Mobile Security

GSM, UTMS, Wi-Fi and some Bluetooth

Today's Lecture:

- Security in the mobile world
- GSM
- 3GPP / UTMS
- Mobile IPv6
- Wi-Fi
- Bluetooth

Introduction:

- Mobile computing one of the fastest growing segments of the PC market

- What is a mobile network?
  - Changing physical / geographical location
  - Changing network topology
  - Attached somewhere to a fixed network
  - Wireless communication

Introduction:

- What is different about mobile networks?
  - Low bandwidth – minimise message size and volume
  - Increased risk of eavesdropping
  - Security issues
    - Authentication
    - Privacy
    - Charging

Introduction:

- Mobile services pose new challenges
  - Some derive from technology
  - Some from applications

- Physical access – no longer a barrier to network
  - Wi-Fi access to corporate networks

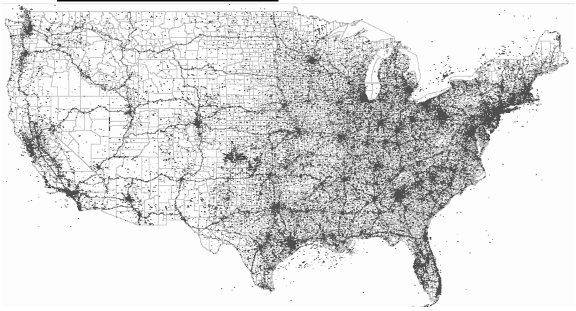
Introduction:

- Current most active mobile technologies
  - GSM
  - 3GPP/UTMS
  - Mobile IP
  - IEEE 802.11
  - Bluetooth

Introduction:

- Other areas of mobile networks with security implications
  - WAP – Wireless Application Protocol
    - -Malicious scripting, Infrastructure issues
  - SMS – Short Messaging Service
    - -Spam, spoofing, viruses
  - MANETs – Mobile Ad-hoc Networks
    - - Rogue nodes, Security only at academic stage

GSM – 220 000 Cell Towers:



GSM:

- 1st Generation Cell Phones
  - Charge fraud – simple authentication
  - Alibi creation – call forwarding
- GSM – Improvement from 1st generation
  - Good voice quality
  - Cheap end-systems
  - Low running costs
  - etc..

GSM:

- Creation affected by political influences
  - Differing national regulations and attitudes towards cryptography
  - Law enforcement requested ability to wiretap
- GSM security goals
  - Protection against charge fraud
  - Protection of voice and signal traffic
  - Phone theft tracking

GSM:

- Components
  - GSM user – subscriber in *home network*
  - Where service requested – *serving network*
  - Mobile station comprises
    - - Mobile equipment
    - - Subscriber Identity Module (SIM)
  - SIM card – smart card chip
    - Performs cryptographic operations
    - Stores keys
    - Stores personal data

GSM:

- IMSI – International Mobile Subscriber Identity
  - Unique subscriber identification
- TMSI – Temporary Mobile Subscriber Identity
  - Used to avoid location tracking
  - Served when device joins a new subnet
- IMSI catchers
  - Device authenticates to network but not vice versa
  - Catcher masquerades as a base station
  - Collects IMSI numbers

GSM:

- Cryptography
  - Uses symmetric cryptography
  - 3 algorithms
    - *A3* – authentication (Provider specific)
    - *A5* – encryption (Standardised)
    - *A8* – key generation (Provider specific)

- No official publication of algorithms exists
- Cryptanalytic attacks do exist

GSM:

- Location Based Services
  - GSM network records location information of mobile equipment
  - Used for various services (e.g. traffic info)
  - Used for emergencies (Medical, Police, etc…)
  - Obligatory in some countries (e.g. the US)

  - Privacy implications

GSM Summary:

- GSM does not transmit secrets in the clear
- Voice traffic encrypted over radio but not after base station
- Some privacy protection through TMSI
- but IMSI catchers exist to avoid TMSI
- Law enforcement has access to recorded location data

GSM Summary:

Criticism:

- Cryptographic algorithms not made public
- Unilateral authentication
  - Only mobile equipment authenticates to the network

Fraud:

- Revenue flow attacked
- *Roaming fraud*
- *Premium rate fraud*

3GPP/UTMS:

- Universal Mobile Telecommunications System
- Next generation of GSM
- Besides technical advancements, contains some security enhancements
- Security architecture similar to GSM

- Avoids IMSI Catchers
  - Due to mutual authentication of mobile equipment to the network and vice versa

3GPP/UTMS:

- Authentication
  - Support for mutual authentication
- Privacy
  - Increased key sizes
  - Support for securing core network signalling data
  - Enhanced user identity confidentiality
- Other
  - Integrity of signalling
  - Cryptographic algorithms made public

Mobile IPv6:

- GSM & UTMS have problems with access control due to lack of pre-established relationship
- In IP if nodes move around:
  - When IP address kept, data will not reach node at new location
  - When IP address changes, communication has to be terminated and restarted

Mobile IP deals with these issues

Mobile IPv6:

- Mobile node has two addresses
  - permanent *Home Address*
  - *Care of Address* – associated with network the node is visiting

- Addresses consist of location as well as interface identification

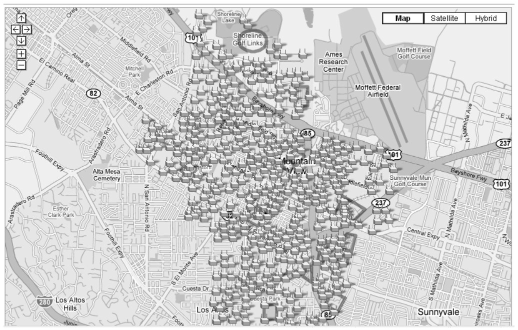
Mobile IPv6:

- *Home agent* – nodes with permanent address within agent's network
- *Foreign agent* – nodes visiting network

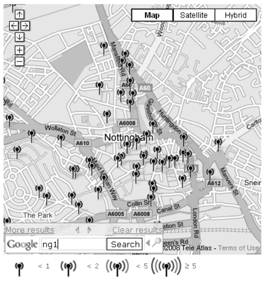
- When a node wants to communicate with another node, it uses its *home address*
- Packets sent are intercepted by *Home agent*
- *Home agent* uses care-of address advertised by *Foreign Agent* to communicate with destination node

Wi-Fi:

- Wireless technology generally based on a set of standards called IEEE 802.11
- A number of standards *(a,b,g,n)* exist depending on speed and technological improvements
- A number of security protocols proposed
  - WEP
  - WPA
  - WPA2



Wi-Fi:



- Wi-Fi Increasingly used at home and as part of businesses

- New uses emerge frequently
  - City wide Wi-Fi
  - BT FON

Wi-Fi:

- Many Issues:
  - Incorrectly setup Access Points
    - Encryption
    - Access control
  - Wi-Fi not included in security policies in many institutions
  - Weak encryption standards used
  - Rogue Access Points
  - War-driving

Wi-Fi:

- WEP
  - Key size a major security limitation
  - Algorithm is susceptible to a cryptanalysis attack
  - It uses the RC4 stream cipher algorithm
  - WEP allows certain packet parts to be reused
  - This allows attacker to obtain some known text
  - The rest is only a matter of statistical analysis

Wi-Fi:

- WEP
  - Original attack required hours of collected data to successfully find encryption key
  - 2007 – WEP cracked under 60 seconds by researchers from Germany
- WPA
  - A quick preliminary solution to WEP issues
  - However vulnerable to a password guessing attack

Wi-Fi:

- WPA2
  - A complete redesign of WLAN security mechanisms
  - Stream cipher RC4 replaced by AES
  - but WPA2 requires new hardware

To Remember:

- For Wi-Fi access points only use WPA2 or in worst case WPA
- WEP is totally broken!

Bluetooth:

- Technology for wireless ad-hoc networks
- For short range communications
- e.g. for keyboards, headsets, etc..
- Contains cryptographic mechanism for traffic protection between devices
- Application level attacks exist
  - Bluesnarf exploits flawed implementations of access control – retrieves personal information
- Viruses are beginning to appear

http://www.f-secure.com/weblog/archives/archive-072007.html

Summary:

- Security in the Mobile environment
- Current mobile technologies