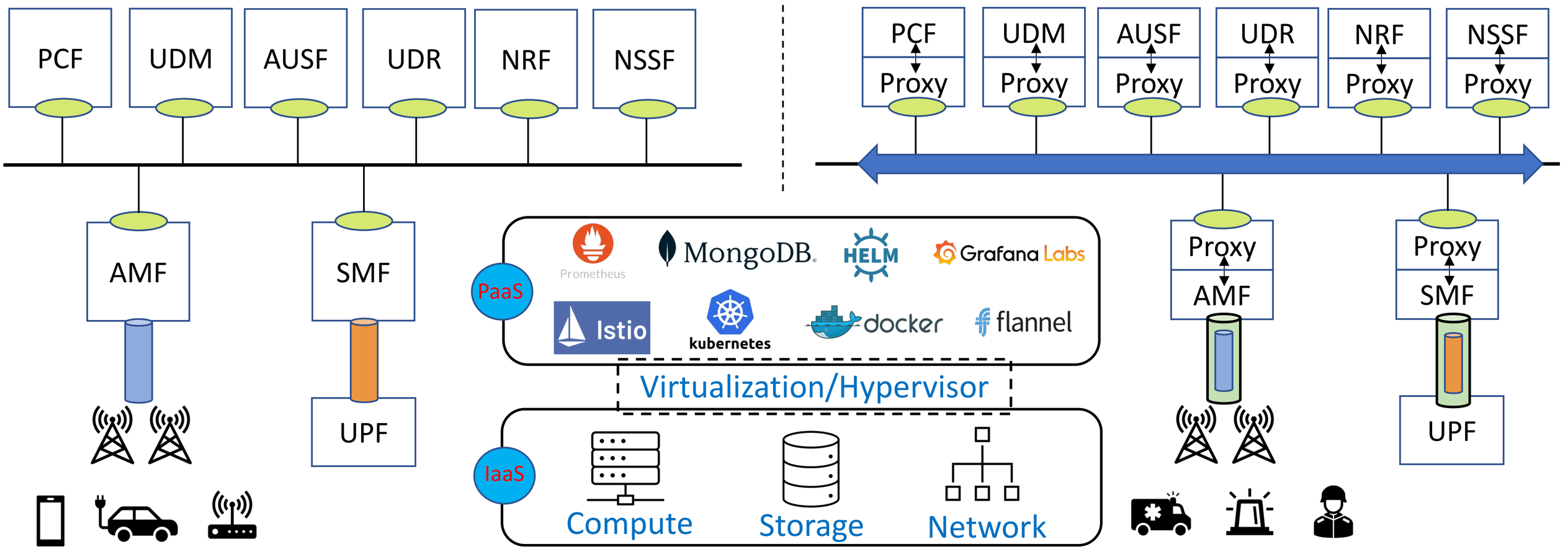
Slicure5G: Secure Slicing for 5G

Umakant Kulkarni, Sonia Fahmy
Department of Computer Science, Purdue University
E-mail: {ukulkarn, fahmy}@purdue.edu

Slicure5G: An end-to-end secure network slicing architecture that secures individual interfaces between 5G network entities

Slicure5G empowers network operators to deploy slices with customized security parameters, co-existing with unsecured, public-use, slices and sharing the underlying platform and hardware resources with them



Unsecured Slice | Shared Resources | Secured Slice

Service-based Interface

Interface between RAN and Control Plane (SCTP)

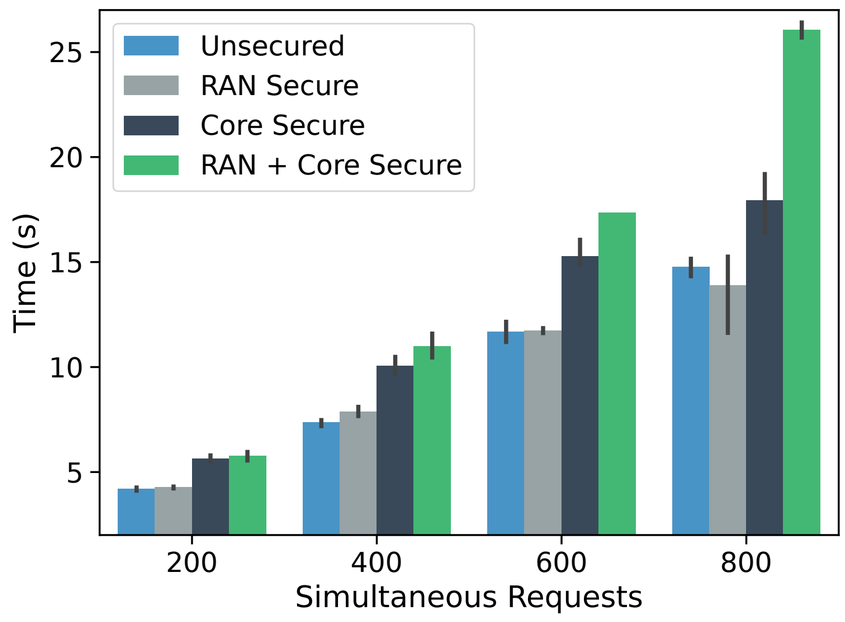
Interface between Control and User Plane (UDP)

TLS

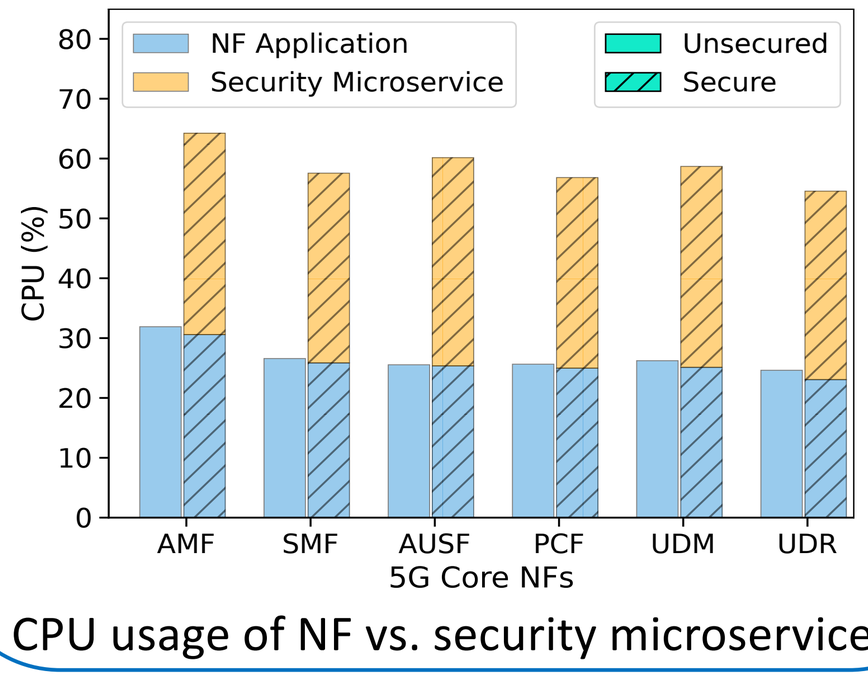
Point-to-point Secure UDP Tunneling

Design

- Isolating NF microservices across different slices per their security configuration
- Using public key infrastructure-based mutual authentication between each core network function
- Encrypting the traffic across
  - Service-based REST interfaces between core NFs
  - Interfaces between the RAN and core network
  - Interfaces between the control and user planes
- Rate-limiting ingress traffic and filtering packets based on slice service, user identifier, request type and access interface



Time to complete 5G registration procedure



CPU usage of NF vs. security microservices

Future Work

Design an adaptive slicing mechanism that determines secure slice configuration parameters based on the results of threat assessment modules

This work has been supported in part by NSF grant 2226447