**Romania**
**University POLITEHNICA of Bucharest**
**Faculty of Automatic Control and Computers**
**Advanced Cybersecurity**

# Cyber Reasoning System

**Supervisor**
Adrian-Răzvan DEACONESCU

**Students**
Claudiu-Florentin GHENEA
George-Andrei IOSIF

**Bucharest**
**2022**

# Context

# Context



- Widespread use of executables

# Context



- Widespread use of executables
- Increase of vulnerabilities

# Context



- Widespread use of executables
- Increase of vulnerabilities
- Approaches

# Context



- Widespread use of executables
- Increase of vulnerabilities
- Approaches
  - Manual

# Context



- Widespread use of executables
- Increase of vulnerabilities
- Approaches
  - Manual
  - Automated

# Cyber Reasoning Systems

# Cyber Reasoning Systems

- Automated vulnerability detection, exploitation and patching

# Cyber Reasoning Systems

- Automated vulnerability detection, exploitation and patching
- Developed solutions

# Cyber Reasoning Systems



- Automated vulnerability detection, exploitation and patching
- Developed solutions
  - DARPA's Cyber Grand Challenge

# Cyber Reasoning Systems

- Automated vulnerability detection, exploitation and patching
- Developed solutions
  - DARPA's Cyber Grand Challenge
    - Mayhem

# Cyber Reasoning Systems

- Automated vulnerability detection, exploitation and patching
- Developed solutions
  - DARPA's Cyber Grand Challenge
    - Mayhem
  - HaCRS

# Motivation

# Motivation

- Not applicable on common operating systems

# Motivation

- Not applicable on common operating systems
- No longer maintained

# Motivation

- Not applicable on common operating systems
- No longer maintained
- Commercial

# Motivation

- Not applicable on common operating systems
- No longer maintained
- Commercial

# Objectives

# Objectives



- Study of the proposed CRSs

# Objectives



- Study of the proposed CRSs
- Creation of a functional and open-source prototype

# Objectives



- Study of the proposed CRSs
- Creation of a functional and open-source prototype
- Initial limitation for x86 ELF executables

# Objectives

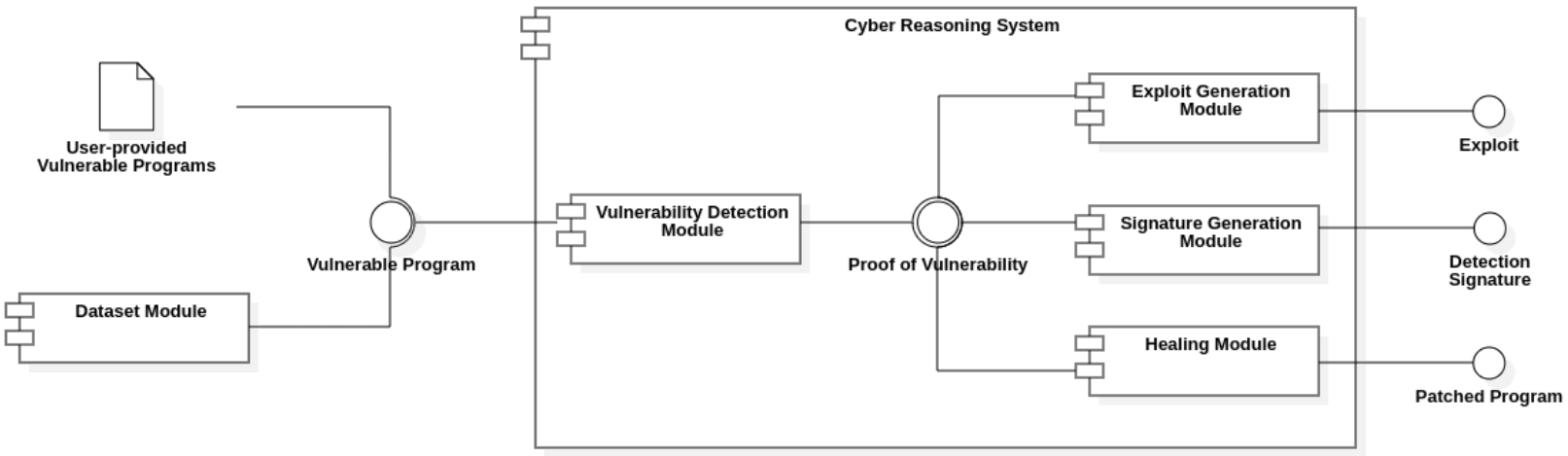


- Study of the proposed CRSs
- Creation of a functional and open-source prototype
- Initial limitation for x86 ELF executables

# Bird's Eye View Architecture

# Bird's Eye View Architecture





# Current Status

# Current Status



- Researching the field of CRS

# Current Status

- Researching the field of CRS
- Proposal of an architecture

# Current Status



- Researching the field of CRS
- Proposal of an architecture
- Started implementation in Python 3

# Current Status

- Researching the field of CRS
- Proposal of an architecture
- Started implementation in Python 3
  - Dataset

# Current Status



- Researching the field of CRS
- Proposal of an architecture
- Started implementation in Python 3
  - Dataset
  - Attack surface approximation

# Further Development

# Further Development



- SotA for the proposed technologies

# Further Development



- SotA for the proposed technologies
- Completion of the vulnerability detection module

# Conclusions

# Conclusions



- Automated approach for binary analysis

# Conclusions



- Automated approach for binary analysis
- Novelty of CRS

# Conclusions



- Automated approach for binary analysis
- Novelty of CRS *(but with the presented downsides)*

# Conclusions



- Automated approach for binary analysis
- Novelty of CRS *(but with the presented downsides)*
- Proposed CRS study and prototype