FMC
(Fixed Mobile Convergence)
What About Security?

Vancouver – June 2008

Franck Veysset, Orange Labs
Firstname.lastname at orange-ftgroup dot com

research & development
Agenda

- Introduction - FMC?
- WIFI-SIP overview
- UMA overview
- Femtocell overview
- iWLAN Architecture
- Security?

"Technology overview (not FTGroup network strategy)"
New needs – new offers

- Simplify the current situation (PSTN, GSM, VoIP phones at home !!)
- Use of a single phone (wireless)
  - At home and on the road
- Enhance quality / coverage at home
  - WiFi: Use your own A.P. at home – improve cellular coverage
  - Handover GSM/WIFI?
- Higher data rate -> new services?
- Lowers communication costs (at least from the customer point of view)
  - Good for ARPU and market shares
- One phone = increase reachability

Different technologies are available

- WiFi-SIP
- UMA (GAN)
- Femtocell / picocell
- Others…
FMC?

- Fixed to Mobile Convergence
- First tests: Denmark, 1997 – PSTN/GSM
  - Single number, one messaging system
  - No handover
- First “real” offers in 2005 – UMA based
  - BT with “Fusion”, Bluetooth based at its beginning
- In France, “emergence” of FMC?
  - After Triple play offers, quadruple play is becoming the standard…
    - Twin / beautifulphone (Dual phone GSM/WiFi SIP?) by n9uf Cegetel
    - Free phone (GSM/WiFi SIP)
    - Unik (GSM/UMA, Orange)
FMC (2/2)

- Real FMC possible with WiFi wide adoption

- Low-power WiFi chips
  - Phone (and WiFi) needs to be always on
Other “technologies” exist...

- More or less in use
- Don’t provide handover

- Bluetooth VoIP
  - Bluetooth dongle (Siemens)

- Dedicated WiFi phone
  - Netgear Skype WiFi Phone
    - Netgear SPH101
  - Other partnerships between pure internet players and manufacturers

- SIM reader on fixed phone (to import contact list!)
Wi-Fi SIP
(Session Initiation protocol)
SIP: Intro

- **Internet World**
  - SIP is an IETF standard (2002)
  - SIP provides signaling
  - Voice transport relies on RTP

- **WiFi-SIP very similar to genuine VoIP-SIP**

- **On the terminal**
  - SIP and RTP stack: signaling and stream
  - Add IP and WIFI stack
  - This is a WiFi SIP-phone

- **SIP: just add another application on your Wi-Fi terminal**
  - Disjoined from GSM access
  - No handover (except with GSM “private extensions”)
Wi-Fi SIP Overview
SIP Security

- **Authentication**
  - At best id and password (http digest)
  - Strong authentication is possible but not mandatory (read: not used…)
    - Need to be supported by terminals and servers

- **Confidentiality**
  - Usually: Clear text… (RTP…)
  - It is possible to use SRTP (and SIP TLS) but…
  - Therefore relies on Wi-Fi security (critical path)

- **Strong lack of security functionalities**
  - Does low cost means lack of functionalities?
  - Sip design & security (IETF way…)

- **Wi-Fi security is then critical**
  - WEP only? 😐
UMA
(Unlicensed Mobile Access)
UMA: Intro

- From the telco world
  - UMA Consortium (Alcatel, BT, Cingular, Ericsson, Motorola, Nokia, Nortel, RIM, Siemens, Sony Ericsson, etc.)
  - UMA not a standard, but specifications pushed into 3GPP (GAN)
- Provides an alternative access to 2G/3G services

- On the terminal
  - IPsec stack: to reach the UMA platform
  - UMA stack: GSM packet encapsulation in IP (includes RTP…)
  - And of course IP+WiFi stack
  - SIM (USIM) for crypto (authentication, encryption…)

- UMA: alternative access to GSM network
  - Full access (Voice, GPRS, SMS…)
http://www.umatechnology.org/
UMA Overview
UMA Functional Architecture
UMA Security

- **Authentication**
  - Authentication relies on the SIM/USIM
    - IKEv2 and EAP-SIM / EAP-AKA (mutual) + X509 (server side)
    - Then genuine GSM authentication (A3/A8)

- **Encryption**
  - Wi-Fi security for domestic link
  - IPsec between terminal and UNC
  - Warning: NULL encryption possible on IPsec link
Femtocell
Principles

- Femtocells are low-power wireless access points that operate in licensed spectrum to connect standard mobile devices to a mobile operator’s network using residential DSL or cable broadband connections (cf femtoforum.org)

- New way to connect to 2G/3G network

- Increase telco. coverage

- IP connection to core network

- Any 2G/3G handset supported
Femtocell Architecture (3G)
Femtocell Security

- No standardization yet (Work in progress)
  - Femtoforum, 3GPP…

- Authentication
  - User and/or network authentication rely on the SIM/USIM
    - Genuine GSM/UMTS world…
  - What about the *cell authentication? Usim?

- Encryption
  - Idem, genuine GSM/UMTS functionalities

- Questions: Iub+ / A/Gb interfaces?
  - BSC/RNC connected to the internet?
  - IPsec on Iub+ link?

- Security of customer’s RNC (thee *cell) is the key point
iWLAN
I-WLAN Architecture
I-WLAN Security

- Security similar to UMA
- PDG located in a different place than in 3GPP architecture (PDG in the core network)
I-Wlan Issues

- For now, data only services
- IPsec gateway on internet
  - Attacks always possible
- Specific attacks on IKE v2, EAP-xxx… fuzzing for example
- When the user is connected, access only to Wi interface
  - Almost identical to genuine GPRS access
  - Core network should not be reachable
- But the technology still looks quite immature
Problems, security issues?
Quick Analysis

- Not exhaustive

- New technology… stay tuned for more information

- Implementation proprietary
  - GAN conformity still to be confirmed
  - SIP: relies on provider implementation / architectural choices
  - Cell: also relies on provider implementation and tech choices
  - I-WLAN: lack of standardization
WiFi AP…

- First thing: needs for a Wi-Fi access point
  - Open, WEP, WPA?
  - WiFi always on?

- This might have strong impact on your security

- Corporate case: deploy or reuse existing Wi-Fi network
  - Mix voice and data on the same network?
  - With uncontrolled internet access?
Authentication (SIP, EAP…)

- **SIP authentication**
  - May rely on clear text 😊 or HTTP digest
  - MD5 is not particularly “on the rise”…
  - Brute force attack is feasible on low entropy passwords
    - 40 Millions MD5 per second on a Bi-Xeon (mdcrack)
    - More than 100M on well chosen hard (PS3…)

- **EAP-AKA or EAP-SIM authentication**
  - Looks quite healthy
  - Tamper resistant hardware is definitively a plus
General comments

- Exposing Telco core network?
  - Fuzzer anyone?
  - This might be the next big threat

- Sensible devices are located at customer premises?

- Handling and locating emergency calls?

- Towards new frauds?

- Impact on customer network
  - QoS on shared network…
  - Power outage…
Questions?

Thanks for your attention