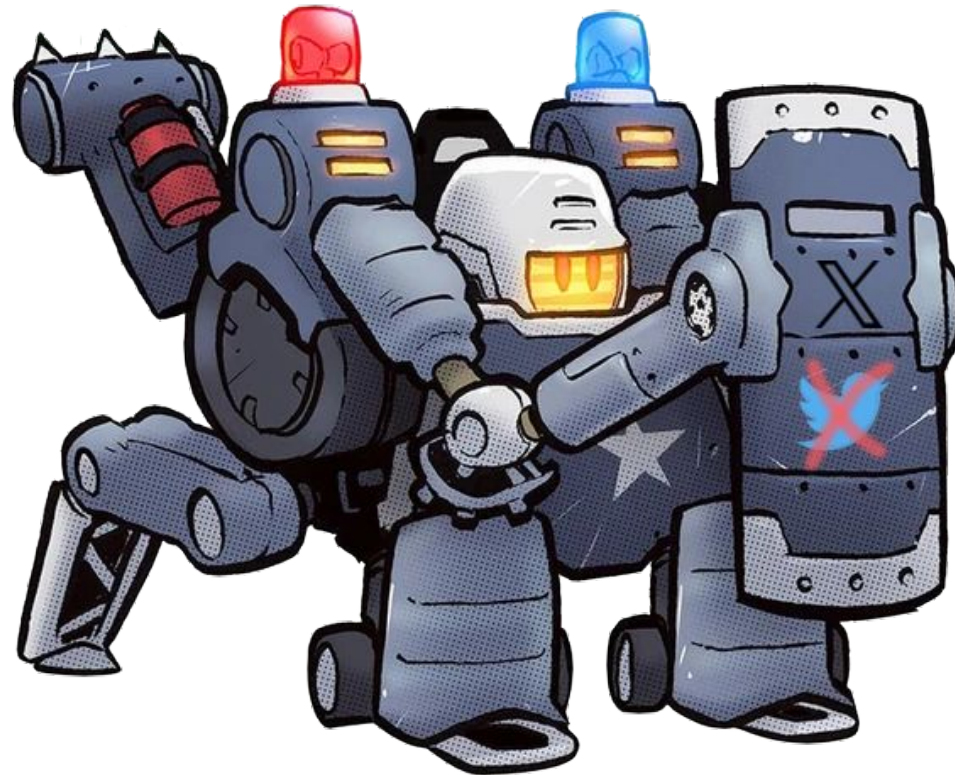
Enhancing Social Media Governance with Policing Bots

Group Members

- Students:
  - Liam Dumbell
  - Gabriel Silva
  - Cody Manning

- Faculty Advisor / Project Client:
  - Khaled Slhoub

- Computer Science Project Instructor:
  - Dr. Phillip Chan

Motivation and Goal

Motivation

- Social Media Sites have had a prolonged issue with malicious bot accounts
- There is a need for a tool that can easily distinguish a bot account from a human as well as a malicious bot from a beneficial one.

Goal

- Allow users to detect malicious bots more easily while still being able to take advantage of the useful bots.
- Categorize bots by different levels of maliciousness
- Properly report bots with a high level of maliciousness to the proper administrators

Key Features

The Three D's:

- Detect:
  - Allows users to detect artificial users (bots) on a social media platform.
- Distinguish:
  - Allows users to distinguish beneficial bots from malicious ones.
- Decide:
  - Allows users to determine the level of maliciousness of a bot account
  - Allows users to decide to report the account after determining that it is a bot and its level of maliciousness

Technical Challenges

Team members currently have:

- No experience using and working with X/Twitter Virtual Environments.

- Little experience using the Twitter API.

- Little experience working with bots and no experience creating and detecting them.

- No experience with the libraries or other methods for developing bots for social media platforms.

- Insufficient HTML experience for the scope of this project.

Milestone 1
Oct 2

- Compare and select technical tools
  - Tweepy Python library
  - OAuth 2.0 Flask Application Approach
- Create small demos to evaluate the tools
  - Create simple Twitter Bots for both Tweepy and Flask App approach
- Resolve technical challenges
  - Make progress on learning how to work with the Twitter API
  - Learn how to create simple Twitter Bots
- 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 a **system** to compile data on bot accounts and store the account data to be analyzed in the future.

► Learn the **Twitter API** well enough to start developing the rest of our features within the API

Milestone 3
Nov 27

- Decide on a better method of detecting bot accounts, by doing research on the topic and improving the algorithm.

- Implement, improve, test, and demo an **algorithm** to detect whether an account is a bot based on our chosen method.

- If possible, also have a basic subroutine to identify different threat levels of bots, and distinguish them by maliciousness.

This concludes our presentation, Thank You