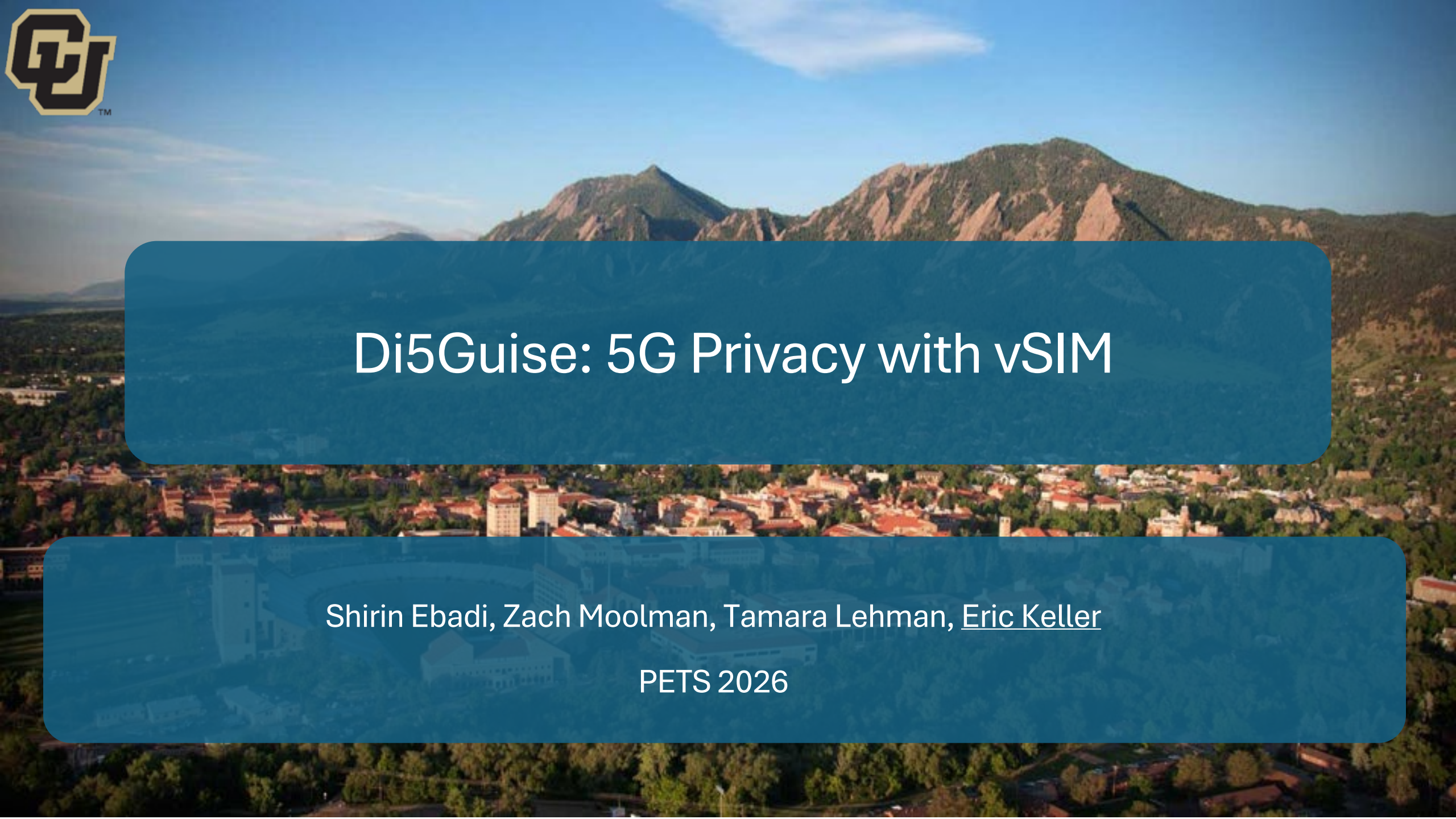
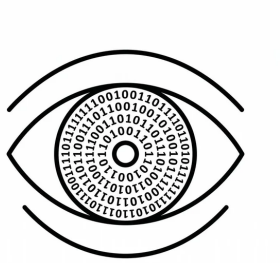


Di5Guise: 5G Privacy with vSIM

Shirin Ebadi, Zach Moolman, Tamara Lehman, Eric Keller

PETS 2026

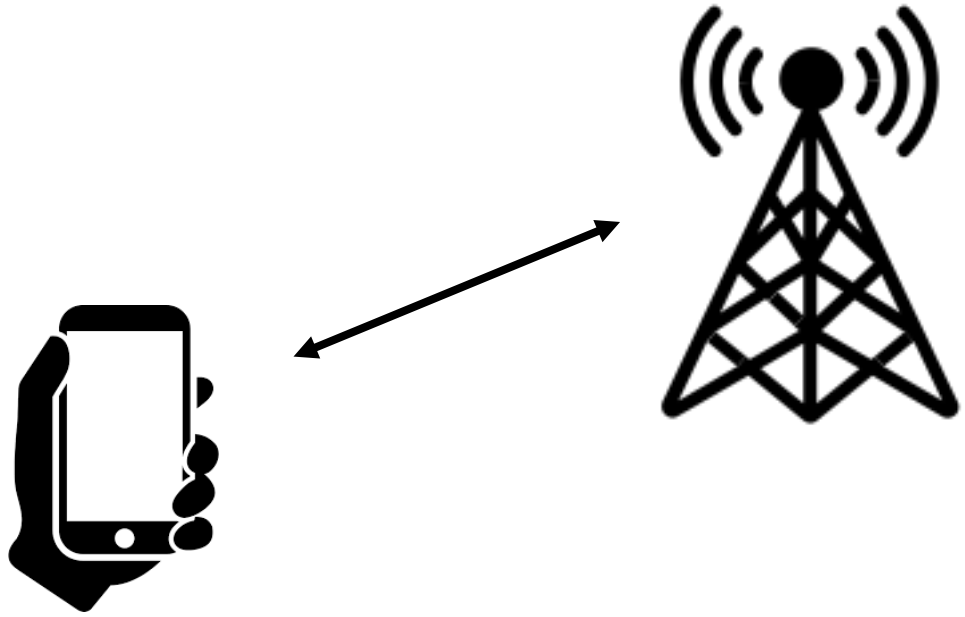
Pattern of Life Analysis



A method of surveillance that documents or understands the habits of a person or population

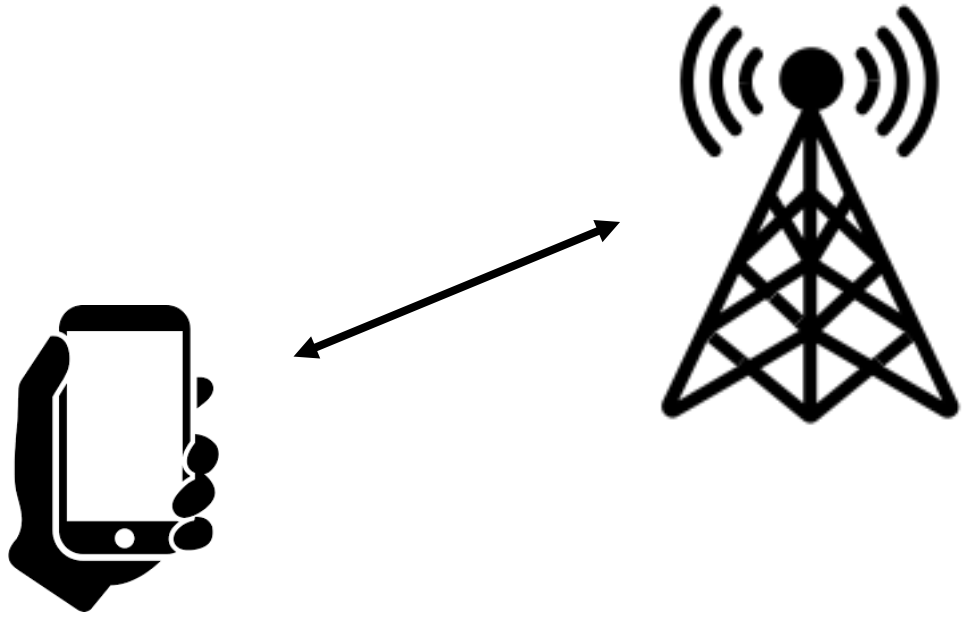
Cellular communication presents a unique privacy concern in that both online and physical activity are observable by operators

Meta Data in 5G



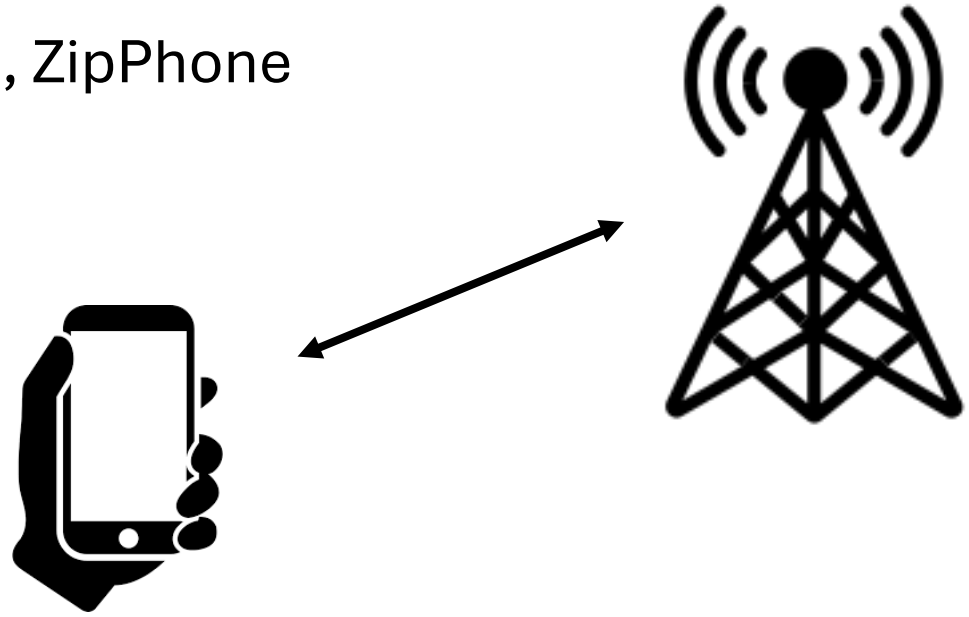
Meta Data in 5G

- Traffic – headers and patterns can expose who you're communicating with, what activity you're doing, etc.
  - Defense: VPNs, traffic obfuscation, etc.



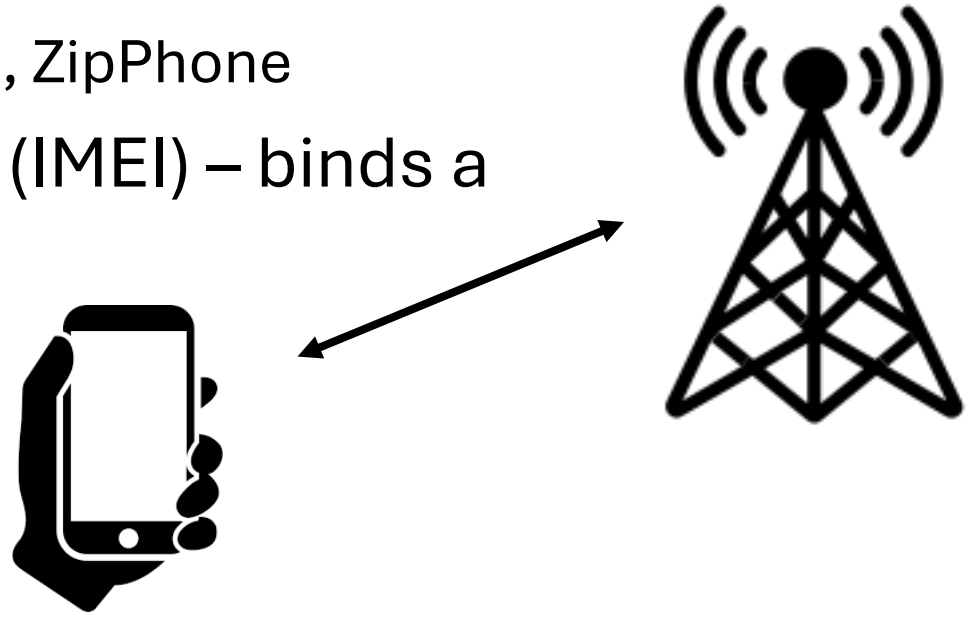
Meta Data in 5G

- Traffic – headers and patterns can expose who you're communicating with, what activity you're doing, etc.
  - Defense: VPNs, traffic obfuscation, etc.
- Subscriber Profile – correlates different traffic to subscriber
  - Defense: Swap profiles (eSIM), PGPP, AAKA, ZipPhone



Meta Data in 5G

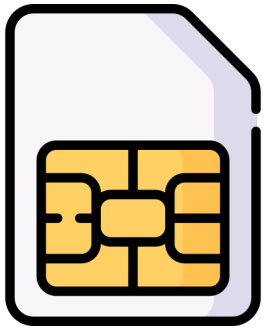
- Traffic – headers and patterns can expose who you're communicating with, what activity you're doing, etc.
  - Defense: VPNs, traffic obfuscation, etc.
- Subscriber Profile – correlates different traffic to subscriber
  - Defense: Swap profiles (eSIM), PGPP, AAKA, ZipPhone
- International Mobile Equipment Identity (IMEI) – binds a subscriber profile to a device
  - Defense: PPIC, ADA



What's Missing?
Linkability through the SIM card

- Even with all of these, an operator can still link various subscriber profiles to same device due to the SIM card

- SIM card has Embedded Identity Document (EID) and Secret Key
  - Provisioned by manufacturer, shared with operator, not changeable, not readable
  - Authentication to 5G network depends on the link between a subscriber profile and the EID/Secret Key

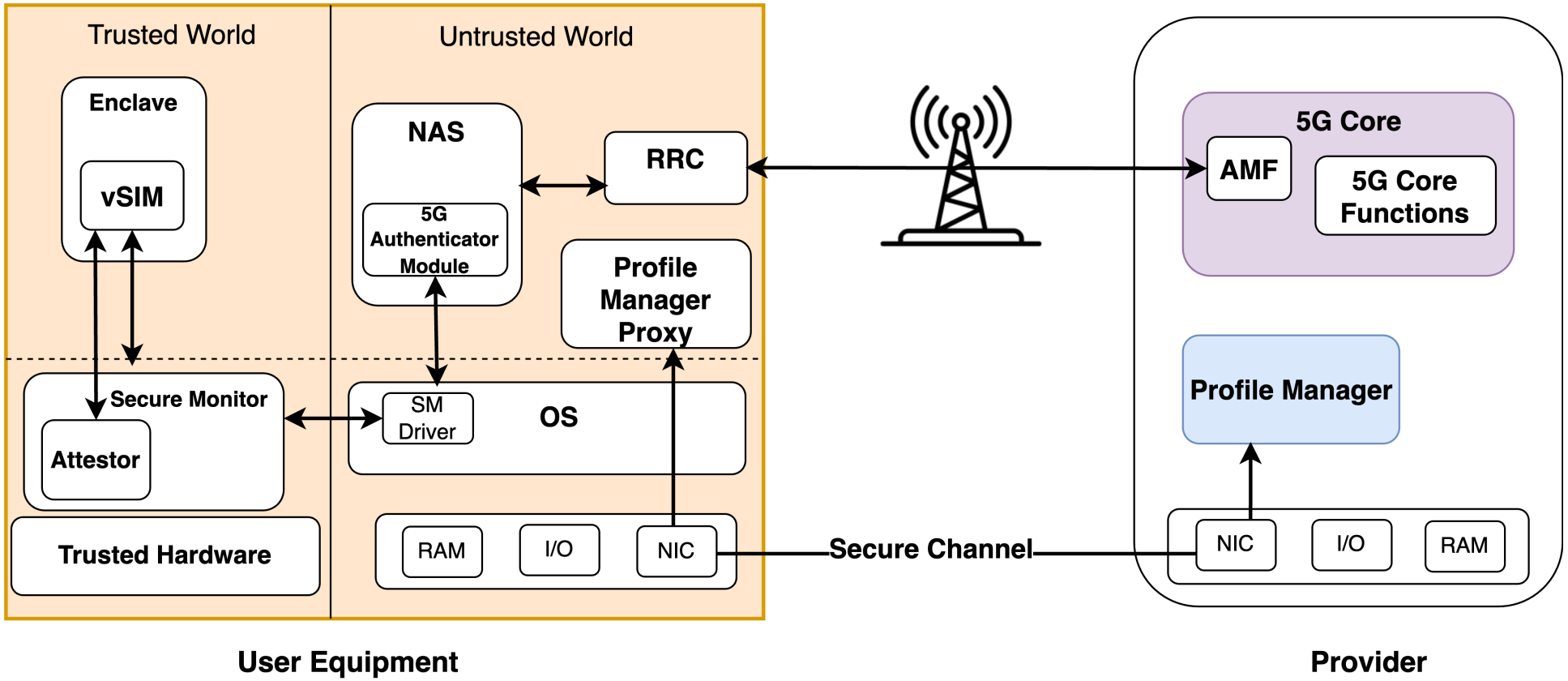


Di5Guise: Breaking the Linkability

- Move the SIM into software and enable dynamically provisioned Device Profile (EID/Secret Key), retaining backwards compatiblilty
- Novelty: Overcoming 5G's implicit trust that relies on the physical nature of the SIM coupled with business relationships.

Di5Guise: Like having multiple burner phones

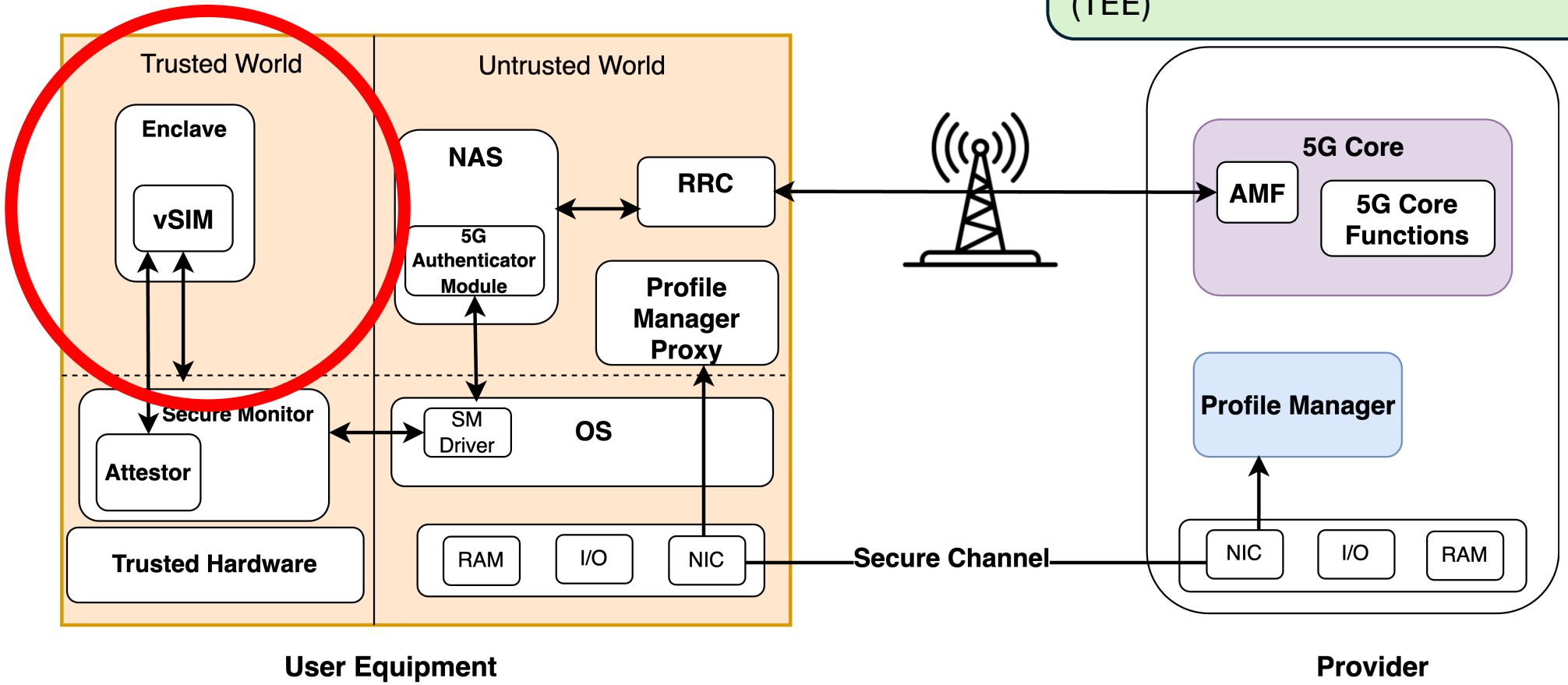
Di5Guise Architecture (4 key aspects)



Di5Guise Architecture (1)

Challenge: how to keep the secret keys secret in software

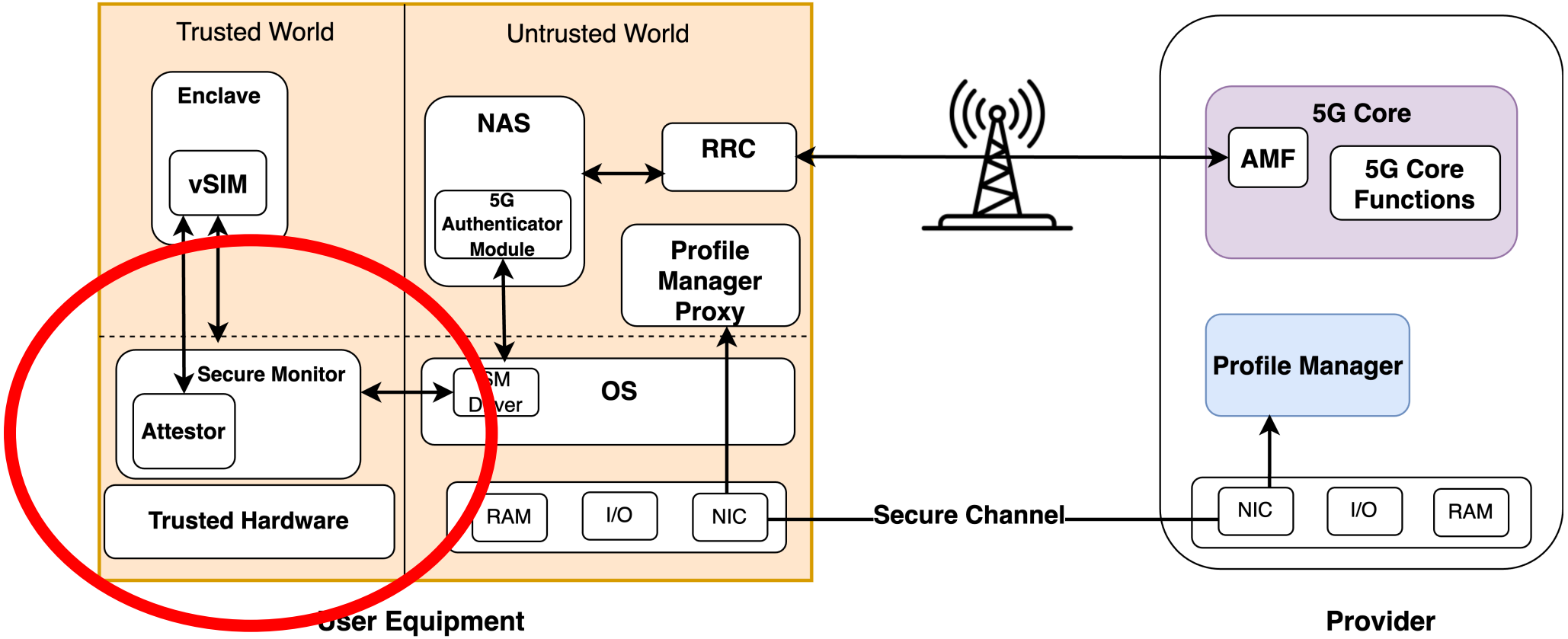
Innovation: Virtualized SIM (vSIM) runs inside of a Trusted Execution Environment (TEE)



Di5Guise Architecture (2)

Challenge: establishing initial trust in SIM

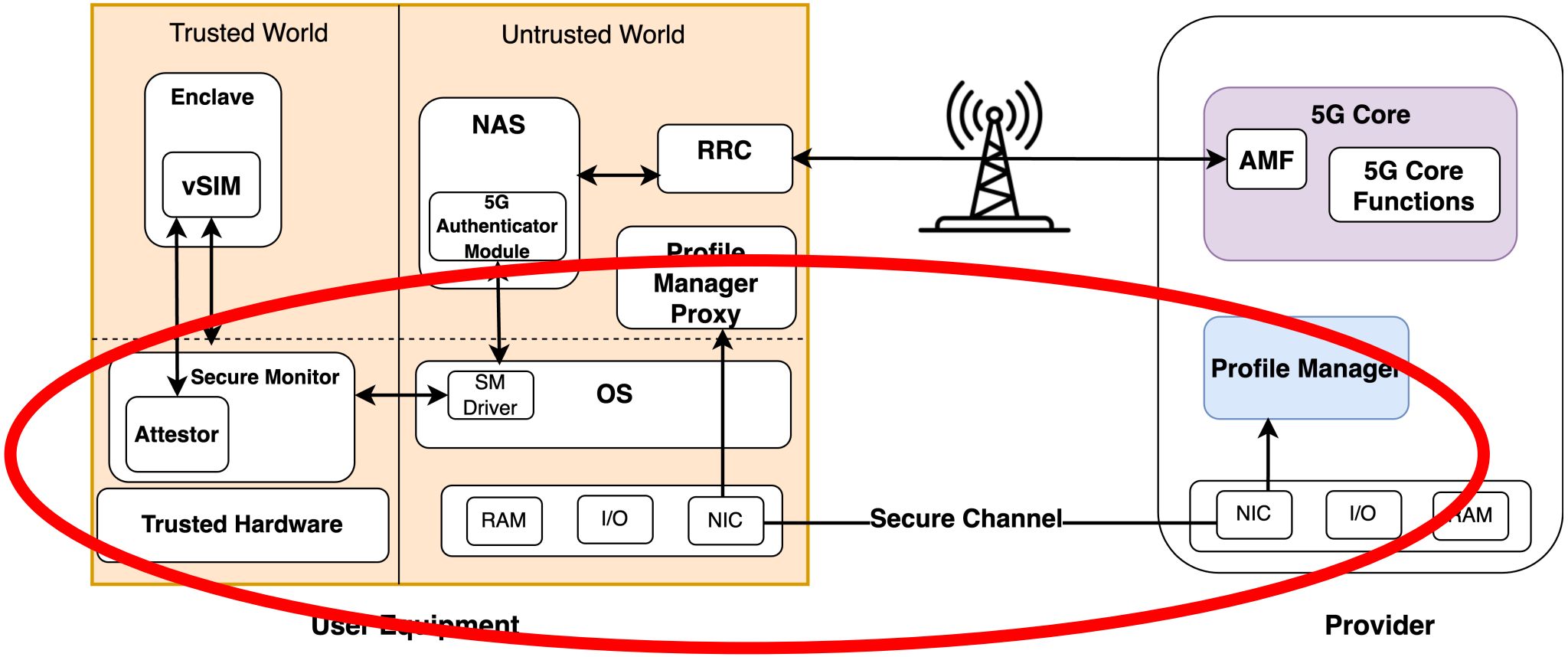
Innovation: Group Keys (trust hw while retaining anon), Secure Boot (known impl.)



Di5Guise Architecture (3)

Challenge: dynamically provision EID/key

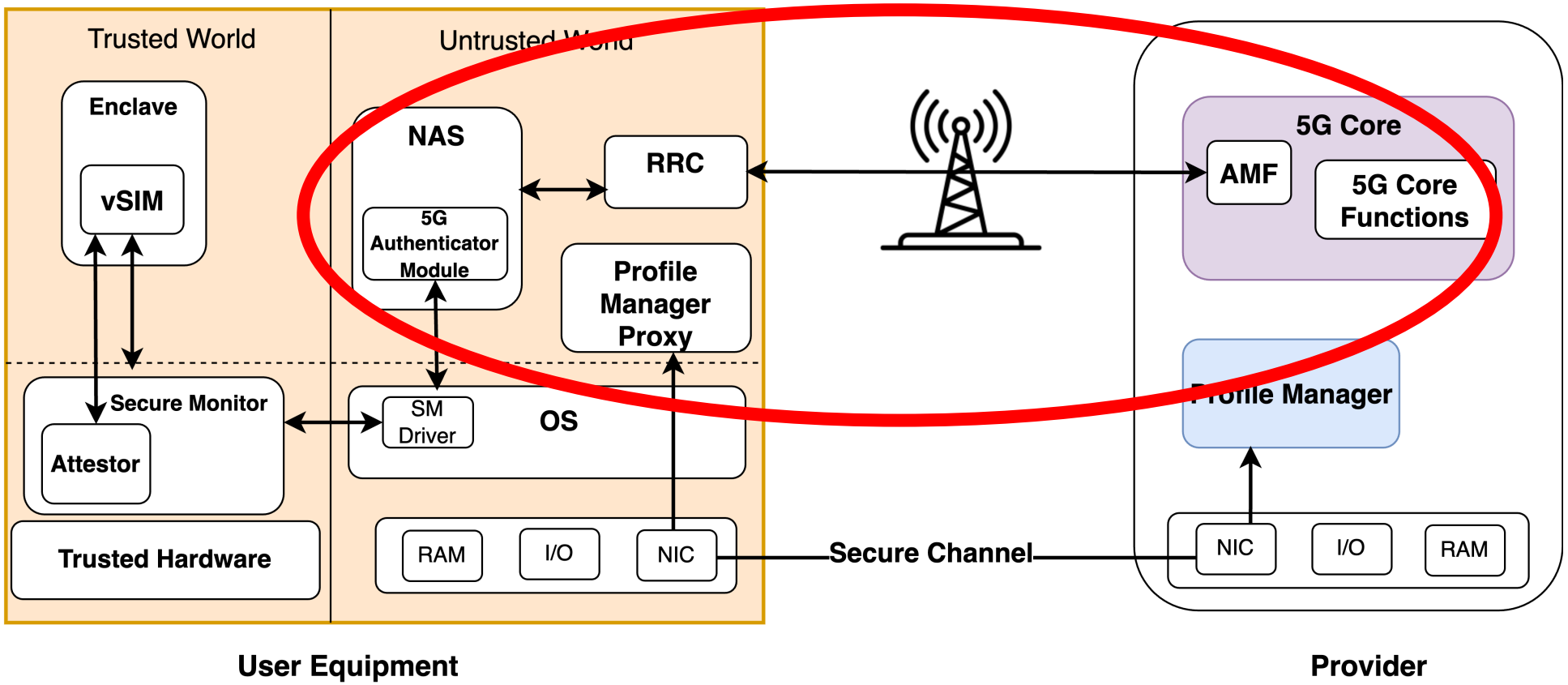
Innovation: Secure Channel, Remote Attestation



Di5Guise Architecture (4)

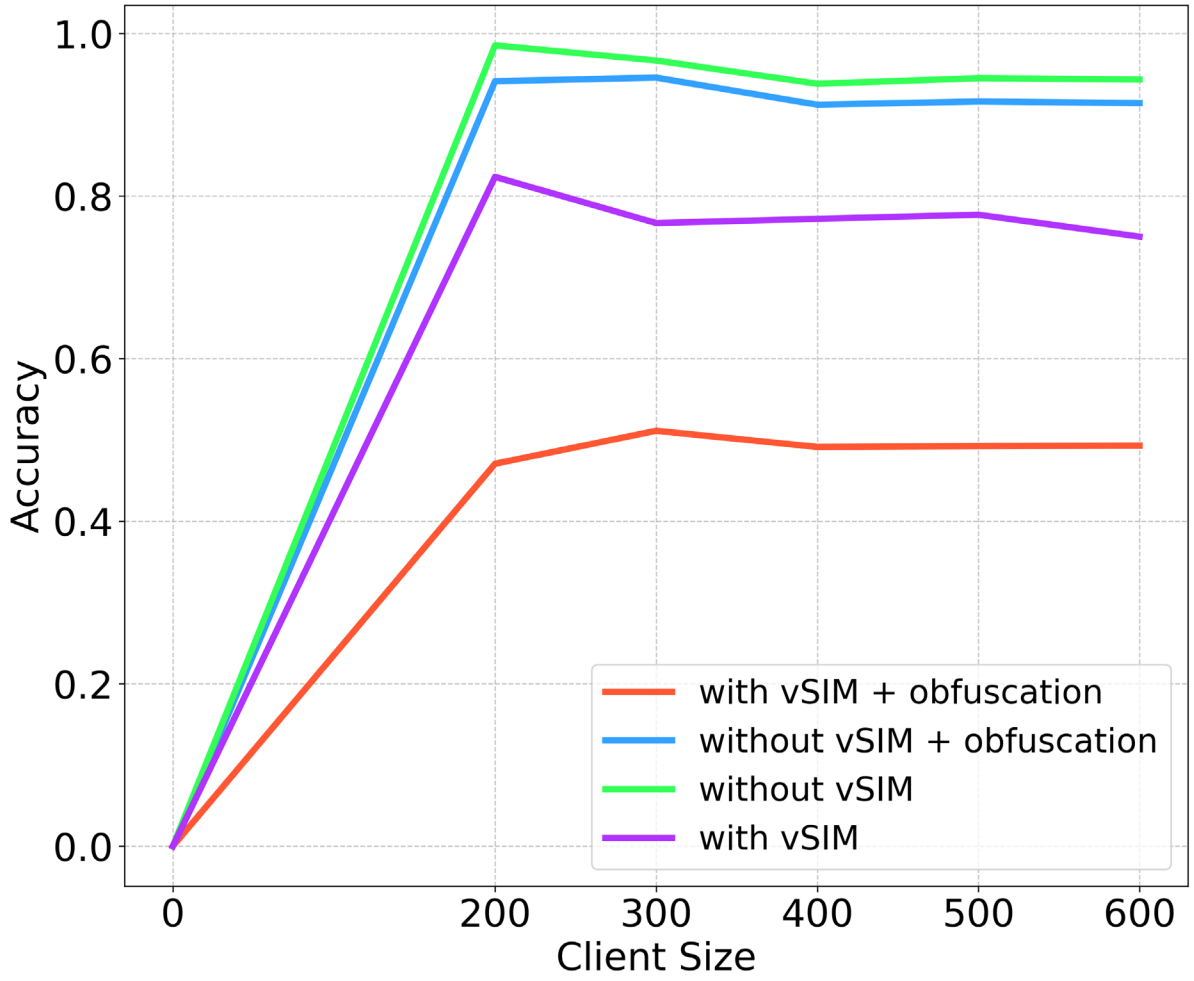
Challenge: dynamically provision and authenticate subscriber

Innovation: Backwards compatible interfaces



Takeaway Evaluation Graph (correlation)

- SIAMHan[USENIX Sec 2024] proxy for live network with changing identifier (every 1-7 days)
- Our use: Dynamically change Device Profile
- Correlation between subscribers drops to 43% (basically guessing)



Conclusion (and Thank You)

Introduced Di5Guise to significantly impair ability of network operator to link various subscriber profiles

See you in the break
(discuss FPGA-based prototype, each challenge, practical considerations, …)

Shirin Ebadi,

Zach Moolman,

Tamara Lehman,

Eric Keller

(eric.keller@colorado.edu)