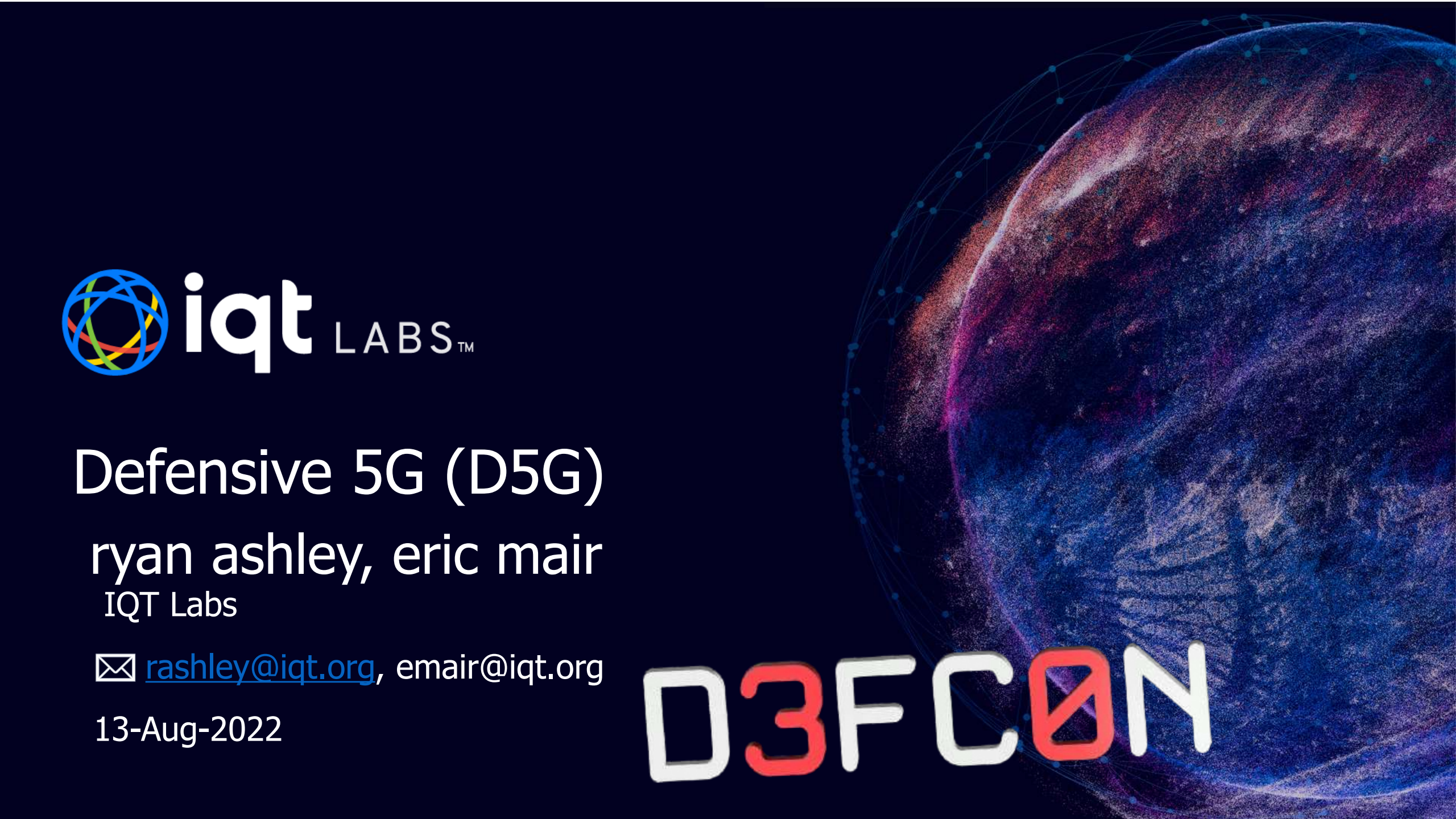


Defensive 5G (D5G)

ryan ashley, eric mair
IQT Labs
✉ rashley@iqt.org, emair@iqt.org

13-Aug-2022

Introduction – About IQT

In-Q-Tel is a not-for-profit that serves the national security interests of the U.S. and its allies, providing the most sophisticated source of strategic technical knowledge, insights, and capabilities.

More at – www.iqt.org

IQT Labs identifies aspects of these problems that can be tackled quickly and open sourced, using lightweight and agile methods. Collaborating with a broad ecosystem of experts from government, academia, and industry to experiment with emerging tools and prototype solutions, IQT Labs shares insights about technology ahead of the startup.

More at – www.iqt.org/labs

Introduction

Objective(s):

1. Develop a highly configurable and reproducible open-source 5G test infrastructure that implements the key functions required for 4G/4.5G/5G deployments.
2. Use our open-source 5G test network(s) along with our unique expertise to exercise different defensive techniques and configurations and test their effectiveness against attacks.

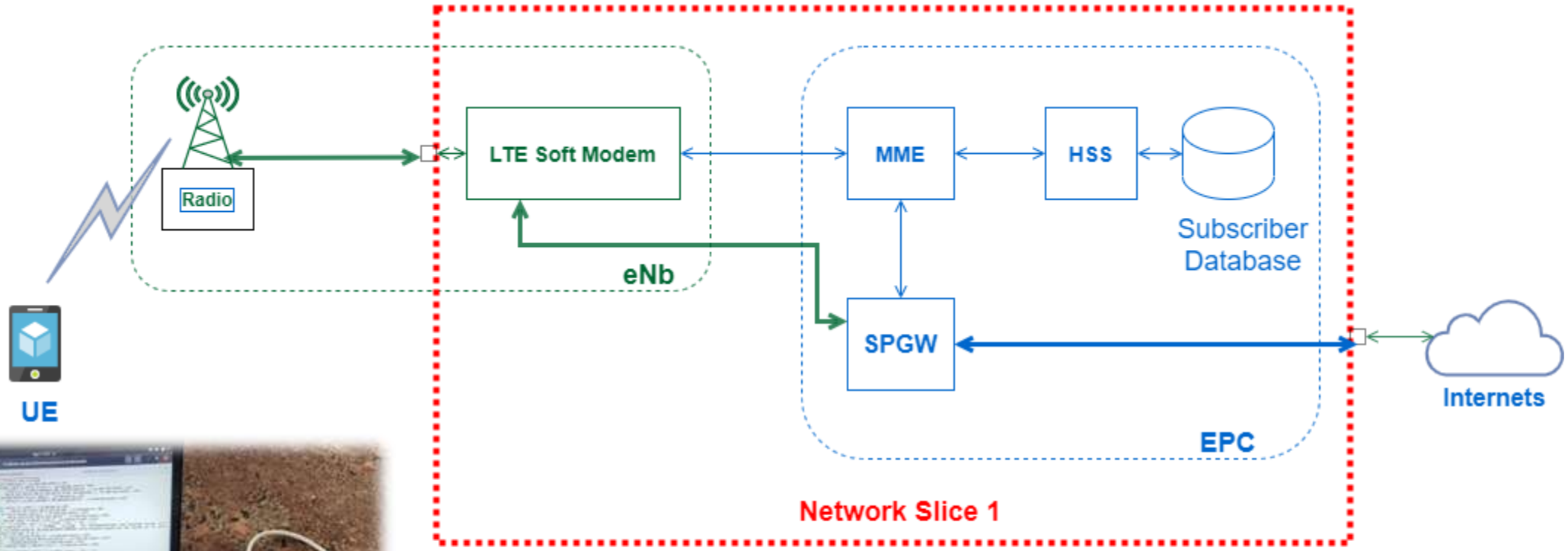
git repos:

Defensive 5G: https://github.com/iqtlabs/daedalus
Faucet: https://github.com/faucetsdn/faucet
Dovesnap: https://github.com/IQTLabs/dovesnap
srsRAN: https://github.com/srsran/srsRAN

A big thanks to the IQT Labs Engineering Team (Charlie L., Ryan A., and Josh B.)

Test-Bed

We needed to build this network.

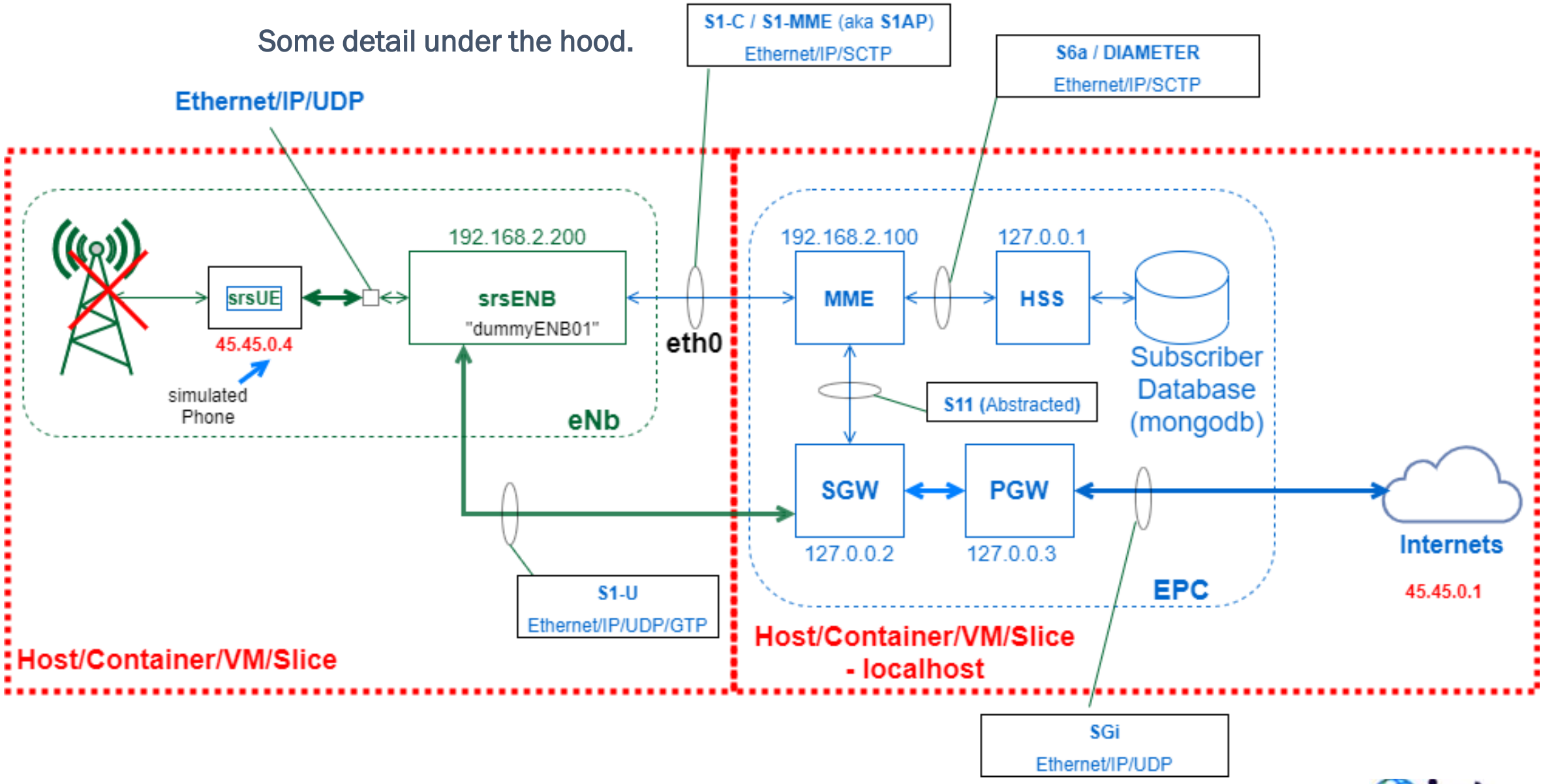


D3FCON

iqt LABS

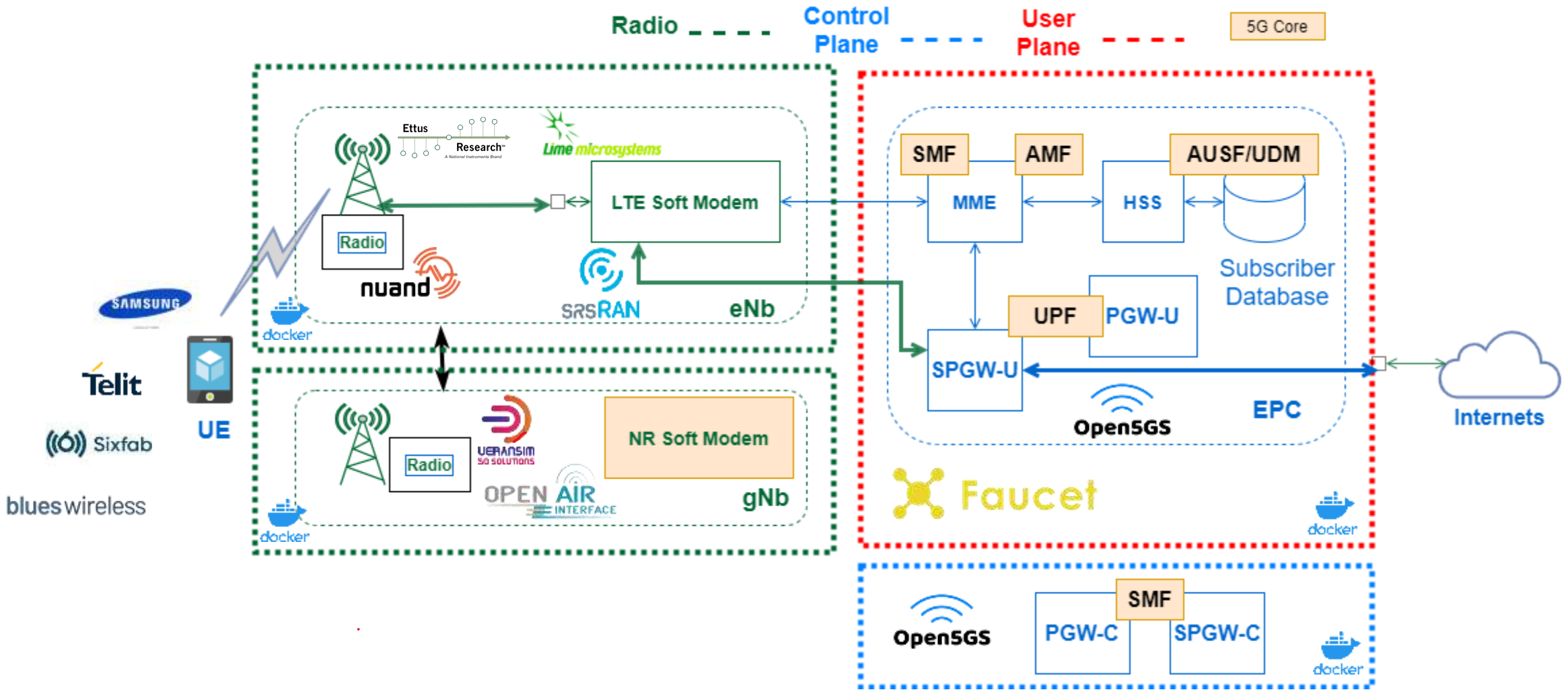
Test-Bed

Some detail under the hood.



Test-Bed

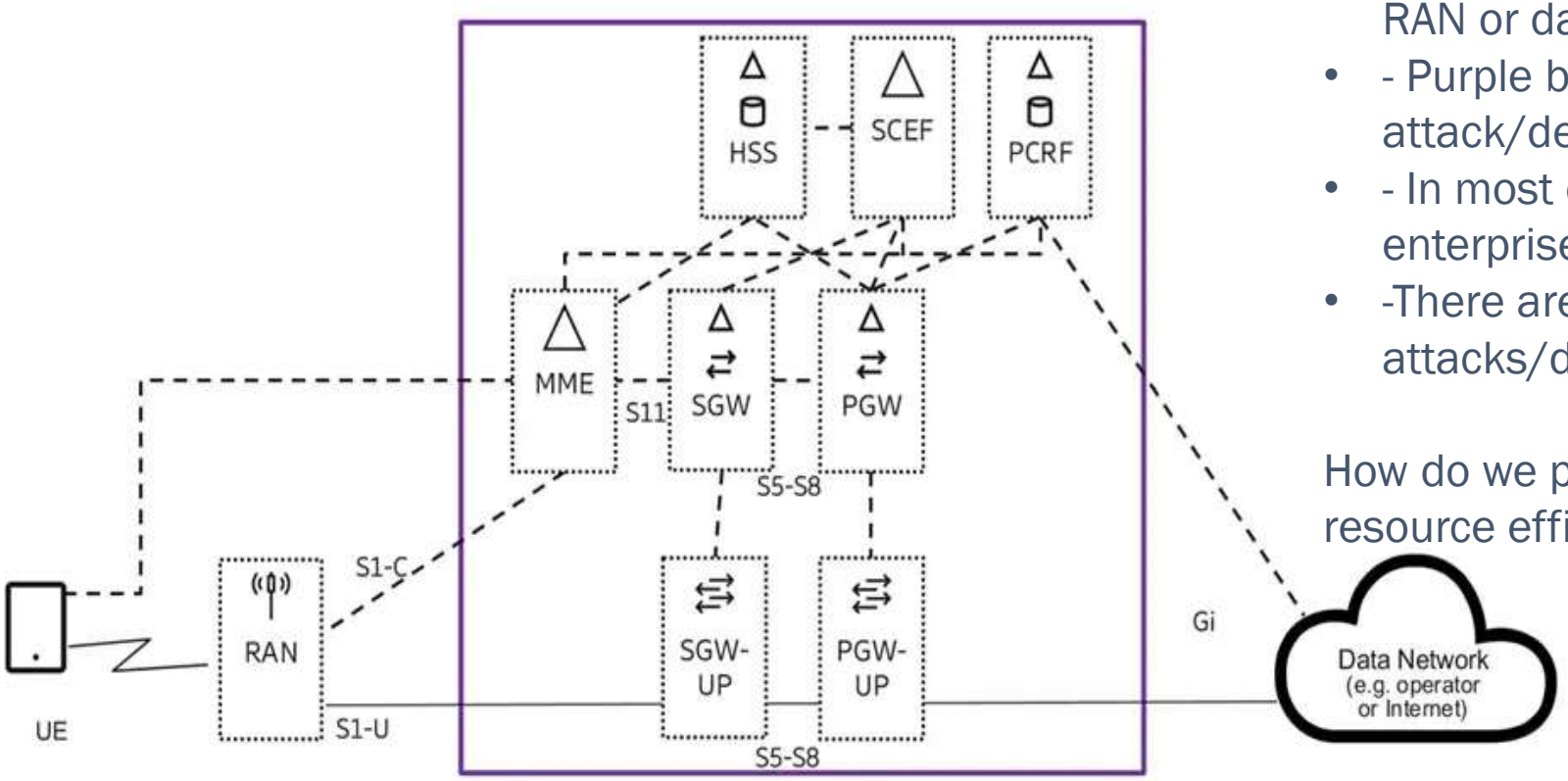
Our Current Network*



D3FCON

iqt LABS

Daedalus – Motivation



The Problem:

- - 5G networks can experience attacks from the RAN or data network side.
- - Purple box defines what we intend to attack/defend
- - In most cases the 5G networks are similar to enterprise networks
- -There are subtleties that make the attacks/defenses different for each.

How do we prototype our TTP's in a repeatable resource efficient way?

Daedalus Background

Enabling technologies:

Software Defined Radio (SDR) - incorporating SDR into the RAN
Software Defined Networking (SDN) - highly configurable infrastructure
Containerization – all network functionality is virtualized in configurable containers

Create a test network that can support:

Control/User Plane separation (CUPS) - enabling separate entities to implement their respective functions independently
Observability – SDN mirror river allows end to end packet capture
Cloud Computing - multi-tenancy, elasticity
Edge Computing - AR/VR, low latency

Daedalus - 1

What is Daedalus?

Daedalus is set of tools to programmatically deploy and manage 5G test infrastructure, primarily using open-source software and COTS hardware, to prototype and compare attacks and defenses.

One of the key differences in 5G networks is the shift from custom hardware appliances to virtualized network functions (NFV) communicating over IP. This presents an opportunity to use existing tools in new ways or to merge RF tooling with network tooling to create new attacks. Defending 5G will require a mix of enterprise network and radio network defense tools/techniques. Part of the work being done in this project is figuring how to create that mix. Additionally, 5G presents a generational opportunity to develop defensive methodologies ***before*** widespread deployment to 5G networks.

5G Background - 1

Radio Access Network (RAN):

LTE/LTE-A: 4G/4.5G

New Radio (NR): The enhanced radio access technology used by 5G SA networks, specifically:

- Diverse Frequency: FR1 (sub 6 GHz), FR2 (> 24GHz)
- Spectral Efficiency: advanced modulation and coding (more bits/Hz)
- Multi-User: MU-MIMO, Beam-forming
- Higher Throughput: mmWave tech, larger bandwidths(@ higher freqs)

Core Network:

4G/4.5G: Evolved Packet Core (EPC): the core network for an LTE system, convergence of data and voice with an IP based architecture. A big step forward from 3G.

5G Core (5GC): the core network for 5G, intended to work with NR and use a much simpler architecture.

User Equipment (UE):

Phones/Handsets

IoT Devices

Vehicles

Attacking 5G – 5G Specific targets/methods

Malicious UE

A device that acts like ordinary user equipment (a phone, IoT device, etc.) but is actually used as a vehicle to launch attacks in the user plane

Attacks on the Subscriber DB

- Grant access to illegitimate users
- Deny access to legitimate users
- Spoof users

GTP/RAN attacks

Attacks using or against RF devices and protocols

iqt LABS

Attacking 5G – Other use cases

Compare attacks across detectors (Zeek vs Snort vs Yara)

- Establish or reduce detections
- Full packet capture from mirror river gives great data source to test Snort rules
- Which rules and detections are unnecessary – weed out false positives

Establish repeatability

I hate the it works 20% of the time so just run it 5 times school of attack

Attacking 5G – Future work

Leverage the isolation provided by Daedalus to explore potential offensive and defensive uses of eBPF

- Kernel Exploits launched from user space
- Malicious code executing on a NIC
- Combine with Faucet Coprocessing
- Packet inspection
- Network wide traceability

D3FCON

iqt LABS

D5G - 3

Our Strategy

Attack Surface/Defense Response: a set of attack classes and defense responses designed to achieve various outcomes in the way that the attacker exploits the network. These scenarios are listed in the matrix below.

A red team/blue team approach will be used (red = attacker / blue = defender)

We started by creating a scenario with DECEPTION as a defense response to GRANT of ACCESS as an attacker objective.

ATTACKER OBJECTIVES: 5G Network / DEFENDER RESPONSES:	RECON/DISCOVERY	THEFT/EXFILTRATION	GRANT OF ACCESS	DESTRUCTION/DELETIO	DISRUPTION/DDOS
DO NOTHING	1A – 5GN	1B – 5GN	1C – 5GN	1D – 5GN	1E – 5GN
DENIAL/ FIREWALLING	2A – 5GN	2B – 5GN	2C – 5GN	2D – 5GN	2E – 5GN
DECEPTION	3A – 5GN	3B – 5GN	3C – 5GN	3D – 5GN	3E – 5GN
DEGRADING	4A – 5GN	4B – 5GN	4C – 5GN	4D – 5GN	4E – 5GN
QUARANTINE/ ISOLATION	5A – 5GN	5B – 5GN	5C – 5GN	5D – 5GN	5E – 5GN
THROTTLING	6A – 5GN	6B – 5GN	6C – 5GN	6D – 5GN	6E – 5GN

D3FCON

iqt LABS

Summary

What we have done:

- Developed a highly configurable 4.5G/5G test network using open-source software and COTS hardware.
- Demonstrated operability across a wide range of hardware (i.e. R-Pi to multi-core server)
- Identified [2] and remediated [9] a vulnerability in subscriber database management
- Developed a solid red team/blue team strategy for identifying potential 5G network vulnerabilities.

What is next:

- Develop and refine our ability to easily and consistently reproduce 5G test infrastructure.
- Put the above to work demonstrating proof-of-concept attacks and evaluating effectiveness of defensive measures.
- Develop a 5G NR/SA Network and explore vulnerabilities unique to this this type of network
- Study the IoT device and ecosystem security posture in 5G

Who Cares and Why:

- Private 5G networks will be more prevalent (campus, municipal, FWA)
- 5G networks for tactical purposes (law enforcement, military, disaster-relief, etc…)
- IoT (industrial, municipal, remote sensing)
- Agile, Inexpensive** and Secure***

iqt LABS

Questions?

Thank You!

Contact:

email: emair@iqt.org

git repo: https://github.com/IQTLabs/Daedalus

Other Labs Projects https://github.com/IQTLabs

