Security and Privacy in Wireless Systems

Professor Randy H. Katz
CS Division
University of California, Berkeley
Berkeley, CA 94720-1776

1

Security Levels

- **Level 0: No Privacy**
- **Level 1: Equivalent to Wireline**
  - For routine conversations
  - Significant level of effort to "crack" conversation (e.g., 1 year)
- **Level 2: Commercially Secure**
  - For "proprietary" conversations
  - 10-25 years to crack
- **Level 3: Government/Military Secure**

2

Privacy Requirements

- **Privacy of Call Setup Information**
  - e.g., calling #, credit card #, type of service, etc.
- **Privacy of Speech**
- **Privacy of Data**
- **Privacy of User Location**
  - Radio link eavesdropping
  - Unauthorized access to VLR/HLR
- **Privacy of User Identification**
  - Encrypt user id to protect against analysis of user calling patterns
- **Privacy of Calling Patterns**
  - Protect against traffic analysis of user: calling number, use of the MH, caller ID, privacy of financial transactions
- ***But law enforcement must be able to wire-tap***

3

Theft Resistance

- **Clone Resistant Design**
  - Over the air eavesdropping
  - Network databases
  - Network interconnect
  - Intersystem validation: enough to authenticate but not enough clone
- **Installation and Repair Fraud**
  - Multiple mobile hosts programmed with same ID
- **Unique User ID**
  - User unique security module (e.g., smart cards)
- **Unique Mobile Station ID**
  - Uniquely identify MS to avoid re-registrations with new users

4

Security and Privacy in Existing Wireless Systems

- MIN/ESN
  - AMPS: 10 digit mobile ID, 32 bit equipment serial number
  - All data sent in clear, systems share info on bad MIN/ESN
- Shared Secret Data
  - TDMA/CDMA cellular: secret key shared between mobile station and system
- Security Triplets
  - GSM: challenge/response pairs plus privacy key
  - Home system generates 3-5 for visited system; One used per connection
- Public Key
  - PACS proposed as an option
  - Avoids need for communications with home system

MIN/ESN Authentication

- Phone is uniquely identified by 10 digit MIN and 32-bit serial number
  - Serial number is supposed to be in “tamper proof” hardware
  - In reality, it is stored in EEPROM--easily duplicated from sniffed MIN/ESN pairs
- At call set-up:
  - First check list of bad MIN/ESNs
  - If not found, authenticate with home system
  - Not all system support realtime authentication
- System has recently been extended to support user entered PIN

Shared Secret Data

- Common authentication key in mobile station and cellular network (64-bit key), in addition to ESN and 15 digit Intl Mobile Subscriber ID (IMSI)
- Registration
  - MS sends IMSI to system; VLR queries HLR; VLR assigns Temp MS ID (TMSI)
  - Latter step used to insure anonymity of user (control link)
- Authentication
  - System transmits RAND om control channel
  - MS encrypts using its key, system does same calculation
  - Airlink is encrypted with shared key
- Call Counter
  - MS and system keep running count of placed calls
  - Helps to defeat cloning based only on ESN/IMSI information

7

Shared Secret Data

- Registration Types
  - Distance-based: re-register when mobile has moved a threshold distance of cells
  - Geographic-based: re-register when entering new region
  - Parameter change: re-register when operating parameters change
  - Periodic: system forces a re-registration
  - Power down: (de)register when MS is turned off
  - Power up: register when MS is turned on
  - Timer-based: MS re-registers whenever a timer expires; allows system to drop registrations that “age”

8

Token-Based Authentication

- Does NOT require the sharing of secrets between local/home service providers
- Triplet: <RAND, Response, Encryption Key>
  - Computed in home authentication center (and MS)
  - Stored in visited VLR
- Registration process:
  - MS sends registration request
  - Network gets triplets from mobile’s HAC (note that local service provider knows nothing about the algorithm to derive responses to challenges!)
  - Network sends unique challenge
  - MS calculates response, and replies to network
  - If match, then MS is registered with local system
- No call counter, but subscriber identity module (SIM)

Public Key Authentication

- MS has private key and public key;
  network has private key and public key
  - Sender encrypts message with receiver’s public key; receiver decrypts message with own private key
  - Sender can digitally sign a message by encrypting it with own private key; receiver uses sender’s public key to decrypt
- MS knows system’s public key; network must know public key of all MS’s
  - Use public key scheme to exchange secret encryption key for connection security

Summary

- **MIN/ESN**
  - Very poor privacy/security support, easily cloned
- **Shared Secret Key**
  - Reasonable privacy/security support, but requires systems to exchange keys of visiting mobile stations
  - Since airlink is encrypted, may need to wiretap at the switch
- **Token-Based**
  - Like shared secret key, but does not require systems to share keys; algorithms used by MS and its home system need not be known by visited system
  - Some potential problems if tokens are reused (because of latency to obtain new triplets)
- **Public Key**
  - Strong privacy/security: MS and network never reveal their private keys
  - Complexity of encryption operations