IMSI Catcher
with OpenBTS and USRP

GSM (2G cell network) Identifiers

- IMEI:
  - International Mobile Equipment Identifier
  - Identifies a handset. Easily changed, illegal to do so.
- IMSI:
  - International Mobile Subscriber Identifier
  - Secret? Kind of.
  - Identifies an account - stored in SIM (Subscriber Identification Module) card.
- TMSI:
  - Temporary Mobile Subscriber Identifier
  - Assigned by network to prevent IMSI transmission.
- Auth with IMSI, use TMSI from then on
  - Unless, of course, the BTS asks for it.

IMSI Catcher

- Big bug in the GSM protocol
  - Network authenticates users
  - But users do not authenticate the network
- Possibility of fake Base Stations
  - Let end users attach and register at a fake base station
    - Get IMSI
  - Possible Man-in-the-Middle attack (MITM)

Our Platform

- Hardware: USRP
  - Universal Software-defined Radio Periphery
  - Configurable hardware to transmit and receive any radio frequency (RF) signals
- Software: OpenBTS
  - Open source GSM base station emulator
  - Protocol implementation

Tricking GSM Phones

- We want to trick GSM phones into thinking that our fake base station is a genuine and better one
  - Then he will handover to our base station
- “Better”
  - Stronger signals. Will trigger handover
- “Genuine”
  - Consistent with nearby base station information
  - Nearby base station will provide handover candidate base stations and frequencies. Copy that information into our fake station.

Attack on 3G Network

- 3G network has mended the vulnerability of GSM
  - Users and base stations must authenticate each other
- However, we may selectively ‘jam’ 3G phones
  - When 3G network fails, phones will fall back to GSM mode