Voicemail Security Guidelines

Version 1.1

16 December 2014

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

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction

1.1 Overview

Voicemail systems protect customer Voicemail accounts using two different types of authentication:

1. Customer authentication and device authentication.
2. Customer authentication ensures that only the legitimate customer is accessing the Voicemail and is usually used to secure access through the fixed line telephone network using a PIN code.

This document is intended to act as guidance for Operators and Customers in the use of Voicemail PINs that secure access to Voicemail.

1.2 Scope

This document deals with, and distinguishes between, the following two types of attacks against voicemail systems:

- **Eavesdropping:** listening secretly to the Voicemail content of a particular customer. Voicemail spying is an issue in particular for business customers who may often leave business confidential information on their colleagues' Voicemail assuming it is secure.
- **Fraudulent calls:** breaking into the Voicemail of any customer in order to carry fraudulent calls. Some Voicemails allow dialling number from the account. For example, the fraudster first leaves a message on the compromised Voicemail from an international or a premium number and then calls back this number through the Voicemail system. This technique allows making fraudulent calls without setting up fake customer accounts.

1.3 Definition of Terms

Term	Description
CLI – Calling Line Identity	Where the telephone number calling you is provided and displayed on your terminal or device
ISO 27000	A family of security standards published by the International Standards Organisation ISO
PIN – Personal Identity Number	A series of digits randomly chosen to authenticate a Customer
PSTN – Public Switched Telephone Network	The conventional telephone system
SMS – Short Message Service	Also known as a text message. A message sent that can be displayed on a telephone
SSL _ Secure Socket Layer	Used to provide secure communications over a link
UICC – Universal Integrated Circuit Card	A Smart Card also sometimes known as a SIM (Subscriber Identification Module) used to provide Customer or Device Authentication in Mobile Radio

2 Voicemail Authentication

Voicemail systems protect customer Voicemail accounts using two different types of authentication: customer authentication and device authentication. Customer authentication ensures that only the legitimate customer is accessing the Voicemail and is usually used to secure access through the fixed line telephone network using a PIN code.

Device authentication ensures that only a mobile with a legitimate UICC is accessing the Voicemail account and is usually used when customers access their Voicemail from their mobile while roaming or from the home network using the calling line number. Typically, device authentication is used on its own when it is reliable (e.g. when CLI can be trusted), so that customers can listen to Voicemails without having to enter a PIN. Customer authentication is used when the device authentication is not reliable. Other types of device authentication exist that use a username and password that are provisioned in the device over the air and are used to authenticate over an SSL connection such as visual Voicemail.

3 Voicemail Vulnerabilities

Voicemail systems can be attacked by exploiting the following vulnerabilities:

- **PIN code guessing:** some Voicemail PIN can be easily guessed because either the customer left the default PIN or inserted a very common PIN such as: 1234, 1111, and 2222.
- **Calling line spoofing:** the attacker exploits the fact that some operators provide access to the PSTN without checking whether the calling number belongs to the number range that was assigned to them. This weakness allows the attacker to call the Voicemail of customers of other operators (to which CLI may not be provided, for example sometimes on International Calls (but not all)) using their calling line number without having to enter the Voicemail PIN. There are web services that offer to make a call with a spoofed CLI by calling back the caller.
- **Social Engineering:** There are many social engineering techniques that can be used to trick or persuade people to give information or do something. For example by tricking customer service staff or the Customer into giving out Voicemail PINs over the phone

4 Voicemail Security Recommendations

As is the case with securing any system, it is important that service providers are mindful of the need to ensure an appropriate balance between usability and security. Although the issue of voicemail security has received a lot of media attention it is important that a sense of perspective is maintained because only a few hundred mobile users had their voicemails intercepted, whereas several million use the service with no real concerns around anyone finding out: “they would be late home” or “needed some bread”. For that reason, it is important to keep voicemail simple and easy to use for the majority whilst allowing users with more sensitive personal or commercial information to protect their messages. The guidance for network operators provided below is designed to achieve an appropriate balance.

4.1 Generation of PINs

Each voicemail PIN should be randomly generated and not derived from any other data or set to a default value. Default PINs should not allow remote access to the voicemail account.

4.2 Length of PINs

PINs should be of variable length of at least four digits, but if possible mobile users with sensitive information should be given the option to randomly choose PINs of greater than four digits in length. Passwords used to authenticate a voicemail box should be at least 8 characters long, generated randomly and provisioned securely in the mobile device.

4.3 Exclusion of Obvious Patterns

PINs composed of simple repeated numbers or sequences should be excluded. It is recommended that the following PINs should not be allowed: 1234, 1111, 2222, 3333, 4444, 5555, 6666, 7777, 8888, 9999, 0000, and 1212.

Optionally, network operators may wish to allow mobile users that have no security concerns to use easily remembered PINs but advise them against using their PINs that may be used for other purposes such as Banking. The use of easily remembered PINs has the advantage of reducing the number of calls to customer care centres from mobile users needing their rarely used PINs to be reset. However, network operators should advise mobile users that may have greater security needs due to their occupation or position in the community and the likely sensitivity of voicemail contents to use more complex PINs and to avoid obvious sequences like their date of birth, marriage date, etc. as these can be found by Internet searches. Allowing a choice has the advantage of increasing security awareness as mobile users are prompted to consider their security needs.

4.4 PIN Provisioning Procedures

Operators should have procedures in place for the distribution, management and provisioning of PINs. Good practice dictates that mobile users should not be able to use SMS to initialise a PIN request. PIN resets should only be sent to mobile devices by SMS or some other separate channel.

It should not be possible for anybody within the network operator, other than the call centre employee who is directly in communication with the mobile user, to reset PINs and it should not be possible to have a PIN reset on the say so of another call centre employee. Call centre staff should not be able to see voicemail PINs and systems should merely allow staff to initiate the generation of the PIN and the sending of it to mobile user’s device. Similarly, PINs must never be given out verbally by customer service staff as such an approach is exposed to the risks of social engineering.
A message can be set in the voicemail message pre-provisioning of a PIN preamble to remind or force the customer to create a new PIN.

4.5 PIN Access Attempts

The number of attempts that mobile users are permitted before they are locked out of the voicemail services should be limited to three. Mobile users should then be required to call the network operators’ customer care centre to authenticate themselves and have their voicemail PINs reset. Alternatively, mobile users should be able to access the voicemail only from their mobile device using device authentication.

4.6 PIN Storage

Where technically possible, infrastructure should securely store both voicemails and voicemail PINs and not allow them to be easily accessed by technical or other network operator staff. Standard Information Security techniques such as ISO27000 family of standards should be deployed on equipment entrusted with the storage of this sensitive data.

4.7 Non-mandatory PIN Usage

If an operator decides not to mandate PIN usage for voicemail, the customer should be fully informed of the risks of leaving their phone unprotected and the operator should advise the customer to protect their phone using a device PIN.

Mobile users should not have PIN access to their voicemail unless they specifically request it for remote retrieval of voicemail messages. Even then, it may not always be necessary to provide this service and operators should carefully consider whether PINs should be activated if requested and whether CLI access should only be provided on the home network.

The majority of customers will only ever access Voicemail from their own handset on their home network so account or device authentication alone should be sufficient for 99% of customers. The situation in the UK arose to a large degree simply because all voicemail users had retrieval numbers and PINs issued, whether the customer needed them or not. If remote access has traditionally been provided, network operators may wish to consider if this really needs to be enabled for every customer or if it can be disabled as a default and turned on by request.

4.8 Accessing Voicemail from CLI Different from Mobile User

Careful consideration must be given to ensuring that appropriate security controls are applied to calls initiated from within the home network and these controls should be distinguished from those required for calls originating from other networks due to the risk that the CLI may be 'spoofed'. In some cases, the mobile user's CLI may not be provided or it may not correspond correctly and this situation can arise when international calls do not provide the CLI or access to voicemail is attempted from a source other than the mobile user's own mobile device. Network operators should always request a PIN when a call is initiated directly to voicemail from outside their networks and where the device authentication, such as CLI, is not used.

Some customers may require access to their voicemail from foreign networks and if they have not set a voicemail PIN prior to travelling a randomly generated PIN should be sent by SMS to them. This PIN should never be visible to customer care staff but the account should be marked that a request for a PIN was made should the customer query when an SMS with PIN is received.

4.9 Notification of Attempted Access

If an attempt has been made to access a voicemail mailbox with the incorrect PIN code, the customer should be notified after the second attempt (assuming failure at three attempts). The user is in the best position to decide whether the access was made by them or not and notification could be sent by SMS. If SMS is used, every effort should be made to ensure it is clear to the mobile user that the notification is from the network operator rather than it being a platform to launch a phishing attacks or premium rate call back scam.

4.10 Last Access Notification

Where technically possible, when mobile users access their voicemail service an announcement should inform them when their mailbox was last accessed.

4.11 Limiting Dial Out and Call Back

Sometimes voicemail service offerings can allow mobile users to place a call to anybody that has left a voicemail message simply by pressing a digit. Capabilities such as this are exposed to fraud and network operators should restrict the ability of mobile users to dial any number from their voicemail accounts and to call back premium rate or international telephone numbers.

4.12 Mobile User Advice

Mobile users should be provided with clear security guidance, both on network operator websites and in written form where possible, on the secure use of voicemail services. Advice to users should also highlight the possible risks and it should outline the various mechanisms by which voicemail can be accessed (e.g. via the handset, by calling the handset and pressing certain keys during the voicemail announcement, by a remote dial-in number, etc.).
In particular, it is important to explain and highlight to mobile users that, where voicemail systems contain information about “new messages” and “old” or “previously listened to” messages, announcements should be carefully listened to as they could indicate attempts to compromise voicemail security. In particular, instances where “old” messages that have not been listened to by the mailbox owner could indicate unauthorised access.

If embarking on a communications exercise on voicemail security network operators could take the opportunity to highlight and provide guidance of additional matters including mobile device locking, backups, SIM locking, recording IMEI details, reporting handset theft, etc.

5 Voicemail Security Recommendations

It is recognised that most mobile users are not particularly concerned about, or have any great need for, voicemail security. However, it is important that they fully understand the security risks associated with the use of voicemail service, how they could be exposed to those risks and what they can do to protect themselves. Network operators should offer adequate levels of protection and advice to all of their customers and the necessary enablers should be in place and on offer for those mobile users that wish to enhance their protection levels. In that regard the guidance that follows may be useful and informative for mobile users.

5.1 Choosing PINs

Mobile users should choose a PIN that is longer than 4 digits, if this option is available from their network operator, and the PIN should not be one that can be easily guessed. When choosing a PIN the following should be avoided:

- Repeated numbers (e.g. 1111)
- Sequential numbers (e.g. 2345)
- Patterns related to the keypad on mobile devices (e.g. 2580)
- Dates of birth (e.g. 2812 for the 28th of December or 1279 for December 1979) as these can often be found on social networking or other Internet sites.
- PINs that are used for other purposes such as banking

5.2 Changing PINs

Mobile users that are concerned about protecting sensitive information that may be contained in messages left in their voicemail should regularly change their PIN as this represents good security practice. Quite aside from routine PIN changes, mobile users should immediately change their voicemail PINs if they believe it may have been observed or compromised by a third party in any way. Mobile users need to be alert to the fact that their PINs can sometimes be recorded and displayed as ‘Last Number Dialled’ data. Caution should be exercised when accessing voicemail services and inputting PINs on other mobile devices and phones, (such as PINs recorded on a hotel billing system), as it could be possible for third parties to play back the PIN used at a later stage.

5.3 Alert to Compromise

If somebody unauthorised has listened to a mobile user’s voicemail messages that person has the option to delete or keep the messages. If messages are retained the voicemail service will generally indicate that the mobile user has “one saved message” rather than “one new message”. If a mobile user hears the first announcement, followed by a message that it has heard for the first time this could indicate mailbox compromise. Consequently, users should listen carefully and take note of whether messages they are hearing for the first time are classified as new or old/saved.

5.4 Leaving Sensitive Information in Voice Messages

As has been highlighted above, voicemail systems can be compromised so anybody prompted to leave a voicemail message for a mobile user shod exercise caution in terms of the contents of the message to be left. In particular, those leaving messages should refrain from leaving from leaving sensitive information such as credit card details etc. in voicemail messages.

5.5 Overheard Calls

People should always be conscious of where they are and who may be listening in the vicinity when they make or receive telephone calls, be they to mobile or other telephone users. Calls made from or received in public places such as airport lounges and railway stations can be easily overheard and have the potential to divulge much more sensitive information than what could be gleaned from a brief voicemail message.

5.6 Call Back Risks

Mobile users should be careful when replying to voicemail messages as systems that allow user to call numbers from which messages originated can be targeted by those seeking to profit from phishing or premium rate call scams. Mobile users should be aware that calling premium rate calls can result in significant calls costs and calls from these numbers should not be returned unless the user is satisfied that the message and caller is genuine.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.1	11-Nov-11	First draft produced by Charles Brookson	SG Mgt. Team	C. Brookson, SG Chair
1.0	20-Feb-12	First version approved by EMC 2012	EMC	C. Brookson, SG Chair
1.1	12 Dec 2014	Transferred PRF from SG to FASG as SG.20 v1.1	FASG	David Chong, GSMA

Other Information

Type	Description
Document Owner	FASG
Editor / Company	Charles Brookson, SG Chair

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.