Mobitex Network Security

olleB of the Toolcrypt Group

olle@toolcrypt.org

Mobitex

- Background
- Network structure
- Security features

Mobitex background

- History of the Mobitex protocol
- Overview of network operators
- Overview of network users

ERICSSON

History of the Mobitex protocol

- Originated at "Televerket" in early 1980s
- Developed by Ericsson (Eritel)
- First operational network in 1986
- Packet-switched, national infrastructure
- Mobitex Technology AB
  - http://www.mobitex.com/

Overview of network operators

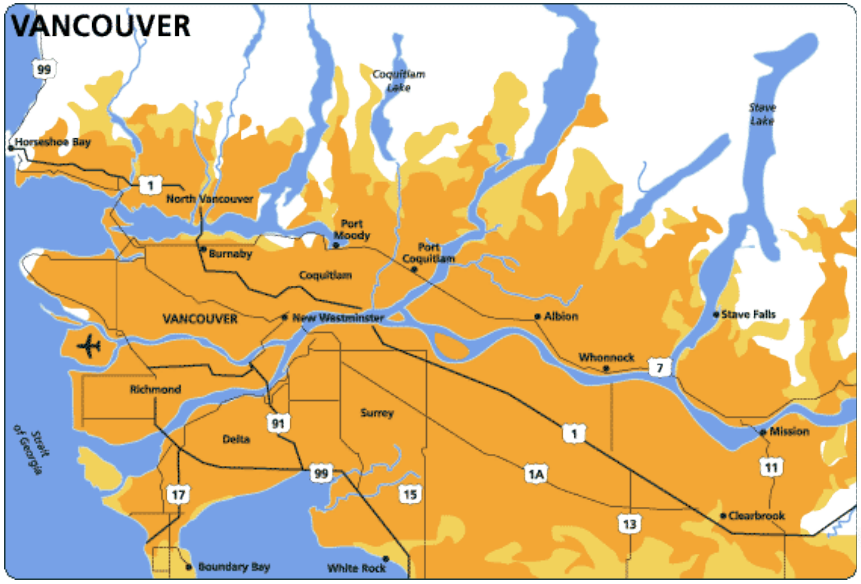
- 30+ networks worldwide today
- 20 public commercial networks
  - Rogers Wireless (Cantel)
  - United Wireless (Velocita, Cingular, RAM)
- Mobitex Association
  - Operators, developers and manufacturers
  - http://www.mobitex.org/

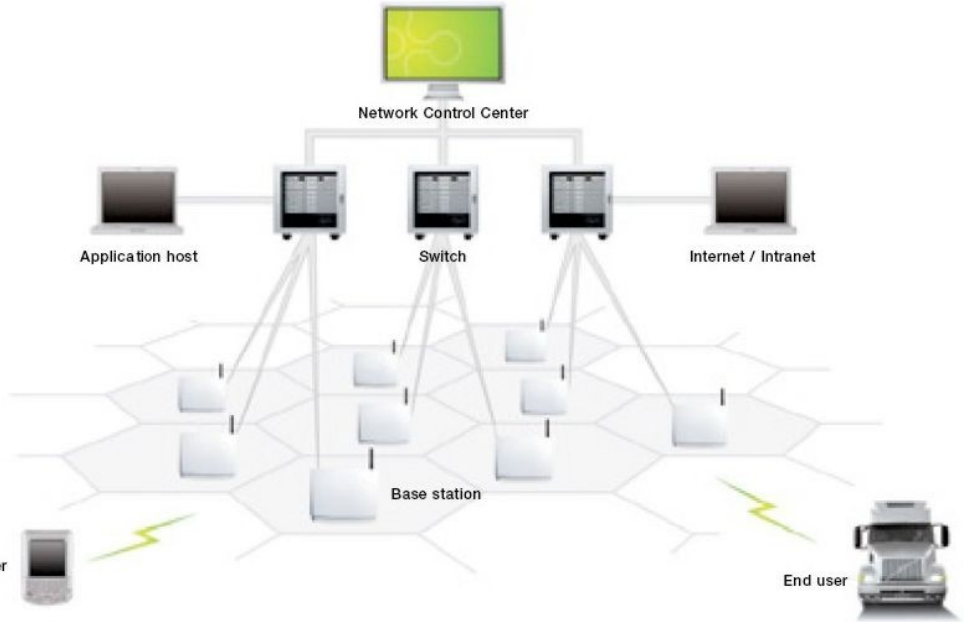
Overview of network users

- Public Safety
- Field service support
- Transport / Logistics
- Card Payments (POS)
- New growth areas
  - Positioning / Resource Management
  - Metering / Remote control
  - Alarm systems

Mobitex network structure

- Mobitex network topography
- The Mobitex protocol suite





Mobitex network topography

- Backbone network connects NCC and one or more main exchanges (MHX)
- Area exchanges (MOX) connected to MHX
- Fixed terminals and mobile radio base stations (BAS) connected to MOX
- Mobile terminals can be restricted to an area or be allowed roaming (with tariff)
- Infrastructure linked by HDLC or X.25

The Mobitex protocol suite

- Roughly corresponds to OSI layers 1-4
  - Hey, so does TCP/IP!
- Data link layer is either ROSI or wired
  - That's like WiFi vs LAN/WAN, right?
- Everything transports or is transported in MPAK packets with src/dst MAN address
  - Hey, that's just like IP packets, I know this!
- Comparison breaks down on layer 4

The Mobitex protocol suite

- Layer 1 – Radio layer
  - 896-901Mhz Mobile / 935-940Mhz Base
    - 900Mhz band in Americas and Korea
    - 400Mhz band in Europe, Australia and Asia
    - 800Mhz band in China
  - Numbered 12.5khz bandwidth channels
  - 8kbaud GMSK modulation
  - Bit-scrambling to reduce same-bit strings

The Mobitex protocol suite

- Layer 2 – ROSI (RadiO Signalling Interface)
  - 20 bit interleaving of coded octets
  - (12,8) shortened hamming code
  - 144 bit data block with 16 bit CRC
  - Radio frame header with base/area ID
  - Link header with frametype and sequence no.
  - Slotted ALOHA access mechanism with automatic repeat requesting (ARQ)

The Mobitex protocol suite

- Layer 3 – The MPAK (Mobitex PAcKet)
  - Maximum 512 byte data payload length
  - Common components (header)
    - Sender and addressee MAN (not swapped in reply)
    - Traffic state flags – mailbox and delivery status
    - Subscription flags – POSACK, sendlist included
    - Packet class / type
      - PSUBCOM / DTESERV packet classes
    - Optional address list

The Mobitex protocol suite

- Layer 3 – The MPAK (Mobitex PAcKet)
- PSUBCOM (Packet-switched SUBscriber COMmunication)
  - TEXT - ASCII / ISO-646 text formatted for printer/display
  - DATA - application data, optional encoding
  - STATUS - single byte status code (user defined meaning)
  - HPDATA - Higher Protocol Data, one-byte protocol ID
  - EXTPAK - used to exchange packets with “external” nets
- DTESERV (Data TErminal SERVice communication)
  - BORN, (IN)ACTIVE, DIE, LIVE, ROAM(ORD), GROUPLIST, INFO(REQ), TIME, AREALIST, ESNxxx, LOGINxxx, etc.

The Mobitex protocol suite

- Layer 4 – MTP/1 (Mobitex Transport Protocol)
  - Not limited to MPAK length
  - In-order delivery guaranteed
  - Error signaling and PDU identification
  - Reliable delivery of PDUs (optional)
  - Basically an UDP / TCP protocol analogue using HPDATA MPAKs as transport
  - Introduced in 1991, not used very often...

The Mobitex protocol suite

- Wired Layer 2 alternatives
  - MASC (Mobitex ASynchronous Communication)
    - Mainly used over V.24 or X.21bis to connect a Mobitex terminal to a computer application
  - MDOT (Mobitex Data Over TCP/IP)
    - "Internet application gateways" enable Ipv4 connected hosts to send/receive MPAKs
  - X.25
    - Standardized profile for connecting fixed terminals to a MOX (area exchange)

Security features

- Subscriber identification
- Privacy protection
- Network snooping
- Live Demo!

Mobitex Subscriber identification

- Subscriber identified by 24 bit MAN
- Issued to each subscriber by operator
- MAN is like an IPv4 address
  - Tied to a subscription, not a network location
- Location of each MAN stored in network
  - Compare IPv4 routing tables
- 3 different subscriber types

Mobitex Subscriber identification

- Terminal subscription (Fixed or Mobile)
  - Identified by 4-byte ESN
- Personal subscription
  - Transferable between terminals
  - Identified by 8-char password
- Host group subscription
  - Login to fixed terminals only
  - More than one active login at a time

Mobitex Subscriber identification

- MS identified on-air by a 4-byte ESN
- ESN calculated from terminal S/N
- ESN only used to “activate” and “roam”
  - Sniff to spoof terminal at later time
    - Spoof logged in personal subscriptions
    - Real terminal may need to deactivate
  - Kill real terminal and hijack session
    - Spoof DIE message to deactivate real terminal
    - ESNREQ / ESNINFO can be sent at any time

Mobitex Subscriber identification

- All subscription data sent ***in the clear***
  - BORN
  - ACTIVE
  - ROAM
  - ESNINFO
  - LOGINREQ

Mobitex Privacy protection

- ROSI (Layer 2) uses bit-scrambling to improve effectiveness of modulation
- Some may confuse this with privacy
- Scrambling generator trivial to reverse
  - rec.radio.scanner on 14 Mar 1997 <332A0580@geocities.com>

Mobitex Privacy protection

- Mobitex protocol specification contains no provisions for privacy or integrity at all
- TEXT messages inherently clear text
- Lots of applications use HPDATA and don't bother with security or privacy
- Very much like IPv4 in that security must be implemented in the application layer

Network snooping - prerequisites

- Radio that receives the correct frequency
- 8kbit GMSK - need FM discriminator tap
  - http://discriminator.nl/
  - Google is your friend...
- Software
  - Commercial software ($$$)
  - PDW (http://www.gsm-antennes.nl/PDW/)
  - Mine, as I'll show you next...

Demo of network snooping

```
19:19:20 BAS:3B48/05/08 f=0 (3196F6) 0/<MRM> seq=AB l=008
             MPAK: (30D757) (3196F6) 00/[HPDATA] t=B5BB41 HPID=002(OVLS)
             4E3A 2447 5047 4741 2C31 3731 3335 352E 302C    N:$GPGGA,171355.0,
             3539 3231 2E34 3836 2C4E 2C30 3137 3538 2E31    5921.486,N,01758.1
             3737 2C45 2C31 2C30 382C 312E 3033 2C30 3030    77,E,1,08,1.03,000
             3732 2C4D 2C30 3233 2C4D 2C2C 2A35 390D 0A2F    72,M,023,M,,*59..⁄
             2447 5056 5447 2C30 3030 2E30 2C54 2C33 3537    $GPVTG,000.0,T,357
             2E39 2C4D 2C30 3030 2E30 302C 4E2C 3030 302E    .9,M,000.00,N,000.
             3030 2C4B 2A34 360D 0A3B 0000 0000 0000 0000    00,K*46..;........
19:19:41 BAS:3B48/05/08 f=0 (3196F6) 0/<MRM> seq=AC l=008
             MPAK: (30D75B) (3196F6) 00/[HPDATA] t=B5BB42 HPID=002(OVLS)
             4E3A 2447 5047 4741 2C31 3731 3431 392E 302C    N:$GPGGA,171419.0,
             3539 3330 2E36 3934 2C4E 2C30 3137 3536 2E37    5930.694,N,01756.7
             3431 2C45 2C31 2C30 372C 312E 3532 2C30 3030    41,E,1,07,1.52,000
             3139 2C4D 2C30 3233 2C4D 2C2C 2A35 430D 0A2F    19,M,023,M,,*5C..⁄
             2447 5056 5447 2C30 3030 2E30 2C54 2C33 3537    $GPVTG,000.0,T,357
             2E39 2C4D 2C30 3030 2E30 302C 4E2C 3030 302E    .9,M,000.00,N,000.
             3030 2C4B 2A34 360D 0A3B 0000 0000 0000 0000    00,K*46..;........
19:29:20 BAS:3B48/11/08 f=0 (30DBB2) 4/<MRM> seq=E0 l=001
             MPAK: (000001) (30DBB2) 01/[LIVE] 00 00 00 00
19:29:21 BAS:3B48/11/08 f=0 (30DBB2) 4/<MRM> seq=61 l=004
             MPAK: (000001) (30DBB2) 01/[GROUPLIST] n=001 (000007)
             0000 0000 0000 0000 0000 0000 0000 0000 0000    ..................
             0000 0000 0000 0000 0000 0000 0000 0000 0000    ..................
             0000 0000 0000 0000 0000 0000 0000 0000 0000    ..................
19:46:50 BAS:3B48/11/08 f=0 (30DBB2) 4/<MRM> seq=E0 l=001
             MPAK: (000001) (30DBB2) 01/[LIVE] 00 00 00 00
19:55:19 BAS:3B48/11/08 f=0 (000007) 1/<MRM> seq=1F l=001
             MPAK: (000001) (000007) 00/[TIME] t=B5BB66 00
20:15:19 BAS:3B48/11/08 f=0 (000007) 1/<MRM> seq=1F l=001
             MPAK: (000001) (000007) 00/[TIME] t=B5BB7A 00
20:25:20 BAS:3B48/11/08 f=0 (30DBB2) 4/<MRM> seq=E0 l=001
             MPAK: (000001) (30DBB2) 01/[LIVE] 00 00 00 00
```

Demo of network snooping

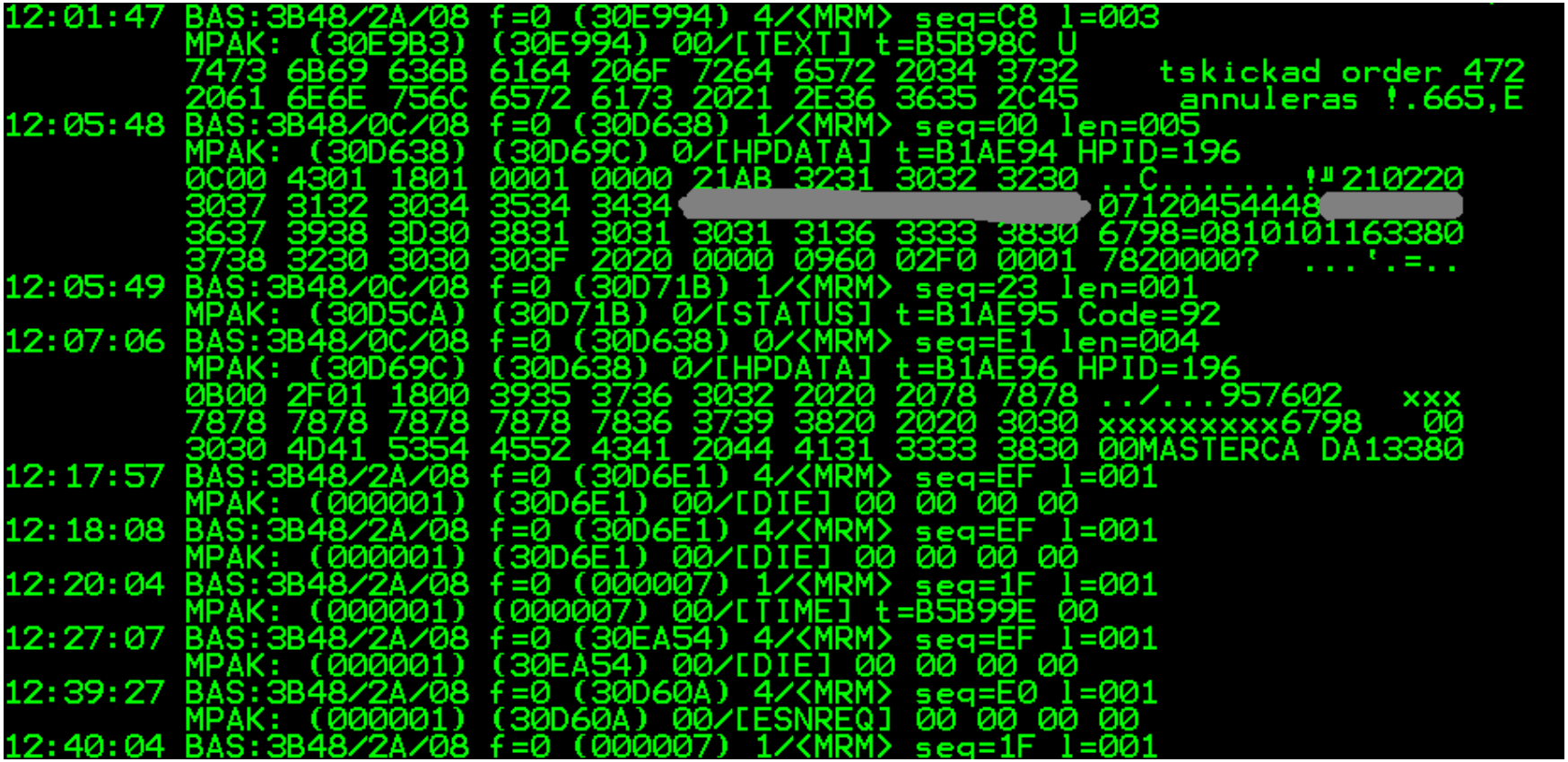
```
04:03:28 BAS:C4D7/08/01 f=0 (A1F930) 5/<MRM> seq=14 l=028
             MPAK: (4C4E60) (A1F930) 02/[DATA] t=BA6FE2 7E
             0000 4000 0200 0220 100D 4742 4953 584E 4143    ..@.... ..GBISXNAC
             3031 5330 3720 0831 3036 3135 3038 3800 6B73    01S07 .10615088.ks
             EF0E 5005 434D 494D 4503 4083 3400 0000 10CA    n.P.CMIME.@Γ4....-
             0048 6565 6431 34FC 5A0F F89F E29F 8AFF 45DE    .Heed14nZ.▒âGâǒáEª
             E5FE 47FA ED29 FD25 FE3B FD57 D5F9 184F BE1E    sªGπf)▒⁄ª;▒W+π.O+.
             04BF 4C5E 4AF6 0472 9681 75CF C826 CD7A 4957    .+L^J≈.r√"u-+&-zIW
             2EC3 B6B0 5D8B B0BB B0C3 7612 5DEB 04BF C061    .+ªª]∩ª+ª+v.]d.++a
             B1A9 6B07 4070 EC51 BF8D CFC1 6974 7E00 DEB5    ª¼k.@p8Q+∞--it~.ªª
             F339 C994 EB90 4D50 75E8 46F0 7A77 D35F 3A47    =9+÷d╔MPuFF=zw+ _:G
             6272 6F4C 2F4B E0AB AF63 751E 940D ED5B 7356    broL/Kaⁿ╗cu.÷.f[sV
```

```
17:21:07 BAS:C4D7/1D/01 f=0 (471BA7) 4/<MRM> seq=70 l=030
             MPAK: (4C4E60) (471BA7) 02/[DATA] t=BA72FF F4
             0001 4000 0200 0220 1007 4735 3035 3530 3520    ..@.... ..G505505
             0734 3636 3031 3335 007C F3F0 F450 0543 4D49    .4660135.|==(P.CMI
             4D45 0340 8374 0000 0010 CA00 5377 7485 7646    ME.@Γt....-.Swt∝vF
             2B0A 0C3F F03F C10B 90AE 42C0 1519 0F5C 10C3    +..?=?-.╔½B+...\.+
             B2EB 8E81 9521 BFF4 07FD 8874 AA96 B911 7FD6    ªd—"≥!+(.▒Ωt¼√ª.ª+
             4E55 30A7 2B24 3850 270E 0402 21AE 07B0 71B8    NU0‖+$8P'...!½.ªq+
             5E53 A0CF 35DE 0EE7 6F26 AA92 B252 AECB 3191    ^Sβ-5ª.to&¼╞ªR½-1μ
             CB51 A038 2814 70FF AD97 1B2A 2876 11AA 7C19    -Qβ8(.páí•.*(v.¼|.
             86E8 B42F FB25 6469 467E 70F3 8C32 A102 5E6B    σFª/v%diF~p=∈2ø.^k
```

Demo of network snooping

```
16:33:00 BAS:C4D7/08/01 f=0 (4CBD4C) 4/<MRM> seq=EB l=001
             MPAK: (000001) (4CBD4C) 00/[ESNREQ] 00 00 00 00
16:33:02 BAS:C4D7/08/01 f=0 (4CBD4C) 4/<MRM> seq=7C l=005
             MPAK: (4CBD4C) (4CBD4C) 00/[DATA] t=BA72CF 20
             4956 4920 4368 6563 6B6D 6174 6520 456C 6974    IVI Checkmate Elit
             6520 3730 3020 2863 2920 3139 3939 2041 524D    e 700 (c) 1999 ARM
             2043 6F6D 7075 7465 7220 5465 6368 6E69 7175     Computer Techniqu
             6573 2049 6E63 2E00 0000 0000 0000 0000 0000    es Inc.............
16:35:16 BAS:C4D7/08/01 f=0 (000007) 1/<MRM> seq=1F l=001
             MPAK: (000001) (000007) 00/[TIME] t=BA72D1 00
20:55:55 BAS:C4D7/1D/01 f=0 (4CC6C2) 4/<MRM> seq=E6 l=005
             MPAK: (018704) (4CC6C2) 00/[HPDATA] t=BA73D6 HPID=192(user specific)
             4353 5620 3230 3020 4F4B 0D0A 7265 633D 3130    CSV 200 OK..rec=10
             2668 6D61 6E3D 3530 3132 3032 3126 6463 746D    &hman=5012021&dctm
             723D 3726 7478 7374 6D72 3D34 3026 7265 6A72    r=7&txstmr=40&rejr
             633D 3326 6973 746D 723D 3230 0D0A 0000 0001    c=3&istmr=20......
20:58:24 BAS:C4D7/1D/01 f=0 (4C9BD8) 4/<MRM> seq=E1 l=001
             MPAK: (000001) (4C9BD8) 00/[ESNREQ] 00 00 00 00
21:01:36 BAS:C4D7/1D/01 f=0 (46D0A6) 0/<REB> seq=08 l=001
             DATA: 01 A0 00 00 00 00 00 00 00 00 00 00 00
21:15:10 BAS:C4D7/08/01 f=0 (4CC581) 4/<MRM> seq=78 l=007
             MPAK: (4C7A35) (4CC581) 00/[HPDATA] t=BA73E9 HPID=193(user specific)
             0020 392E B8B1 B836 B1B1 B433 30B2 A0A0 A0A0    . 9.+ª+6ªªª30ªßßßß
             A0A0 A0A0 A0A0 A0A0 A0A0 30B8 3033 B236 B133    ßßßßßßßßßß0+03ª6ª3
             B130 B4B8 C6CF 3030 3030 3030 30B1 9CC6 B2B1    ª0ª+ª-0000000ªúªªª
             B739 B4B8 A0A0 9C47 B4B2 42B1 3535 C535 9C55    +9ª+ßßúGªªBª55+5úU
             339C D830 309C E7BD 9CE8 3030 B130 36B2 30B1    3ú+00út+úF00ª06ª0ª
             3930 9CF3 3044 3000 0000 0000 0000 0000 0000    90ú=0D0............
21:15:18 BAS:C4D7/08/01 f=0 (000007) 1/<MRM> seq=1F l=001
             MPAK: (000001) (000007) 00/[TIME] t=BA73EA 00
```

Demo of network snooping



Q & A

- Questions?
- Experiences?
- Comments?
- Requests?