IMEI Security Technical Design Principles

Enhancing Device Identifier Integrity to Combat Device Theft

V4.0 November 2016

Table of Contents

1. Introduction

Although the problem of device theft is not of the industry's creation, a range of stakeholders recognize device theft as being a major public policy concern and the need to reduce the attractiveness of stolen mobile devices by preventing their reuse after a theft. To that end, mobile network operators have the ability to block specific devices from accessing their networks. This functionality was originally created to block devices that were not approved or could cause interference on mobile networks and can now be used to take action against stolen devices. The blocking of devices is premised on a unique device identifier in conjunction with the operator blacklist database. It is incumbent on both device manufacturers and network operators to ensure they are adhering to the recommended practices in order for the industry to successfully combat theft.

To control network access, operators can create databases within their networks in which the electronic identities of devices can be stored. Devices to be disabled can then be registered on a "black list". During the registration and authentication process that occurs whenever a device attempts to connect to a mobile network the identity of that device is checked against the database and if it is contained in the blacklist, access will be denied.

Despite the need for mobile devices to have secure unique identities that cannot be changed, some devices had back doors designed in so that the identities could be easily changed for servicing reasons. Unfortunately, these back doors were discovered and exploited by unauthorized parties. This has resulted in identities being tampered with and network operators have reported the presence of devices on their networks with duplicated and invalid identities. This circumvention of the requirement that identities should not be capable of being changed outside the control of the original device manufacturer has the potential to undermine the efficacy of network blocking of stolen devices.

2. Device Identity Security

The effectiveness of device blocking on mobile networks is dependent on the secure implementation of device identities. Therefore, although network blocking does not represent the finite solution to device theft it is essential that it is complemented by the efforts of the device manufacturing community to ensure that devices delivered to market incorporate appropriate security features. Enhanced device identity integrity is essential to the efficient and effective network blocking of stolen mobile devices.

Although the mobile standards require that device identities should not be capable of being changed after the point of manufacture it became apparent over a number of years that identities were being changed with relative ease. This had the effect of jeopardising industry efforts to combat device theft as identities could be changed on stolen devices from the original identities that had been blocked thereby bypassing the action taken by network operators. That necessitated a concerted industry effort to consider what could be done to improve the mobile device security landscape. Significant efforts were made to improve the situation with real commitment and engagement by the device manufacturing community and these led to a series of initiatives that have been central to improved device identity security levels.

3. Design Principles

The commitment of the world's leading device manufacturers to GSMA led initiatives has been encouraging and indicated that initiatives could be taken that would have a positive impact on device identity security which would help increase confidence in the effectiveness of network blocking of stolen devices.

Although 3GPP TS 22.016 clearly mandates that IMEIs should not be changeable, the specification does not indicate any details on implementation characteristics. In order not to stifle innovation, the GSMA retains the view of not proposing to mandate a standardised way to achieve IMEI integrity but it is desirous to set out handset security principles to provide guidance to handset manufacturers and to provide operators with a set of high level criteria against which handset security can be assessed. It is recognised that further efforts have been made in this domain, for example OMTP TR0 and TR1 as well as individual manufacturer and operating systems vendors efforts to improve device and operating system security against well-funded and motivated attackers, but additional efforts are still required to maintain high levels of security and to address gaps in a rapidly moving threat and attack landscape.

Modification of device identities is a criminal offence in some jurisdictions but not in every country where websites and outlets exist that openly advertise the ability to change device identities. Developers of attacks against device identities are known to the based in the USA, Israel, India and Eastern Europe. Legislation to criminalize unauthorized device identity reprogramming, and enforcement of it and prosecution of offenders, could help reduce the attractiveness of this activity and the attendant problem of device identity changing.

4. IMEI Security Technical Design Principles

The following device security principles are provided to help device manufacturers develop a comprehensive security architecture that facilitates the deployment of a range of solutions to protect the platform on which the IMEI mechanism is stored.

Principle 1 – Uploading, downloading and storage of executable code and sensitive data related to the IMEI implementation

Mechanisms should be implemented that are capable of validating the integrity of software resident on the platform related to the IMEI implementation and after any software update download and installation e.g.

- Detecting any alterations to data and/or software used for security purposes
- Prohibiting operations designed to disable or bypass protection mechanisms
- Maintaining trace logs of attempts to alter data and/or software

Principle 2 – Protection of electronic hardware components' executable code and sensitive data related to the IMEI implementation

Mechanisms should be implemented to protect the executable code and sensitive data related to the IMEI implementation contents of various electronic hardware components against unauthorised modification. The data paths that handle sensitive data should be secured to ensure the IMEI value sent to the mobile network interface is unchanged and matches the IMEI value originally set by the device manufacturer during the final production process, regardless of subscriber or unauthorised third party behaviour. The processing chain should be securely controlled and the control mechanism should be protected e.g. by using security buses and through the use of trusted execution/storage hardware.

Principle 3 – Protection against cloning of sensitive code or data between devices

In the absence of any relationship between hardware and software, data and software can be exchanged between devices and this is one of the reasons why different devices can contain the same IMEI. Therefore, the device should incorporate a robust link between the device hardware[1] and software to prevent cloning or "hot-swapping" of components from one device to another. Data should be bound to the platform and protected from being exported to other devices. Methods to achieve the above may include, support by trusted execution and secure storage mechanisms, encryption and by linking serial numbers e.g. the micro-processor to the One-Time Programmable ROM that contains the boot code.

Principle 4 – Protection of executable code and sensitive data related to the IMEI implementation from external attacks

In order to mitigate the threat posed by malicious software, and to reduce the risk of reverse engineering, executable code and sensitive data related to the IMEI implementation should be inaccessible from outside of the device by an unauthorised third party.

[1] At least one electronic component containing memory and soldered on the PCB

Strong access control mechanisms should be implemented to ensure that only authorised access to internal resources is permitted.

Principle 5 – Prevention of introduction of previous software versions

The ability to introduce previous software versions to a device could allow malicious attackers to circumvent implemented fixes and therefore this should be prohibited by any means (e.g. over the air or via direct installation on the platform).

- Reversion to the existing installed version on a device is permitted, for example if an installation fails.
- Updates should always increment software version numbers, never decrement (e.g. EQ21 to EQ22).

Principle 6 – Prevention, detection of, and response to, unauthorised tampering

To combat and to disrupt interference with the device, manufacturers should implement mechanisms that can help prevent, detect and respond appropriately as soon as an illegitimate attempt to change the IMEI or related implementation is detected by the device. Examples could include:

- Runtime integrity checking and software mechanisms,
- Hardware-based detection mechanisms,
- Resin encasement of components.

Principle 7 – Software quality measures

All software should be developed in accordance with well-defined and rigorous software quality, information security and secure coding processes and techniques.

Principle 8 – Hidden menus

There should be no hidden menus that access or modify areas related to executable code or sensitive data related to IMEI implementation.

Principle 9 – Prevention of substitution of hardware components

Attackers will often seek to remove components and replace them with other components as part of their attacks or to create non-deterministic functionality which could break a device. Means should be implemented to prevent the substitution of hardware components containing memory.

Annex 1

This matrix may be used by manufacturers to indicate whether all the devices they manufacture satisfy each principle and if not, the dates by when they expect to be able to satisfy those principles which are not met.

Principle	Supported in all Devices? Yes/No	If No, Date Available
Principle 1 Uploading, downloading and storage of executable code and sensitive data related to the IMEI implementation		
Principle 2 Protection of components' executable code and sensitive data related to the IMEI implementation		
Principle 3 Protection against exchange of data/ software between devices		
Principle 4 Protection of executable code and sensitive data related to the IMEI implementation from external attacks		
Principle 5 Prevention of introduction of previous software versions		
Principle 6 Prevention, detection of, and response to, unauthorised tampering		
Principle 7 Software quality measures		
Principle 8 Hidden menus		
Principle 9 Prevention of substitution of hardware components		

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601