Collaborative Research: SaTC: CORE: Medium: Enabling Practically Secure Cellular Infrastructure

Challenge:

5G fundamentally changes the operation and threat model of cellular systems by adopting an **open** and **multi-tenant** core.

Vast increase in capabilities and access to the core will spur innovation similar to smartphones in the late 2000's.

Solution:

We will use program analysis to

- **Crypto:** verify code assumptions made by formal protocol models
- **Access Control:** ensure correct specification and enforcement of policy that protects network tenants from one another.
- **Core Functionality:** ensure implementations are free of backdoors and logic bombs.

Analysis inherently spans the many microservice Network Functions (NFs) that comprise the 5G infrastructure.
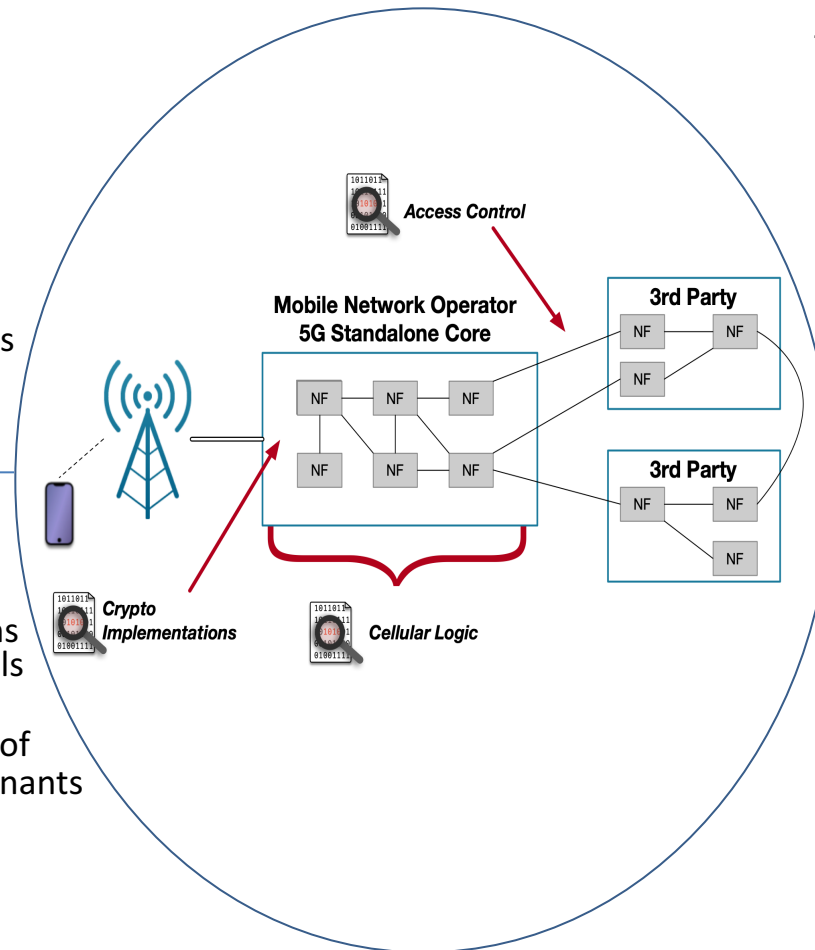
Scientific Impact:

- Techniques to extract, model, and analyze security-sensitive logic in source and binary code of cellular network infrastructure.
- First work to investigate the **software** in cellular infrastructure; prior work is limited to formal analysis of protocols.

Broader Impact and Broader Participation:

- The security of 5G software presents a significant risk to critical infrastructure.
- We will work with 3GPP and vendors to fix vulnerabilities and adopt our tools.
- **BPC:** new activities will attract underrepresented populations to CS through technology interaction to empower individual privacy.

Access Control

Mobile Network Operator 5G Standalone Core

3rd Party

NF NF NF

NF NF NF

3rd Party

NF NF

NF

Crypto Implementations

Cellular Logic

NF NF NF

NF NF NF

William Enck, NC State, CNS-2054911

Kevin Butler, U Florida, CNS-2055014