Introduction

- Introduction/Background – Ken
- Hardware/Architecture – Drew
- Hardware/Architecture – Koy
- Risk Analysis – Ivan
- Applications – Jeff
Background

- Used for transmitting voice and data services
- Supports speeds up to 3Mbps
- Operates on 800MHz and 1.8GHz bands in Europe
- Operates on 850MHz and 1.9GHz bands in US, Canada and Australia
- Roaming capability allows contact in 219 countries
History

- 1982 – Groupe Speciale Mobile formed in Europe
- 1987 – GSM standard is defined
- 1991 – First GSM phone call made
- 1994 – One million subscribers
- 1995 – The US network goes online
History

- 1996 – Networks go live in Russia and China
- 1996 – 50 million subscribers worldwide
- 2002 – 95% of countries worldwide are subscribed
- Today – over 7 billion GSM connections worldwide
Base Transceiver Station

- Coverage split into cells
- Base Transceiver Station covers one to multiple cells
- Capacity based on number of transceivers
Base Station Controller

- Controls several base stations
- Handles handover from one station to another if needed. May handle some basic processing.
- Local and hard wired to stations.
Mobile Switching Center

- Connected to the base station controller at one end and to the carrier network and external networks at the other
- Responsible for routing calls to and from other networks and tolling. Connected to the PSTN.
Mobile Switch Center (MSC) Contd.

- Additional connections to the Visiting Location Register and Home Location Register

- The Home Location Register (HLR) is the permanent data base that holds identity of all registered subscribers to the service.

- The HLR validates all active calls and registers them with the VLR. The MSC routes call if the VLR shows the caller is registered.
So far...
When you make a phone call through GSM. You also NEED:

- Secret Identity Module
- Authentication Center (AUC)
- Equipment Identity Register (EIR)
- Operation & Maintenance Center (OMC)
When you make a phone Call...

- When you make a phone call as originator, the signal will go through:
  - Base Transceiver Station
  - Base Station Controller
  - Mobile Switching Center

- Then as a terminated receiver, the signal will continue from:
  - Mobile Switching Center To
  - Base Station Controller
  - Base Transceiver Station

- Time Division Multiple Access (TDMA)
Concerns with GSM

- Theft of Service
  - Theft of cell phone results in theft of user’s service
  - Able to make phone calls and use other services without user’s permission
  - SIM cards can be switched to another phone to use it’s service and information
    - PIN codes help prevent this
Concerns with GSM

Privacy

- GSM relies on encryption algorithms to secure traffic.
  - If compromised others can read information sent over GSM
- The A5/1, A5/2 and A5/3 stream ciphers used for over-the-air voice privacy.
  - Weaknesses have been found in each one
  - A5/2 seen to be cracked in real time; Retired
Concerns with GSM

- False Base Transceiver Station (BTS)
  - Able to emulate a GSM base station
  - Can make cell phones connect to false base station by changing Mobile Country Code and Mobile Network Code
    - All traffic goes through station; can do whatever you want with the data that goes through
    - Able to record calls
Uses of GSM

- 7 billion cell devices world wide
- 80% of all worldwide subscribers
- Entire land–mass of Earth (major cities)
- Every United Nations official members (192)
- United Kingdom over 1 billion text messages every week.
Innovation

- OnStar equipped vehicles
- Life Alert
- Globally controlled devices
- Credit card / ATM machines
  - Wire tap
- Alarm systems
- Satellite powered remote server
Questions?

- GSM Network
- Phone Call Initiation
- Security Concerns
- Uses and Innovation