Scaling up baseband attacks:

More (unexpected) attack surface

Black Hat USA 2012

2012-07-25

36.117038, -115.174562

Ralf-Philipp Weinmann
SnT, University of Luxembourg
<ralf-philipp.weinmann@uni.lu>

UNIVERSITÉ DU LUXEMBOURG

Security issues with SUPL implementations

Black Hat USA 2012
2012-07-25
36.117038, -115.174562

Ralf-Philipp Weinmann
SnT, University of Luxembourg
<ralf-philipp.weinmann@uni.lu>

UNIVERSITÉ DU LUXEMBOURG

whoami

- Ralf-Philipp Weinmann
- Research associate at the University of Luxembourg
- Ph.D. in cryptology
- After Ph.D. interest shift towards mobile/ embedded security and digital privacy
- PWN2OWN
- Co-author of iOS Hacker’s handbook

UNIVERSITÉ DU LUXEMBOURG

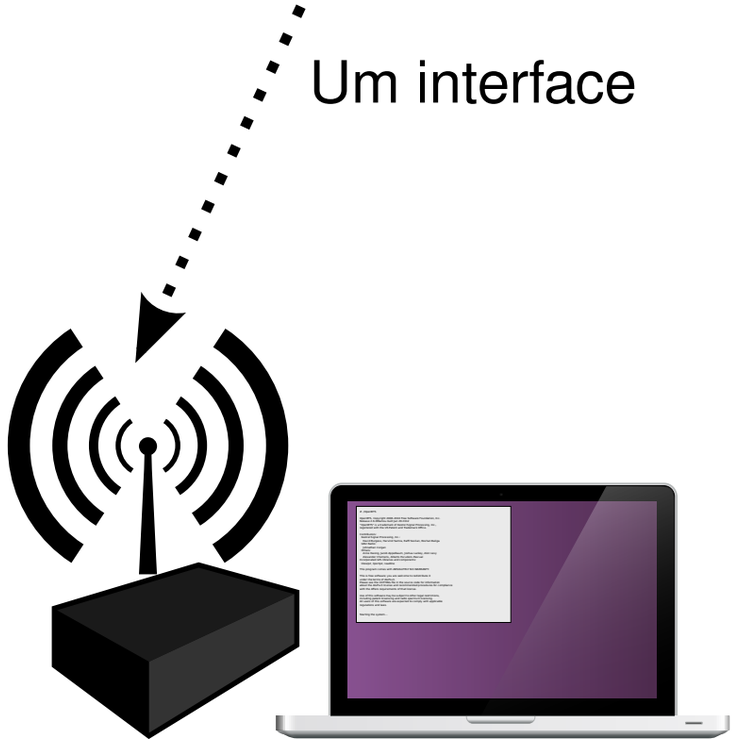
Overview

- Quick intro: baseband attacks
- GPS basics
- How does A-GPS work?
- A-GPS, an attack vector?
- An attack scenario on SUPL
- SUPL processing in the baseband
- Conclusions

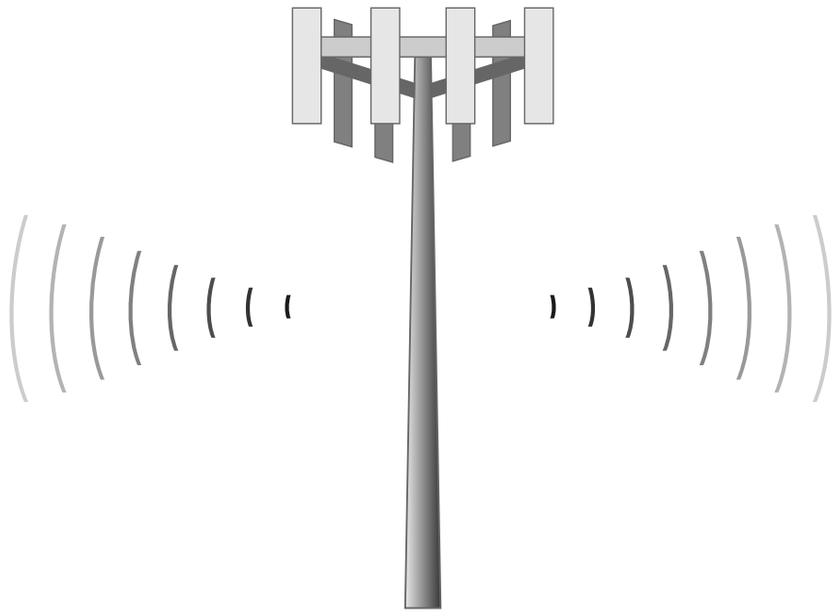
Baseband attacks

Target cellphone

Um interface



Rogue BTS operated by attacker

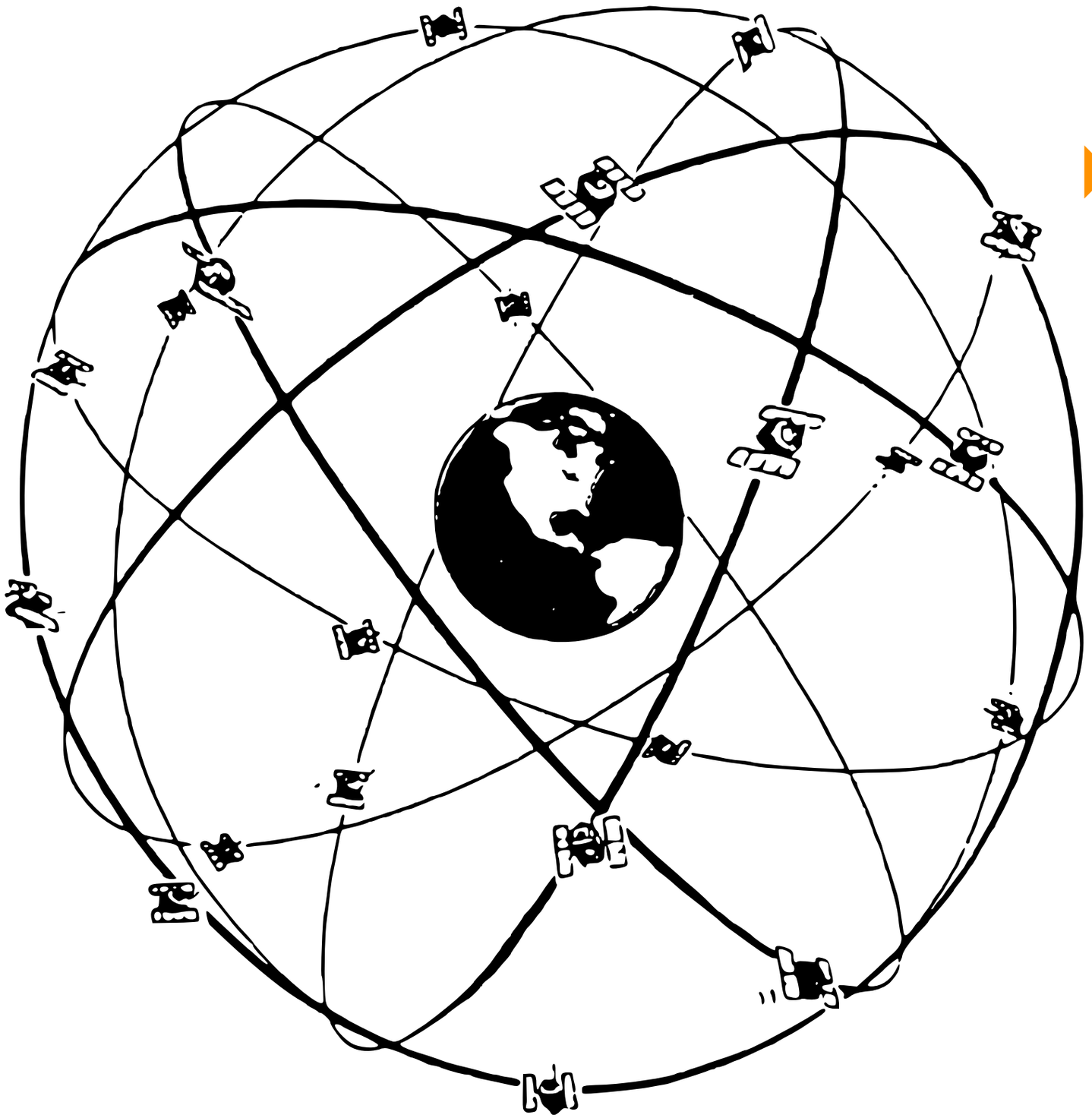


Legitimate BTS operated by carrier

This talk: special case that opens attack surface in baseband over a TCP connection. No control over a BTS needed.

UNIVERSITÉ DU LUXEMBOURG

NAVSTAR GPS



- Transmit messages with:
  - Accurate time stamp
  - Satellite position at time of transmission

More data transmitted

- GPS ephemeris:
  - Params of equations for sat. orbit model
  - Clock offset data
    UTC offset, time of week, submillisecond satellite clock offset, clock offset rate, clock offset acceleration
- GPS almanac [valid for approx. 180 days]:
  - Simplified ephemeris of all satellites; coarse, accuracy of several kilometers

GPS basics

- To ground observer: each satellite on a different frequency due to Doppler shift
- Without knowledge of location, Doppler shift cannot be computed
- Exhaustively search all frequencies
  - This is why a cold-start GPS lock takes time

Standalone GPS

- Compute distance to satellites
- Determine satellite positions from ephemerides
- Calculate its own position by solving equations in 4 variables (position and time)

Challenges

- GPS satellites at altitude of approx. 20km, moving at 5km/s
- Received signal very weak (10^{-16} W)
- Data transmission is slow (50 bits/sec)
- GPS almanac is 15000 bits [25 frames]
  - only 1/25 of almanac per 1500 bit frame
  - transmission takes 12.5 minutes

GPS aiding

- Control Plane
  - Radio Resource Location Protocol (RRLP)
  - IS-801 [CDMA]
  - Radio Resource Control (RRC) in UMTS [Type 15 SIBs, 3GPP 25.331]
  - LTE Positioning Protocol (LPP)
- User Plane:
  - OMA Secure User Plane Location (SUPL)
  - v1.0 - v3.0

AGPS modes

- **MS-based:**
  - MS requests assistance data from network/ server
  - MS computes its own position
- **MS-assisted:**
  - MS requests assistance data from network/ server
  - MS sends measurements
  - server/network sends computed position to MS

Location requests

- MO-LR: mobile-originated location request
  - example: opening mapping or navigation application on phone
- MT-LR: mobile-terminated location request
  - third-party service requesting location
- NI-LR: network-initiated location request
  - usually used for emergency services

Advantages of SUPL

- Control Plane aiding requires upgrades to many elements of the carrier's core network
- SUPL allows to keep carrier investments small
- More flexibility than control-plane protocols

SUPL transports

- TCP (secured with SSL)
- UDP
- SMS
- WAP PUSH
- SIP PUSH (for LTE)

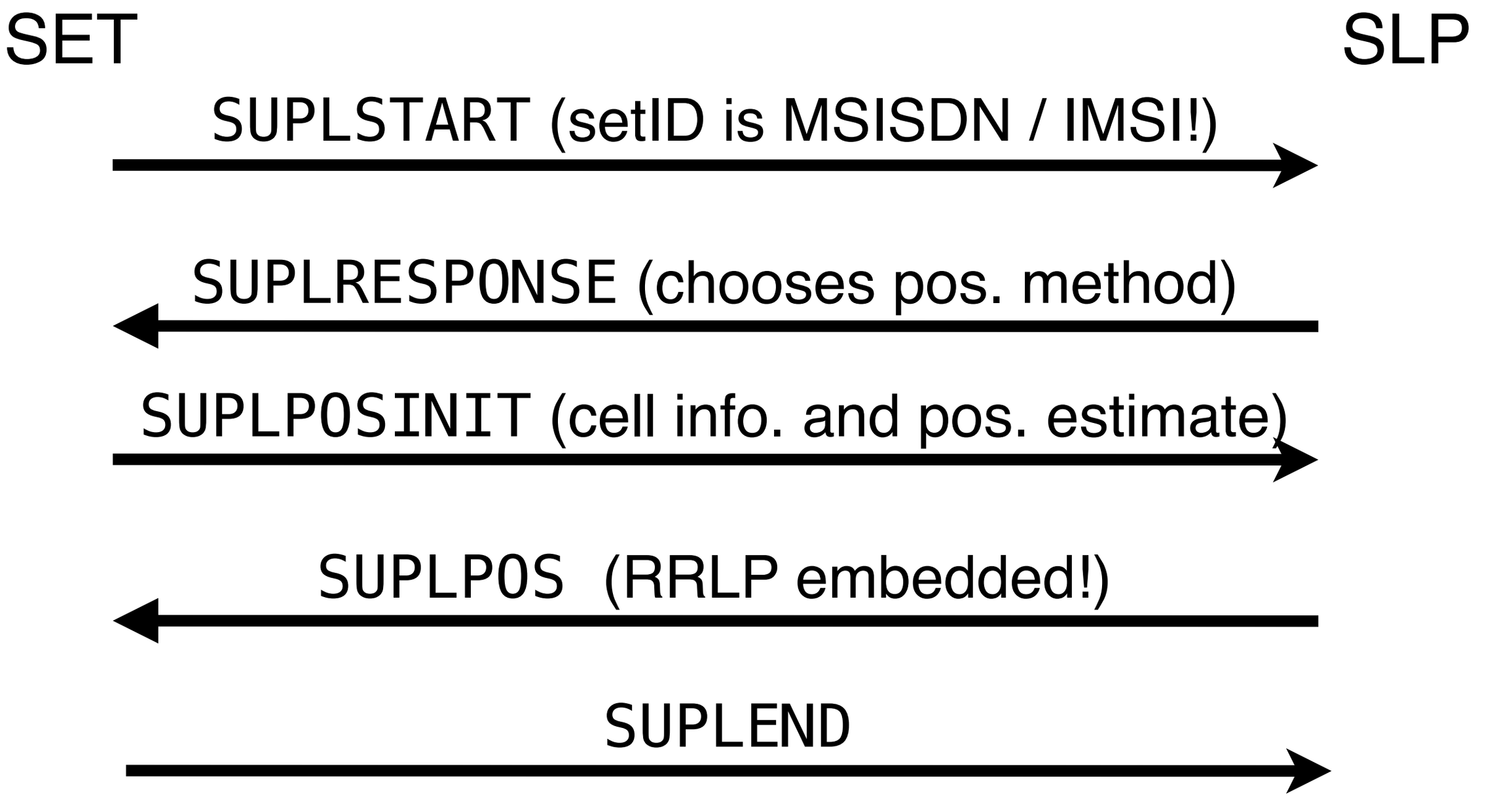
SUPL v2

- Fun features:
  - periodic trigger
  - area-based trigger (geo-fencing)
  - third-party queries
- Support of WLAN, WiMAX, TD-SCDMA, LTE
- Support of A-GANSS (Galileo)

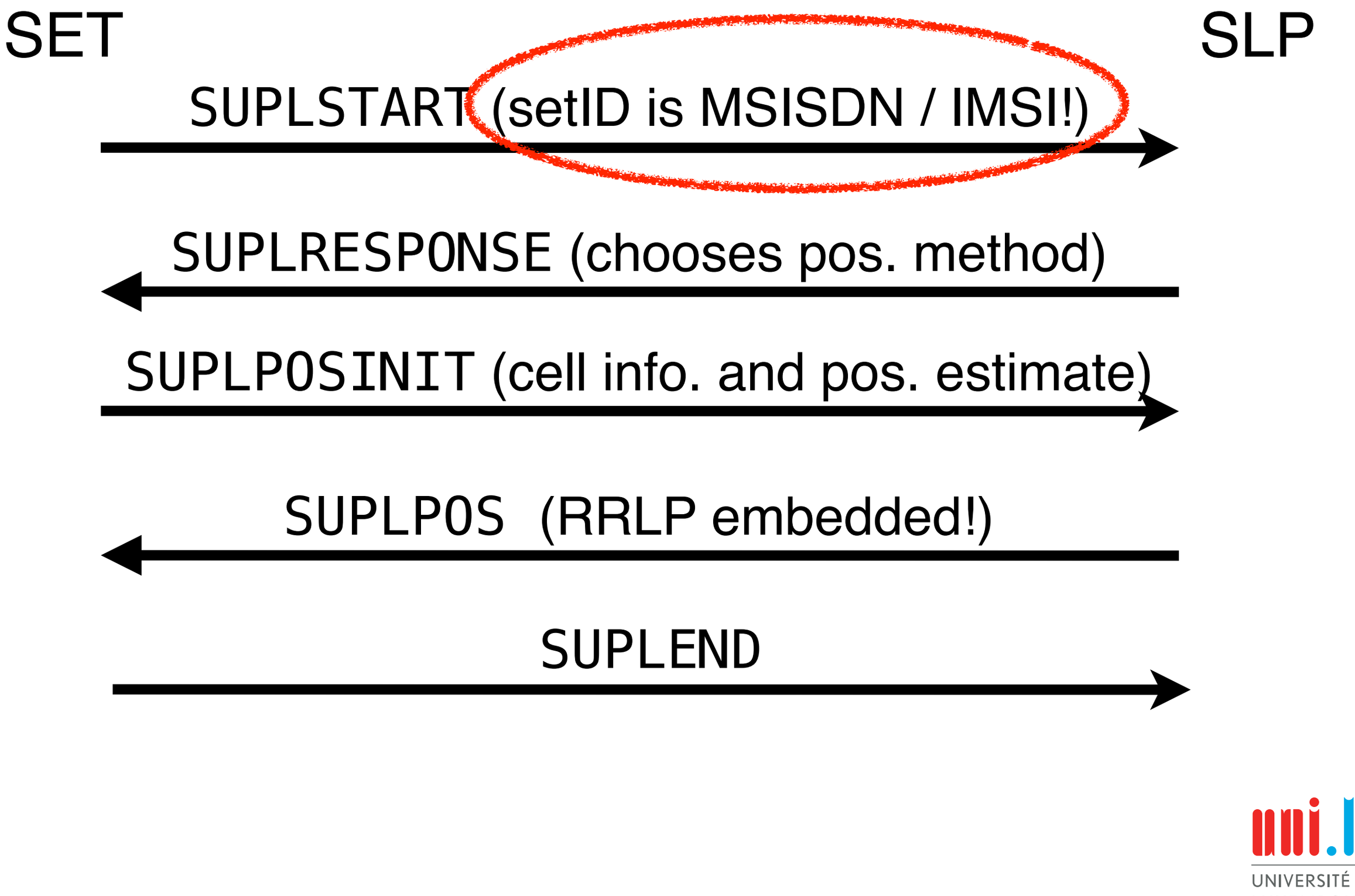
Privacy

- SUPL allows user notifications
- At the same time, there is a flag for a *“privacy override”*
- In a NI scenario, setting a privacy override will cause user’s decision to be ignored

Example SUPL flow



Example SUPL flow



Implementations

- SUPL implementation done by the OEM
- Different components involved, usually
  - Application processor (for TCP/IP)
  - Baseband processor
  - GPS chip

SUPL servers

- Oldschool: `h-slp.mnc`*`xxx`*`.mcc`*`yyy`*`.pub.3gppnetwork.org`
  - AT&T: `h-slp.mnc410.mcc310.pub.3gppnetwork.org`
    - operated by carriers
    - MNC/MCC derived from IMSI
    - not widespread in Europe
- Many Android handsets: `supl.google.com`
- Nokia: `supl.nokia.com`

A-GPS on Android

- `/etc/gps.conf` [exemplary]:

```
SUPL_HOST=supl.google.com
SUPL_PORT=7275
```

← SSL port is on 7276!

- `/system/lib/hw/` usually contains some `.so` with vendor interface code

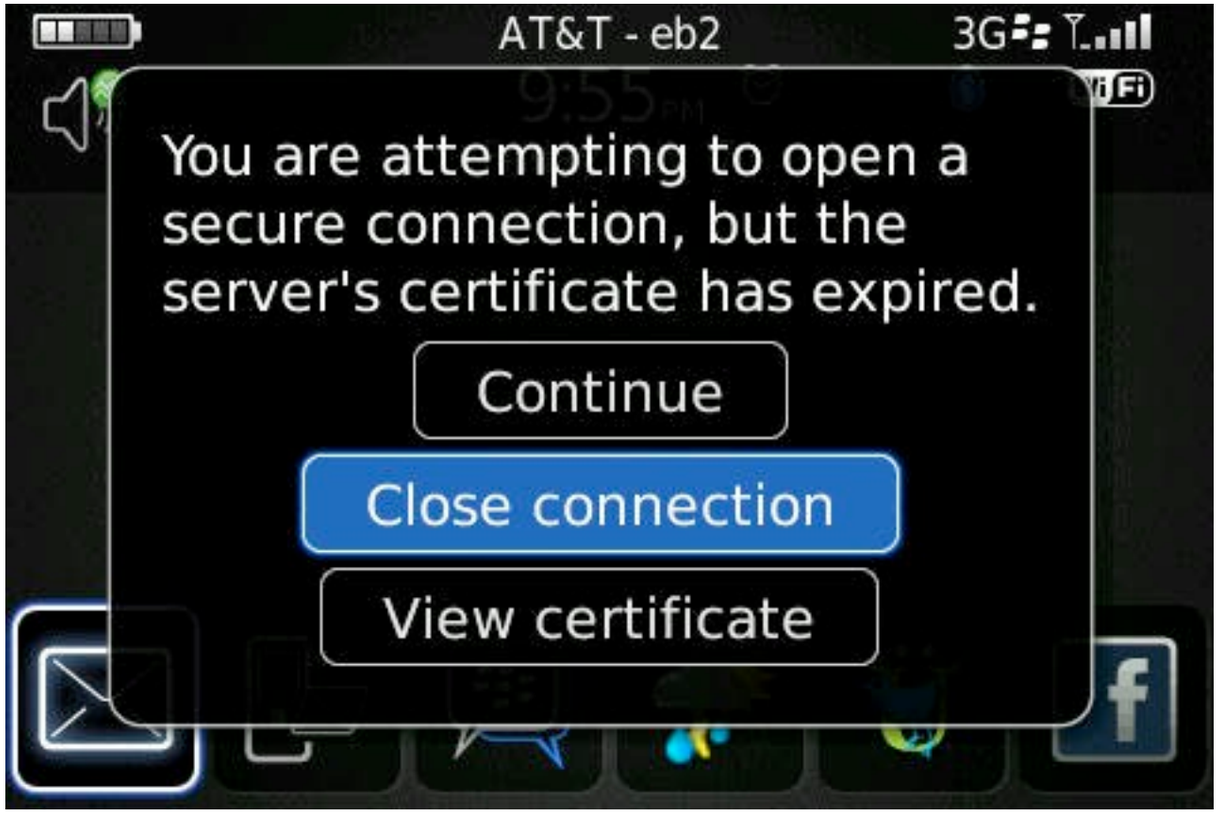
Abusing SUPL

- Although SSL is mandatory for transmitting ULP over TCP, it is often not used
- Even if implementation does use SSL, more often than not this happens:
  - [ ] Certificate checks
- DNS spoofing:
  - 0x20-bit encoding and source port randomness hopefully implemented on most carriers' DNS caches

Android attack scenario

- Announce `attwifi` or other commonly used hotspot
- Wait for target to connect to network
- Resolve any query with CNAME to `supl.google.com`
- Resolve `supl.google.com` to A record with high TTL pointing to own supl-proxy server
- Track target over live of TTL
(no reboots assumed)

Locking it down tight

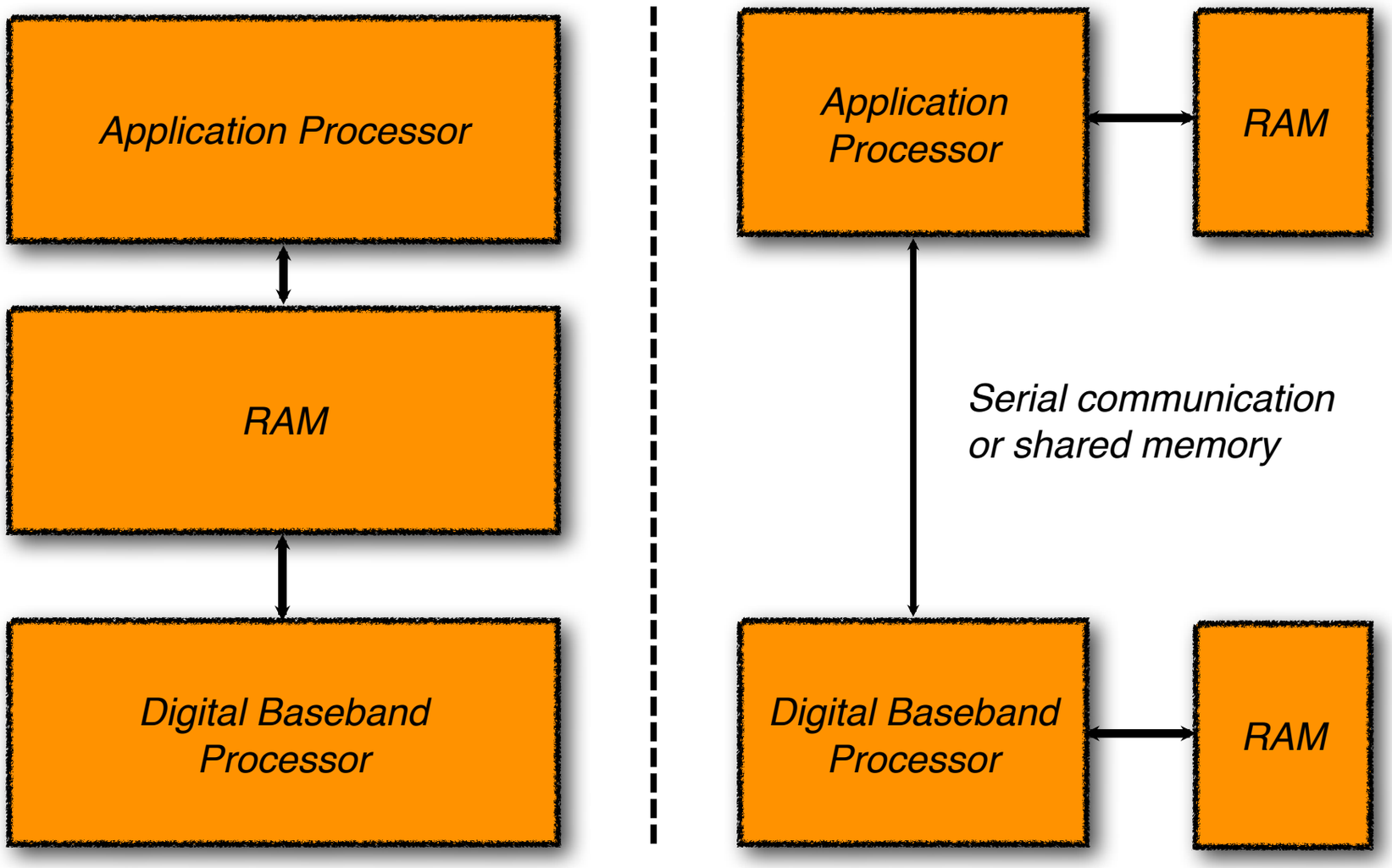


from http://forums.crackberry.com/blackberry-bold-9000-f83/annoying-certificate-expired-popup-270587/

Apparently the certificate for AT&T's SUPL server was expired for some time in July 2009 :)

Basebands?

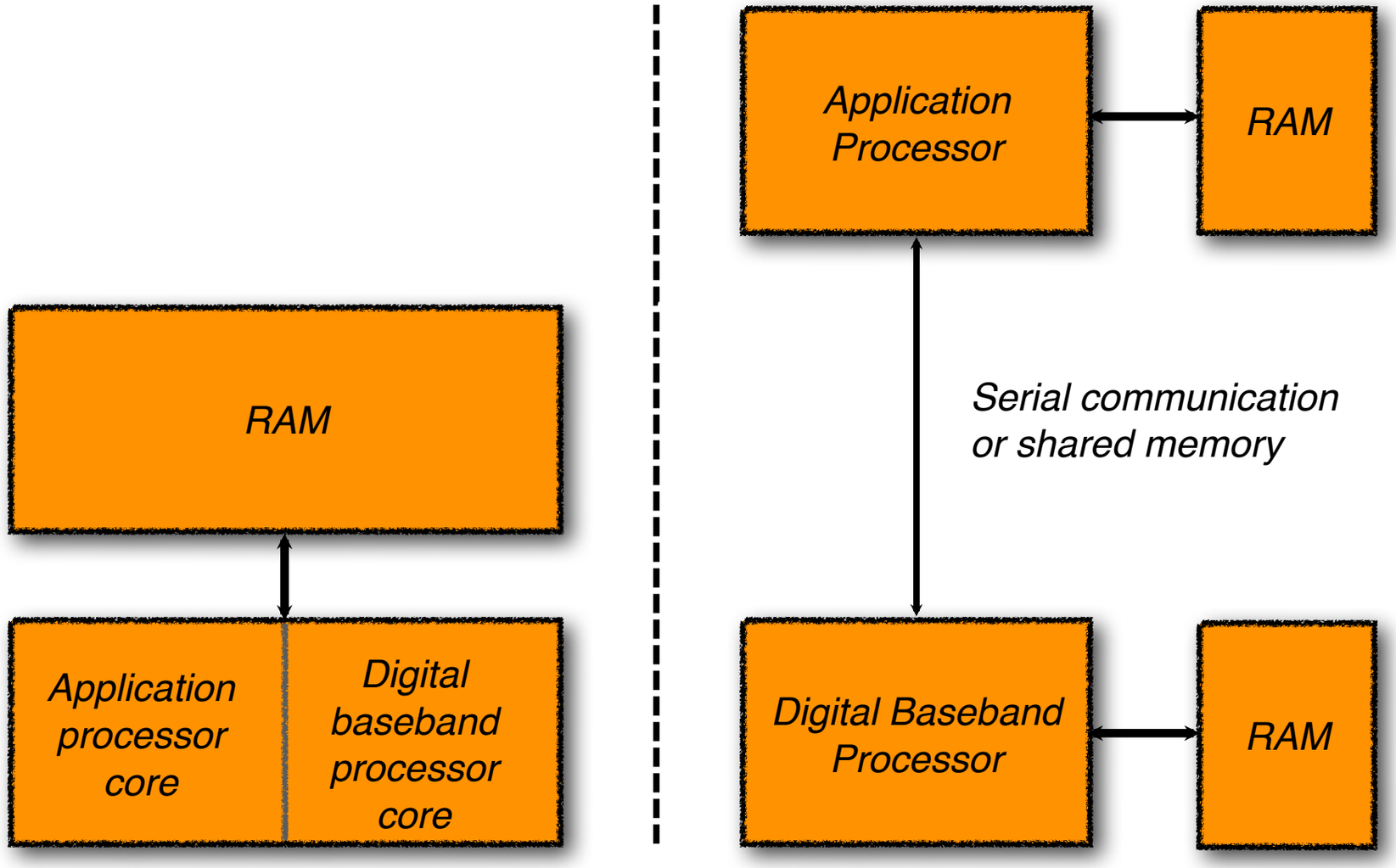
Smartphone anatomy



Shared memory architecture

Baseband as modem

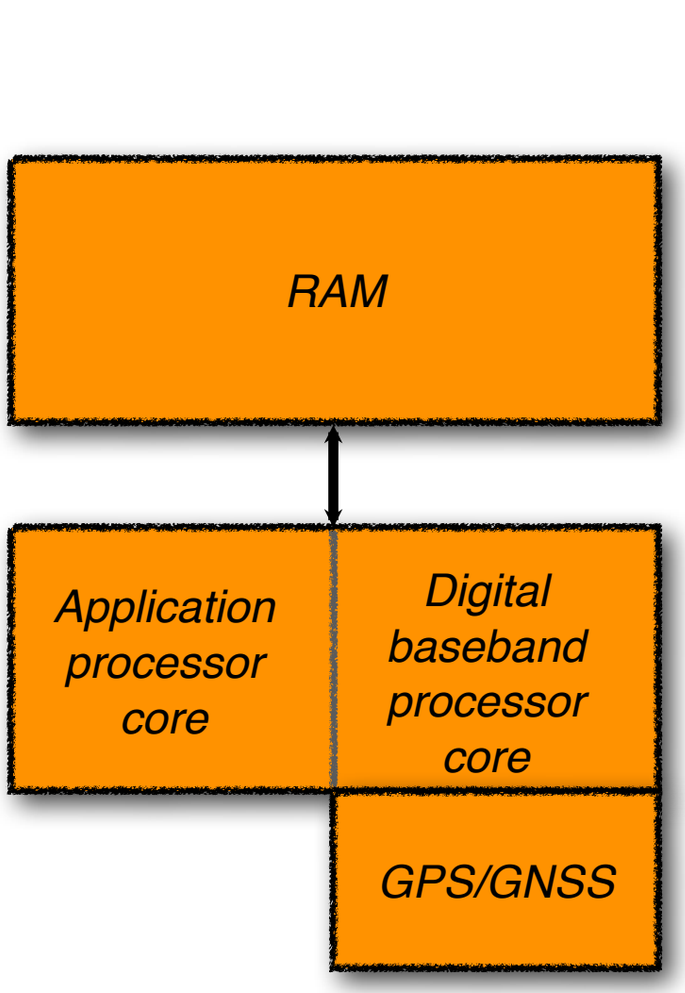
Smartphone anatomy



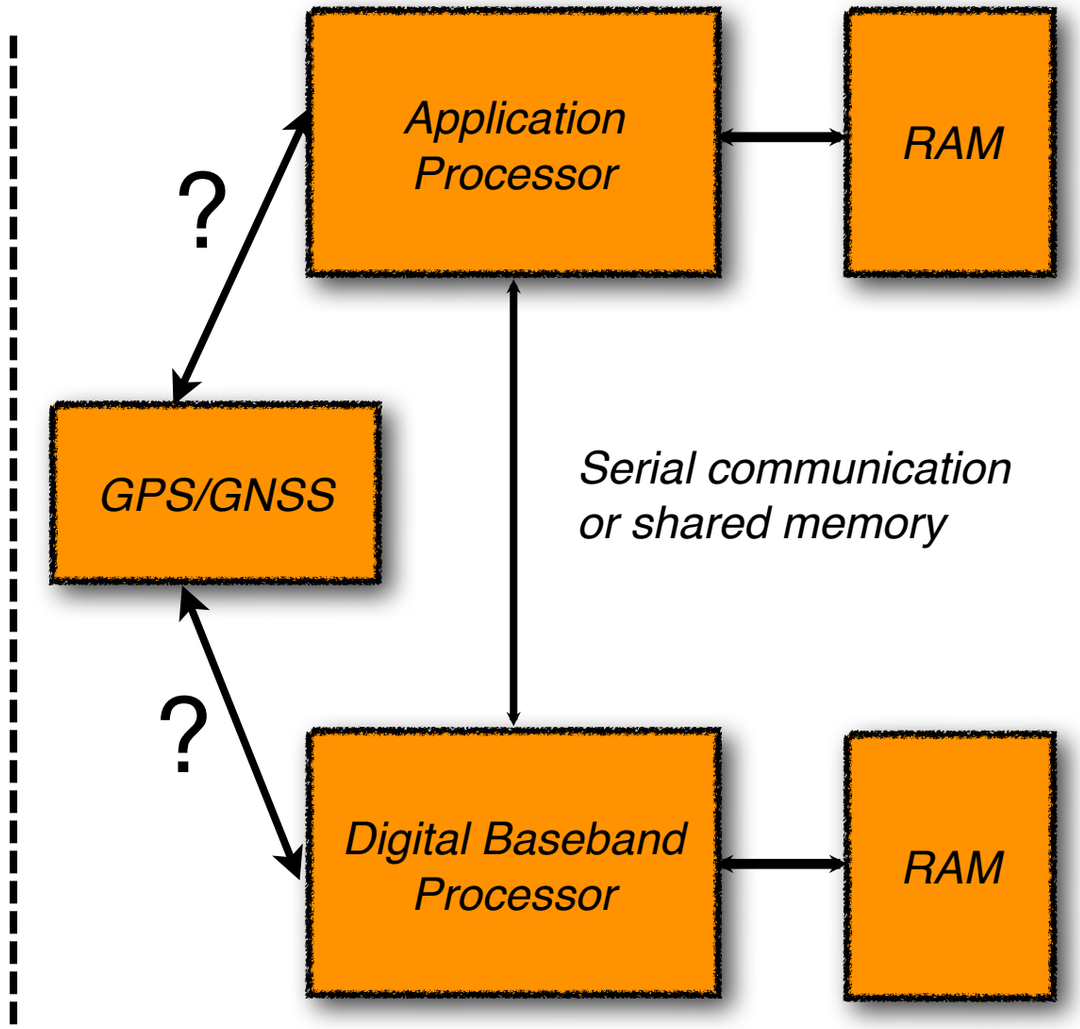
Shared memory architecture

Baseband as modem

Smartphone anatomy



Shared memory architecture

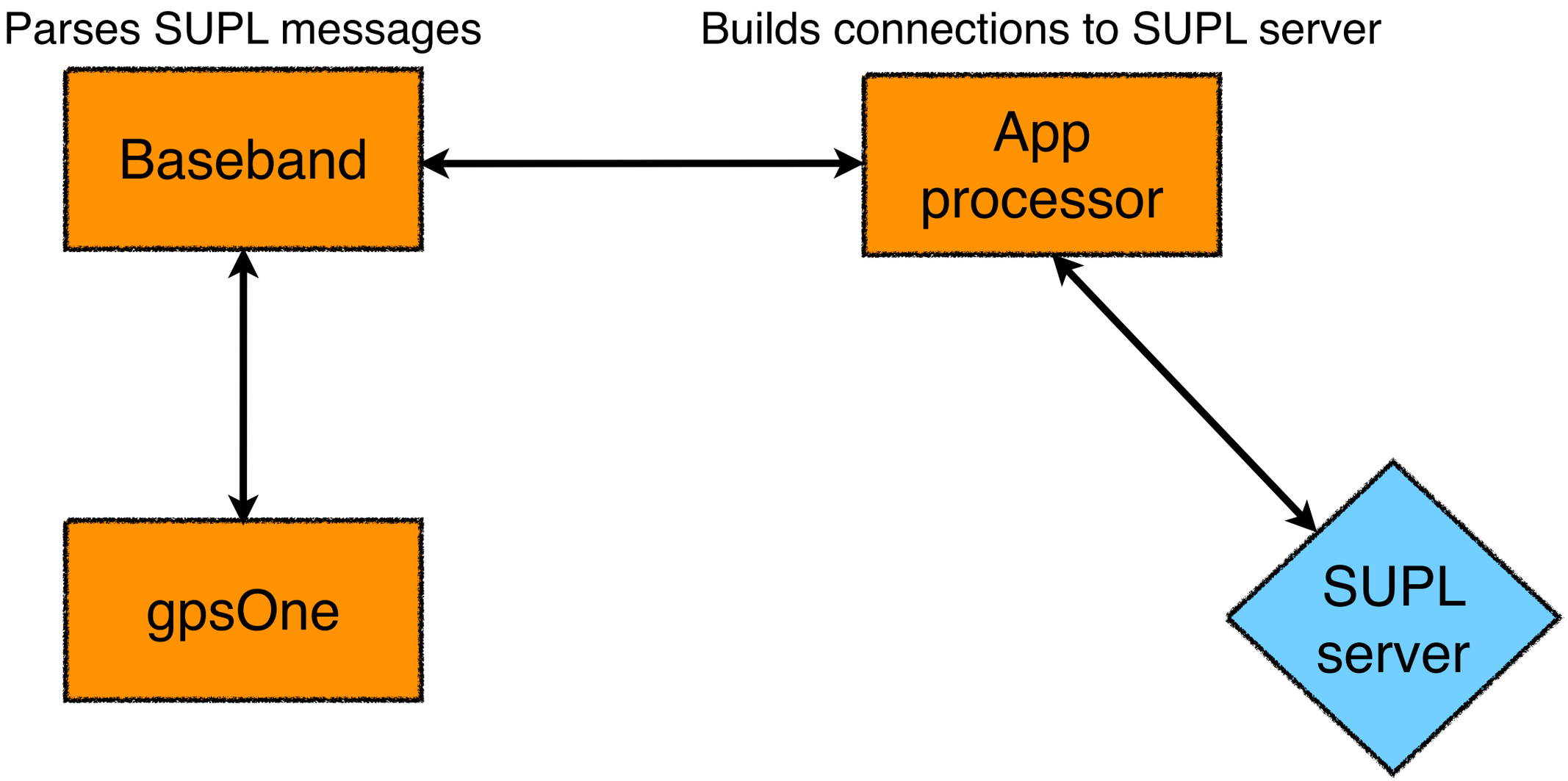


Baseband as modem

Qualcomm's gpsOne

- > 400 million handsets with gpsOne chipsets
- > 50 mobile operators offer handsets with gpsOne technology
- > 40 OEMs/ODMs produce handsets with gpsOne technology
- Reason for success: high integration
  - GPS integrated into MSM chip
  - No separate RF chip required for GPS

Qualcomm's gpsOne



Baseband bugs found

- Buffer overflow when parsing WAP PUSH SUPL messages. Somewhat difficult to exploit. Already fixed in recent handsets (hence assumed to be fixed in upstream as well).
- Potential bug in IS-801 parsing. If exploitable, only affects CDMA handsets, though. [Edit after BH: unclear whether code path can be triggered]

SUPL on the AP

- SET implementations apparently written by OEM (handset manufacturer)
- On Android: services parsing SUPL messages restart after crash (ex. `glgps` on Samsung phones)
- OS mitigations apply to those daemons, though

Good news for defenders

- Attack surface is small at the moment
- Baseband attacks over carrier infrastructure can be detected by carriers
- Privacy problems fixable, but don’t count on it

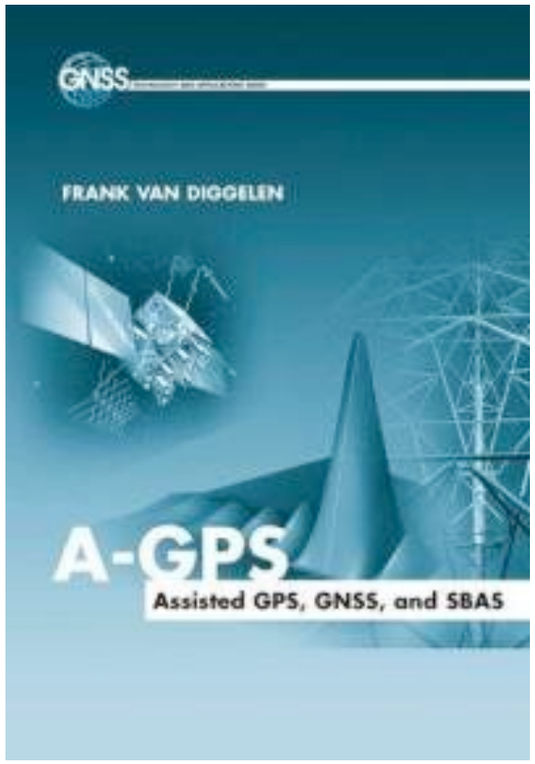
General observations

- Baseband attacks are getting harder
- Many bugs have been / are being killed
- Especially Qualcomm stands out here
- Mitigations are being added
- Qualcomm’s LTE chips moves AMSS to Hexagon DSP architecture. Fun times!

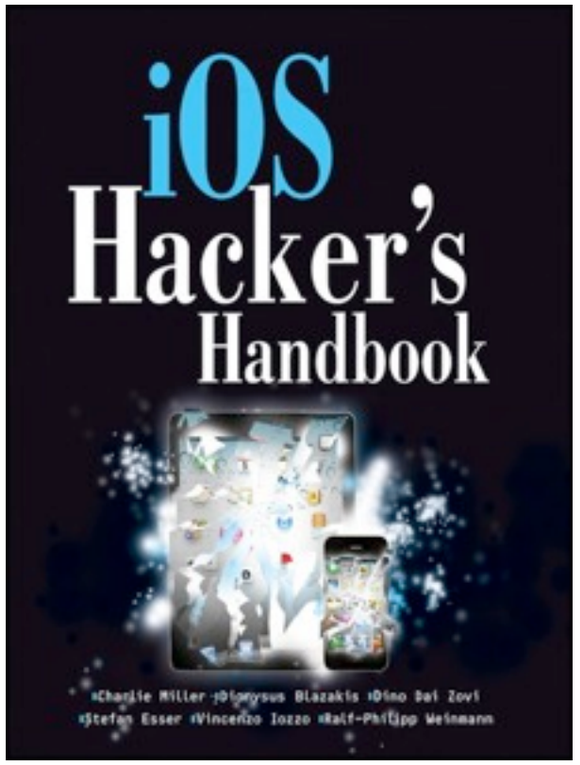
TCP/IP in the baseband?

- Haven't found TCP/IP in baseband stacks of GSM/UMTS smartphones [haven't looked much at LTE firmware yet].
- TCP/IP is often found on running on the baseband chip of M2M devices
- Don Andrew Bailey has some cool upcoming work on long-range attacks against these!

Book recommendations



Frank Van Diggelen: *A-GPS: Assisted GPS, GNSS, and SBAS*, Artech House Publishers, ISBN 1596933747, 2009



Charlie Miller, Dion Blazakis, Dino Dai Zovi, Stefan Esser, Vincenzo Iozzo, Ralf-Philipp Weinmann: *iOS Hacker's Handbook*, Wiley Publishing, ISBN 1118204123, 2012