build night 1

2022-02-07

ACM Research

- 10 build nights
- 6 teams
  - 4 participants: you
  - team lead: me
  - faculty advisor: Wei Yang
- Poster
- Presentation night
  - Low-stakes competition
  - We will win!!

about me

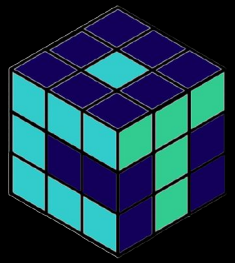
- freshman at UTD
- computer Science major
- did ACM Research last semester
- interests
  - mathematics
  - cybersecurity
  - internet privacy
  - free and open-source software
    - Join OpenUTD!
  - rollerblading
- https://roman.hn

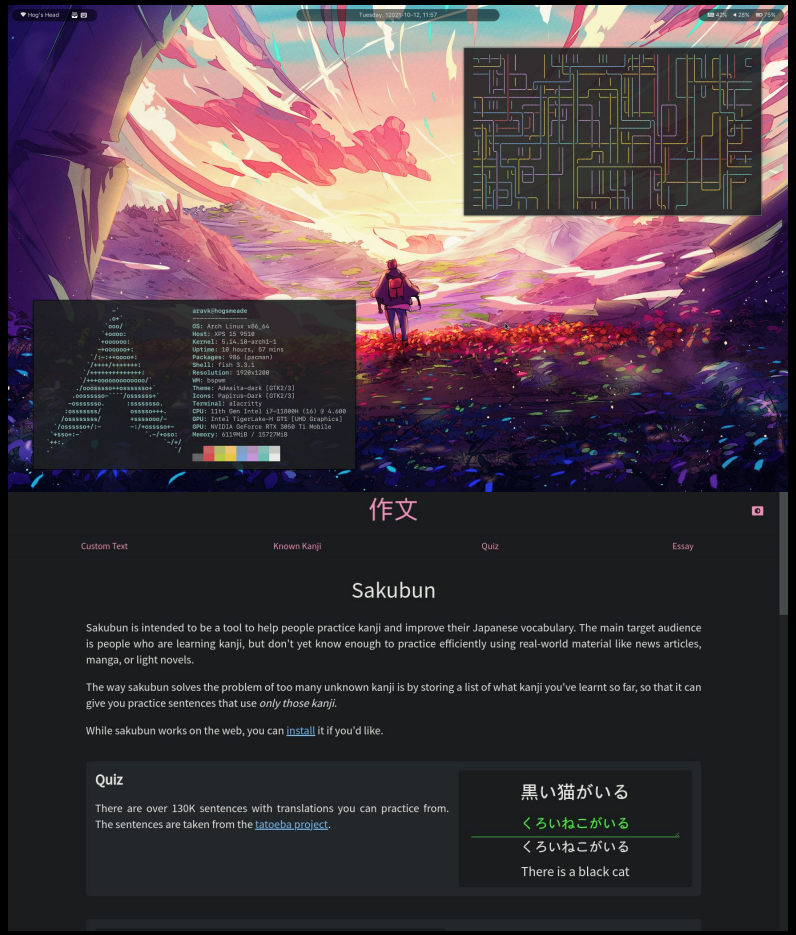
photo by Jacob Dong

about you

Aravindan Kasiraman

- FOSS enjoyer 
  - I love your Arch setup
- many cool projects
  - Japanese language learning website
  - Rubik's Cube website
  - I'm learning Rust rn and really like your Rust programs





Bradley Johnson

- full-stack development internship at Cadenhance
- team projects
  - spaced repetition app last semester in ACM Projects
  - stock price web app
  - image-based global game

Pranav Nair

- Pong game in assembly
- Roblox phone 😳
- flight path algorithm

Sisira Aarukapalli

- published cool paper about cybercrime
  - i haven't read it yet but i will!
  - warning: i will not let you leave without telling me all about this paper (it seems very interesting)

ISM 4A
Cyber Criminology

Dark Web: An Exploration of Communication in Black-Hat forums

Abstract
This paper explores how dark web members involved in criminal activity use forums are used to create new criminal servers on the dark web after old ones have been shut down. I conducted a study on a Tor-based dark web forum, during the shutdown of Utopia and Silk Road 2, two marketplaces known for drug-trafficking. My analysis suggests that distrust is all too common in the forum during the marketplace shutdowns. I analyzed debates filled with suspicious claims and conspiracies. The results suggest that a black-market crisis potentially offers an opportunity for cyber-intelligence to disrupt the dark web by engendering internal

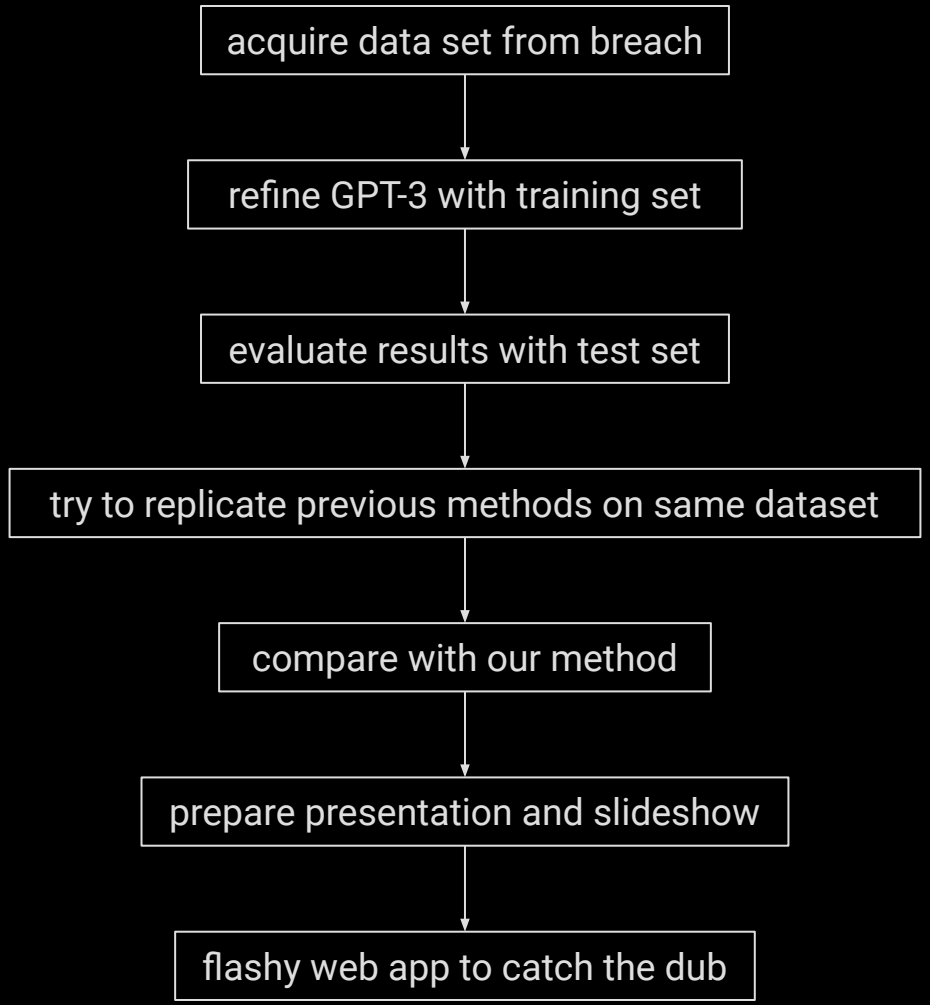
the project

project overview

- Hackers use password lists to crack password hashes
- Researchers have extended password dictionaries using various methods
  - Machine learning is the most effective method
- Targeted password guessing uses information about a victim to try to guess their password
- Researchers have used personal information about targets to extend password lists
  - full name, username, email address prefix, site name, birthday
- We will extend this research with a more generalized approach

project overview

- Researcher Victor Gevers apparently accessed Donald Trump's Twitter account with the password "maga2020!"
- This claim is disputed, but it demonstrates the kind of password guessing attack that previous research would not be able to simulate
    - This sort of targeted password guess could be based off of Trump's Tweets, rather than his personal information
- For example, our model should be able to pick up someone's interests or perhaps pick out their pet's name, which would be factored into generating password guesses


acquire data set from breach
refine GPT-3 with training set
evaluate results with test set
try to replicate previous methods on same dataset
compare with our method
prepare presentation and slideshow
flashy web app to catch the dub

GPT-3

- Generative Pre-trained Transformer 3
- Created by OpenAI
- On 2020 Sep 22, Microsoft announced exclusive use of GPT-3, with public API :(
- absurdly huge natural language model
  - trained on ~500 billion tokens
  - 175 billion parameters

administrivia

- Slack
  - I would never force you to download a proprietary app, but make sure you get message notifications
- GitHub
- GPT-3 API team

homework

- skim through past research
  i. Fast, Lean, and Accurate: Modeling Password Guessability Using Neural Networks
  ii. Targeted Online Password Guessing: An Underestimated Threat
  iii. PassGAN: A Deep Learning Approach for Password Guessing
- go through GPT-3 docs
  i. Each section under "GET STARTED"
  ii. "Fine-tuning" section