Lecture 23: Security and System-Level Limitations

GSM and CDMA Systems

DI05011011: Mobile Communication

Agenda for Today

- 1. GSM Security Vulnerabilities (Unilateral Authentication)
- 2. The 'Stingray' / IMSI Catcher Threat
- 3. Ciphering Algorithm Weaknesses
- 4. CDMA Security Limitations
- 5. The Global Roaming Problem
- 6. Summary of the 2G Era

1. GSM Security: Unilateral Authentication

- In GSM, the network authenticates the mobile device (SIM card).
- **Major Flaw:** The mobile device DOES NOT authenticate the network.
- The phone simply trusts that any tower claiming to be its home network is legitimate.
- This is called 'Unilateral Authentication'.

2. The IMSI Catcher ('Stingray') Threat

- Because of Unilateral Authentication, attackers can create 'Fake Base Stations' (IMSI Catchers).
- The fake tower broadcasts a stronger signal than the legitimate tower.
- Phones automatically connect to the fake tower.
- The attacker can then intercept calls, read SMS, or track the user's location.

3. Ciphering Algorithm Weaknesses

- GSM uses A5/1 and A5/2 stream ciphers to encrypt voice data over the air.
- These algorithms were kept secret initially (Security by Obscurity).
- Both have been heavily reverse-engineered and cracked.
- A5/1 can now be decrypted in real-time using rainbow tables and a standard laptop.

Lack of End-to-End Encryption

- GSM encryption only exists 'Over-The-Air' (from the phone to the base station).
- Once the signal reaches the base station, it is decrypted and sent over the core network in plain text.
- Anyone with access to the core network (or the microwave links connecting towers) can intercept the communication.

4. CDMA Security Limitations

- CDMA inherently offers better privacy because signals are spread across a wide band and look like noise.
- However, early CDMA (IS-95) also lacked mutual authentication.
- While harder to intercept than GSM, it is not impossible.
- Key management and distribution in early CDMA networks were complex and prone to administrative errors.

5. The Global Roaming Problem

- 2G fragmented the world into two camps: GSM and CDMA.
- A GSM phone could not talk to a CDMA tower (different modulation, different protocols).
- Even within GSM, different regions used different frequencies (900/1800 MHz in Europe/Asia, 850/1900 MHz in the Americas).
- **Result:** Early phones only worked in their home continent.

The Push for a Unified Standard

- The limitations of 2G (low speed, poor security, lack of global roaming) drove the ITU to create the IMT-2000 standard (3G).
- Goals for 3G/4G included:
- 1. Mutual Authentication.
- 2. IP-based packet switching for high-speed data.
- 3. Unified global standards to allow true worldwide roaming.

Summary of Unit 2 Limitations

- **GSM:** Limited by TDMA slots, hard handoffs, and weak (unilateral) security.
- **CDMA:** Limited by interference (near-far problem, cell breathing).
- **Systemic:** Lack of mutual authentication allows IMSI catchers.
- **Global:** Incompatible standards and frequencies prevented easy international roaming.

Next Lecture Preview

- In Unit 3, we move away from the network and look at the device in your pocket.
- **Next Lecture:**
- 1. Mobile Handset Block Diagram
- 2. The Baseband Processor
- 3. The RF Transceiver Section