

Wednesday, March 8, 2023, 4:00 pm

COLLOQUIUM TALK

Speaker: Andrew Mertz (EIU)

Old Main 2231

Capturing Flags, More Fun, More Profit?¹

Abstract:

Cybersecurity is an important aspect of Computer Science. The number of systems having access to personal information, protected health information, intellectual property, and other sensitive data is only growing. The push for global connectivity, the rise of sophisticated attackers, and the increasing number of advanced persistent threats shows the need for software developers to understand cybersecurity and the need for more cybersecurity experts.

One way to get started in learning about cybersecurity issues is by participating in cybersecurity Capture the Flag (CTF) events. These are computer security competitions where participants compete to solve security themed challenges for points. Challenge categories often include web exploitation, cryptography, reverse engineering, forensics, and binary exploitation. There are events for all skill levels happening routinely. CTF time (<https://ctftime.org/>) is a website that tracks such events.

I competed in picoCTF 2022 (<https://picoctf.org>) as part of the zemotau team. We came in 32th place out of 7794 in the global rankings and had a great time with the challenges. This CTF has well thought out challenges for all skill levels (they start off easy and ramp up to challenges based on real world security flaws). It is a great CTF to start with and you do not have to wait as picoCTF 2023 starts on 3/14. So go get some flags!

This presentation will cover how to get started with CTFs and the basic tools that are needed. It will also highlight solutions to some of the picoCTF 2022 challenges, so you can see what goes into developing exploits. Once you have seen how a single simple coding error can lead to remote code execution (RCE) or data leaks, you will never look at your own code the same way.

¹well, still mostly just for fun