

# CYBERSECURITY AT KUDU DYNAMICS

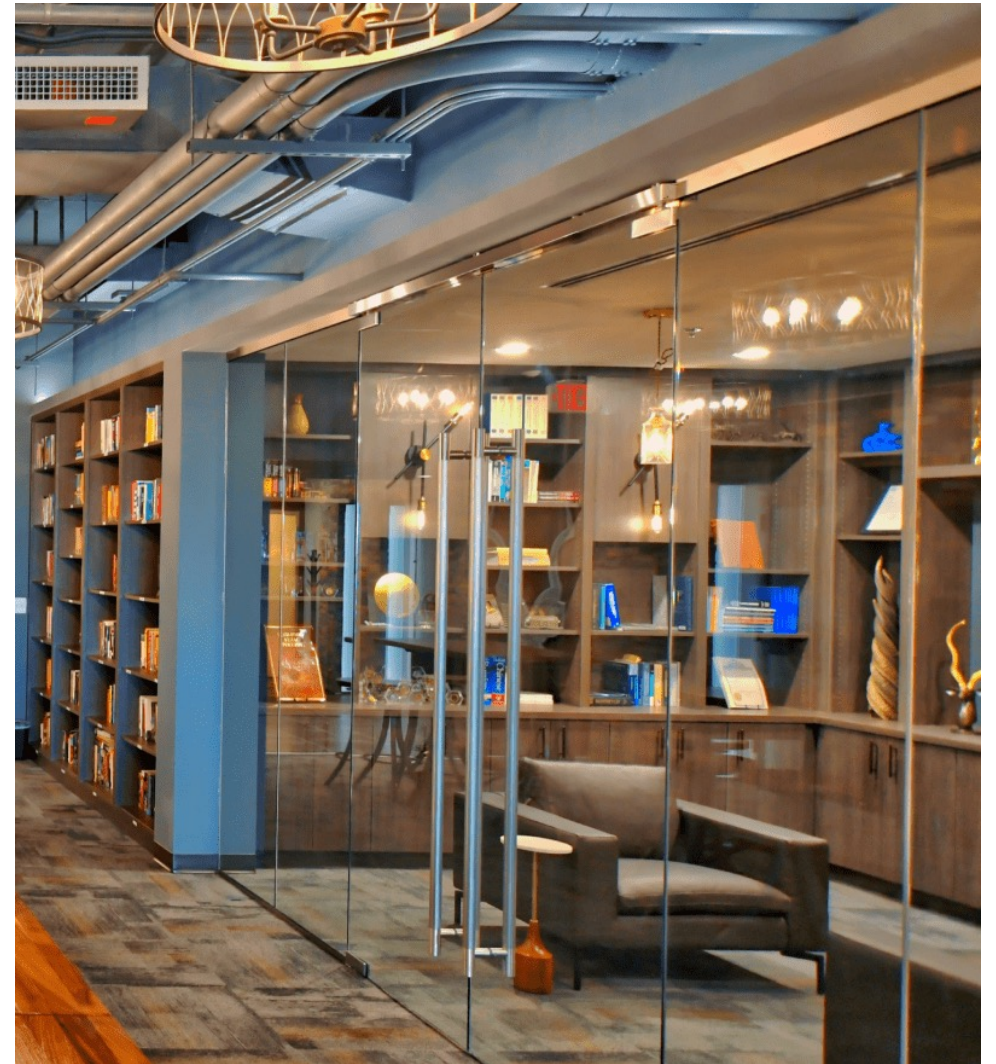
2023 May 1 | Montana State University

Matt (drone) Revelle  
[drone@kududyn.com](mailto: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

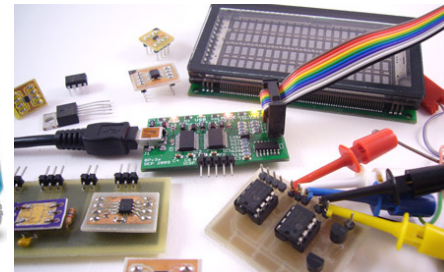
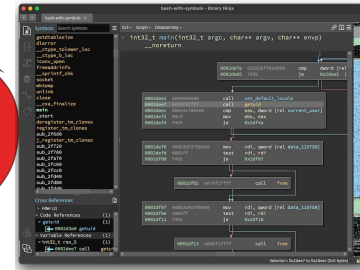


# Finding and Proving Vulnerabilities

## Vulnerable Hardware and Software



## Reverse Engineering and Vulnerability Research Tools



american fuzzy lop 1.06b (test)			
process timing		overall results	
run time :	0 days, 0 hrs, 0 min, 2 sec	cycles done :	0
last new path :	none seen yet	total paths :	1
last uniq crash :	0 days, 0 hrs, 0 min, 2 sec	uniq crashes :	1
last uniq hang :	none seen yet	uniq hangs :	0
cycle progress		map coverage	
new processing :	0 (0.00%)	count coverage :	1.00 bits/tuple
paths timed out :	0 (0.00%)	findings in depth	
stage progress		new paths :	1 (100.00%)
new trials :	have	new edges on :	1 (100.00%)
stage execs :	1464/5000 (29.28%)	total crashes :	30 (1 unique)
total execs :	1659	total hangs :	0 (0 unique)
exec speed :	626.5/sec	path geometry	
fuzzing strategy yields		new hits :	1
bit flips :	0/10, 1/15, 0/13	pending :	1
byte flips :	0/2, 0/1, 0/0	pending fan :	1
arithmetic :	0/12, 0/25, 0/0	own finds :	0
known ints :	0/10, 0/28, 0/0	imported :	n/a
dictionary :	0/0, 0/0, 0/0	variables :	0
known :	0/0, 0/0		
trin :	n/a, 0.00%		

## Knowledge

Vulnerabilities

Exploits

Lessons Learned

Reverse Engineering and Vulnerability Research

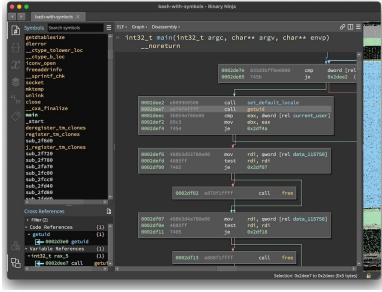
Wireless Router



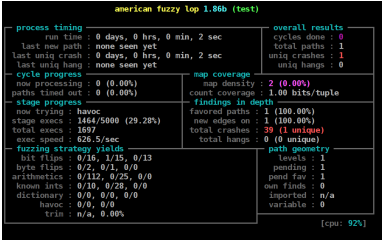
Firmware

```
00000060 007c 1819 0019 9898
00000070 0057 7b7a 007a bab9
00000080 8888 8888 8888 8888
00000090 3b83 5788 8888 8888
000000a0 d61f 7abd 8818 8888
000000b0 8b06 e8f7 88aa 8388
000000c0 8a18 880c e841 c988
000000d0 a948 5862 5884 7e81
000000e0 3d86 dcb8 5cbb 8888
000000f0 8888 8888 8888 8888
00000100 0000 0000 0000 0000
```

Manual Tools



Automated Tools



Vulnerabilities

Lessons Learned

New Tools



Program Analysis Research





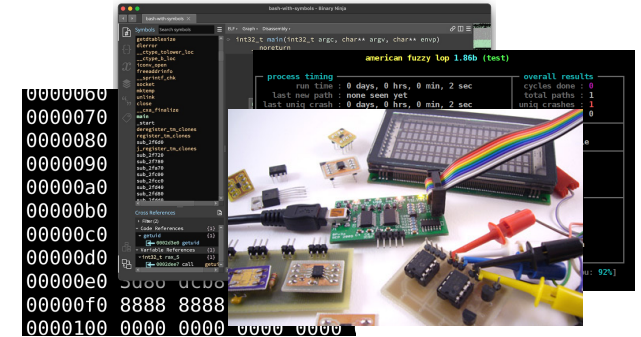
# An Average Day at Kudu



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



Sync up with  
teammates



Break things in creative  
and useful ways



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



# 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   | • gdb    | • Binary Ninja |
| • angr     | • WinDbg | • IDA Pro      |
| • afl-fuzz | • Qiling | • QEMU         |

## Misc. Topics

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

There is always a way to:

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



# 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](mailto: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](mailto:drone@kududyn.com)