Council 2018
Geneva, 17-27 April 2018

Document C18/INF/9-E
3 April 2018
English only

Report by the Secretary-General

GSMA BRIEFING NOTE: IMEI SECURITY

Summary

This information document contains the GSMA briefing note on IMEI Security.

Action required

This document is submitted to the Council **for information**.

____

References

Document C18/76

GSMA Briefing Note: IMEI Security

March 2018

1. Background

The IMEI is the International Mobile Equipment Identifier that is used to uniquely identify individual mobile devices in accordance with 3GPP standards. Those standards require each device to have a unique IMEI that has been allocated by GSMA, and that the IMEI be protected against change. Evidence exists that not all manufacturers have complied with these requirements. In some cases, particularly involving the production of counterfeit and spurious devices, manufacturers fail to properly obtain IMEI number ranges from GSMA, instead choosing to use ranges that have been allocated to other manufacturers or to use none at all. In other cases, the insecurity of some IMEI implementations provided by legitimate device manufacturers means the identities of devices can be changed and that is causing problems for some nation states because of the way in which law enforcement activities and device blocking initiatives are being undermined.

2. What is GSMA's role?

Industry has, since 2000, entrusted GSMA with responsibility for allocating IMEI number ranges to eligible device manufacturers in exchange. Erosion of trust in the IMEI as a reliable means of identifying devices is of concern to GSMA and some nation states believe we should assume responsibility for compliance and take action against manufacturers that do not comply with the IMEI number range allocation rules or the security requirements pertaining to their implementation.

3. Why is the ITU involved?

Some ITU Member States proposed that the ITU should replace GSMA as the global IMEI administrator. This proposal was rejected by the ITU membership at large. In response, new proposals have emerged suggesting that the IMEI be replaced with an alternative ITU-administered identifier. However, the security advantages of alternative identifiers are not apparent and there is no evidence to suggest the ITU has the capability to address security concerns related to the production of devices by private sector manufacturers.

4. What has GSMA done on this issue?

GSMA has invested significantly in reaching out to device manufacturers to ensure they understand the need for devices to have unique identifiers and how to apply for them. Strict legal provisions have been defined that govern the allocation and use of device identifiers and GSMA is willing to take enforcement action against those engaged in the misuse of these valuable resources.

GSMA has long recognised the need for IMEIs to resist unauthorised change and it worked closely with mobile device manufacturers and defined IMEI Security Technical

Design Principles to provide guidance to manufacturers on how to secure their IMEI implementations and criteria against which operators could benchmark the security of mobile devices. GSMA also developed an IMEI Security Weakness Reporting and Correction Process to ensure that compromised devices could be identified and reported to GSMA which would then refer the issue to the affected manufacturer to have the matter investigated and remedial action proposed within 42 days. In the immediate aftermath of the introduction of these initiatives a significant increase in security levels was noticeable but it is universally acknowledged that security levels have since dropped in the absence of industry or regulatory monitoring.

5. What is GSMA's position?

GSMA is concerned that some device manufacturers may not be doing all they should to comply with the IMEI number range registration and allocation rules or to secure the IMEI implementations in their products because the integrity of the IMEI is of strategic and economic interest to a wide variety of stakeholders.

GSMA is willing to take remedial and reinforcement action against manufacturers where misuse of device identifiers is reported and proven. This should ensure that all devices use valid and unique IMEIs and regulators and national authorities are encouraged to report suspected issues to GSMA.

GSMA recognises that some legitimate manufacturers need to do more to improve security levels of the IMEI implementations in their products and it is in the final stages of retaining a third party to provide monthly intelligence reports to increase visibility of the security landscape to target offending manufacturers. This represents a significant investment by GSMA and provides evidence of its commitment to the IMEI and its continued usefulness to a range of stakeholders. GSMA will use the information received from its supplier to produce regular security landscape updates for interested parties and it will address reports of specific security weaknesses to the relevant manufacturers to ensure those product security issues are addressed leading to continuous improvement and increased security levels.