Satellite Telephony Security
“WHEN TERRESTRIAL COMMUNICATION FAIL, WE PREVAIL!”
Satellite Communications

- Broadcast Video to Cable Headends
- Direct Broadcast TV Last-mile Broadband
- Corporate Data Networks (Interactive & Multicast)
- Teleport
- PSTN
- Internet
- End Users
- Local ISPs
- Video Contribution

End Users

Corporate Data Networks (Interactive & Multicast)
Satellite Phone
Satellite Phone Network
Satellite Orbits

- **Medium Earth Orbit**
  - Altitude: 8,000-20,000 km

- **Low Earth Orbit**
  - Altitude: 500-2,000 km

- **Geostationary Orbit**
  - Altitude: 35,786 km

- **Highly Elliptical Orbit**
  - Altitude: >35,786 km

**Average distance to moon:**
384,400 km
GEO (Geostationary Earth Orbit)
Satellite Operators
ACeS, ICO, Inmarsat, SkyTerra, TerreStar, Thuraya

LEO (Low Earth Orbit)
Satellite Operators
Globalstar, Iridium
LEO Communication Satellite Constellation System

- **LEO Satellite i**
  - Feeder Downlink
  - Feeder Uplink
  - Intersatellite Link (ISL)

- **LEO Satellite i+1**
  - Terminal Downlink
  - Terminal Uplink

**Gateway**
- PSTN
- Cellular

**End User Terminal**
Frequency Band Designations
TDMA (Time Division Multiple Access)
Timeframe Structure and Timeslots

1 hyperframe = 4,896 superframes = 19,584 multiframes = 313,344 TDMA frames
(3h 28mn 53s 760ms)

1 superframe = 4 multiframes = 64 TDMA frames (2.56s)

1 multiframe = 16 TDMA frames (640 ms)

1 TDMA frame = 24 timeslots (40ms)

1 timeslot = 78 bit durations (5/3ms)

1 bit duration = 5/234ms
CDMA (Code Division Multiple Access)
Coverage: Iridium
Coverage: Inmarsat
Coverage: Thuraya
Spotbeams: Regional Coverage
GMR (GEO-Mobile Radio Interface)
Evolution Path

Extension to Satellite

GSM

GMR Release 1

GPRS

GMR Release 2

3GPP

GMR Release 3
GMR-1 Protocol Architecture

- **MES**
- **Satellite**
- **GSC + GTS + TCS**

**GSM**
- **SIM**
- **GPS RECEIVER**

**GMR-1 Um-Interface**
- **Spotbeams L-Band**
- **Feeder Link Ku or C-Band**
- **GSM/A-Interface (CCS7)**

**CM**
- **MM**
- **RR**
- **DLL**
- **PHYS**

**GMR-1 Um-Interface**
- **BSSMAP**
- **SCCP**
- **MTP**

**CM**
- **MM**
- **RR**
- **DLL**
- **PHYS**
- **BSSMAP**
- **SCCP**
- **MTP**
GMR-1 Logical Channel Mapping onto Physical Channel

**Logical Channels**
- TCH (Traffic)
- CCH (Control and Signalling)

**Physical Channels**
- Timeslot Number
- TDMA Frame Sequence
- RF Channel

**Physical Resource**
- Frequency (RF Channels)
- Time (Timeslots)

**Mapping**
- Uplink
- Downlink

**User Channels**
- Mobile Earth Station
- Satellite
GMR-1 (GSM-based) Services

- Standard GSM-based services (Phase 2)
- Roaming
- Single number routing
- Numbers and addressing
- Authentication and privacy
GMR-1 Extended Services

- Single-hopped terminal-to-terminal calls
- Optimal routing
- High penetration alerting
- Position based services
C-band Regional Coverage for Signalling & Communication

C-Band

Traffic

Signalling
L-band Spotbeams for MSS Users
GMR Satellite Monitoring System

Intercepting
Satellite Phone Interception

- Law-enforcements require tapping
- Test equipment
- Limited use of encryption
- Modifiable phone equipment
Tactical Interception
Receives L-band from satellite and line-of-sight from handset

Strategic Interception
Receives L-band from satellite and C-band from satellite
Tactical Satellite Interception Operation

Gateway

RADIO LINE-OF-SIGHT

1.6 GHz UP

3.5 GHz DOWN

1.5 GHz DOWN

6 GHz UP

1.5 GHz DOWN

1.6 GHz DOWN

1.6 GHz UP

MES

Monitoring Agent
Tactical Satellite Interception Operation

Satellite antenna

Downconverter

Channel 1

Channel 2

Uplink antenna

IF

Computer
Call Analysis

- Spotbeam IDs, GPS co-ordinates, operating frequency.
- Date, time and duration of call.
- MES IMSI.
- GPS co-ordinates of MES.
- Random Reference Number (CallerID).
- TMSI called by MES.
- Mobile or Fixed Originated Call (Voice, Fax, Data or SMS).
- Terminal type.
- Ciphering key sequence number.
- RAND and SRES.
- Encryption Algorithm
What’s next?
GEO Mobile Radio

This is the homepage of the Osmocom sub-project GEO Mobile Radio.

It is collecting information and software related to the ETSI GEO Mobile Radio specification and its practical implementations like the Thuraya satellite phone network.

GEO Mobile Radio is a set of specifications describing a satellite based mobile phone network.

Radio aspects

It uses the L-band frequencies 1634 to 1656 MHz (earth to space) and 1532.5 to 1554.5 MHz (space to earth) for communication between mobile phones and the respective satellites. The polarization is circular (left) and the modulation is pi/4 QPSK, using a channel spacing of 31.25 kHz.

Index

- GMR_Specifications -- An Introduction and Overview into the GMR specifications
- Thuraya_SD2510 -- A popular handset for use in the Thuraya system.
- Thuraya_SG2520 -- A dual-mode GSM/ Thuraya handset running WindowsCE.
- Thuraya_Beams -- Information about the Thuraya beams
  - http://bit.ly/nInTOi -- Google Maps view of the Thuraya beams that we have found so far
- OsmoGMR_Software -- Software that we wrote for GMR analysis
- Receiver_Setup -- How to receive GMR signals coming down from a satellite

Download in other formats:

Plain Text
27th Chaos Communication Congress
We come in peace

Wideband GSM Sniffing

GSM is still the most widely used security technology in the world with a user base of 5 billion and a quickly growing number of critical applications. 26C3’s rainbow table attack on GSM’s A5/1 encryption convinced many users that GSM calls should be considered unprotected. The network operators, however, have not woken up to the threat yet. Perhaps the new capabilities to be unleashed this year – like wide-band sniffing and real-time signal processing – will wake them up.

Now that GSM A5/1 encryption can be cracked in seconds, the complexity of wireless phone snooping moved to signal processing. Since GSM hops over a multitude of channels, a large chunk of radio spectrum needs to be analyzed, for example with USRPs, and decoded before storage or decoding. We demonstrate how this high bandwidth task can be achieved with cheap programmable phones.

Attached files

- GSM Sniffing [Slides] (application/pdf – 755.6 KB)
@geovedi
http://www.slideshare.net/geovedi/presentations