ND1407:1997/10

Voluntary Code of Practice for Security of Access to Dial-Through Functions in communications systems

Issue 1

Network Interoperability Consultative Committee
Ofcom
Riverside House,
2a Southwark Bridge Road,
London
SE1 9HA
UK
http://www.nicc.org.uk

Normative Information

Liability

Whilst every care has been taken in the preparation and publication of this document, NICC, nor any committee acting on behalf of NICC, nor any member of any of those committees, nor the companies they represent, nor any person contributing to the contents of this document (together the "Generators") accepts liability for any loss, which may arise from reliance on the information contained in this document or any errors or omissions, typographical or otherwise in the contents.

Nothing in this document constitutes advice. Nor does the transmission, downloading or sending of this document create any contractual relationship. In particular no licence is granted under any intellectual property right (including trade and service mark rights) save for the above licence to copy, store and distribute this document and to produce derived copyright works.

The liability and responsibility for implementations based on this document rests with the implementer, and not with any of the Generators. If you implement any of the contents of this document, you agree to indemnify and hold harmless the Generators in any jurisdiction against any claims and legal proceedings alleging that the use of the contents by you or on your behalf infringes any legal right of any of the Generators or any third party.

None of the Generators accepts any liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from any use of or reliance on the contents of this document for any purpose.

If you have any comments concerning the accuracy of the contents of this document, please write to:

The Technical Secretary,
Network Interoperability Consultative Committee,
Ofcom,
Riverside House,
2a Southwark Bridge Road,
London,
SE1 9HA,
UK.

Foreword

Oftel, via the Network Interoperability Consultation Committee, requested that a Code of Practice be developed to provide advice and guidance on best practice on the design of dial through and software access functions.

The Task Group was convened under the PSTS Interest Group.

It is anticipated that, from time to time, this Code of Practice will be revised.

Although the recommendations are couched in terms of call routing systems and similar types of systems they are equally applicable to any telecommunications apparatus that incorporates a similar function.

CONTENTS

1. INTRODUCTION

Secure operation of systems requires good co-operation between all elements in the supply, installation, commissioning and operation chain. To limit the opportunity for fraud such systems must comprise apparatus with appropriate access security functions and be operated correctly.

A system can comprise one or more products that together should include access security functions that when operated correctly provide the level of access security required by the user of the installation and thereby comply with this Code.

Fraud arising from unauthorised access to dial through functions can be exacerbated by nonexistant or ineffective access security measures being in place to protect against unauthorised access to on-site or remote maintenance functions. The unauthorised reconfiguration of or access to system information can facilitate unauthorised access to dial through functions.

Text in this CoP is based on “Advice on the Avoidance of Dial through Fraud” drafted by an industry group and published by BABT.

2. SCOPE

This voluntary Code of Practice provides advice on best practice for the design, supply and operation of access security functions of telecommunications apparatus that incorporates dial through functions so that system owners and managers can operate and manage their installations in a way that limits their exposure to fraud arising from unauthorised access to system functions, in particular, the ability to attempt outgoing PSTN calls.

Systems that are vulnerable to fraud arising from unauthorised access to dial through functions include call routing apparatus and voice mail systems.

> Note. Further information can be found in the document “Advice on the avoidance of dial through fraud in communication systems,”

3. DEFINITIONS & ABBREVIATIONS

3.1	CLI	Calling line identification
3.2	DISA	Direct Inward System Access
3.3	PIN	Personal Identification Number
3.4	PSTN	Public Switched Telecommunication Network
3.5	Direct Inward System Access	Functionality that enables a caller, who dials a designated number in the PSTN number range, to access private system or network features as if they were an extension user. Normally, after answer of a PSTN call, the caller has to pass an authorisation or identification procedure before

access is granted. The procedures vary from system to system as do the capabilities of the systems to provide access to internally available services.

3.6 Dial through

A function of call routing systems and voice mail systems that enables a call received at one port, usually a PSTN exchange line port, to be switched, usually under control of a caller, to another port that also is a PSTN exchange line port.

3.7 Call routing system

A system that incorporates a function that allows calls received at one port to be switched to another port by the caller. Call routing systems may also have other functions.

3.8 Maintenance functions

Functions that enable the correct operation of a system to be verified or restored following a fault report. On-site access to maintenance functions is usually provided via an on-site Data Terminal Equipment, e.g. a PC. Remote access to maintenance functions is usually provided via the PSTN.

3.9 Voice mail system

A system that provides for a number of “mail boxes” to which callers are directed, when the respective users are unavailable. The “mail boxes” are for the recording of messages from callers. It is usual for voice mail systems to provide a notification to the user that message(s) are waiting. Voice mail systems are often integrated with a call routing or similar apparatus in a manner that enables a caller to dial further digits to select an alternative user.

4. REFERENCES

Advice on the avoidance of dial through fraud in communication systems: Drafted by an Industry group and published by British Approvals Board for Telecommunications.

5. SPECIFICATION OF DIAL THROUGH ACCESS SECURITY FEATURES

Note. The measures available in a particular product to limit the extent of unauthorised DISA access may have been designed-in during the initial development stage or may need to be added as an enhancement.

5.1 Where PIN codes, password or similar are used to authenticate callers they should comprise at least 4 characters, each character being 1 of 10 combinations (10000 code options).

> Note. It is recommended that a capability for variable length PIN or similar codes should be provided with any combination of the widest practical range of characters including alpha and numeric, e.g. 12^8 combinations. A lexicon check to confirm random nature of the character string could be provided.

5.2 Where the CLI's of callers, who are allowed access to a system, are known in advance and available over the exchange line interface connected to the PSTN they should be used to authenticate callers.

> Note. CLI information is not universally available and may be withheld by the caller.

5.3 Where CLI or PIN code authentication procedures are considered not to be secure enough a callback function should be provided.

> Note. Callback or dial back functions are most appropriate to remote maintenance access where they can operate automatically between suitably configured modems.

5.4 Capability that would allow a system manager to change certain parameters, such as the number of ring cycles before answer, time delay between call arrival and answer, or number of call attempts before lockout should be provided.

> Note. Monitoring the pattern of unsuccessful access attempts could be used to identify an unauthorised access attempt and cause an access function lockout.

5.5 Capability should be provided that would allow a system manager to select on a per PIN code or equivalent basis the system features, e.g. leased line routes, PSTN numbers, accessible by the user of each PIN code,

> Note. Access should be selectable to be permanent or for a period starting on a predifined time-of-day to all or selected DISA PIN code users.

5.6 A feature for recording outgoing call attempt details, including CLI, PIN code or equivalent if available, on PSTN calls originating from DISA accesses should be provided.

> Note. A history file for DISA access attempts should be provided.

5.7 PIN code management features, e.g. forced password change after elapsed time or number of access attempts, should be provided.

5.8 Where a product has a feature that enables its DISA access security functions to be changed or reconfigured whilst the system is operational, use of those functions should be secured against unauthorised access.

> Note. Access should be secured by use of combinations of password, CLI and callback/dialback appropriate to the potential impact of

unauthorised changes to configurations. For example, security of access to off-site (remote) maintenance ports could be improved by including personal intervention by system manager.

6 SPECIFICATION OF MAINTENANCE ACCESS SECURITY FEATURES

Note. The measures available in a particular product to limit the extent of unauthorised access to maintenance functions may have been designed-in during the initial development stage or may need to be added as an enhancement.

6.1 Where PIN codes, password or similar are used to authenticate callers they should comprise at least 4 characters, each character being 1 of 36 combinations (appx 1.68 million code options).

Note. It is recommended that a capability for variable length PIN or similar codes should be provided with a any combination of the widest practical range of characters including alpha and numeric, e.g. 12^8 combinations. Increased security can be obtained by inclusion of a lexicon check to confirm random nature of the password character string.

6.2 Where PIN code authentication procedures are considered not to be secure enough a callback function should be provided.

Note. Callback or dial back functions are most appropriate to remote maintenance access where they can operate automatically between suitably configured modems or equivalent functions.

6.3 Capability that would allow a maintainer to change certain parameters, such as the number of ring cycles before answer, time delay between call arrival and answer, or number of call attempts before lockout should be provided.

Note. Monitoring the pattern of unsuccessful access attempts could be used to identify an unauthorised access attempt and cause an access function lockout.

6.4 Capability that would allow a maintainer to select on a per PIN code, password or equivalent basis the maintenance features accessible by each user.

6.5 PIN code and password management features, e.g. forced password change after elapsed time or number of access attempts, should be provided.

7 SUPPLY

7.1 The information provided with a product should include details of the DISA functions and measures available to secure against unauthorised access. The information should also include details about configuration of the product.

7.2 Where the DISA functions are reconfigurable whilst the system is operational the information provided with a product should include details of measures that can be adopted to secure access.

> Note. Passwords, CLI, dialback and operational procedures can be used to provide security of access to system management and maintenance functions for on-site and off-site (remote) maintenance access.

7.3 During the commissioning of a DISA function its configuration should either be verified to be in accordance with a customers requirements or, where no requirements have been stated, be set so that access is denied.

> Note. Where the feature has not been offered or has not been requested the feature should be set so that access is denied. Obvious or common codes should be avoided.

7.4 Those engaged to install or commission systems should treat information about individual customer's access procedures confidentially.

7.5 Where a system has capability to set configuration data values, e.g. time to answer, they should be set to a non-zero value.

7.6 If a callback function is available either set it up to customer provided information or disable the function.

> Note. Callback is usually used for off-site (remote) Maintenance access security.

7.7 DISA access should not be used to provide off-site (remote) access to maintenance functions unless there is another level of security, e.g. Password or PIN code.

> Note. Use of immediate answer on calls accessing remote maintenance facilities should not be set because it reduces the search time for these numbers. Whilst this does not prevent access it frustrates the unauthorised caller.

8 OPERATION AND MAINTENANCE

8.1 Where maintenance services are provided by a third party they should treat information about individual system access procedures in confidence and store any records securely. Staff should be reminded of the importance of keeping information on access procedures secure.

8.2 When staff leave the company’s employment or maintenance arrangements are changed any access codes which they may have known should be changed by the system manager.

8.3 A maintainer should allow access to maintenance facility access codes on a “need to know” basis only. If possible, allocating individuals different access codes.

8.4 A maintainer on acceptance of a system should change all passwords needed to access system maintenance (and configuration) functions.

8.5 Maintainers should change access codes frequently and use the maximum numbers of characters the system will allow.

Note. The PIN codes and passwords should be random strings of characters without any meaning.

8.6 The number of invalid access attempts should be restricted and when exceeded should alert the telecommunications manager that there had been unauthorised access attempts.

Note. The number of unsuccessful attempts before a(n extended) period of access denial should be 3.

8.7 Where Call Barring or Restriction features are available they should be used to control the destinations accessible to breakout calls.

Note. Call barring or restriction services may be provided by the PSTN or within the system itself.

8.8 DISA breakout should not be configured from freephone 0800, 0500, or equivalent, exchange lines, where the system manager is responsible for incoming call charges..

8.9 System activity reports, e.g.Call Logger outputs, should be reviewed on a frequent (daily or weekly) basis for evidence of unauthorised call attempts..

8.10 All the information available, including itemised bills, should be checked for evidence of calls to unusual destinations and at unusual times.

8.11 Maintainers should establish a protocol with the system manager that enables and disables remote system access by, for example, physically plugging and unplugging the system into or from a line socket through which the system is accessed.

Note. Where systems are self-maintained care should be exercised to ensure that there is no inadvertent remote access path to systems, particularly those with a DISA dial through capability.

END