Security Implications and Considerations for Femtocells

Marcus Wong
mwong@huawei.com
Agenda

- Introduction
  - Architecture
  - Latest attack
- Overview
  - Threats and attacks
  - Security Requirements
  - Security Considerations
- Femto Success Stories
- Q&A
Femtocell Commercial Deployments

- Sprint launched AIRAVE (CDMA) at Sep, 2007
- Vodafone launched “3G INN” at Nov, 2009
- AT&T launched “3G MicroCell” at Mar, 2010
- China Unicom launched “HomeZone” at Nov, 2008
- SoftBank launched “Wireless Network extender” at Jan, 2009
- StarHub launched “CallZone” at Oct, 2009
- DoCoMo launched “MyArea” at Nov, 2009
- Optimus launched “Sinal ON” at Jan, 2010
- SFR launched “Home 3G” at Nov, 2009
- KDDI launched “au Femtocell” at 1st of July, 2010

...significant growth over the next few years, reaching just under 49 million femtocell access points in the market by 2014. (source: Informa)
Architecture

• Femto AP: home-based base station
  – Low cost solution to extends operator network (~$100 / unit vs several $k for larger cells)
  – Provides new services with higher data rate at relatively lower cost
  – 3GPP terminology for FAP = HNB (UMTS) or HeNB (SAE/LTE)
  – Vulnerable to attacks (e.g. traditional-IP based attacks and accidental hackers)

• Requires IP connectivity
  – Connects to home-based or small office-based IP network
  – Accesses operator core via insecure connections

• Operates at licensed spectrum

• Accommodates different billing models
  – Depending on ownership of FAP: subsidy-based or traditional billing
Recent Attack

• What happened?
  - XXX’s early 2009 BSR 9356 model using Picochip PC202
  - Admin interface not disabled inside the case
  - Root password used to gain access to console
  - disabled firewall and changed configurations

• Damage
  - listening on conversations
  - change to open mode CSG
  - use in unauthorized areas
Threats and Attacks

- Compromise of Femto Credentials
- Physical attacks on a Femto
- Configuration attacks on a Femto
- Protocol attacks on a Femto
- User Data and identity privacy attacks
- Attacks on the core network
- Attacks on Radio resources and management
Femto Security Requirements

- Strong credentials, authentications, confidentiality, and integrity
- Secure backhaul link to the operator core network
- Secure Access Control
- Protection for clock signaling and synchronization
- Location verification and authentication
- Local interface protection
- Tamper proof platform
- Firewall and high layer protection
- Secure configuration, software, firmware download
- Remediation and recovery
- User data and privacy protection
Authentication Considerations

- **Who and what to authenticate**
  - MS (i.e. subscription) vs User ("owner" of Femto)

- **Device Authentication**
  - Need to authenticate equipment physically located in user premise
    - Additional risk for being located in user accessible location
  - Device credential either PSK or certificate

- **"Subscription" Authentication**
  - "Subscription" depending on operator model, may not be tied to billing
  - SIM-based credentials for simpler "subscription" management

- **Combined authentication**
  - Binding device/subscription id and/or credential
  - Local or network binding further limit usage of Femto
Secure Backhaul Considerations

- Insecure backhaul between Femto and SeGW over public IP network
  - SeGW is single point of entry into a private operator network
  - Mutually authentication alone is insufficient
  - Link should be secure as well (e.g. HTTP vs HTTPS) as robust
    - Secure tunnel is a MUST for this link
    - May need separate tunnels for control/user/management traffic
      - better security and better QoS handling
  - IPsec or TLS can be used
    - Benefits of IPsec outweighs the overhead associated
Location Security Considerations

- Femto assumed to be fixed in location
  - Users generally not allowed to relocate Femto to another location
  - Maybe based on billing/charging arrangement
  - Need to satisfy regulatory requirement (e.g. E911, spectrum license)
  - Not 100% precise, but close enough

- Location Authentication
  - Femto-based GPS or A-GPS
    - Cost of Femto increases
  - Femto IP
    - IP assigned by internet service provider
      shared with the wireless operator
  - Femto + macro cell
    - Femto within neighboring macro cell coverage area
  - Femto IP + MS
    - MS maybe GPS-equipped
    - CN may provide location service to UE
    - Only works if/after MS attaches to Femto
System Security Considerations

- **Femto Platform Physical Security**
  - Trusted Environment provide root of trust for the femto device
  - Trending toward TPM (Trusted Platform Module) technology

- **Access Control**
  - ACL (Access Control List)
    - List of MS allowed to access a particular Femto
    - Can be “black” or “white”
    - Management of ACL by owner or operator
  - CSG (Closed Subscriber Group)
    - List of cells or Femtos a MS is allowed to access
    - UE and CN need to maintain CSG list

- **Clock Signaling**
  - Protection needed for vital Femto functions, such as device-certificate based authentication (e.g. checking expired certificates)
  - Synchronization with either macro cell or Clock Server in IP network
Other Security Considerations

• **FMS (Femto Management System)**
  – Protects software and configuration download
    • IPSec for traffic going through SeGW
    • TSL for direct connection to FAP

• **Minimize/Eliminate Local Interfaces**
  – Protect internals of FAP
    • Maintain integrity of configuration and/or software
    • Prevent accidental attack
  – Prevents attacks cascading to CN via FAP

• **Firewall**
  – Necessary protection for
    • Common IP-based attacks (DoS, scanning, spoofing, etc.)
    • Attacks coming from backhaul
Nation-wide Femto networks deployment

- **Challenges and Needs**
  - Grasp new 3G users
    - Second large operator; launched 3G UMTS in 09Q1
    - and iPhone in 09Q3
  - Poor Indoor Coverage
  - Heavy MBB traffic load after iPhone shipment

- **Solution and Benefits**
  - Huawei’s E2E femto solution covered 18 provinces platform ready for commercial launch, 11 pre-commercial site, 1 commercial case
  - Resolved 3G fast-deployment problem, accelerated 3G applications.
  - Deployed following subscribers’ needs, accurately coverage and billing through customer authentication
Aiming at High value SME Customers

SingTel brings You Easier Office with CallZone!
Aiming at High value users and improve coverage

Vodafone Greece: Consumer Market
150€.
If ARPU > 40 €, free
If 20 € < ARPU < 40 €, 75 €

Vodafone Spain: Business market
€15 per month.
branded 'Voz y Datos Premium Oficina Vodafone,'
High Speed Home MBB for StarHub

Business Plan of Starhub

- Brand: HomeZone
- Monthly rental: $16.05
- Contract period: 12 months
- AP replacement: $369.15

Global 1st commercial mobile broadband network with Femto cell in StarHub
SINAL ON to improve end user’s experience