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
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
  - Velocita Wireless (AT&T, Cingular, RAM)
  - Rogers Wireless (Cantel)
- 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!

• Everything revolves around MPAK packets with 24-bit src/dst MAN addresses
  – That's just like IP packets, I know this!

• Poor adoption of layer 4 standards
  – Most applications “roll their own”
The Mobitex protocol suite

• Layer 1 – Radio layer
  – 896-901Mhz Up / 935-940Mhz Down
    • 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
  – Radio frame header with base ID and flags
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
  - Link header with frametype and length
  - Slotted ALOHA access mechanism with automatic repeat requesting (ARQ)
  - Network parameters broadcasted
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, etc.
    • Packet class and type designation
      – PSUBCOM / DTESEerv packet classes
    • Optional address list appended
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, ESNREQ, LOGINREQ, 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
    • Standard profile for connecting fixed terminals to area exchanges (MOX)
Security features

- Privacy protection
- Subscriber identification
- Denial of service
- Network snooping
- Live Demo!
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
  MsgId: <332A0580@geocities.com>
  From: arron5@geocities.com
  Subject: Fun mobitex stuff
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
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)
  – Mobile terminal 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

- Terminal subscription identified by ESN
- ESN calculated from terminal S/N
- ESN only req. 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 denial of service

- Wide-band jamming transmitters
  - Available off-the-shelf and as DIY kits
- “Rogue base station”
  - Implement wireless base using e.g. USRP
- Selective DOS targeting specific terminal
  - Spoof “DIE” DTESERV packets with dst MAN
Network snooping - prerequisites

• Radio that receives the correct frequency

• 8kbit GMSK - need FM discriminator tap
  – Google is your friend...

• Software
  – Commercial software ($$$)
  – Mine, as I'll show you next...
Demo of network snooping
Conclusions

- Mobitex wireless networks insecure
  - Compare IPv4 over unencrypted WiFi
- No confidentiality, serious problems with integrity and availability under attack
- Application developers and system owners need to address these issues
- Security needs to be built into apps
  - Authentication, message integrity, encryption
Q & A

• Questions?
• Experiences?
• Comments?
• Requests?