Challenges related to unique identifier alteration, ITU-T SG11 activities, resolution through CEIR

Presenter: Biren Karmakar
Group Leader, C-DOT, India.
ITU SG11 Webinar, 13th Oct 2023.

Unique Identifier - concerns

- The international mobile station equipment identity (IMEI) is an identifier defined by 3GPP that aims to uniquely identify a mobile device across the globe.
- Mobile network access of any mobile device is allowed or rejected based on IMEI.
- If the value of the IMEI is compromised if the IMEI is not unique, not allocated by the global decimal administrator and cannot be relied upon.
- Such IMEI can not be used to track the original mobile.
- Modified value could be same with existing valid one – which will cause duplicate identifier.
- Make and models could not be detected with the modified identifier.

सी-डॉट
C-DOT

ITU

Use of IMEI in mobile communication

- Each time a mobile device is switched on, a call is made, or a location update/ IMSI registration is performed the network provider, it runs a check on the IMEI number of the device through the Equipment Identity Register (EIR) on its network – which also cross reference it with the blocklist.
- If it is on the blocked list, then the network will refuse to allow the device and its related subscription to access the network.
- In case IMEI is in tracked list, it's allowed for network access but with monitoring.
- In case IMEI is in permitted list, it's allowed for network access without any restriction.

सी-डॉट
C-DOT

ITU

IMEI reprogramming

- IMEI reprogramming refers to unauthorized changing or tampering of the IMEI which was programmed into a particular mobile device at the time of manufacturing.
- A mobile device's IMEI could be altered to enable illegal re-sale, thus facilitating theft and resale of mobile devices.
- According to 3GPP specification TS 22.016, IMEIs should not be changeable, but the specification does not indicate any details on implementation characteristics.

सी-डॉट
C-DOT

ITU

Impacts of tampered IMEI

- Non-traceability of stolen mobile devices
- Non-traceability of miscreants
- Restrict option of blocking IMEIs
- Limit Lawful interception
- Tax evasion
- Increased mobile theft
- National security challenge

सी-डॉट
C-DOT

Related Major SG11 Activities

- ITU-T Technical Report: QTR-RLB-IMEI-Reliability of International Mobile Equipment Identity (IMEI)
- Recommendation ITU-T Q.5052 - Addressing mobile devices with a duplicate unique identifier.

सी-डॉट
C-DOT

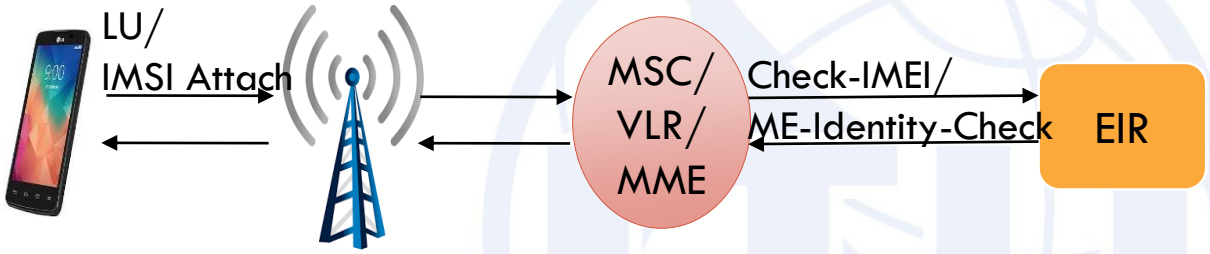
Role of CEIR in detecting

- IMEI tampering could be detected if Re-programmed IMEI is -
  - invalid.
  - non-allocated by GSMA.
  - allocated by GSMA and not used by manufacturers.
  - already in use in the network (duplicate).

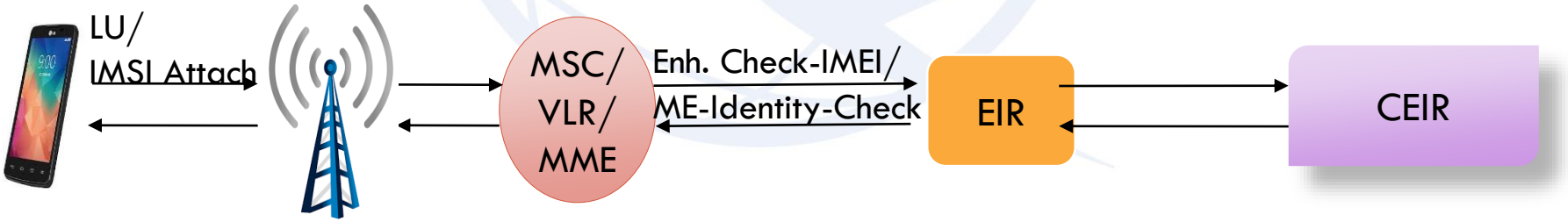
सी-डॉट
C-DOT

EIR to CEIR communication

Earlier Information Flow



Current Information Flow



Major CEIR features

- Detection of fresh cloned/ duplicate mobile and permit the use of existing mobile phones.
- Block stolen/lost mobile devices all over the country.
- Maintain Device Registry for
  - ✤ Locally manufactured devices
  - ✤ Imported devices
- Enhanced mechanism to report stolen/lost mobile devices
- Verification of cloned/duplicate/ blocked mobile devices - even before buying it - through Web-portal, Mobile App and SMS.
- Cloned/duplicate device authentication by competent authorities/ mobile manufacturers.

सी-डॉट
C-DOT

ITU

EIR – CEIR Interface

- As per ongoing ITU-T Q.Sup.CEIR-EIR-int "Common approaches and interfaces for data exchange between CEIR and EIR“, there are 3 interface options –
- API-Based (synchronous) interface
- API-Based (asynchronous) interface
- File-Based offline interface

सी–डॉट
C-DOT

सी-डॉट
C-DOT