# OpenC2

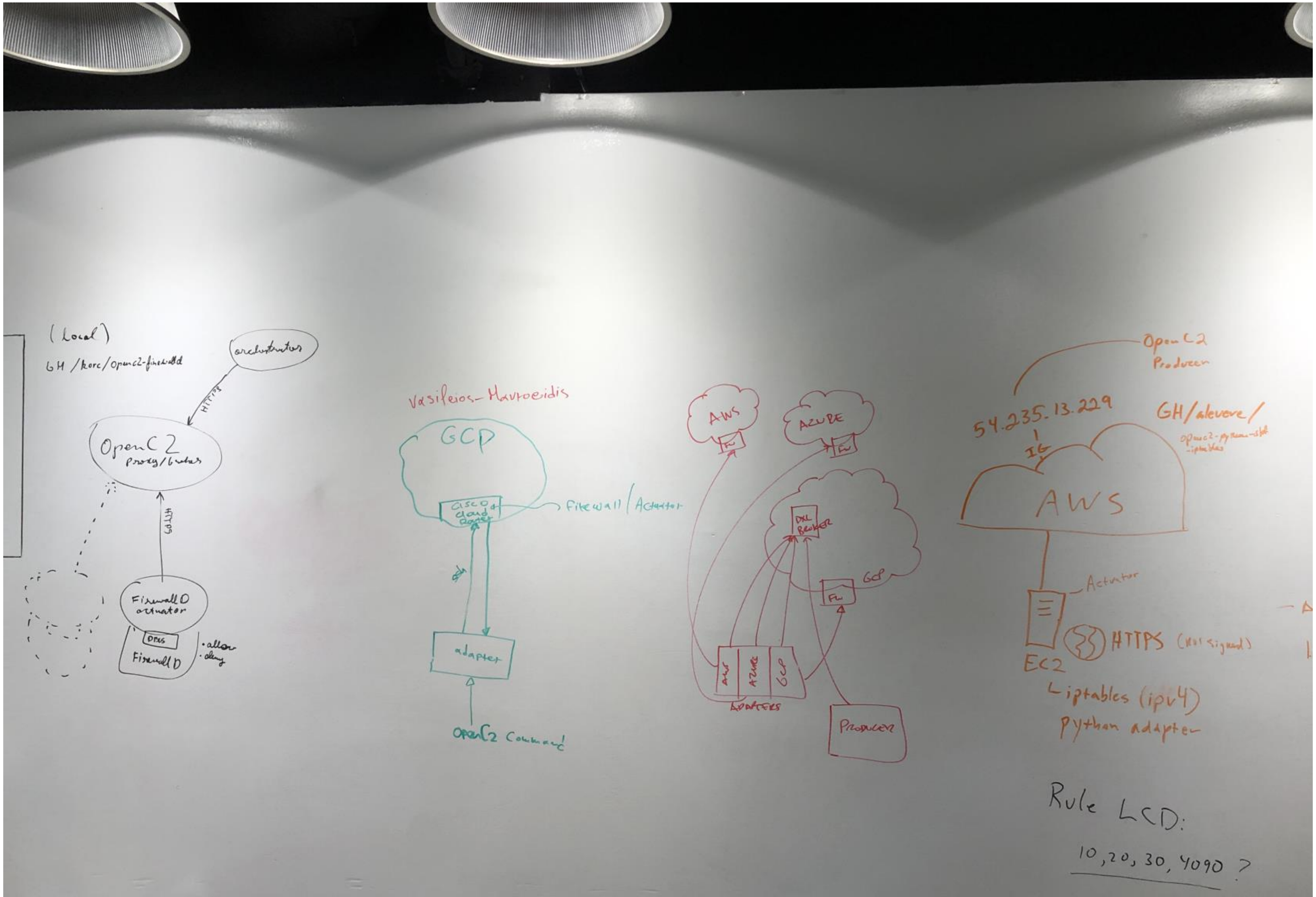
## PLUG FEST/ HACK-A-THON

27, 28 JAN 2020
UMBC Training Center
Columbia, Maryland

# Day1Update from Firewall/SLPF/SFPF

- OpenC2 Actuator Profiles
  - 5-10 participants today
    - Univ. Of Oslo, Univ. Of North Carolina, AT&T, NetScout, New-Context, CyberDefense Institute/NEC
  - 4 implementations: public clouds, firewalld, Cisco, iptables
  - Demo'd of each implementation
  - 14 issues identified

# Overview of Implementations



# Issues Discussed

- Issues
  - Authentication
  - Limited data in responses from actuators
    - Rules, which actuator, support for temporal?
  - Temporal Requirements – start/stop
  - Multiple targets or similar commands
  - Logging per rule?
  - Comment on rule
  - Ipv4net should be clarified as ANY->ipv4net AND ipv4net->ANY : 2 rules
  - Response=none, HTTP requires response (204?)
  - Forward packet/duplicate packet/offload
  - What knows the security-group name and priority to use?

# Question and Answer on OpenC2 Message Signing

- John-Mark Gurney, New Context

- HTTPS Transport
  - 3.2.4 Authentication
  - Each participant in an OpenC2 communication MUST authenticate the other participant.

# Demo OpenDXL

- Michael Stair, AT&T

- Implemented in Google Cloud Platform
- Uses pub/sub to issue commands to AWS, GCP, Azure firewalls and/or network ACLs

# Next Steps

- Happy to get feedback; take a look at code or online demos
  - Generate pull requests or email openc2 list
- Have a producer connect to multiple implementations
  - Connect OpenDXL to Cisco IOS XE
  - Bridge OpenDXL to HTTP

# References

- https://github.com/alevere/openc2-python-slpf-iptables/
- https://github.com/korc/openc2-firewalld
- https://github.com/Vasileios-Mavroeidis/openc2-plugfest/tree/master/2020-January
- Look next week for AT&T code