NICC ND 1438 V1.1.1 (2016-03)

NICC Document

Voluntary Code of Practice
Mitigating Theft of Service from End User Voice over IP Communications Systems

NICC Standards Limited

Michael Faraday House,
Six Hills Way,
Stevenage
SG1 2AY

Tel.: +44(0) 20 7036 3636

Registered in England and Wales under number 6613589

NOTICE OF COPYRIGHT AND LIABILITY

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be that printing on NICC printers of the PDF version kept on a specific network drive within the NICC.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other NICC documents is available at:

http://www.niccstandards.org.uk/publications/

If you find errors in the present document, please send your comments to:

mailto :help@niccstandards.org.uk

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

The Technical Secretary, NICC Standards Ltd.,

Michael Faraday House,
Six Hills Way,
Stevenage
SG1 2AY

Contents

Intellectual Property Rights 4
Foreword 4
Introduction 4
1 Scope 4
2 References 4
2.1 Normative references 4
2.2 Informative references 5
3 Definitions, symbols and abbreviations 5
3.1 Definitions 5
3.2 Abbreviations 6
4 Introduction to Theft of Service 7
4.1 The IP-PBX 7
4.2 Threats 7
4.3 Solutions / mitigations / controls 7
5 Architecture 8
5.1 Sample Architecture of a SIP PABX connection. 8
6. Specification of Dial Through Security Access Controls. 9
6.1 Generic Controls 9
6.2 Overall network security 12
7. Good Practice Guides 13
7.1 Cyber Essentials Scheme 13
7.2 ITSPA Recommendations for secure deployment of an IP-PBX 13
7.3 TalkTalk 13
7.4 FCS Fraud Mitigation Standard Specification 14
History 15

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to NICC. Pursuant to the NICC IPR Policy, no investigation, including IPR searches, has been carried out by NICC. No guarantee can be given as to the existence of other IPRs which are, or may be, or may become, essential to the present document.

Foreword

This NICC Document (ND) has been produced by NICC TG Security.

Introduction

Ofcom have requested that the NICC produce a technical specification to assist third parties when securing IP-PBXs infrastructure so as to prevent fraud or Theft of Service. This is to address the technology change in the delivery of voice services since the production of ND1407.

The NICC Security Task Group has been convened to produce a specification guidance document to good practise and is designed to be used in conjunction with manufacturer guidance and instructions for installation, operation and maintenance.

1 Scope

This document contains advice on best practice for the design, supply and operation of the security functions of Internet Protocol (IP) based telecommunications systems, Customer Premises Equipment (CPE) and devices, the misuse of which can lead to Theft of Service. By following such advice system owners and managers can operate and manage their installations in a way that limits their exposure to Theft of Service arising from unauthorised access to system functions, for example, the ability to make fraudulent outgoing calls.

2 References

For the particular version of a document applicable to this release see ND1610 [1].

2.1 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ND1610 Next Generation Networks, Release Definition

2.2 Informative references

[I1] UK government Cyber Essentials Scheme (Protect your business against cyber threats)
[I2] UK government: Cyber Essentials Scheme
[I3] ITSPA: Recommendations for Provisioning Security
[I4] ITSPA: Recommendations for secure deployment of an IP-PBX
[I5] TalkTalk: Telecoms fraud Find out more online at talktalkbusiness.co.uk A brighter place for business How you can avoid becoming a victim
[I6] FCS: FCS Fraud Mitigation Standard Specification
[I7] FCS: TELEPHONE SECURITY CHECKLIST
[I8] SIPConnect (available from the SIP Forum)

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and apply:

CPE and devices	For the purposes of this document, the devices used and operated with an IP based telecommunications system. This includes, but not limited to, soft phones, SIP handsets, IP-PABXs, both dedicated and software based.
Denial of Service	The use of external traffic generation resources or communications protocols to affect the correct operating functions of a target communications system.
Dial Plan	A set of numbers, area codes etc. that are defined on the IP-PBX that are permitted to be dialled.
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.
Direct Inward System Access	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.
IP-P(A)BX	Hardware or software based telephone system used with customer networks or premises.
IP Voice Switch function	Any system providing IP based Telephony services.
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.
PIN Codes	Personal Identification Number: May be numbers only or on newer systems, a combination of numbers and letters.
Passwords	A string of characters that allows access to a computer, interface or system.

PBX	Also known as PABX. Hardware or software based telephone system used with customer networks or premises
SIP	Session Initiation protocol. This protocol is the technology used to operate and connect with IP-PABX systems.
SIP-T	SIP Trunk connection. This is the common abbreviation for the connection service from the carrier network connection and / or the type and specification of interface used.
SIP Connect	The SIPconnect Technical Recommendation is an industry-wide, standards-based approach to direct IP peering between SIP-enabled IP PBXs and VoIP service provider networks
SIP handsets	SIP hardware phones and other hardware technology.
Theft Of Service	The unauthorised use of system functions with the intent of financial gain or restricting legitimate use of system resources.
Virtual P(A)BX	These are hosted P(A)BX service based on cloud technology where the main functions operate within a remote virtual environment.
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.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

DISA	Direct Inward System Access
CPE	Customer Premises Equipment
FCS	Federation of Communication Services
IP	Internet Protocol
IP-PBX	Private Branch Exchange
ITSPA	Internet Telephony Services Providers' Association
LAN	Local Area Network
SIP	Session Initiation Protocol
SIP –T	SIP Trunking
TDM	Time Division Multiplexing
VOIP	Voice over IP
VOIP-SP	VoIP Service Provider
PBX	Also known as PABX

4 Introduction to Theft of Service

Theft of Service is a form of fraud whereby hackers are able to gain access to a business's telephone system by exploiting vulnerabilities in the communications system's implementation. The hacker uses the compromised telephone system as a way of generating traffic and revenue, leaving the organisation with the cost within their phone bill (for the fraudulent calls). Often the premium rate telephone number being dialled is owned by the hackers so they are generating revenue for themselves. Fraud of this type can be exacerbated by ineffective security measures that offer insufficient protection against unauthorised access and use of the telephone system.

Small and medium sized businesses often use telephone systems known as Private Branch Exchange (PBX) for internal and external communications. One type of Theft of Service, known as Dial Through Fraud, where a hacker will gain access to a Time Division Multiplex (TDM) PBX and use it to generate revenue, is well understood. NICC's ND1407 Voluntary Code of Practice provides guidance on securing such a device. The growth of Internet enabled VoIP services, where an organisation's IP PBXs is accessible via the Internet, exposes the organisation's communications system to a range of new threats which could lead to Theft of Service. With ND1438, NICC offers a Voluntary Code of Practice to mitigate such threats.

4.1 The IP-PBX

Voice over IP (VoIP) protocols govern how a telephone call may be made over an IP network such as the Internet. Interconnections between the Internet and public telephone networks exist to enable telephone calls to originate on one network and terminate on the other. Well known products which make use of this technology include Skype, Viber and Vonage.

An IP-PBX connects to IP networks such as the Internet and performs all the functions of a traditional PBX. It often provides further capability which is enabled by VoIP protocols. An organisation's IP-PBX uses VoIP protocols to connect to the organisation's VoIP provider, who will route outgoing calls to their intended recipients, who could be on any VoIP enabled or circuit switched network in the world.

4.2 Threats

Having a presence on the Internet exposes the IP-PBX to hackers who may try a number of techniques to exploit an insecure system. Mitigation of the threats used by hackers is described in section 6 of this document, with useful references identified in section 7.

4.3 Solutions / mitigations / controls

A VoIP communications system contains many components which can be configured to help to prevent or minimise the harm caused by Theft of Service.
By considering the guidance in this document and working with its VoIP equipment and service providers, an organisation can implement the recommended combination of hardware and software security measures, service monitoring tools and bill management agreements.

5 Architecture

This section describes the general architecture of VoIP deployments common in business environments.

The architecture shown in Section 5.1 is a standard layout of the connection between a SIP Voice provider and the VoIP user.

5.1 Sample Architecture of a SIP PABX connection.

Figure 1 below is a system diagram of the building block of a SIP PBX with a connection(s) to a network for the transmission of data either specifically for the delivery of voice or in common with other data traffic such as the Internet.

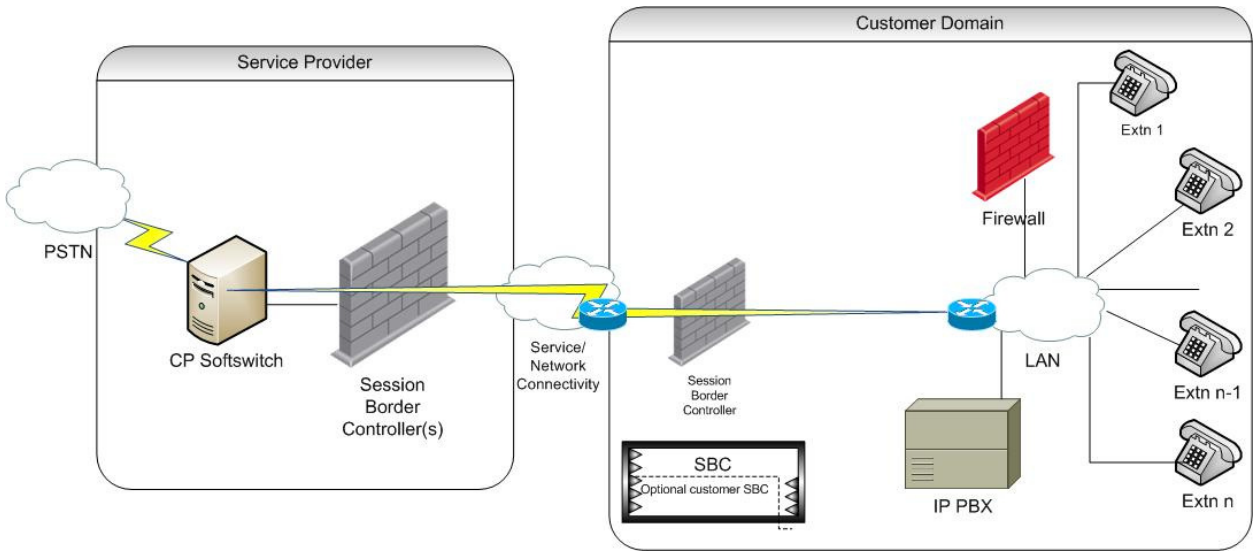

Figure 1

The key areas that need initial consideration by an end customer are

1. Registration of SIP phones to the IP PBX.
2. Access to customer Local Area Network (LAN).
3. Access Control to and management of IP PBX features. (Unauthorised use of Direct Inward System Access Functionality [DISA] is still an issue on IP-PBX and careful consideration is needed to prevent it's misuse)
4. IP-PBX connectivity to the SIP communications provider (good network security should be implemented e.g. use of network logical separation). In general a SIP Trunk (SIP-T) service will be used - reference SIPConnect [I8]

6. Specification of Dial Through Security Access Controls.

6.1 Generic Controls

There are a number of technical security guides available for use by UK PLC. Specifically, the ISO framework provides for a robust framework of controls and procedures for the generic control of risk and security.
There are also a number of good practice guides, including the UK government's Cyber Essentials Scheme [I2], which provide for good operation and control of generic security for an organisation.
The controls presented below are specific to the objective to mitigate the theft of service from end user voice over IP communications systems, and reference existing good practice guides where available.

6.1.1 Access controls

Securing access to the IP PBX is a critical step in preventing theft of service.

1. PIN codes
   In many systems PIN codes are used to secure access to system functions such as administrative interfaces and voicemail. When choosing PIN codes
   a. Codes should be of at least 4 characters and not allow more than 2 repeated values. Where available they should not be sequential. i.e. 1234.
   b. 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,. A lexicon check to confirm random nature of the character string could be provided.
   c. Do not use default PIN codes or manufacture default passwords. Ensure that these have been changed for a new or re-installed IP-PBX at the earliest opportunity.

2. Passwords
   In many systems passwords are used to secure access to system functions. Where a choice is available between passwords and PIN codes, passwords should always be preferred.
   a. All access should be controlled by password authentication where possible.
   b. Strong passwords should be used. (Strong passwords are defined in the referenced good practice guides.)
3. User Access Management Process & procedure
   As good practice, organisations should maintain and operate good processes and procedures for user access control.
   a. The measures described in section 3 User Access Control of the HM Government Cyber Essentials Scheme [I2] should be applied.
   b. As part of the setup of every PBX end user, the IT policy should make the user change their voicemail PIN before they can use the voicemail service.
4. Network access
   As good practice organisations should maintain operational Network access controls to maintain good security practice within their managed environments

a. The measures described in section 1 Boundary Firewalls and Internet Gateways of the HM Government Cyber Essentials Scheme [I2] should be applied.
b. Further guidance on network based access control is available in section 4 VoIP Security of the Internet Telephony Services Providers' Association (ITSPA) Recommendations for secure deployment of an IP-PBX [I3]
c. Further guidance on the use of firewalls in VoIP environments is available in section 5 Using Firewalls to Protect Traffic of the ITSPA Recommendations for secure deployment of an IP-PBX [ref]
d. Block access to unallocated mailboxes.

6.1.2 Controls to limit the impact of theft of service

Should an attacker successfully compromise an IP IPX the amount of revenue available to the attacker depends on the number and type of calls they are able to execute. Implementation of the controls described in the section will help to limit the cost of a successful attack.
In some cases the controls can be implemented by the system administrator using features available on the IP PBX (dependent on functionality) and in some cases they will require agreement with and implementation by the VoIP service provider.

1. Choosing a VoIP service provider (VoIP SP) and IP PBX
   Choose a VoIP service provider and IP PBX solution which support the implementation of the measures described in this guidance.
   Choose a VoIP SP who, as a minimum, will only accept SIP messages from pre-defined IP address(es) and choose an IP PBX that supports this function.
   Where possible additional network connectivity security protections should be utilised, such as VPN connectivity or TLS transport security etc.

   The reader should also consider choosing a provider that holds the Federation of Communication Services (FCS) Mark of Excellence. The FCS Fraud Mitigation Standard Specification [I4] describes the requirements which a SIP trunking provider must meet to obtain the Gold, Silver or Bronze standard.

2. Define normal use
   Many of the techniques employed by an attacker to generate revenue will fall outside the normal use of the IP PBX. By defining what normal use of the VoIP service will be, rules can be created to block fraudulent behaviour.
   a. Time blocked calls
      Restricting the ability to make calls to within office hours will prevent an attacker from using the IP PBX to make calls when no one is around to monitor the service, e.g. at the weekend, late at night and Public Holidays.
   b. Concurrent calls
      Placing a limit on the number of concurrent calls will prevent an attacker from connecting many expensive calls simultaneously. For example, if you have only eight employees, consider limiting the number of allowable concurrent calls to eight.
   c. Maximum call duration
      Limiting the maximum call duration will restrict an attacker's ability to generate revenue.
   d. Frequency of dialled numbers (short bursts)

Limit the number of calls which may take place over a given period of time, e.g. a maximum of 100 calls per minute. An attacker may use the IP IPX to execute a large number of short calls in a short space of time. These calls may have a high connection charge and can generate significant revenue.

e. Call barring
Block calls to number prefixes which you do not intend to dial by omitting them from your IP PBX dial plan Examples may include numbers in the following categories:

- UK premium rate
- UK local / national
- UK mobile
- UK non-geographic
- UK directory enquiries
- International regions (Africa, Asia, Australasia, Europe, North America, South America
- International countries

Where fine grained control is required specific country codes or geographic area codes can be blocked.

f. Text message services
If you do not intend to make use of text message services ensure that they are disabled. Text messages can be used to generate revenue for an attacker, e.g. text donation services.

g. Calling pattern analysis
Some service providers have the capability to learn your normal pattern of calling, and detect when there is activity outside of the normal usage.
For example - repeated bursts of calls to the same number, this is a common mechanism used by fraudsters using diallers.

3. Agree spending limits
Setting a limit on the bill with the VoIP service provider will limit your exposure to an attacker.

a. Credit limits and prepay
Agreeing a prepay contract with your VoIP service provider will limit your exposure to theft of service to the amount of your prepay balance.

b. Alternately, for contractual arrangements where a bill is paid in arrears an auto-suspend threshold could be implemented (where the service stops making outbound calls after a specified call spend limit has been reached).
Usage profiles
Where possible arrange a credit limit which reflects the normal usage pattern. For example, agree a daily or weekly minutes based limit with the VoIP service provider.

c. Call Cost Limits
Consider setting a call cost limit based on your normal usage. For example if the majority of your calls are made to UK numbers, then calls to high cost destinations could be a red flag that there had been a breach in your network.

6.1.3 Operation and maintenance controls

Access control security must not be compromised during the normal operation or maintenance of the IP PBX

a. Where maintenance services are provided by a third party they should treat information about individual system's access procedures in confidence and store any records securely. Staff should be aware of the importance of keeping information on access procedures secure.
b. When staff leave the company's employment or maintenance arrangements are changed any access credentials which they may have known should be changed by the system manager.
c. A maintainer should control access to maintenance facility access codes on a "need to know" basis only. If possible, allocating individuals different access codes.
d. A maintainer on acceptance of a system should change all passwords needed to access system maintenance and configuration functions.
e. Maintainers should change access PINs and passwords frequently.
f. The number of invalid access attempts should be restricted and when exceeded should alert the telecommunications manager that there had been unauthorised access attempts.
g. All the information available, including itemised bills, should be checked for evidence of calls to unusual destinations and at unusual times.

6.2 Overall network security

Most organisations will operate IP PBX equipment within an enterprise network other technologies and connectivity. These will have an impact on the security and operation of the IP PBX and supported service.

As well as specific controls to the IP PBX, then other connectivity must be considered within the overall security policies and procedures.

If the network you operate has both VOIP and LAN traffic, care should be taken to ensure the security of both types of traffic.

Consideration should be given to Quality of service and security controls. A starting point for this is the HM Government Cyber Essentials Scheme [I2]

7. Good Practice Guides

The following references are designed by and sourced from the industry supporting the technology and devices in scope of this NICC Standard.
They are based on current best knowledge and experience.

The URLs listed in this section were correct at the time of publication.

For any further information about the documents referred to in this section, please contact the relevant document owner.

7.1 Cyber Essentials Scheme

Cyber Essentials is a government Scheme which is supported by industry. It enables organisations of all sizes to be tested against a set of criteria to ensure they have good basic cyber hygiene in place. A description for the Scheme can be found here –

https://www.gov.uk/government/publications/cyber-essentials-scheme-overview [I1]

http://www.cyberstreetwise.com/cyberessentials [I2]

Publisher: HM Government
Email - cybersecurity@culture.gov.uk

7.2 ITSPA Recommendations for secure deployment of an IP-PBX

ITSPA produces a series of guide to assist operators of systems to provision, protect and operate the devices and technology supplied by their members.

Useful guides are -

Guide 1 - http://www.itspa.org.uk/wp-content/uploads/1407_ProvisioningBCP.pdf [I3]

Guide 2 - http://www.itspa.org.uk/wp-content/uploads/1311-Recommendations-for-secure-deployment-of-an-IP-PBXV2.pdf [I4]

Owner - Dave Cargill
Email - david@cargill.ch

7.3 TalkTalk

TalkTalk has produced a guide to help limit fraud. That guide is available here - https://www.talktalkbusiness.co.uk/Global/Final-Assets/Collateral/white_papers/Telecoms%20Fraud%20White%20Paper%20-%20PARTNER.pdf [I5]

Enquiries - enquiries@talktalkbusiness.co.uk
Owner – TalkTalk Business
Email: fnugent@talktalkbusiness.co.uk

7.4 FCS Fraud Mitigation Standard Specification

The FCS has produced a standard for mitigating fraud. The FCS Fraud Mitigation Standards can be found here - http://www.fcs.org.uk/image_upload/files/FCS%20Fraud%20Mitigation%20Standard%20Specification.pdf [I6]

The FCS also produces a Telephone Security Checklist available here - http://www.fcs.org.uk/image_upload/files/FCS%20Security%20Checklist.pdf [I7]

Owner – Cathy Gerosa
Email - cgerosa@fcs.org.uk

History

Document history		
Version	Date	Status
1.1.1	March 2016	Initial publication