HOW WE DELIVER

A SECURE & ROBUST

HOSTED TELEPHONY SOLUTION

inclarity

01

INTRODUCTION

Inclarity is the UK's leading provider of Hosted Telephony, Hosted UC and Hosted Video solutions. We help our customers - who are generally small businesses, mid-sized enterprises and branch networks - to communicate more effectively while reducing costs, by migrating them to our cloud-based solutions.

Formed in 1991 as a telecommunications provider, Inclarity anticipated the potential of voice over IP (VoIP) technology and the way it would transform the way businesses communicate. In 2003 we launched our first cloud-based telephony service, and since then we have continued to evolve and enhance our platform to deliver one of the most comprehensive portfolio of services available in the UK.

Key to our success has been building a hosted telephony platform that is not only reliable, but also secure. As a customer's organisation transitions from traditional voice solutions to VoIP, a different set of challenges emerge in regards to protecting itself from cyber threats and telephone fraud.

This paper outlines the various security measures taken by Inclarity to protect both the VoIP platform and the customers that use it.

02

VOIP SECURITY OVERVIEW

Voice over IP by its very nature requires IP network infrastructure. Therefore, the delivery of any VoIP service is subject to the same challenges and threats as any other kind of computer network.

There are three main potential threats to any hosted VoIP installation:

1) Any party in the path of the call stream between the core platform and the remote site may attempt to 'snoop' on the call for their own purposes

2) Any third party may attempt to disrupt service by targeting either the core platform or the customer site in a denial of service (DOS) type attack

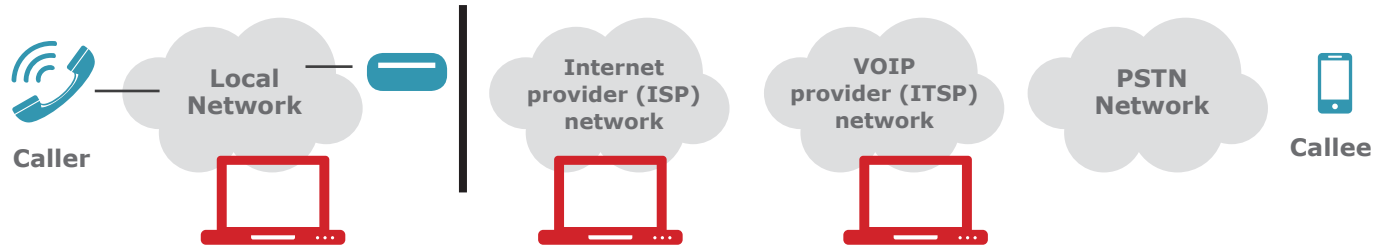
3) A third party may exploit service access loopholes to send their own VoIP calls either a) via the customer's own equipment, or b) via other equipment using the customer's credentials

Inclarity takes precautions to protect the core network where the telephony platform is situated, but considerations must also be given to a) the state of the local network where the customer endpoints are installed, and b) the state of the local broadband Internet connection that allows those endpoints to talk to the Inclarity core.

03

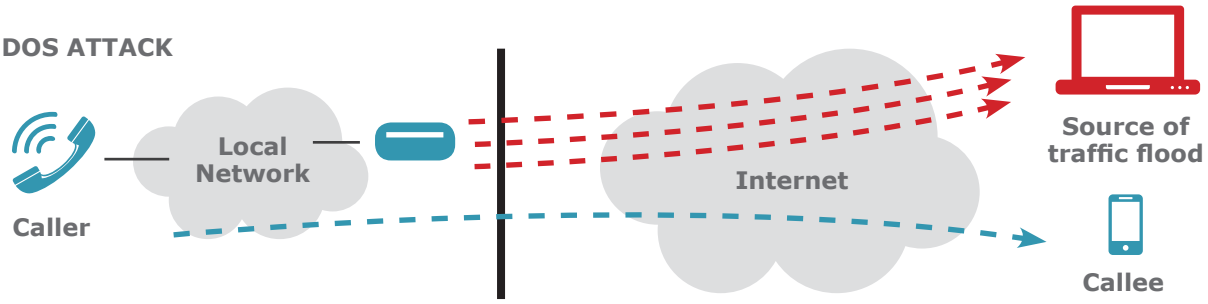
VOIP VULNERABILITIES IN PRACTICE

VOIP CALL SNOOPING

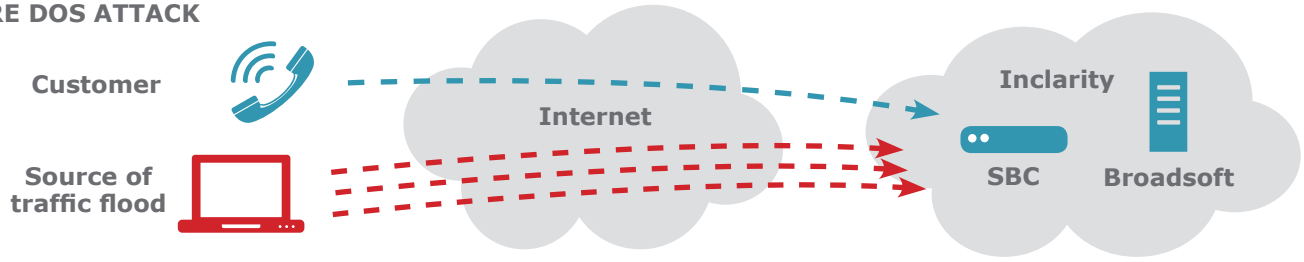


Call snooping is a difficult – but not impossible – proposition as it requires the 'snooper' to be in a network location through which the calls are being delivered. This means they either need to sit directly on your network, your ISP's network, on the VoIP provider's network, or at some other point in between, all of which are unlikely scenarios. If however they are able to gain access to the network path – and they know what they are looking for - then using a software diagnostic tool such as Wireshark they can potentially capture all the data packets of the call and play back its audio content.

LOCAL DOS ATTACK

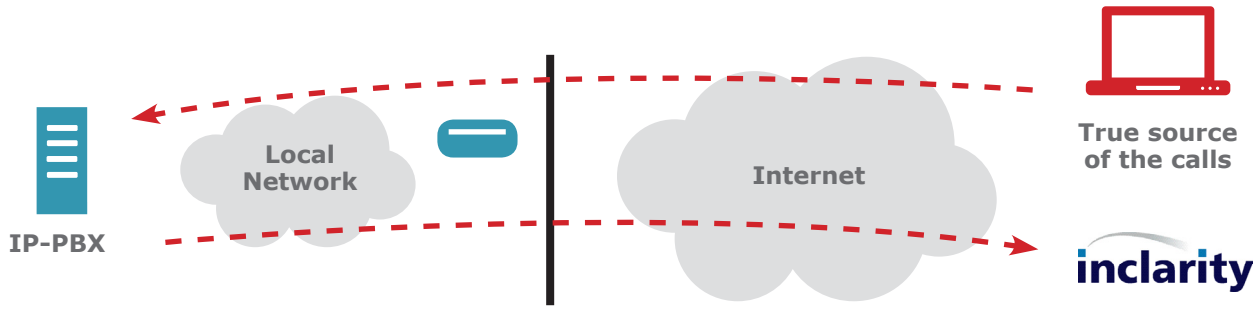


CORE DOS ATTACK



VoIP service DOS attacks are very easily implemented, but seldom happen in practice as the activity is currently considered to have little value. As VoIP technology becomes more prevalent in the years to come however we can fully expect large businesses to be held to ransom over the state of the availability of their telephony, in a similar manner to the way cyber terrorists attack and suspend web sites today. What is more commonplace right now is the phenomenon of spam over internet telephony (SPIT) – i.e. unwanted VoIP calls from unknown parties – but this is generally more of a nuisance than a real threat to any business.

IP-PBX EXPLOIT



The most serious threat to VoIP based technology is the delivery of illicit third party calls, which normally results in international toll fraud, to the extreme detriment of the customer and/or the provider. There are a number of large and sophisticated criminal operations who dedicate themselves to setting up high cost call-share numbers in overseas countries, and then arrange to call these numbers though other people's systems so that they receive large pay-outs for receiving the calls, but then leave the owner of the exploited system with the bill for making the calls in the first place. The financial impact of this activity could range from a few hundred pounds, to tens of thousands of pounds. Despite lobbying by providers not just in the UK but in many other countries, the wider international telecommunications industry has yet to take any action to curb this kind of activity.

04

INCLARITY PLATFORM SECURITY

Inclarity maintains a robust set of policies and procedures to ensure the security of all platform assets.

Proven Technologies

All of the elements of the Inclarity Hosted VoIP platform and core network are sourced from industry-leading suppliers and manufacturers which have a reputation for reliability and security.

Broadsoft by Broadworks is the de facto standard for delivering business telephony features. Cisco and Juniper are reputable brands for switching and routing hardware. AcmePacket session border controllers (SBCs) are world class devices for mediating and monitoring telecommunications traffic.

Access Controls

Our server maintenance policies include strict guidelines for server configuration, monitoring and auditing.

Our online network access policies emphasise the importance of IP hardening and cover secure local and remote access methods, password rules and user authentication guidelines.

Physical access to critical systems is limited to authorised personnel only. Access to servers, routers and switches is monitored 24/7 and utilises two-factor authentication.

Network Routing

The switches in our core network utilise VLANs to logically separate voice and data traffic. Comprehensive access rules and IP filters make sure we only let the right traffic in to the right servers.

All SIP (VoIP) traffic in/out of the network goes via session border controllers (SBCs) with complex monitors and filters. The SBCs also have safeguards to resist reconnaissance attempts, traffic floods and DOS style attacks.

Note though that there is no blanket solution to deal with all DOS type attacks, which can vary a great deal in nature, scale and intent. As this activity continues to evolve, so will Inclarity (and the rest of the IT and telecommunications industries).

Service Authentication

All VoIP calls must be authenticated either by IP address, or with a unique SIP username and password provided by Inclarity. Anonymous calls without credentials will be rejected. The platform also issues a double ‘digest’ challenge in response to all requests to discourage random access attempts.

In addition, all hosted VoIP Subscribers must pre-define the make and model/version of the endpoint they will use to make their calls. Even if the correct Inclarity credentials are used, if the call originates from an unknown device then it will still be rejected.

Voice Portal Hardening

As customers can access their service details online, steps are taken to mitigate the risk of abuse of this access by hardening the password used by the portal for user authentication.

- Password must be at least 6 characters
- Repeated characters are not permitted
- Using the extension number or the phone number is not permitted
- Online access is disabled if the system detects 3 failed log-in attempts
- Passwords regularly expire and must be reset by the user

Feature Restriction

Through online portal access the customer can choose to restrict or deactivate certain features of the hosted VoIP platform – e.g. call diversion.

The customer can also self-specify what national and international destinations can be called through the service from a single extension, or from any user on their installation.

Inclarity enforces an upper limit to the number of simultaneous calls any VoIP installation can make, mitigating the scale of any potential call abuse.

Pro-Active Blacklisting

Inclarity subscribes to a number of services which report on source IP addresses and area code destinations which are suspect or which have been associated with incidents of hacking or fraud. Bad IP addresses are categorically denied access, and bad destinations are blacklisted so they cannot be called by any VoIP user.

Real-Time Service Monitoring

Inclarity has deployed sophisticated network monitoring tools which quickly alert our Support team to any unusual activity. Reporting tools on the SBCs also provide real-time information concerning calling profiles and traffic volumes.

Comprehensive Logging & Auditing

All changes made to the VoIP platform are logged with both a date/time stamp and the user's login for reference. The majority of the other elements within the Inclarity network have similar logs. All customer queries, problems and change requests are ticketed online with a unique id for reference. Inclarity follows best practice procedures which are regularly audited and reviewed.

05

CUSTOMER NETWORK SECURITY

In a caveated installation a business chooses to run VoIP over its own network, possibly using all of its own equipment. In such case the customer themselves should ensure that this network is properly secured and protected from internal and external threats.

Where an IP-PBX in particular is deployed the customer should take care to change the default credentials of all extensions and harden remote access from illicit intrusion. The customer should also restrict the outgoing dial plan of the IP-PBX to approved dialled destinations only.

It is recommended that the firewall on the network border is set to reject all SIP requests from non-Inclarity IP addresses – this rules out the possibility of call relaying, and also unwanted locally terminating SPIT calls.

Of course, the customer should also ensure that sensitive credentials provided by Inclarity (and any other IT supplier) are properly secured. Every PC desktop should have active anti-virus and anti-malware tools installed to ensure that the local network cannot be exploited from the inside. Similarly, the customer should take care to ensure that physical access to phones and other IT equipment is limited to authorised personnel only.

Where Inclarity does provide equipment to the customer, the following additional security measures are taken.

Router Configuration

Any broadband router provided by Inclarity will be pre-configured using a tried and tested template which includes active firewall rules to reject unwanted requests. Local and remote management access is secured with a strong, secret password.

IP Handset Configuration

Any IP telephone handset provided by Inclarity will auto-provision over the Internet without the user requiring sensitive credentials – the true SIP authentication details are entirely hidden. As part of this process all handsets are password-protected from both local and remote management access.

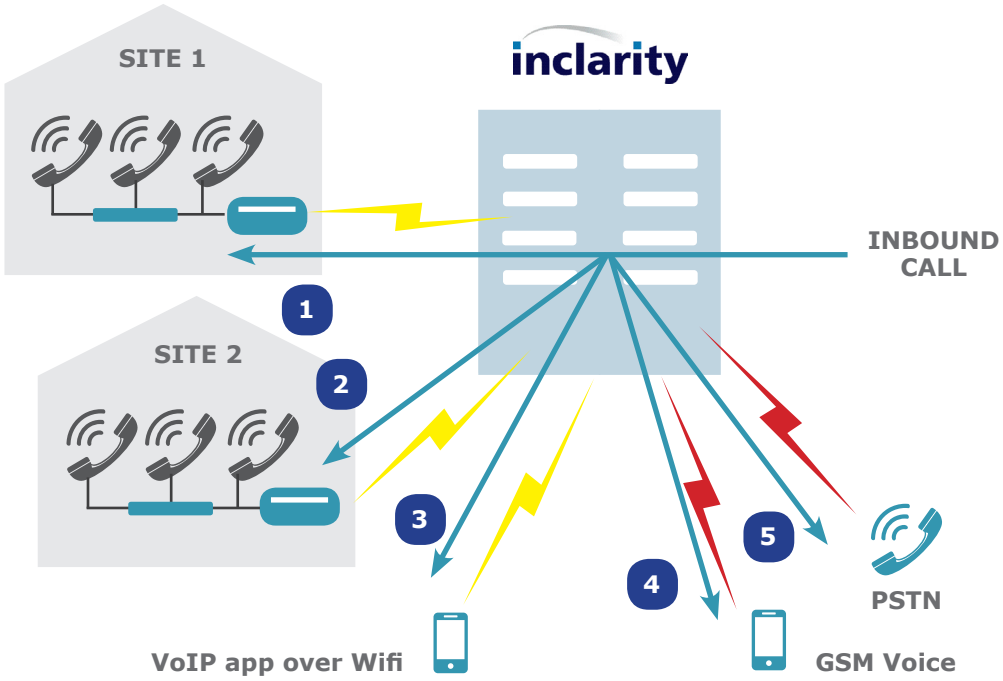
06

INHERENT BUSINESS CONTINUITY

Any modern business relies heavily on telecommunications, to the extent that any loss of connectivity or telephony services can be devastating. More and more IT decision makers are seeking solutions which ensure their business continuity.

Traditional voice solutions such as PSTN and ISDN offer little in the way of business continuity, in that they are susceptible to faults, and there is no recourse if the service to customer site becomes unavailable. In some extreme situations a traditional telephony fault may take many days to resolve.

Moving call response and control into the Cloud via a service such as Inclarity Hosted VoIP provides much greater resilience and flexibility. If anything should happen to your local network infrastructure then your inbound calls can easily be redirected to another site, a backup landline or mobile telephone number, or to platform-side voicemail.



The Inclarity platform itself is fully redundant with no single point of failure, allowing us to offer 99.99% availability, ensuring that your calls are always delivered.

07

SUMMARY

In summary, if your business has an IP network connected to the Internet then this will present a number of challenges.

Using VoIP over such a network introduces a small number of additional risks, which can be addressed with due care and attention.

At Inclarity we continue to invest heavily in our Hosted VoIP platform, and we implement a wide range of measures to protect that platform and its users from harm.

Inclarity’s proven track record of delivering reliable and secure services via industry-leading technologies such as Broadsoft and AcmePacket provides you with the peace of mind you need to concentrate on driving your business effectively.

ABOUT INCLARITY

We are the UK's leading provider of Hosted Telephony, Hosted UC and Hosted Video solutions. We help our customers, who are generally small businesses, mid-sized enterprises and branch networks, to communicate more effectively while reducing costs by migrating to our cloud-based platforms.

Formed in 1991 as a telecommunications provider, Inclarity saw the potential of VoIP and foresaw that hosted telephony could transform the way businesses communicate. In 2003 we launched our first cloud-based telephony service and since then, have continued to evolve and enhance our platform to deliver one of the most comprehensive range of services available in the UK.

Today we deliver a highly secure, resilient and feature-rich, cloud-based telephony, unified communications and video service on a pay-as-you-use basis.

At Inclarity, we combine a flare for innovation with a passion for service. This combination enables us to be a market leader with our technology and to deliver exceptional value to our customers.

Inclarity Communications Limited
96 – 98 King Street
Hammersmith
London
W6 0QW

Telephone
0800 987 80 80

Website
www.inclarity.co.uk

@Inclarity1

Follow Us on Linkedin