Thesis Project Portfolio

Securing Every Link: Expanding Cybersecurity Education to the General Public

(Technical Report)

Machines Making Art: How Can Artists Protect Their Art from Generative AI?

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Michelle Nguyen
Spring 2024
Department of Computer Science

Table of Contents

Executive Summary

As reliance on technology grows, cyberattacks become increasingly dangerous and costly. Although many technical measures can be put in place to prevent such attacks, human users themselves are often a major point of weakness. To address this, I propose that cybersecurity education be treated as an important facet of cyber defense by expanding it beyond schools and businesses to the public in various ways, with a focus on workshops helmed by qualified students. Workshops like these could be run by students under the supervision of a professor teaching the basics of personal cybersecurity. To determine the potential efficacy of such programs, I reviewed research on prior methods for teaching cybersecurity and similar computing-related subjects, such as public service announcements and games. I anticipate that a workshop program such as this could benefit both the attendees and the workshop students in that both would be honing their cybersecurity skills. In the future, this proposal could be properly tested by implementing it in a real-world setting, at UVa or at a community center.

Awareness of artificial intelligence (AI) products has exploded in recent years, with generative AI at the forefront. Among generative AI's most contentious forms is AI art, or images created via generative AI. I argue that AI art is a dangerous competitor to artists that infringes on their intellectual property and I investigate tools available to protect them. My research began with prior knowledge of AI art and expanded to include ethical concerns around algorithms, informational pages documenting anti-AI tools, and releases from the U.S. Copyright Office, among others.

I found that AI art inherits social issues from its machine learning background and additionally creates new problems. The unchecked nature of collecting training data for AI,

called ‘scraping,’ means that training data includes the works of artists who did not consent to their images being used, putting AI art under questionable copyright. Because of its lower cost, generative AI serves as a direct competitor to artists, who can be specifically targeted via user prompts in a process called style mimicry. I used an Actor Network Theory analysis to determine that the major deterrents to AI art becoming more widespread are technologies created by artists and their allies (defensive artistic technology) and legal protections. Popular defensive artistic technologies include Kudurru, the Spawning browser extension, and the ‘Do Not Train Registry,’ which protect artists’ works against being scraped; and Glaze and Nightshade, which filter training images to disrupt a generative AI’s processing. Regarding legal protections, most of a class action lawsuit against AI companies for copyright infringement was dismissed in a California federal court. However, copyright was denied to an image mostly generated via Midjourney. I conclude that, while these tools are better at protecting artists in some ways than others, they provide a promising start to hindering AI. As more tools and legislation are created, additional research must be done to assess the impact of AI on artists.

Computer science encompasses a diverse and ever-growing set of fields. As the global population increasingly relies on the internet and its associated technologies, awareness of these fields becomes more important. I address two of computer science’s most rapidly growing fields: cybersecurity and generative AI, which are both frequently discussed and reported on. Additionally, rather than focusing on specific specifications or implementations of either, I chose to discuss how both fields interact with the general public. Cyber threats and generative AI (such as LLMs or AI art generators), while being technologically impressive, both pose varying levels of danger to different audiences who may not be aware of the risks present. Education and outreach is an often overlooked area of research, and such information can be technical and

unapproachable for the average person. In analyzing the ways that these rapidly evolving technologies affect different areas of the public, I aim to describe how lay people can best interact with or be protected from new advancements in the fields that comprise computer science.