TSN: Lecture 30
Satellite based Data Networks II

Topics Covered

- GSM Security Goals
- Anonymity
- Authentication
- User data and signaling privacy
- Cryptographic Algorithms
- SIM Conversation

GSM Security Goals

The objective of security for GSM system is to make the system as secure as the public switched telephone network. The use of radio at the transmission media allows a number of potential threats from eavesdropping the transmissions. It was soon apparent in the threat analysis that the weakest part of the system was the radio path, as this can be easily intercepted.

The GSM MoU Group produces guidance on these areas of operator interaction for members. The technical features for security are only a small part of the security requirements, the greatest threat is from simpler attacks such as disclosure of the encryption keys, insecure billing systems or corruption ! A balance is required to ensure that these security processes meet these requirements.

At the same time a judgment must be made of the cost and effectiveness of the security measures.

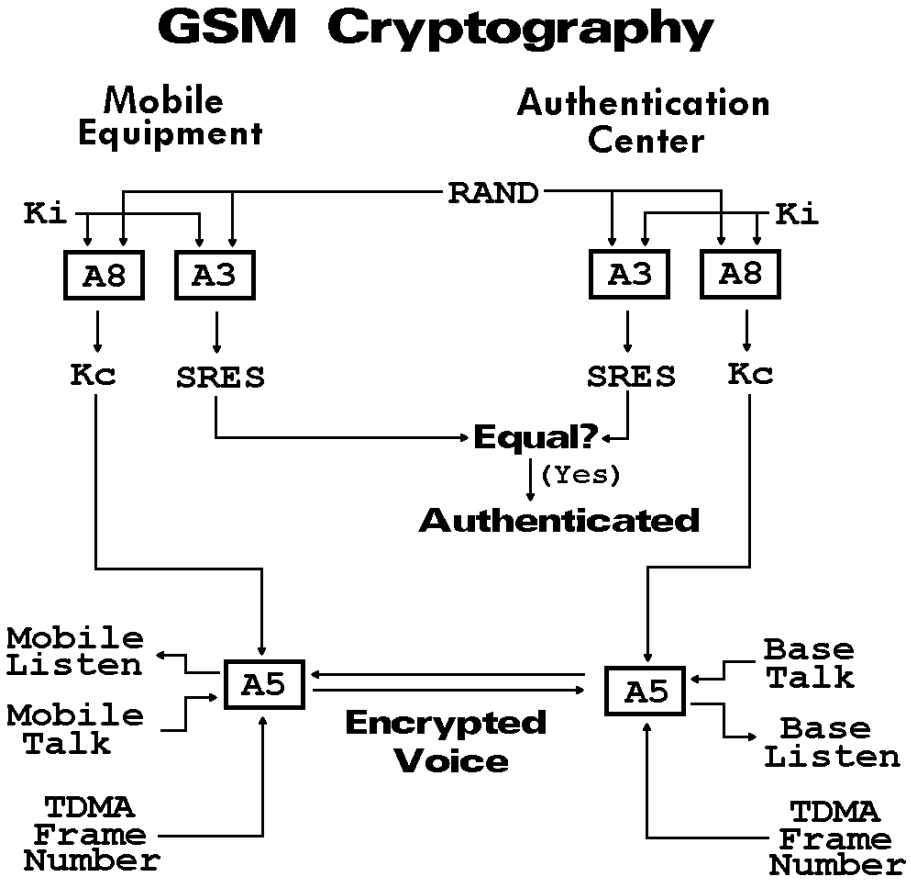
Charles Brookson
Chairman GSM MoU Security Group
Mercury one2one

Anonymity

- Temporary identifiers.
- When a user first switches on his radio set, the real identity is used, and a temporary identifier is then issued.
- From then on the temporary identifier is used.

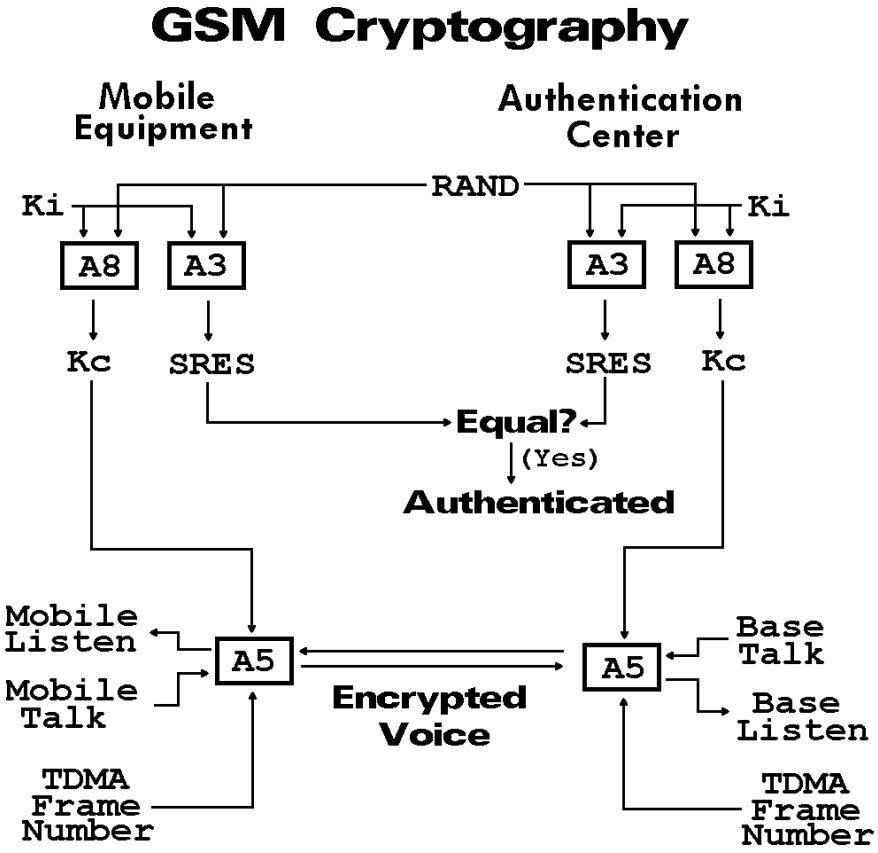
Authentication

- A random challenge is issued to the mobile
- Mobile encrypts the challenge using the authentication algorithm (A3) and the key assigned to the mobile (Ki)
- Mobile sends response back (SRES)
- Network checks that the response to the challenge is correct.



User data and signaling privacy

- A8 algorithm to compute Kc
- Used to encrypt the airlink
- A5 series privacy algorithms



Cryptographic Algorithms

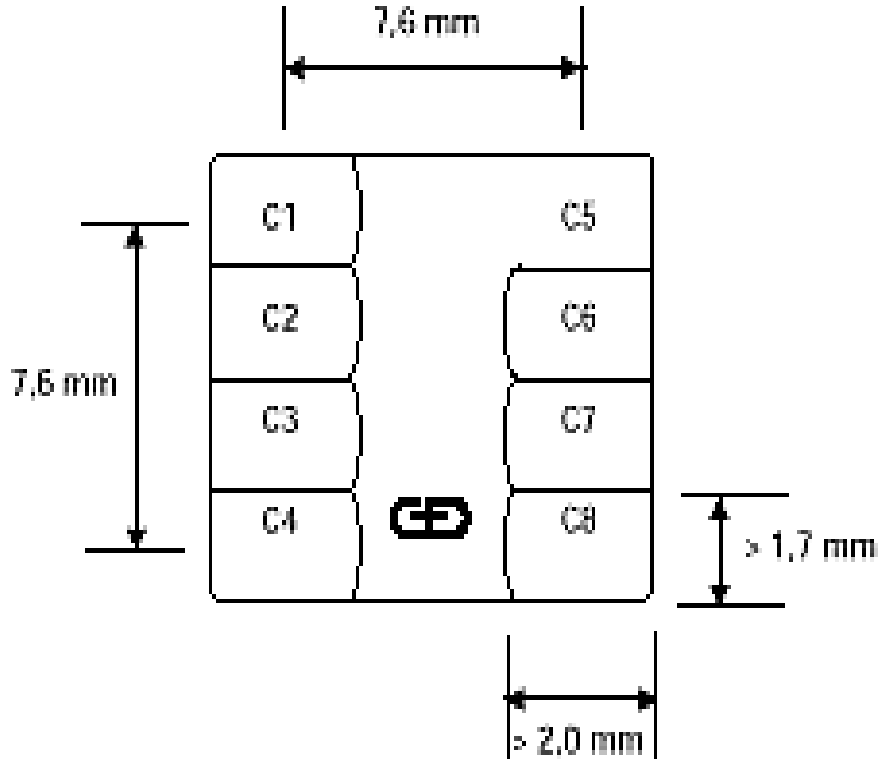
- A3 and A8 are in the SIM
  - Operators can choose their own A3/A8
  - COMP-128 provided as example algorithm
  - Can securely pass (RAND,SRES,Kc) while roaming
- A5 is built into the hardware
  - A5/1 - more secure
  - A5/2 - less secure
  - Unencrypted

GSM weaknesses

- COMP-128 leaks `Ki` (April 1998)
- A8 has effective security of 54 bits
  - (last 10 bits set to 0)
- A5
  - 64-bit key (`Kc`) and 22-bit frame number, three shift registers
  - A5/1 (western Europe)
  - A5/2 (used in North America)
  - A5/0 (no encryption)
- Rogue base station
- Unencrypted network links
  - Eavesdropping
  - Query HLR/AuC for new triples
- `Kc` refreshed only occasionally

Subscriber Identity Module

- C1: Supply voltage
  - (4.5 to 5.5 volts DC).
- C2: Reset signal
- C3: Clock signal
  - (1 to 5 MHz, external)
- C4: Reserved
- C5: Ground
- C6: Programming voltage
  - (if available)
- C7: Input/Output
  - Baudrate is (clock frequency) / 372.
- C8: Reserved



Talking to a SIM

- Defined by ETSI document GSM 11.11
- Five bytes:
  - Class of instruction (CLA)
    - (always `0xA0` for GSM)
  - Instruction Code (INS)
  - Parameter 1 (P1)
  - Parameter 2 (P2)
  - Parameter 3 (P3)
    - (length of optional data segment)
- SIM card readers may require additional bytes

Listening to a SIM

- Three fields:
  - Data
    - (variable length)
  - Status Word 1 (SW1)
  - Status Word 2 (SW2)
- 90 00 is normal response

SIM Commands

COMMAND		INS	P1	P2	P3
SELECT	A4	00		00	02
STATUS	F2	00		00	length
READ BINARY	B0	offset	(high)	offset (low)	length
UPDATE BINARY	D6	offset	(high)	offset (low)	length
READ RECORD	B2	record	number	mode	length
UPDATE RECORD	DC	record	number	mode	length
SEEK	A2	00		type/mode	length
INCREASE	32	00		00	03
VERIFY CHV	20	00		CHV number	08
CHANGE CHV	24	00		CHV number	10
DISABLE CHV	26	00		01	08
ENABLE CHV	28	00		01	08
UNBLOCK CHV	2C	00		00 (for CHV1)	10
				02 (for CHV2)	10
INVALIDATE	04	00		00	00
REHABILITATE	44	00		00	00
RUN GSM ALG	88	00		00	00
SLEEP FA	00	00		00	
GET RESPONSE	C0	00		00	length

SIM Conversation

Setup card for access

```
Activating card...01
Sending ATR 1...
Sending Inverse ATR 1...3F 2F 00 80 69 AF 02 04 01 31 00 00 00 0E 83 3E 9F 16
```

SIM Conversation

Read Master File

```
A0 A4 00 00 02                                          Select file
A4                                                      ok
3F 00                                                   Master File
9F 16                                                   file access ok, 0x16 byte response
A0 C0 00 00 16                                          Read 0x16 byte response
C0 85 14 00 00 3F 00 01 80 FF FF FF 43 09 89 03 09 04 00 83 8A 83 8A 90 00
```

Master File Header

```
  [MF/DF] RFU: 85 14
  Free Memory: 00 00
  File ID:     3F 00 (MF)
  File Type:   01 (Master File)
  RFU:         80 FF FF FF 43
  Length:      09
  File characteristics:    89
    Clock stop:     Allowed, low level preferred
    Required speed: 13/8
    CHV:            Disabled
  Child DFs:                03
  Child EFs:                09
  CHVs, Unblock CHVs, etc: 04
  RFU:                      00
  CHV1 Status:              83 (Initialized, 3 remaining)
  Unblock CHV1 Status:      8A (Initialized, 10 remaining)
  CHV2 Status:              83 (Initialized, 3 remaining)
  Unblock CHV2 Status:      8A (Initialized, 10 remaining)
```

SIM Conversation

Read Dedicated File

```
A0 A4 00 00 02                                          Select file
A4                                                      ok
7F 20                                                   GSM Dedicated File
9F 16                                                   access ok, 0x16 byte response
A0 C0 00 00 16                                          Read 0x16 byte response
C0 85 14 00 04 7F 20 02 00 FF FB FF 23 09 99 00 19 04 00 83 8A 83 8A 90 00
```

Dedicated File Header

```
  [MF/DF] RFU: 85 14
  Free Memory: 00 04
  File ID:     7F 20 (DF-GSM)
  File Type:   02 (Directory File)
  RFU:         00 FF FB FF 23
  Length:      09
  File characteristics:    99
    Clock stop:     Allowed, low level preferred
    Required speed: 13/8
    CHV:            Disabled
  Child DFs:                00
  Child EFs:                19
  CHVs, Unblock CHVs, etc: 04
  RFU:                      00
  CHV1 Status:              83 (Initialized, 3 remaining)
  Unblock CHV1 Status:      8A (Initialized, 10 remaining)
  CHV2 Status:              83 (Initialized, 3 remaining)
  Unblock CHV2 Status:      8A (Initialized, 10 remaining)
```

SIM Conversation

Read Elementary File

```
A0 A4 00 00 02                                          Select file
A4                                                      ok
6F 07                                                   (GSM) EF-IMSI
9F 0F                                                   access ok, 0x0F byte response
A0 C0 00 00 0F                                          Read 0x0F byte response
C0 85 0D 00 09 6F 07 04 00 1B FF 1B 23 02 00 00 90 00
```

Elementary File Information

```
  [EF] RFU:     85 0D
  File Size:    00 09
  File ID:      6F 07 ((GSM) EF-IMSI)
  File Type:    04 (Elementary File)
  RFU:          00
  Access:       1B FF 1B
    Read/Seek:     CHV1
    Update:        Admin 11
    Increase:      Never
    RFU:           Never
    Rehabilitate:  CHV1
    Invalidate:    Admin 11
  Status:       23 (Not Invalidated)
  Length:       02
  EF Structure:  00 (Transparent)
  Record Length: 00
A0 B0 00 00 09                                          Read file, 9 bytes
B0 08 39 01 13 10 00 43 98 44 90 00                IMSI
```

SIM Conversation

Select GSM Dedicated File

A0 A4 00 00 02	Select File
A4	ok
9F 16	GSM Dedicated File

Perform A3A8 computation

A0 88 00 00 10	A3A8 with 0x10 bytes
88	ok
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	RAND challenge
9F 0C	ok, 0x0C bytes waiting
A0 C0 00 00 0C	get response
C0 D0 70 89 C4 8F 23 C4 EB 59 78 EC 00 90 00	

Perform A3A8 computation

A0 88 00 00 10	A3A8 with 0x10 bytes
88	ok
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01	RAND challenge
9F 0C	ok, 0x0C bytes waiting
A0 C0 00 00 0C	get response
C0 9B 8E 05 84 FF 8A E8 60 45 A7 30 00 90 00	

SIM attacks

- Repeated authenticate, leaks `Ki`
  - (New SIMs have a limit (about 50k) on the number of times the authentication algorithm can be run)
- Side-channel attacks
  - Power consumption
  - Timing
  - Electromagnetic emanations

COMP-128 Updates

- COMP128-2
  - 54-bit Kc
  - Secret algorithm
- COMP128-3
  - 64-bit Kc
  - Secret algorithm
- Proposal for new A3A8 based on MILENAGE
  - Milenage based on Rijndael (AES)
  - Algorithm will be public
- New A3A8 requires
  - AuC software upgrade
  - New SIMs

A5/3

- Based on the Kasumi algorithm
  - 3GPP confidentiality and integrity algorithms.
- Kasumi derived from the MISTY algorithm, created by Mitsubishi.
- Specifications are publicly available on the 3GPP web site (`www.3gpp.org`).

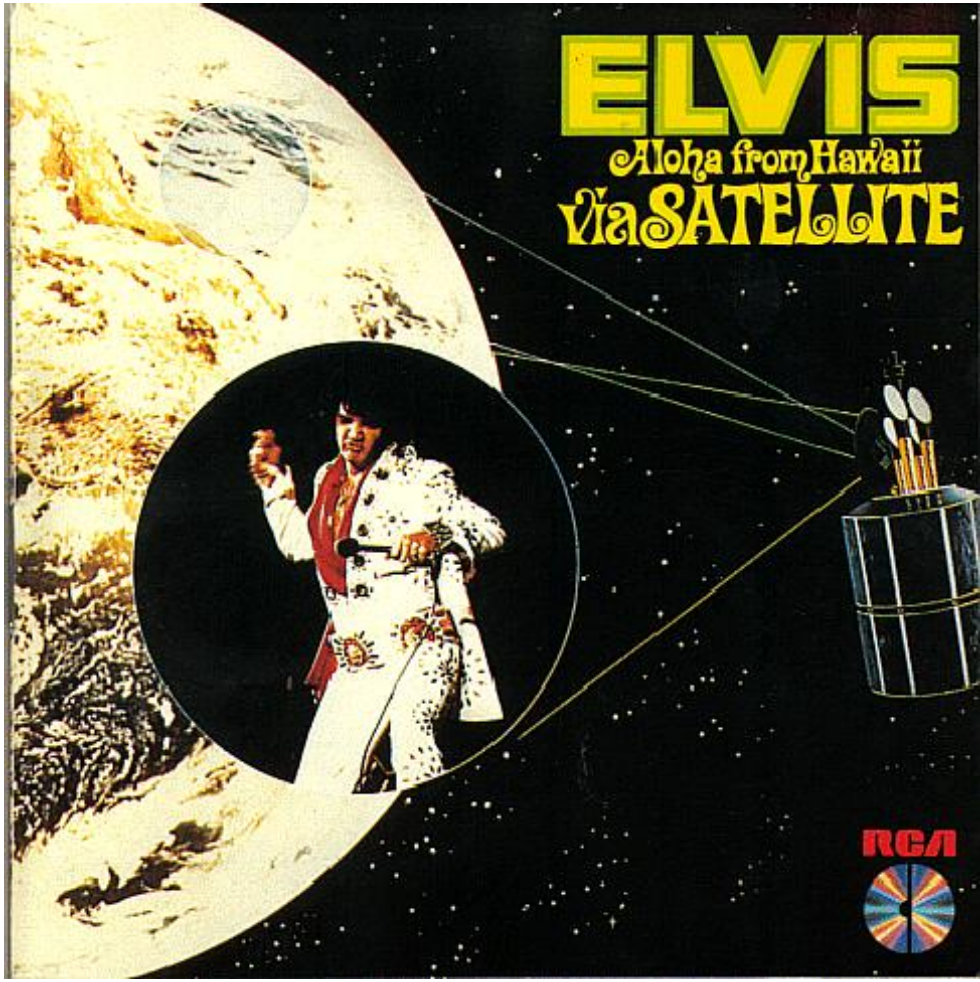
Cellular Jamming

- Low-power private base station transmits a forward link overhead message
- Mobiles register with base station
- Base station never sends a page
- The FCC view on this:

- The Communications Act of 1934, as amended, and the Commission's rules do not permit the use of transmitters designed to prevent or jam the operation of wireless devices in hospitals, theaters and other locations. Section 302(a) of the Communications Act, 47 USC 302(a), prohibits the manufacture, importation, sale, offer for sale, or use of devices that fail to comply with the regulations promulgated pursuant to this section.
- Based on the above, the operation of transmitters designed to jam wireless communications is a violation of 47 USC 301, 302(a), and 333. The manufacture, importation, sale or offer for sale, including advertising, of such transmitters is a violation of 47 USC 302(a). Parties in violations of these provisions may be subject to the penalties contained within 47 USC 501-510. Fines for a first offense can range as high as $11,000 for each violation or imprisonment for up to one year. The equipment can also be seized and forfeited to the U.S. Government. These regulations apply to all transmitters that are designed to cause interference to, or prevent the operation of, other radio communication systems.

Satellite Networks

- Big LEOs
- Little LEOs
- Mobile Satellite Ventures
- INTELSAT
- INMARSAT
- VSAT
- GPS



Big LEO

- Constellation of satellites in Low Earth Orbit (as opposed to geosynchronous)
- Base stations in the sky
- Linked to network of ground stations
- Voice as primary service
- 1610 to 1626.5 MHz up
- 2483.5 to 2500 MHz down

Iridium

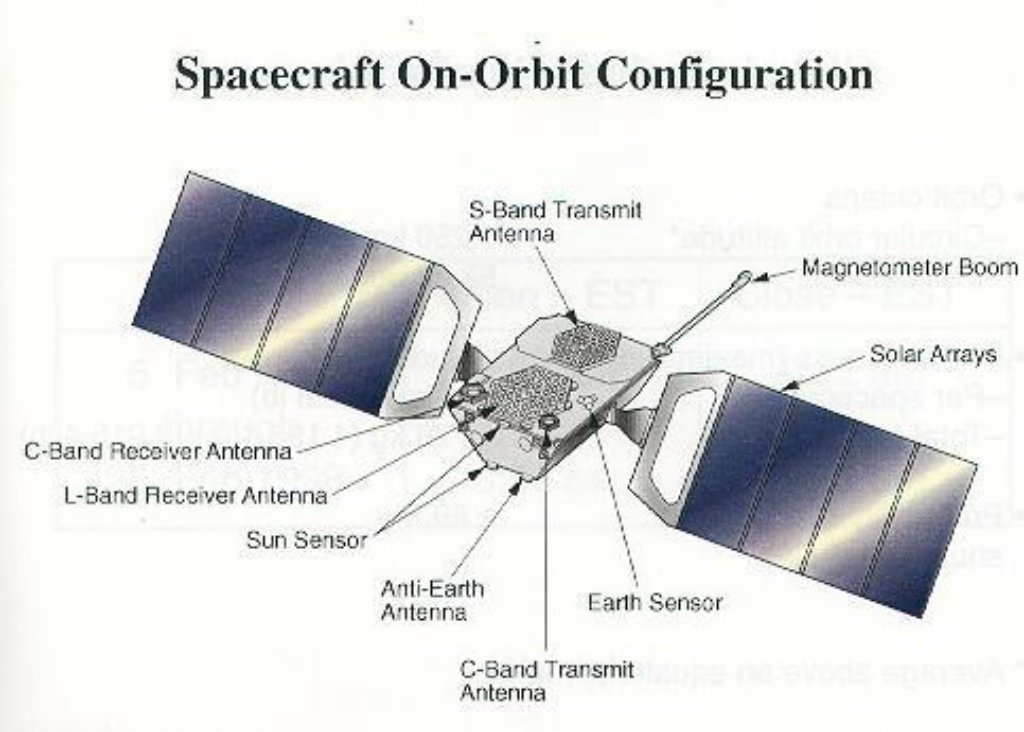
- $5 billion
- 66 satellites (plus spares)
- TDMA, processing on-board
- 1621.35 to 1626.5 up and down
- 2.4 kbps data service
- Service start November 1998
- Bankruptcy in August 1999, only 55,000 customers

Iridium Satellite LLC

- Paid $25M for Iridium assets
- Relaunched commercial service in 2001
- Large government contract ($72M/2 years via DISA)
- Dedicated gateway earth station in Hawaii
- Defense Information Systems Agency
  - Department of Defense
  - Department of State
  - Inter-satellite links
- Enough money to replenish satellites?

Globalstar

- Loral, Qualcomm
- 48 satellites in LEO
- Start of operations February 2000
- Currently under bankruptcy protection
- Bent-pipe
- CDMA service
- Underpowered satellites
  - Recharge over oceans
- 9.6 kbps data



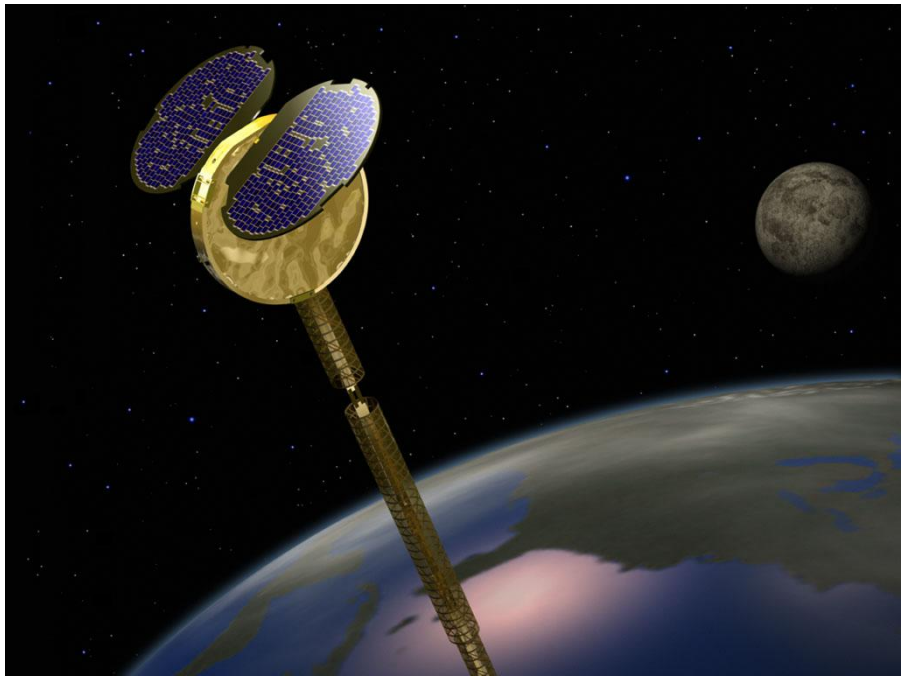
ICO

- $4.7 billion
- Hughes-built satellites
- 10 satellites in Medium Earth Orbit (MEO)
- GSM-based

- New ICO
- Craig McCaw
- Merged with Teledesic

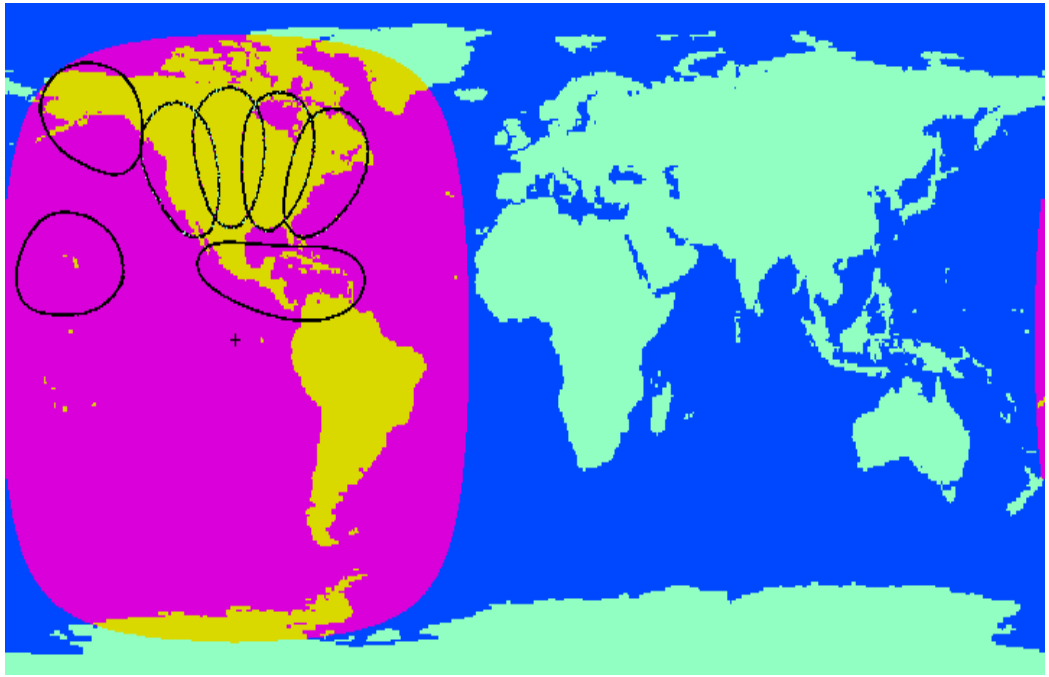
Orbcomm (Little LEO)

- 28 satellites
- 14 earth stations
- VHF operation
- Data only
- Store and Forward if ground station not in view
- "GlobalGrams" = X.400 e-mail
- Latency



Mobile Satellite Ventures

- Motient
  - AMSC-1 ($500M)
  - Spar Aerospace
- TMI
  - MSAT-1 (identical)



- Mobile satellite voice and data
- L-band
- Digital voice

Interception

- Gateways require tapping
  - FBI, CALEA requirements
  - Iridium agreement
  - Globalstar agreement
  - TMI on-demand access
  - National intelligence and police forces
- Test equipment
- Limited use of encryption
- Modifiable phone equipment

INTELSAT

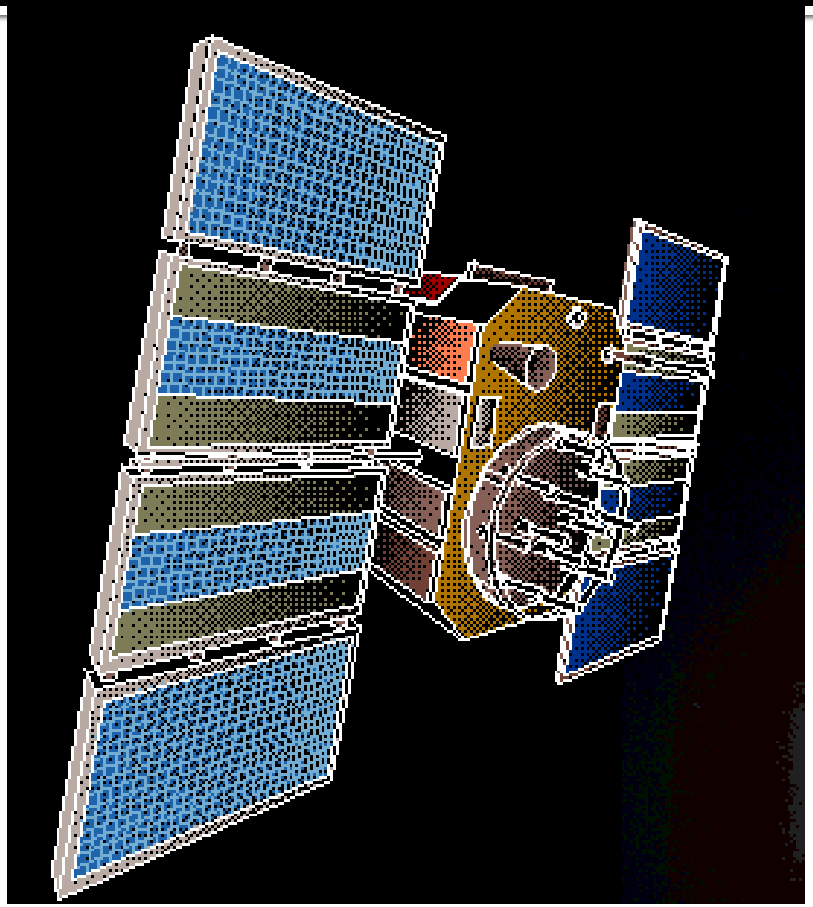
- Was a consortium of nations as signatories
- Now privatized
- Large fleet in geostationary orbit
- Primarily telephone and television traffic
- Carries unencrypted voice, data and fax
- Used by US DoD for UAV datalink

INMARSAT

- International Maritime Satellite Organization
- AOR, POR, IOR coverage
- L-band

Global Positioning System

- 24 satellites
- Selective Availability turned off May 2000
- 30 meter accuracy
- Can be jammed (denial of service)
- Can be spoofed



GPS Frequencies

L1: 1575.42 MHz: Coarse Acquisition (C/A) code
L2: 1227.60 MHz: Precise (P) or Y (encrypted) code
L3: 1381.05 MHz: Nuclear burst detectors
L4: 1841.40 MHz: Ionospheric correction (under study)
L5: 1176.45 MHz: Civilian safety-of-life signal (proposed)

GPS Enhancements

The new architecture also requires new user equipment and an upgraded ground control segment, as well as M-Code. All of those elements should be in place by 2008, when 18 satellites with M-Code - 12 IIRs and 6 IIFs - will be up.