Title: *Redbot: an automated and distributed red team and traffic generation system*

Abstract:

*In 2018, Iowa State University (ISU) offers numerous courses focused on cybersecurity, many of which provide hands-on lab experience where students have the chance to test offensive and defensive tools in a safe environment. It can only be assumed that more courses will appear as student interest continues to rise, and the graduate and undergraduate programs in this field will continue to expand and develop. Additionally, the ISEAGE (Internet Scale Event and Attack Generation Environment) Lab at ISU holds 5 Cyber Defense Competitions (CDCs) each year, requiring students (the "Blue Teams") to set up and secure a virtual network from real-life professional hackers (the "Red Team"). Throughout this time, the network must remain usable to the users (the "Green Team") as they perform their day-to-day activities.*

*However, when targeted attacks by the Red Team cease and usability checks by the Green Team are not in progress, the environment is like a vacuum. Unlike the real internet, where automated attacks happen on a massive scale at almost every moment, these environments are very quiet, and students' systems are not subjected to a realistic cacophony of attack traffic. In this paper, Redbot attempts to fill the void by providing a platform to intelligently generate attacks and other traffic in order to simulate the noise of the internet.*