FOS LTE IMSI CATCHER

DOMI

WARNING!

This talk will be about classic IMSI catchers – do not expect MITM calls, data etc.

GSM IMSI catcher - recap

- Create a fake BTS with
  - high reselection value (C1, C2)
  - random location area code
- Phones will connect and initiate Location Update
- Reply with Identity Request (request IMSI)
- After getting the IMSI send LU Reject – cause 13 or any other depending on your intention

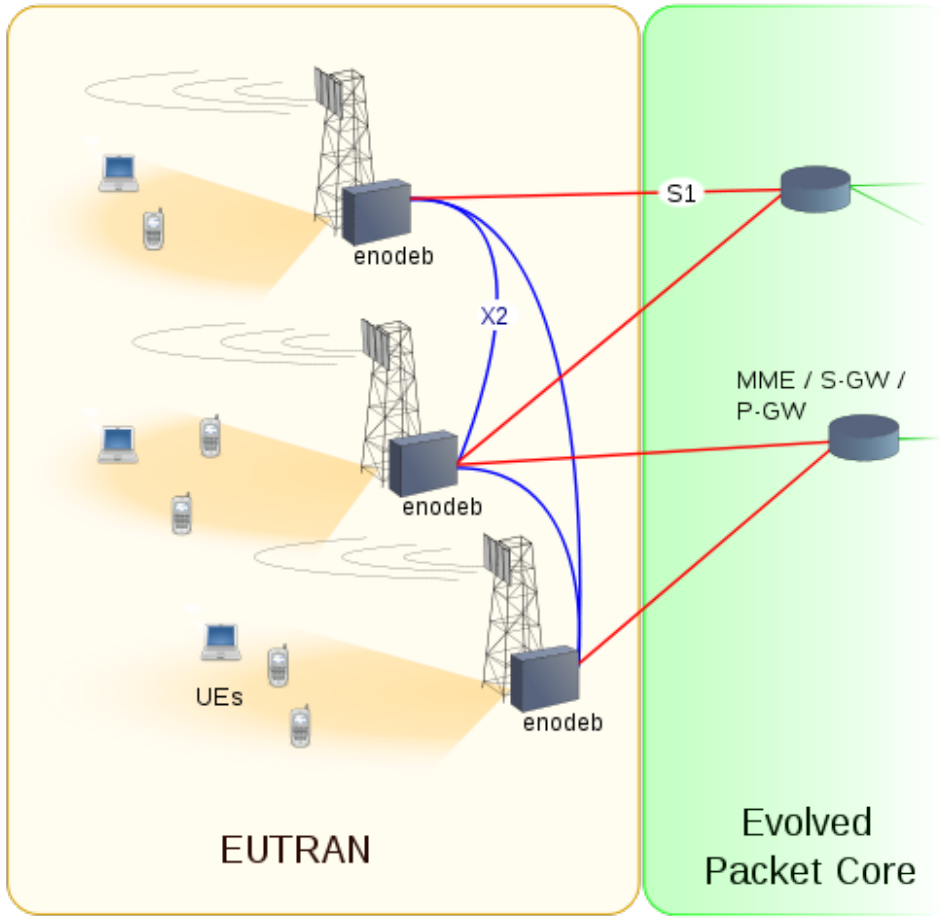
Why could we do this?

No mutual authentication, the network is always trusted

Reject messages need to be unencrypted

(Sh*tty or null crypto also lead to MITM etc.)

LTE Architecture



INTERNET
PSTN
PLMN

Changes in LTE

- Mutual authentication
- Integrity protection
- Better crypto

Procedure improvements

- Most procedures require AS security enabled (integrity protection)
- UEs drop non-protected messages once they have established security context

- Should be fine, right?


NOPE!

Tiny little protocol problem…

Tracking Area Update Reject

- UE sends a Tracking Area Update Request
- Rogue eNodeB rejects it with cause 9

#9 (UE identity cannot be derived by the network);

The UE shall set the EPS update status to EU2 NOT UPDATED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and eKSI. The UE shall enter the state EMM-DEREGISTERED.

If the rejected request was not for initiating a PDN connection for emergency bearer services, the UE shall subsequently, automatically initiate the attach procedure.

3GPP TS 24.301 -5.5.3.2.5

Catching the IMSI

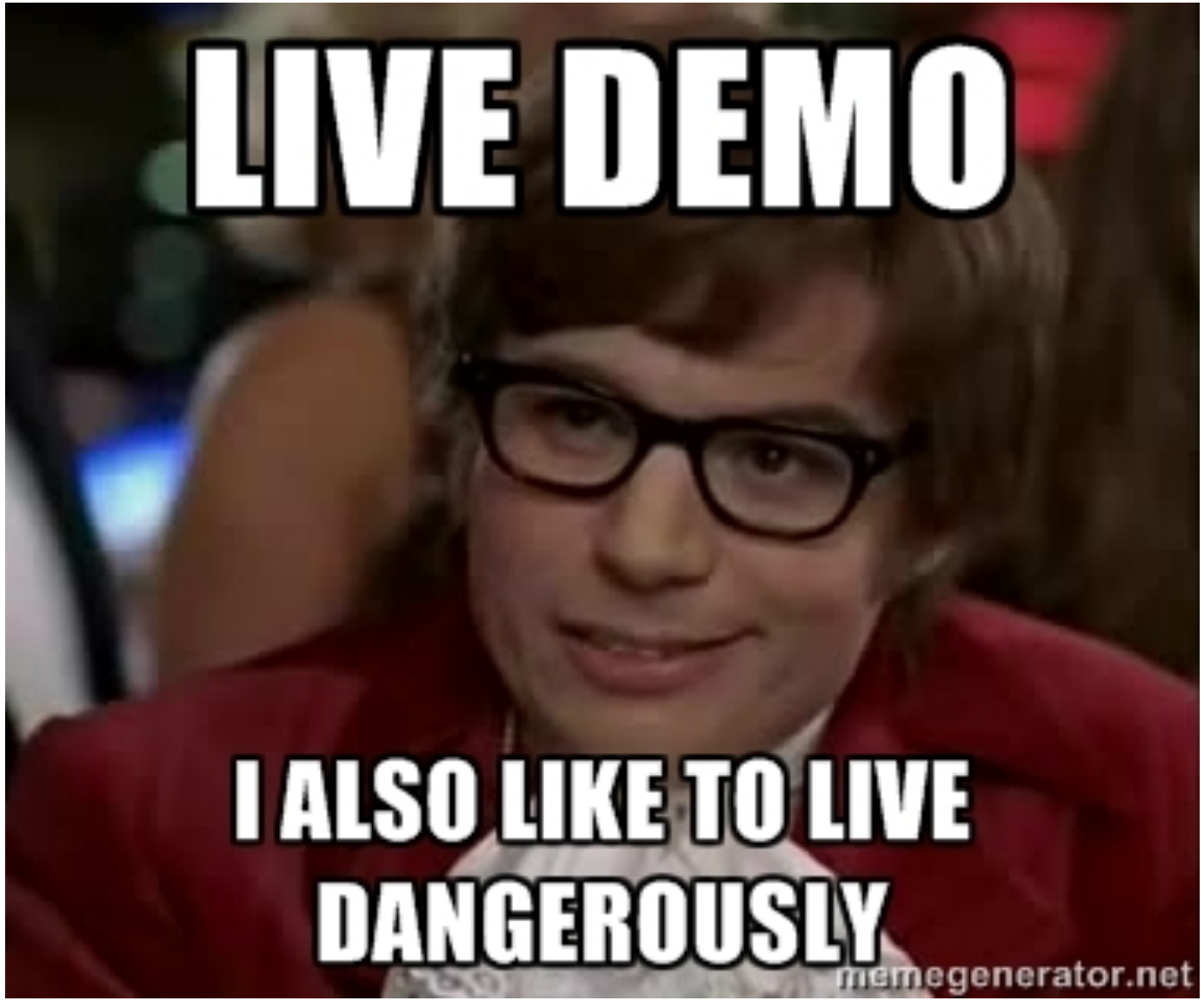
- No more key/security context in UE
- UE will initiate attach
- It is allowed to ask for its IMSI in an IDENTITY REQUEST
- After getting it we send an ATTACH REJECT with cause #12 (Tracking Area not allowed)

HW and SW

- USRP and laptop
- Many open source LTE projects (this is AWESOME btw):
  - openLTE
  - OpenAirInterface
  - srsLTE and srsUE
- Own implementation of MME/core network (pending request to open source it)

Rogue eNodeB

- Need to somehow ‘lure’ UEs
- In GSM you just needed a neighbor cell’s frequency + high reselection value
- In LTE a list of frequencies are broadcasted with their priorities –> you need to decode the list, and select the frequency with the highest priority


LIVE DEMO
I ALSO LIKE TO LIVE DANGEROUSLY
memegenerator.net

These People are great! *APPLAUSE*

- Ravishankar Borgaonkar and Altaf Shaik for discovering the TAU Reject vuln (and many other problems) in LTE
- Benoit Michau for the library my core network is based on
- Philippe Langlois and Elvis Pfützenreuter for pysctp

- My mentors during my internship at Qualcomm: Kevin Redon and Nico Golde

Q & A

Thank you!

Key-ID: E2712651

Fingerprint: 811C3FC3CFCB16E4BAEBF5FB7440DF59E2712651