Cybersecurity at Kudu Dynamics

2023 May 1 | Montana State University

Matt (drone) Revelle
drone@kududyn.com

Kudu Dynamics

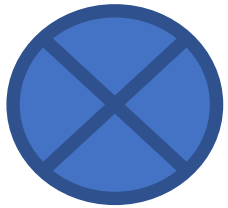
- Founded in 2015 by a small group of hackers
- First task was running the DARPA Cyber Grand Challenge event
  - The first fully autonomous cyberwar held in front of an audience of 4,000 at the 2016 DEF CON conference
- There are now over 130 Kudites and 4 offices
- Work in different areas, including:
  - Program analysis
  - Reverse engineering (RE) and vulnerability research (VR) of hardware and software
  - Machine learning

KUDU DYNAMICS

Finding and Proving Vulnerabilities

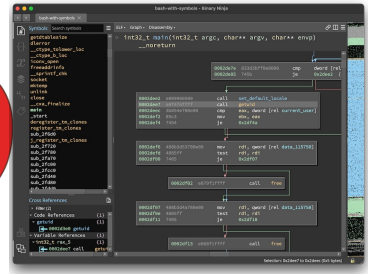
Vulnerable Hardware and Software

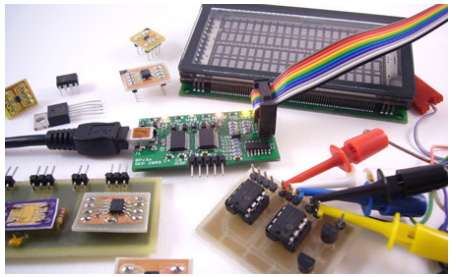
Microsoft Windows

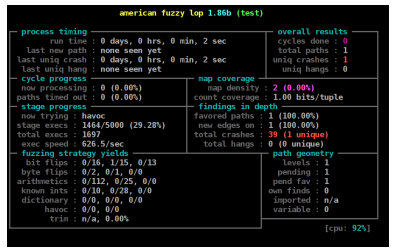


Reverse Engineering and Vulnerability Research Tools

GHIDRA





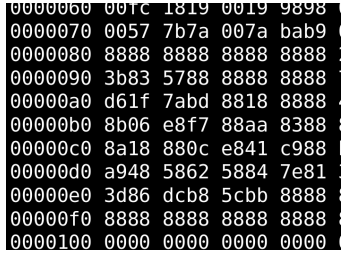


Knowledge

- Vulnerabilities
- Exploits
- Lessons Learned

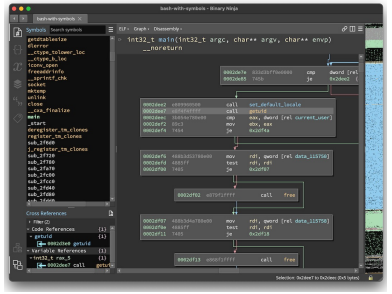
Wireless Router

Firmware

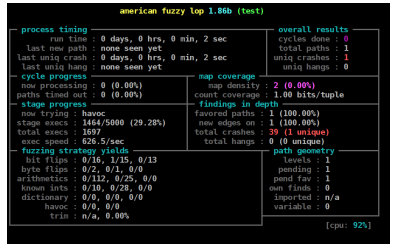


Reverse Engineering and Vulnerability Research

Manual Tools



Automated Tools



Vulnerabilities

Lessons Learned

Program Analysis Research

New Tools

An Average Day at Kudu

Grab coffee, tea, snacks, and more at the Kudu Café

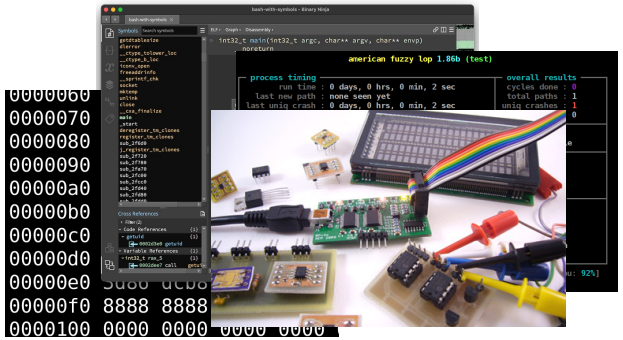
GitLab

Google Meet

slack

IRL

Sync up with teammates



Break things in creative and useful ways

python

Haskell

The Rust Programming Language

Write some code

Join the Kudu band

Learn how to build circuits

Learn to make latte art

Serve on a committee

Join the book club

Go climbing

Peer-pressure fitness

Be involved

KUDU DYNAMICS

Keep Learning

Challenge Problems

- https://pwn.college
- https://exploit.education
- Play CTFs (picoCTF, PlaidCTF, etc.)

Reading

- PoC||GTFO (https://github.com/angea/pocorgtfo)
- Phrack Magazine (http://www.phrack.org)

Tools

- Ghidra
- angr
- afl-fuzz
- gdb
- WinDbg
- Qiling
- Binary Ninja
- IDA Pro
- QEMU

Misc. Topics

- Binary analysis
- Static analysis
- Dynamic analysis
- Symbolic execution
- Shellcode
- Packers
- Heap exploitation
- Fuzzing
- Formal methods
- Code embeddings
- Weird machines
- Data-flow analysis

There is always a way to:

1. Figure out how it works
2. Use it differently than intended

KUDU DYNAMICS

Join Kudu

General Info

- Website: https://www.kududyn.com
- Four office locations:
  - Chantilly, VA; Columbus, OH; Boulder, CO; San Antonio, TX
- Great benefits, including:
  - Flexible work-from-home, discretionary fund, health care, employee ownership program, and more
- Eligibility:
  - US citizenship and ability to hold a security clearance

Internships

- Send your resume to interns@kududyn.com
- More info: https://www.kududyn.com/#:~:text=INTERNSHIP

Jobs

- Open positions at all of our offices
- More info: https://www.kududyn.com/#jobs

Contact Info

Matt (drone) Revelle
drone@kududyn.com