

# Cyber@UC Meeting 89

Lab Update

# If You're New!

- Join our Slack: [cyberatuc.slack.com](https://cyberatuc.slack.com)
- Check out our website: [cyberatuc.org](https://cyberatuc.org)
- Organization Resources on our Wiki: [wiki.cyberatuc.org](https://wiki.cyberatuc.org)
- **SIGN IN!** (*Slackbot will post the link in #general every Wed@6:30*)
- Feel free to get involved with one of our committees:  
*Content Finance Public Affairs Outreach Recruitment Lab*
- Ongoing work in our research lab!



# Announcements

- Bi-weekly lab events!
  - Socket Programming!
- Executive meeting Sunday, all are welcome
- Dodgeball Thursday
- CTF team
- Gathering!
- Outreach Events!



***BATTELLE***

***WEDNESDAY APRIL 10TH, 2019***

***GUEST SPEAKER:  
AARON MCCANTY***

***RE/VR AUTOMATION***

***SATURDAY APRIL 20TH, 2019***

***FULL DAY EVENT  
11AM - 4PM***

***VIDEO GAME + CTF = 🤖***

***COLUMBUS OH***

# Weekly News

# ASUS Confirms Backdoor

- ASUS update servers compromised and used to push malware
- Malware indexes MAC's of all infected devices for targeting purposes
- Malware pushed for 5 months in 2018, estimates are about tens of thousands to 1 Million devices

[https://motherboard.vice.com/en\\_us/article/bjgez4/asus-confirms-it-was-used-to-install-backdoors-on-its-customers-computers](https://motherboard.vice.com/en_us/article/bjgez4/asus-confirms-it-was-used-to-install-backdoors-on-its-customers-computers)



# Are We in a Cyberwar?

- Survey Conducted by Venafi from RSA Conference with Cybersecurity Professionals
- 87% Believe World is in a Cyberwar
- 72% Believe Nation States should “hack-back”
- 58% Believe Private Organizations should “hack-back”

<https://securityboulevard.com/2019/03/are-we-in-a-cyberwar-yes-say-many-it-security-pros/>



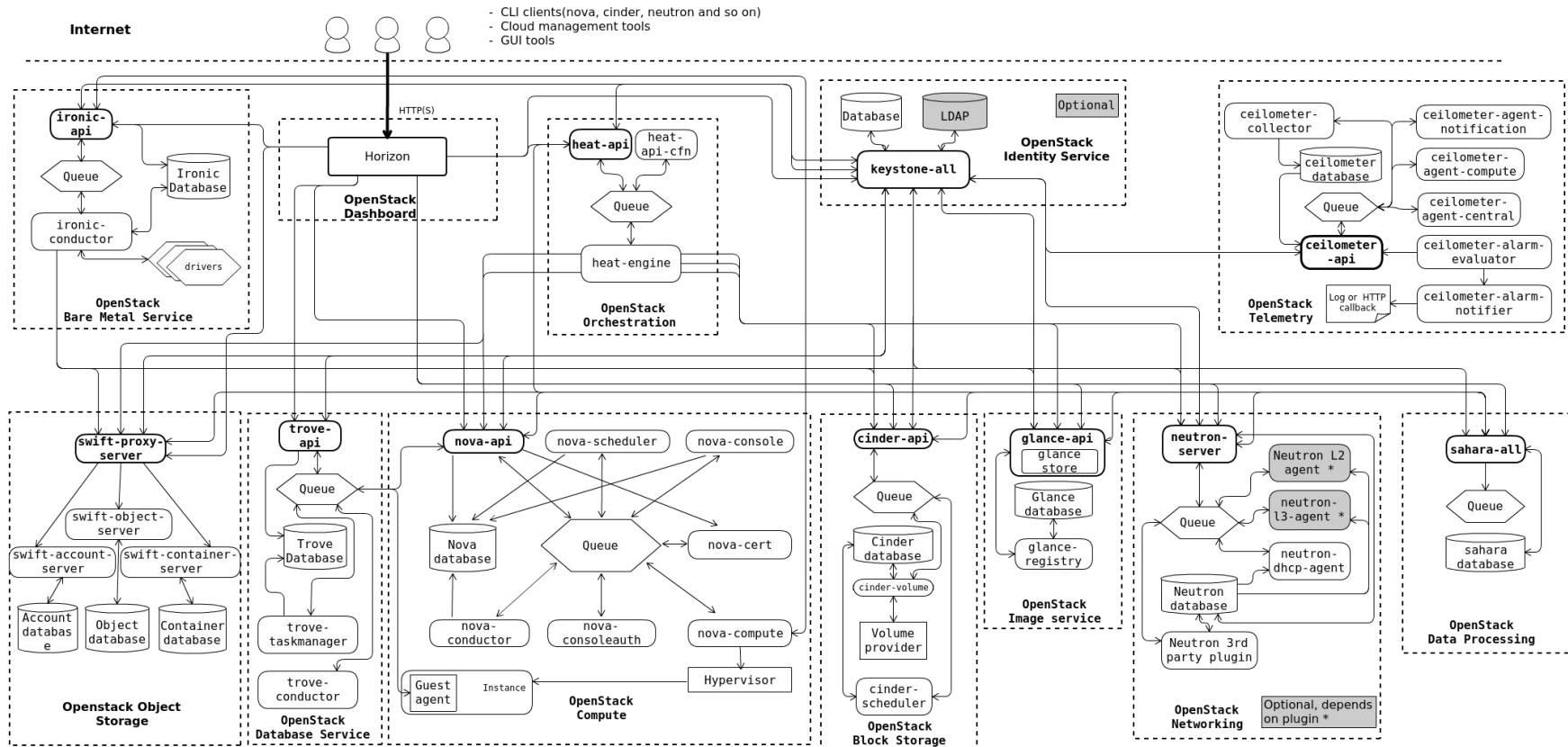


# Learning the Lab

## Part 1: Connecting

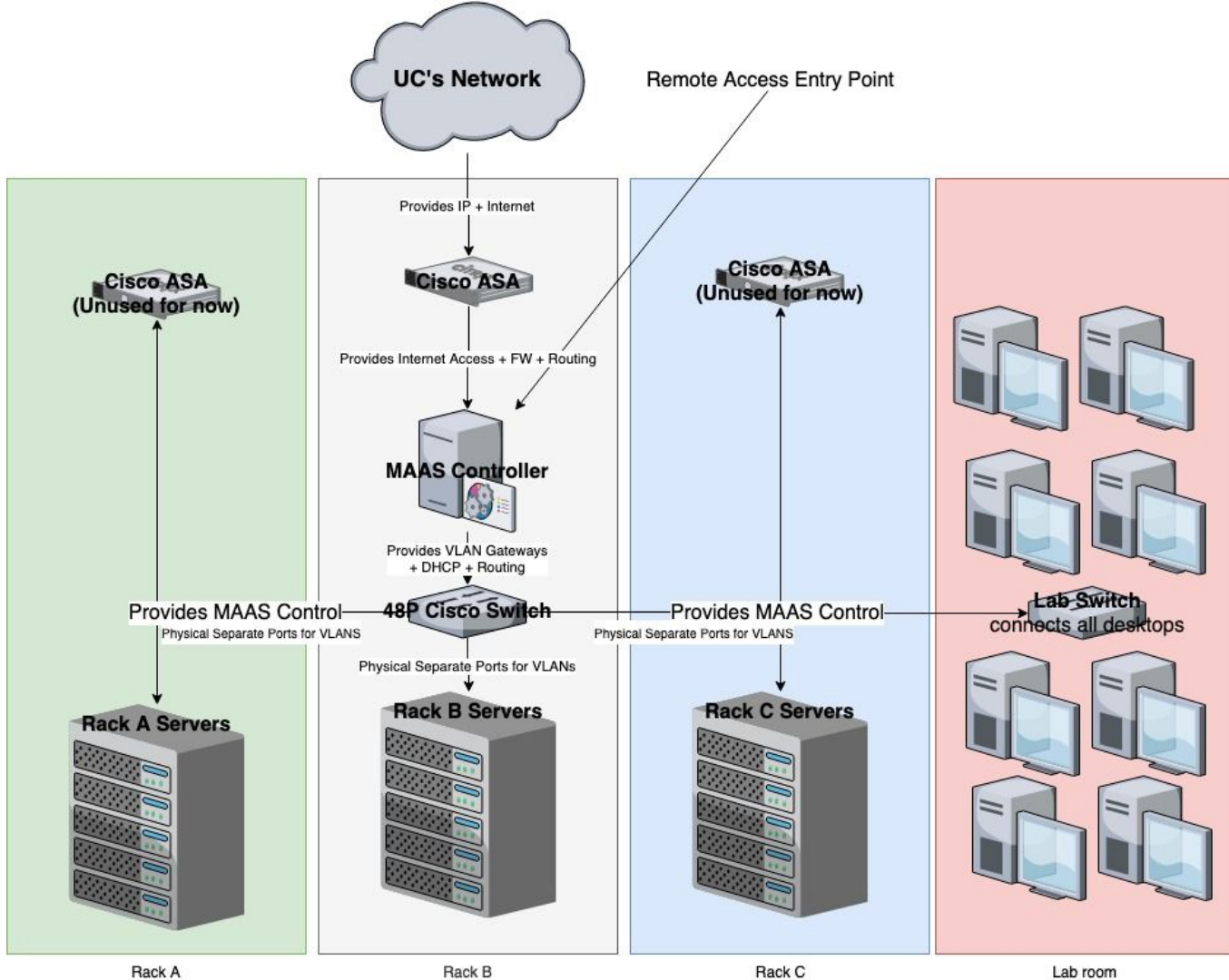


# OpenStack



# Openstack Design Patterns

- Modular
- Producer and consumer
- Loosely Coupled



# ZeroTier

- A “**virtual switch**” for connecting devices
- Allows us to **remotely access our lab!**
- **Open Source and Free!**
- E2E Encrypted
- The basics:
  - Each ZeroTier **Client** has a **10-digit address** like: 89e92ceee5
  - Each ZeroTier Network has a **16-digit Network ID** like: 8056c2e21c000001

Lets download the ZeroTier Client: <https://www.zerotier.com/download.shtml>

Manual: <https://www.zerotier.com/manual.shtml>





Install + Config  
working time

# ZeroTier Command Line Interface

First of all, make sure you run the zerotier-cli command as **root**.

- **zerotier-cli info**
  - Displays your ID, zerotier version, and status
- **zerotier-cli join <network id>**
  - Allows you to join the zerotier network
  - *You have to be authenticated in order to access the lab*
- **zerotier-cli leave <network id>**
  - Leaves a zerotier network
- **zerotier-cli listnetworks**
  - Lists all connected networks




# Connecting to the Lab Network

- Our labs **network ID** is: **REDACTED**
- The ZeroTier client **we need to connect to** has the IP of: **REDACTED**
  - This is the IP of our “Rack controller” AKA **the server for managing all other servers/VMs**
- **Now that we know** *where to connect to and are a part of the ZeroTier lab network* we need to **gain access to our running webapps**
  - To be able to access machines on our network **we need to set up a SOCKS Proxy**
  - **This is different for each operating system**, *you may need to do some googling*

**SSH cli cmd:** `ssh -D 9002 -q member@REDACTED`

For additional privs and access please talk to Ryan Young





Connection +  
SOCKS working  
time