

Pretty Good Phone Privacy

Paul Schmitt, Barath Raghavan

Tim Wisotzki

OST Plattform Security 2021

Overview

- Problem
- Theory mobile communication
- proposed solution
- discussion
- questions

Problem

A phone exposes the following data:

- location (TA, paging)
- Identity (IMSI, SUPI, IP, etc.)
- Transmitted data (voice, IP, metadata)

these are collected through:

- bulk attacks:
 - internal (providers sell/leak data)
 - locally (scanners)
 - combination (government surveillance)
- targeted attacks (paging)

Theory Mobile Communication I

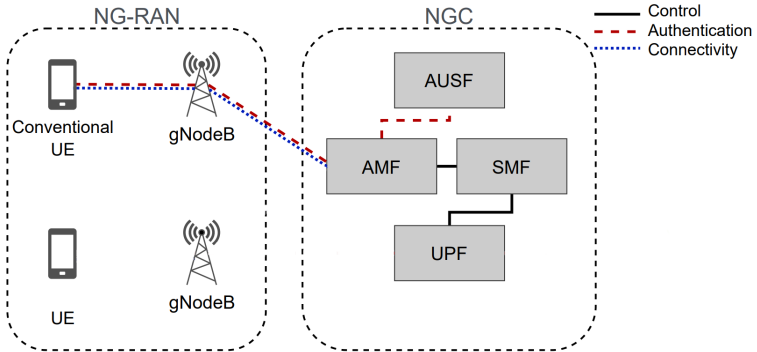


Figure 1: AMF: Access and Mobility Management Function, AUSF: Authentication Server Function, SMF: Session Management Function, UPF: User Plane Function

Theory Mobile Communication II

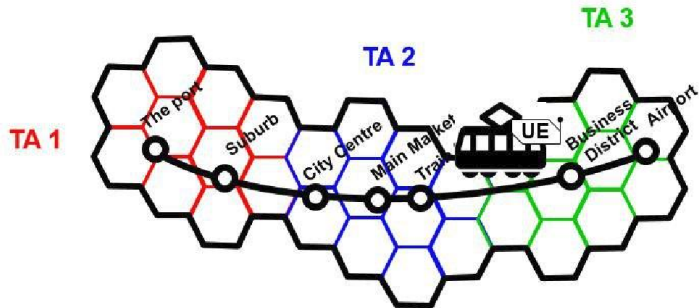


Figure 2: Tracking Areas

Proposed solution

goals:

- decoupling identity/location from connection
- no changes to
 - physical infrastructure
 - latency
- no direct cooperation from current operators
- provide “pretty good” privacy to users

primary changes:

- provide identical SUPI to all
- bigger TA

solution: identity protection

nullify SUPI:

- only proves valid SIM (Subscriber Identity Module)
- assign IP and GUTI (Globally Unique temporary identifier)
- post-attach to PGPP-GW

authentication goals:

- authenticate that user is valid customer
- preserve anonymity
- verify that user is unique (no shared credentials)

solution: PGPP tokens

Receiving tokens:

- tokens represent access unit
- users generate their tokens and get them signed anonymously
 - using adjusted Chaum's classic scheme

Authentication:

- PGPP-GW verifies signature to allow access
- process is automated with an agent on the device

solution: architecture change

MVNO (Mobile Virtual Network Operator) runs PGPP

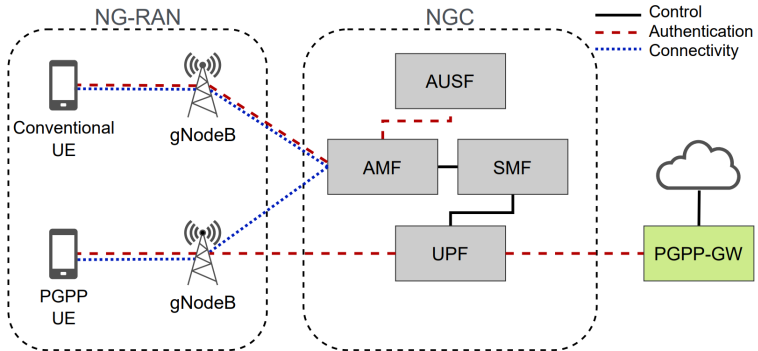


Figure 3: PGPP architecture

solution: location protection

extend TA with TAL

- bigger area -> less information
- generate a unique list per user and attachment

increased traffic load:

- more control messages are send
 - reduced capacity
 - higher latency

Discussion I

Did they fulfill their goals?

- decoupling identity/location from connection
- no changes to
 - physical infrastructure
 - latency
- no direct cooperation from current operators
- provide “pretty good” privacy to users

Discussion II

Limitations:

- only for data
- 5G provides increased privacy
 - SUCI (Subscriber Concealed Identity)
- PGPP providers are assumed trustworthy
- lack of technical description
- requires user participation

Questions

Any questions?

sources:

- paper: Pretty Good Phone Privacy
- picture: apistraining.com