OpenC2

PLUG FEST/ HACK-A-THON

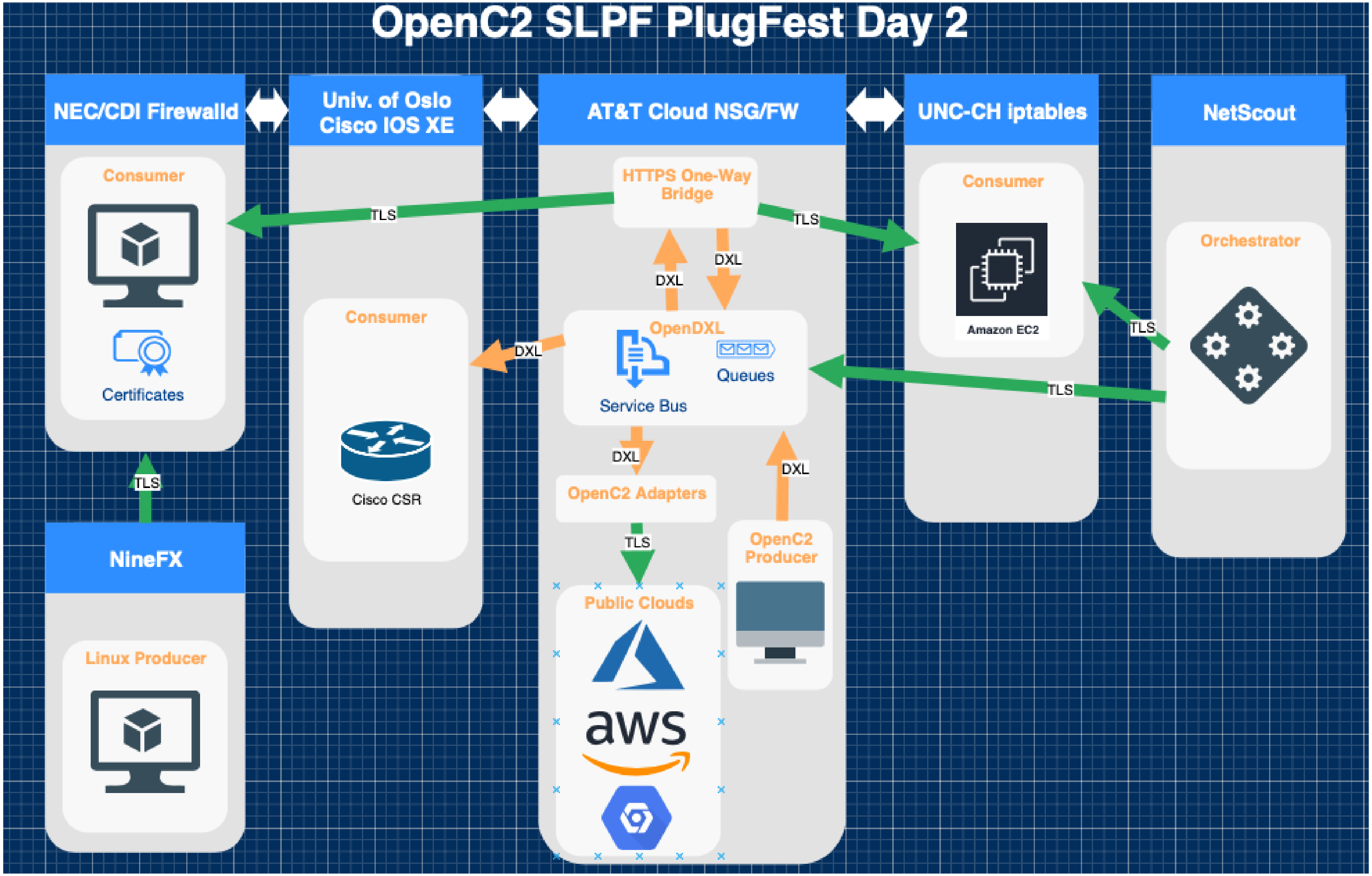
27, 28 JAN 2020
UMBC Training Center
Columbia, Maryland

28 JAN 2020

Day2 Update from Firewall/SLPF/SFPF

- OpenC2 Actuator Profiles
  - 5-10 participants today
    - Univ. Of Oslo, AT&T, NetScout, New-Context, CyberDefense Institute/NEC, Univ. Of North Carolina
  - 4 implementations: Azure/AWS/GCP, firewalld, Cisco IOS XE, iptables
  - Integration work
    - Utilized two transport layers and built a 1-way bridge
    - Commands in OpenDXL to (OpenDXL and HTTPS)
    - Incorporates Request-ID in topic
    - Responses from HTTPS to OpenDXL message bus
  - 17 issues identified during plugfest

Overview of Integration



Demo OpenDXL

- Michael Stair, AT&T

Next Steps

- Happy to get feedback; take a look at code or online demos
  - Generate pull requests or email openc2 list for issues identified

Day 2 Issues

- □ Protocol not set, but port set
- □ Protocol String or Int ? 0-255 is cleaner
- □ Ambiguity in ipv4/ipv6_connection
- □ What if actuator doesn’t support SCTP, ICMP Type?

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
- □ https://www.netscout.com
- □ Look next week for AT&T code