TSN: Lecture 29
Satellite based Data Networks

Topics Covered

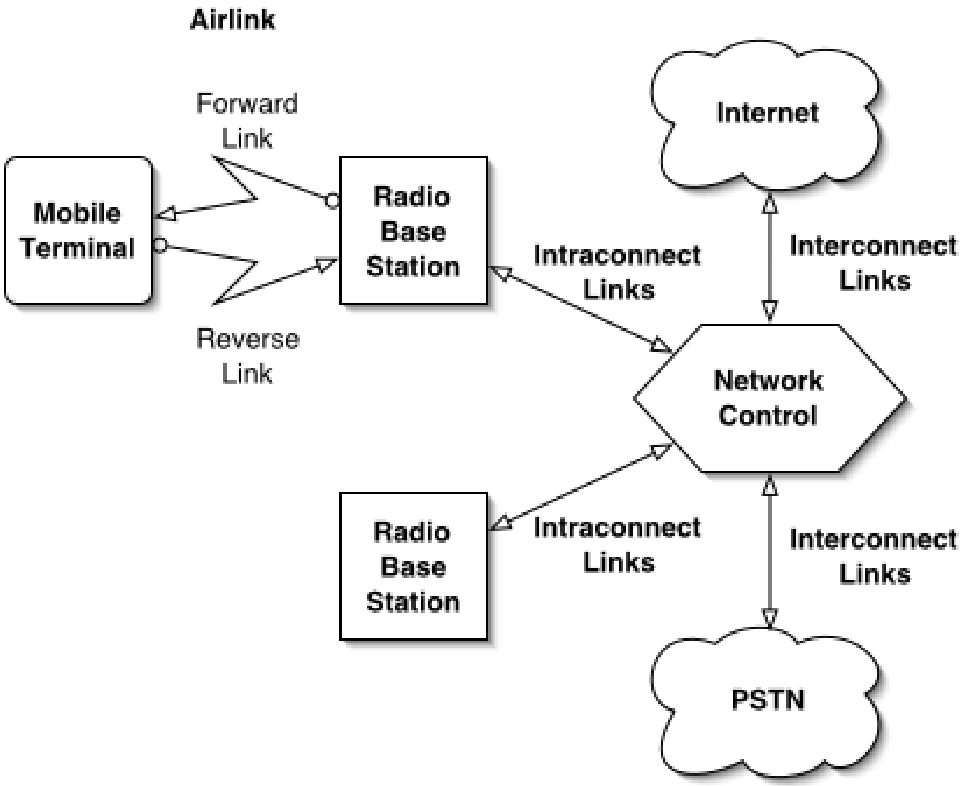
- Practical Operator Considerations
- Cellular
- Analog Cellular
- Rogue Base Station
- Tumbling
- Cloning

Practical Operator Considerations

- Getting paid
  - Prevent (limit) subscriber fraud
  - Ensure accurate clearing with other operators
- Reduce churn
- Ensure sufficient capacity
- Provide CALEA compliance
- Maintain public perception of security
- Provide a2dditional features (marketing)

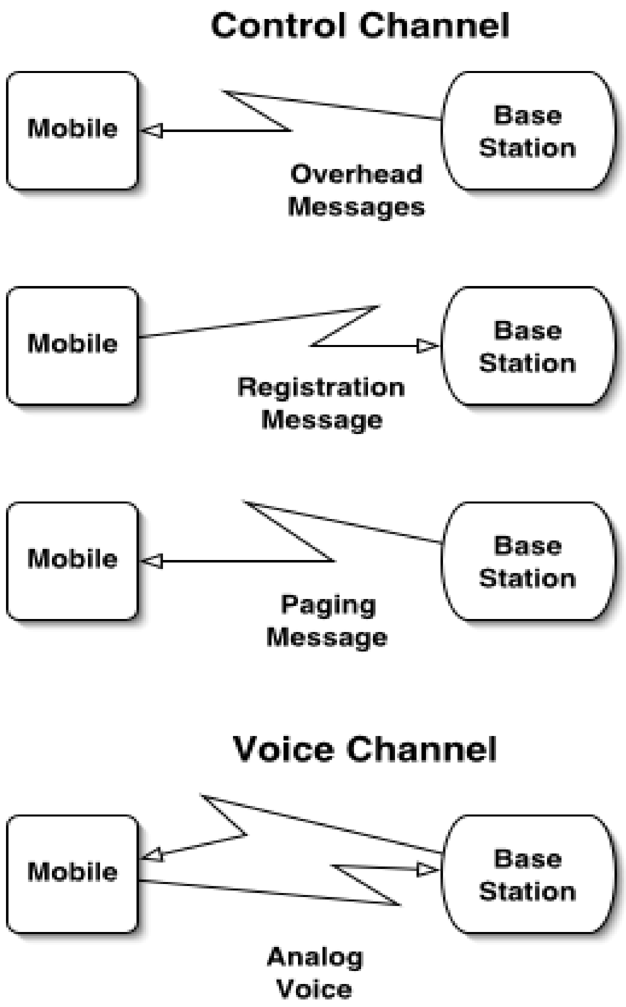
Cellular

- Analog
- Digital - TDMA
- Digital - CDMA
- Digital - GSM



Cellular Signaling

- Control channel
  - Forward is continuous
  - Reverse is shared
- Voice (Traffic) channel
  - Assigned for the call
  - Shared in digital systems



Analog Cellular

- Authentication is valid Electronic Serial Number (ESN) and Mobile Identification Number (MIN) pair
- Sent from mobile to base in the clear

- Early systems had just a “deny” list
- Not all systems initially available to each other for roaming verification

Phone Theft

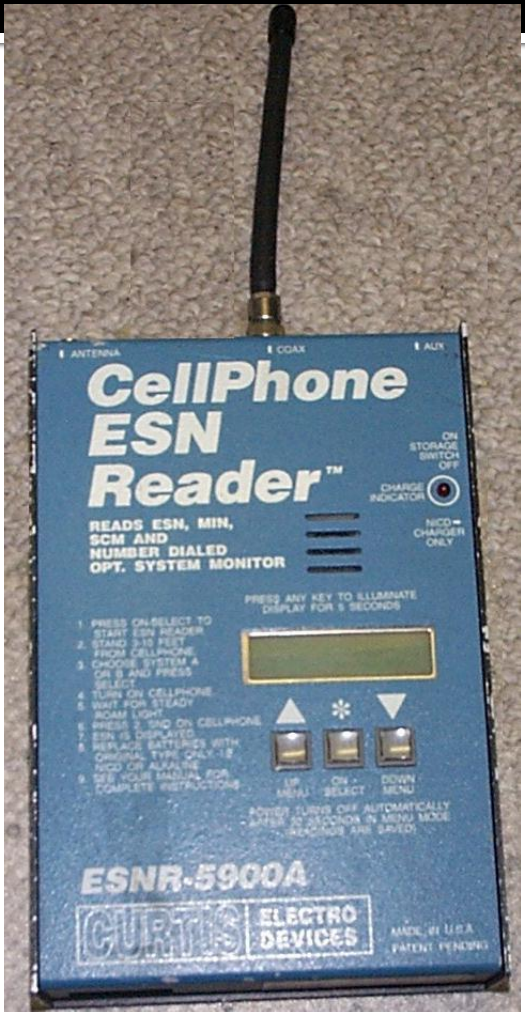
- Automobile “smash and grab”
- Use until service is canceled
- Call-sell operations

Database Theft

- Dumpster diving
- Insider account maintenance
- Hack into authorization database
- Hack into switch maintenance port

Rogue Base Station

- Forward link has no authentication
- Mobiles lock to false outbound
- Cell phone suppressor
- Test equipment (ESN readers)



Network Interception

- Read pairs on link between base station and switch
- Microwave in many areas

Tumbling

- ESN/MIN pair sent to home system
- Pre-call validation not available
- First call allowed to go through
- “Tumble” through random ESN/MIN pairs

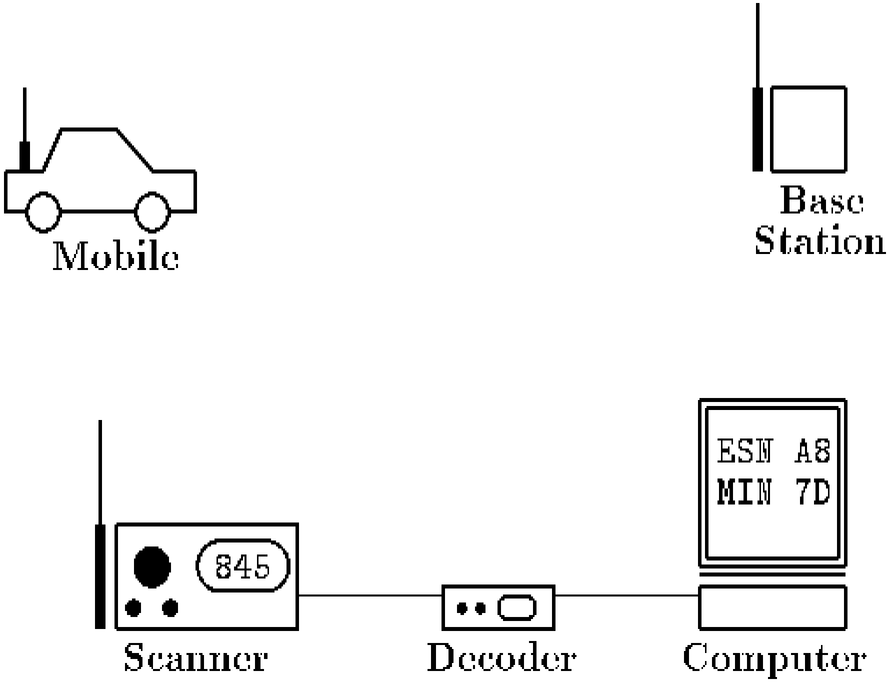
Cloning

- Replace legit ESN with snarfed ESN
- Reprogram MIN
- “Extension” phones
- Rewrite phone firmware

- (Chip in lower left corner is conveniently socketed)

Snarfing

- Tune scanner to control channel
- Decoder monitors inbound data
- Computer stores ESN/MIN pairs when the mobile registers
- AMPS data is simple FSK, in the clear

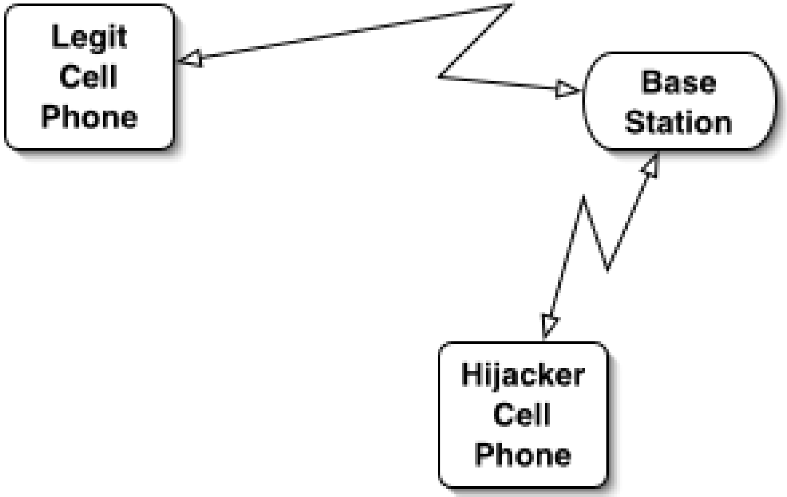


Subscription Fraud

- Sign up for service under false identity
- “Identity Theft”

Session Hijacking

- Overpower base station during legitimate call
- Use cell phone test mode to match Supervisory Audio Tone (SAT)
- Flashhook and place another call



Fighting Analog Fraud

- Legal
  - Illegal to eavesdrop
  - Illegal to clone
  - Illegal to possess equipment that might be used to clone
- Technical
  - PINs
    - Customers hated this
  - Velocity checks
    - Good for roaming, not great for local clones
  - Don't allow more than one active at a time
  - RF Fingerprinting

2G Authentication

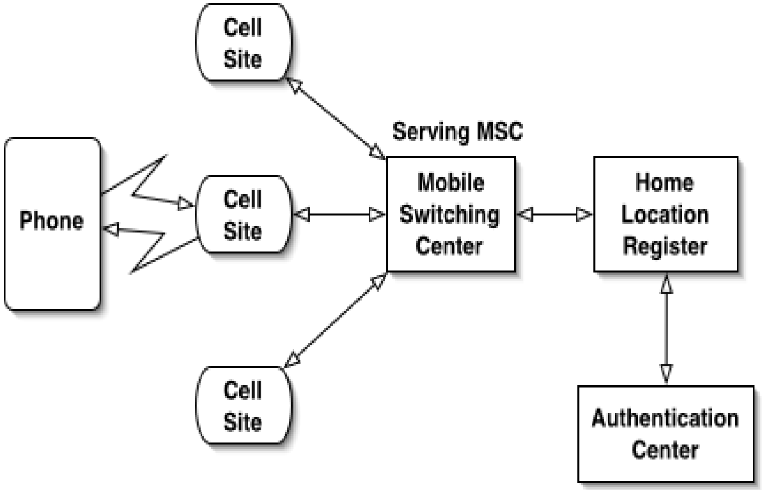
- Generally, mobile is given a challenge and network checks the response
- US Digital Cellular
  - Cellular Authentication and Voice Encryption (CAVE)
  - Control Message Encryption Algorithm (CMEA)
  - Voice Privacy Mask (VPM)
- GSM
  - A3 Authentication
  - A8 cipher key generation
  - A5 privacy

Cellular Authentication and Voice Encryption

- A-key, 64 bits (20 digits plus 6 check digits)
- RANDSSD: 56 bits
- Electronic Serial Number (ESN): 32 bits
- Shared Secret Data (SSD)
    - SSD_A: 64 bits, for authentication
    - SSD_B: 64 bits, for encryption
- Authentication Result, AUTHx: 18 bits
- Unique Challenge
    - Uses voice channel during call attempts
- Global Challenge
    - Uses control channel, checks during registration, call attempt and call delivery
    - All phones challenged with the same number

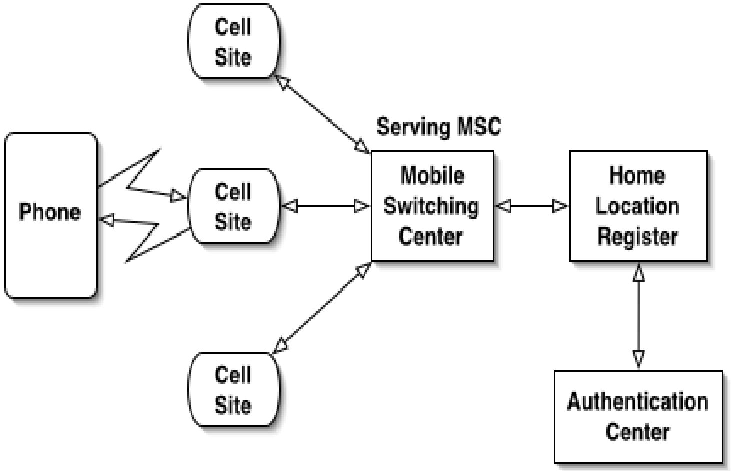
Authentication

- Phone attempts to access the network
  - indicates authentication capability
- Serving MSC contacts HLR and AC
  - indicates whether it can do CAVE
    - (if not, `SSD` cannot be shared, AC must do all the work)
  - Gets profile
    - Includes whether authentication should be done
  - Generates random number `RANDU` and sends it to phone



Authentication

- Phone runs CAVE (`RANDU, SSD, MIN, ESN`)
  - Produces `AUTHU`
  - Sends `AUTHU` to MSC
- MSC runs CAVE (`RANDU, SSD, MIN, ESN`)
  - Produces local `AUTHU`
- At MSC, if received `AUTHU` matches local `AUTHU`, authentication is successful



Shared Secret Data Update

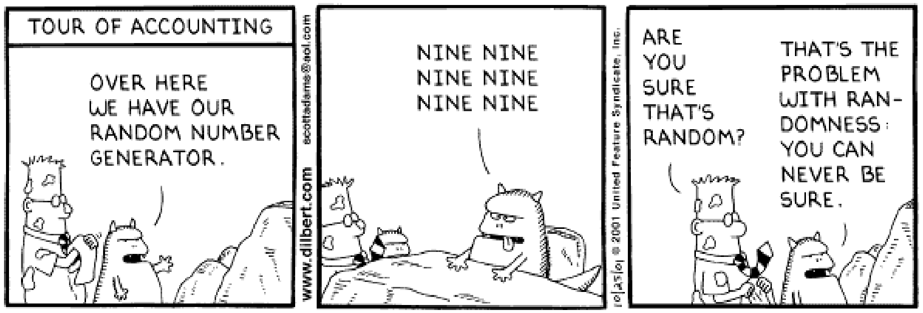
- Phone and AC update their SSD
  - AC generates RANDSSD
    - Sends it to Serving MSC
    - Computes SSD from RANDSSD, ESN, A-key
  - MSC sends RANDSSD to phone
  - Phone generates SSD from RANDSSD, ESN, A-key
- Phone authenticates Base Station (or AC)
  - Generates RANDBS
  - Calculates AUTHBS from RANDBS and new SSD
  - Sends RANDBS to Serving MSC
  - Either MSC or AC uses RANDBS and new SSD to calculate AUTHBS
  - MSC sends AUTHBS to phone
  - If phone AUTHBS and MSC AUTHBS match, phone stores new SSD
  - Another authentication process is performed
    - If successful, AC stores new SSD

Count

- Mobile maintains a 6-bit `COUNT` variable
- Incremented on instruction from AC
- AC maintains `COUNT` for each mobile
- `COUNT` values must match in order for mobile to gain access

Weaknesses

- Information sent in the clear on interconnection networks (SS7, etc)
- Secret information held in vulnerable locations (HLR, VLR, etc)
- CMEA “broken”
- Small keysize
- Poor A-keys
- VPM fixed for the length of the call
  - XOR against known voice (e.g. silence)


TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
NINE NINE NINE NINE NINE NINE
ARE YOU SURE THAT'S RANDOM?
THAT'S THE PROBLEM WITH RANDOMNESS: YOU CAN NEVER BE SURE.
www.dilbert.com
scottadams@aol.com
© 2001 United Feature Syndicate, Inc.

Copyright © 2001 United Feature Syndicate, Inc.

Global System for Mobiles

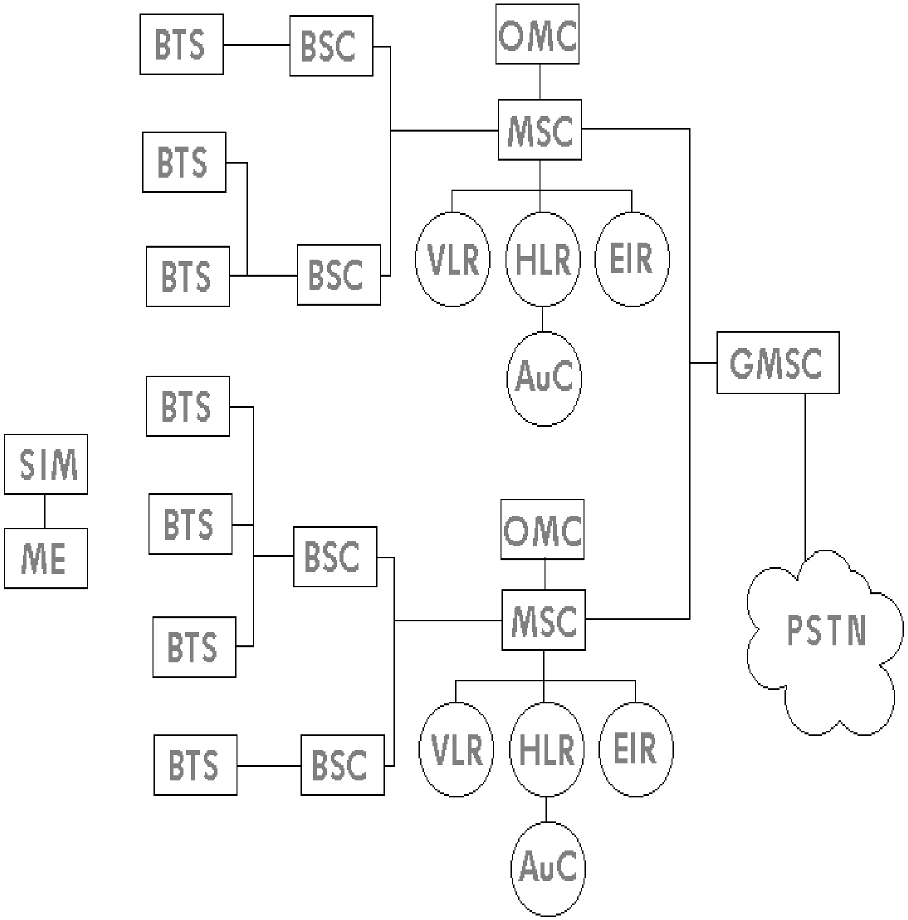
- Handsets and SIMs
- International Mobile Equipment Identifier (IMEI)
- International Mobile Subscriber Identity (IMSI)

GSM

GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

GSM Network Elements

- AuC: Authentication Center
- BTS: Base Transceiver Station
- BSC: Base Station Controller
- EIR: Equipment Identity Register (white, black, grey)
- HLR: Home Location Register
- ME: Mobile Equipment
- MSC: Mobile Switching Center
- OMC: Operations & Maintenance Center
- SIM: Subscriber Identity Module
- Visitor Location Register


BTS
BSC
OMC
MSC
BTS
BTS
BSC
VLR
HLR
EIR
AuC
GMSC
SIM
ME
BTS
BTS
BSC
OMC
MSC
BTS
PSTN
BTS
BSC
VLR
HLR
EIR
AuC