Requirements for Mobile Device Software Security Updates

Version 1.0

18 September 2017

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

1.1 Overview

Security vulnerabilities in smart devices can result in significant harm to users worldwide. In the past, it was not possible to provide remote software/firmware security updates to devices. Today, those updates together with new feature capabilities can be implemented on a regular basis, both preventatively and reactively as vulnerabilities and problems are discovered.

The objective for this document is to enumerate requirements that encourage mobile industry action to improve mobile device security, thereby enhancing overall global cyber security. It focuses on the most important requirements rather than dealing with the detail of aspects such as process inefficiencies. The rationale and background, including case studies, are well documented elsewhere.

1.2 Scope

This document establishes high level requirements for security updates for mobile device software, with a particular focus on critical security updates which need to be deployed widely and quickly due to a major security incident of some kind. The software on devices has historically been, and is often still, referred to as firmware. This includes the baseband software, drivers, operating system, communications stacks and application framework. It also includes manufacturer supplied, pre-installed applications such as browser updates which are also controlled and deployed by the manufacturer, rather than through an “app store.”

Updates for applications which a user has installed are specifically out-of-scope for this document, but the requirements here may lead to future recommendations for such applications. Also specifically out-of-scope at this time are inconsistent software version numbering, updating devices older than the specified end-of-life, or the timeframe for producing and delivering security updates. These matters may be covered in future work.

Whilst Internet of Things (IoT) and machine-to-machine (M2M) devices are not explicitly in the scope of this document, many of the principles and methods will be applicable for these devices as well. It is expected that the work established here will also be adopted in the GSMA IoT Security Guidelines for IoT Endpoint Ecosystem [1].

1.3 Definitions

Term	Definition
Device	A handheld cellular radio telephone that includes all of the following features: • utilises a mobile operating system; • possesses the capability to utilise mobile software applications, access and browse the Internet, utilise text messaging, utilise digital voice service, and send and receive e-mail; • has cellular network connectivity. Examples are smartphones. In the context of this document, the term device does not include a radio

	cellular telephone commonly referred to as a “feature” or “messaging” telephone, a laptop, so-called “wearables”, a tablet device, or a device that only has electronic reading capability (an “e-book”).
Device manufacturer	A company that designs and produces a device, including its mobile operating system software (also known as firmware). The mobile operating system may be developed by the device manufacturer or by some other entity, in which case the device manufacturer typically performs some kind of customization and adds device drivers. The device manufacturer is able to develop software updates for his devices (products).
End user	A person who is using the device. If security updates are not available for a device, the data of the end user using the device could be at risk.
Mobile network operator	An entity which offers licensed telecommunications services over an air interface. Mobile network operators may sell devices to end users together with their contracts and promise the availability of certain services, such as telephony, messaging, or internet access. In order to guarantee service availability, mobile network operators usually perform testing to validate devices and software updates before approving them.
Security update, software security update	A software update (see below) whose main intention is to fix security vulnerabilities that were identified in the original mobile operating system, often after the device has been produced and delivered.
Software update	An update of the mobile operating system software controlled and deployed by the device manufacturer, rather than through an app store. Software updates may implement additional features (also called feature update), fix bugs (also called maintenance release), or they may be focused on fixing one or more security vulnerabilities (security update). Although this document does not require any specific delivery method of such updates, updates of certain operating system components may require the installation of a complete firmware update.

1.4 Abbreviations

Abbreviation	Definition
COM	Communication-related requirement
CVE	Common Vulnerabilities and Exposures - https://cve.mitre.org/
GSMA	The GSM Association – www.gsma.com
IoT	Internet of Things
M2M	Machine to Machine
MNO	Mobile Network Operator
PLMN	Public Land Mobile Network
SEC	Security-related requirement
SSU	Software Security Updates
TES	Testing-related requirement

1.5 Requirements Format

Requirements are denoted using the format XXX-YYY-ZZZZ, where:

- XXX denotes this document: SSU (Software Security Updates),
- YYY denotes the related section: e.g. SEC (Security Only Updates),
- ZZZZ denotes a four digit numbering format which increments by 10 numbers for each requirement, allowing for future updates: e.g. 0020, 0030 etc.

Normative text (i.e. the requirements) is contained within the requirements tables. The remainder of the text is considered to be non-normative and therefore informative and supporting text.

1.6 References

Ref	Doc Number	Title
[1]	GSMA CLP.13	IoT Security Guidelines for IoT Endpoint Ecosystem https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[2]	RFC 2119	"Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997. Available at http://www.ietf.org/rfc/rfc2119.txt

1.7 Conventions

The key words "must", "must not", "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this document are to be interpreted as described in RFC2119 [2].

2 Device Security Updates Requirements

The following requirements are expected to be implemented by device manufacturers and mobile network operators (MNOs).

2.1 Security Only Updates

Req. Number	Requirement
SSU-SEC-0010	Device manufacturers must provide security updates that *only* fix the security problems they are designed to address (as identified by a list of CVEs (Common Vulnerabilities and Exposures), for example) and not other, non-security related issues.

Separating mobile security software updates from other types of updates minimises both the development time and the quality assurance overhead for security updates, and allows them to be deployed as quickly as possible.

2.2 Monthly Security Updates

Req. Number	Requirement
SSU-SEC-0020	Device manufacturers must provide regular monthly security updates throughout the lifetime of the device.
SSU-SEC-0021	Device manufacturers, where the device software is under their control, should

	deploy the security updates across their device range by prioritising the update on the most popular models.

Historically, device manufacturers have prioritised security updates on device models based on various different business reasons. However, device vendors can significantly reduce the risk of known vulnerability exploitation by deploying security updates starting with the most popular device models.

2.3 End-of-Life Policy

Req. Number	Requirement
SSU-SEC-0030	Device manufacturers, where the device software is under their control, must continue to provide software security updates for at least 24 months after the last day of sales of a product by the device manufacturer.

NOTE: This means that when the last product is sold by the manufacturer it must dedicate engineering resources or “patch teams” to ensure that a product is adequately supported with security updates for another two years, where the device software is under its control.

3 Communication of Security Updates to End Users

These requirements cover the communication of the availability of security updates to end users.

Req. Number	Requirement
SSU-COM-0010	Device manufacturers and mobile network operators must notify end users about the availability of a security update via one or more of the following channels: • Device based notification (strongly preferred) • Website • Other communications
SSU-COM-0020	Device manufacturers and mobile network operators must explicitly communicate to users that a security update is a security update. Device manufacturers and mobile network operators should make available information to end users about the content of a security update.

NOTE: It is important to consider that security can be undermined by fraudsters and phishing emails/push messages claiming to be updates. Implementers should design notification mechanisms to take these threats into account.

4 Device Security Updates Testing & Release Requirements

4.1 Device Update Testing, Approval & Release

The following requirements are expected to be implemented by mobile network operators.

Req. Number	Requirement
SSU-TES-0010	Where software testing needs to be carried out by mobile network operators, they must ensure that device testing of security only updates is completed within 2 weeks.
SSU-TES-0020	In the case that a device is unable to be updated by the mobile network operator, the device may revert to the device manufacturer's update servers.

The following requirement is expected to be implemented by both device manufacturers and mobile network operators.

Req. Number	Requirement
SSU-TES-0030	Device manufacturers and mobile network operators, as soon as updates are approved for release, must not prevent customers from receiving device software security updates. Unless: the device has been relinquished from the mobile network operator's control temporarily or permanently, by e.g. • User rooting of the device / user-driven other software update • If the SIM has been changed to another network operator

NOTE: No implementation details are discussed and the conditions for this requirement to be satisfied are a matter for individual operators and manufacturers to agree bilaterally.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	18 Sep 2017	First version	TG	David Rogers, Copper Horse Solutions Ltd.

A.2 Other Information

Type	Description
Document Owner	Device Security Group
Editor / Company	David Rogers, Copper Horse Solutions Ltd.

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.