Can CLI be trusted?

Richard Clayton

University of Cambridge, Computer Laboratory,
JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom

Abstract

Calling Line Identification (CLI) tells the recipient of a telephone call the number at the other end of the line. However, various insecurities mean that even on traditional telephone systems, CLI cannot be entirely relied upon to be accurate. Once Voice-over-IP (VoIP) enters the picture, CLI validity effectively depends upon the integrity of Internet traceability, and must therefore be treated with considerable suspicion.

1. Introduction

There has long been an interest in knowing where a telephone call has originated. We're all familiar with Hollywood's version of call tracing, where the gallant police lieutenant keeps the kidnapper talking whilst the origin is narrowed down by city, neighbourhood, block and... well in Hollywood, it's never quite that easy.

In modern computerised telephone systems, learning the source of a call is merely an automated query into the live system, or perhaps a matter of consulting the stored transaction logs. In addition to this specialised access, since the mid-1990s the calling number has been made available to consumers and businesses as Calling Line Identification (CLI). [1]

Although CLI display systems tend to be an optional extra on landlines, CLI is universally provided on mobile telephones (cell phones) – it's precisely the mechanism that tells you who is calling, or causes a customised ringtone to play. It isn't generally perceived to be a security mechanism by the public, although it's the assumed validity of the CLI that makes you decide whether or not you are going to answer the call at an otherwise inconvenient moment.

In theory CLI is unreliable, although in practice it is seldom inaccurate on POTS (the Plain Old Telephone Service). However, the advent of Voice-over-IP (VoIP) telephone systems running over broadband Internet connections has raised considerable doubts as to whether CLI can be relied upon in the future, and has sparked a policy debate, on both sides of the Atlantic, as to whether generating fake CLI is (or should be) a criminal offence.

In Section 2, I describe how CLI works, then in Section 3, I discuss how trustworthy it ought to be considered to be. In Section 4, I consider the complexities introduced by VoIP, and in Section 5, the legal issues that arise with CLI, both in terms of privacy and data protection, and also as to whether faking CLI is lawful.

2. Calling Line Identity

Every UK phone line [2] has an "A" Number that is the "real" number of the line (that appears on the phone bill). A line can have several "presentation" numbers as well, which may be selectable by the user when placing calls, with a typical user being a doctor who wishes to be able to call a patient out-of-hours from home, but who wants to present the CLI for the surgery. A line may even be flagged to allow callers to present any number they wish; for example in cases where call centres are generating calls on behalf of several clients with different phone numbers. Where the telephone network providers do not generate the number themselves, Ofcom (the UK industry regulator), insists that a contract is made with the subscriber, requiring that they only present numbers to which they have a valid entitlement.

Email address: richard.clayton@cl.cam.ac.uk (Richard Clayton).

[1] CLI is also known as Caller ID (CID), Calling Number Identification (CNID), Caller Display or a myriad similar terms invented by marketing departments who half-listened to the engineers' explanations. In this article, CLI will be used throughout.

[2] For simplicity, the mechanisms described are for the UK phone system. The operation of CLI (and an associated American system called ANI, Automatic Number Identification) differs in relatively minor details in other countries. Non-UK readers should locate detailed technical descriptions of their own country's mechanisms.

The CLI will usually be provided to the phone being called so that the receiver can determine whether or not to answer, or perhaps to allow the called system to present an operator with the details of the caller from a customer support database. However, the CLI can also be withheld by the caller, and every line has a default CLI Presentation Restriction (CLIR) state for an outgoing call which specifies whether the CLI is usually to be provided or withheld. The CLIR state may be overridden on a per call basis (in the UK, on a BT line, by dialling 141 in front of the called number for a temporary suppression; or 1470 to allow a temporary reveal).

At a protocol level the system is complex. The two main protocols involved are DSS1 for ISDN (Integrated Services Digital Network) communications between customer equipment and the telco switch and SS7 (Signalling System 7) for communication between the telco switches. These protocols were developed by the Telecommunication Standardization Section of the International Telecommunication Union. DSS1 is described in ITU Recommendation Q.931 [14] and SS7 is described in ITU Recommendation Q.763 [13].

The calling party number and associated state are passed in DSS1 SETUP messages and in SS7 IAM (call setup) packets and the same byte level format is used in each. The detailed rules for handling the various states and user preferences are set out in clauses 3 and 4 of ITU Recommendation Q.951 [15].

If the calling user does not provide a number, as would be the case for non-ISDN "analogue" calls, then the switch will generate a "network provided" number (usually the A number). If the calling user does provide a number then it will be validated and if acceptable it will be passed on. If it fails validation then Q.951 requires the network provided number to be sent (although there is also provision in the packet formats for sending a failed indication). Where there is a "special arrangement" the switch will not validate the number and will set an appropriate state.

The bit settings are recorded in two bits in the calling party number field (ITU Q.763 3.10, ITU Q.931 4.5.10) as described in Table 1.

Screening indicator
0 0 user provided, not verified (National Use Only)
0 1 user provided, verified and passed
1 0 user provided, verified and failed (National Use Only)
1 1 network provided

Table 1
The validity of the CLI is mapped to two bits

The calling user's preferences for CLI Presentation Restriction, either a default setting or a per-call override, is recorded into another two bit field in the same byte as the screening indicator, as shown in Table 2. The user preference may be discarded and replaced by an indicator that the CLI value is unavailable. This can occur when a telco fails to pass the CLI to systems that they do not trust to operate the same data protection procedures as they do.

Address presentation restricted indicator
0 0 presentation allowed
0 1 presentation restricted
1 0 address not available (National Use Only)
1 1 reserved for restriction by the network

Table 2
The settings for disclosing the CLI are mapped to two bits

The terminating telco, or a subscriber with the "presentation override facility", such as a 999 operator, [3] will always see the CLI value. If this value is marked as "presentation allowed" then a normal subscriber will be able to see the number; if the marker is "presentation restricted" they will see "withheld"; otherwise they will see "unavailable".

Internet Service Providers (ISPs) who provide dial-up access to the Internet do not tend to be treated as anything other than or a normal subscriber when it comes to CLI. Although the number (and its associated flags) can be passed across the Q.931 interface to an ISP's NAS (Network Access System) equipment, the telco will withhold the number if instructed to do so by the caller.

3. Is CLI really trustworthy?

Trustworthy CLI is clearly desirable. Beyond the decision of whether or not to answer your mobile, businesses are increasingly using it for customer relationship management (CRM) or to short-cut some identification procedures: treating calls which are not from a customer's "home phone" as requiring extra levels of authentication. Unfortunately, there are a number of flaws.

3.1. *Generic CLI*

Many systems supply a generic CLI rather than an actual CLI. For example, all calls made from the University of Cambridge (many thousands of phones) have the same CLI, provided by the central switch. Similarly, some cut-price calling card systems (where you enter a card number before the number you wish to reach) do not relay the CLI from the originating phone. As will be discussed in more detail below, Voice-over-IP systems, a fast-growing sector, usually offer a customised CLI for calls that break-out from the IP world into the traditional phone system, but generic CLI will be provided for systems that offer universal SIP access to "800" numbers (the phone calls are free to the person operating the gateway, so this isn't uncommon).

Of course, in all these scenarios, the system that generates the generic CLI will have some logs and some traceability of its own. However, the recipient of the call cannot easily judge the quality of this traceability. The system may accept incoming calls where the CLI is withheld, or the logs

[3] An operator may also have SS7 level access, which would permit access to the calling party number (the A Number). Therefore any investigation involving that telco would have access to SS7 data and would also be able to learn this value, in addition to the CLI information.

may be kept for a relatively short period. I have personal experience from my time working at an ISP of investigating an account that had been created solely for spamming Usenet, and finding that the CLI was generic (a calling card system marketed to students). So this is not only an actual problem, but also one that is not immediately obvious to an ISP. [4] Only when a particular CLI is investigated will it become clear that the ISP's security policy has been subverted by another system which operates different criteria for admission control.

3.2. *Forged CLI*

As mentioned earlier, the industry regulator, Ofcom, requires that subscribers are contractually bound to provide only the CLI numbers they are permitted to use. However, there is no general requirement to configure telco switches to reject incorrect CLI. This is currently formulated in an Ofcom Network Interoperability Consultative Committee Specification [10] as a requirement on the telco to validate the CLI (and fix up incorrect values) unless there is a contractual "special arrangement" in which case the customer promises to behave. A customer who breaks the contract would lay themselves open to civil action, but at present in the UK (and USA), they may not commit a criminal offence for the deception itself as discussed further in Section 5 below.

In practice, very complex arrangements are often in place, which make it hard for the phone company to validate the CLI values they are presented with. A large corporation may wish to present a standard "reception" number no matter which of dozens of individual sites made a call. Another company may route outgoing calls from dozens of sites, with many disparate CLI values, across their own infrastructure and deliver calls to the public network wherever it is cheapest to do so. In both cases, almost every phone company switch would need to validate every CLI value offered against a remote database, which is not currently practicable.

Consequently, the CLI value provided by a PABX (private automatic branch exchange, i.e. the customer's own phone system) will often be trusted to be correct – and this in turn means that anyone who can reprogram the PABX will be able to provide any CLI they wish, with the changes they make unlikely to be logged anywhere. In the UK, in practice, ISDN connections that might be purchased by individuals will restrict CLI provision to a very small number range; however the freedom to set a wide range of values is available on the more high-end products.

It should be noted that the reprogramming of a PABX to supply forged CLI may be done by unauthorised insiders, or by external intruders who have access to a control interface – commonly left enabled by phone system installers to allow them to correct faults remotely, and which may well still have the manufacturer's default password. Much of PABX related fraud relates to inadequate controls on DISA (Dial In System Access or Direct Inward System Access), i.e. the ability to dial in to a PABX and make an outgoing call at the company's expense. However, some fraud is done by means of remote access interfaces and it would be naïve to believe that people with this level of access would always refrain from altering the CLI on the fraudulent calls that they placed.

Recently, intentional forging of CLI has become available in the USA and Canada as an openly advertised service. In September 2004, a company called Star38 announced a commercial service for spoofing CLI which they were targeting at Law Enforcement, debt collectors, private investigators and similar "good guys". The mechanism appeared to be their system calling both ends of the conversation, with any CLI of the caller's choosing given to the target to mislead them. The system was withdrawn within days, with the entrepreneur claiming to have been harassed and delivered a death threat [2]. A similar system continues to be offered by many other companies such as Spooftel (`www.spooftel.com`) and Telespoof (`www.telespoof.com`), and in practice the CLI can be forged by almost anyone with a copy of `asterisk` [5] and a telephone operator that does not police the values being set.

4. VoIP

Voice-over-IP (VoIP) telephony (i.e. the transmission of voice calls using TCP/IP protocols over the public Internet) is generally associated with services that permit such calls to break out to the traditional telephone network. In some cases these outgoing calls are assigned a CLI of a specific geographical number, which the operator will accept incoming calls on, routing them across the Internet to the VoIP system. The user is expected to choose a number prefix which either reflects their location, or that minimises the cost of other parties calling them.

In other cases, the VoIP call will be given a CLI number of the user's own choice. In the UK, the Ofcom rules mean that that a user must promise the VoIP provider that the phone number provided is theirs, but in the past providers have permitted any number to be set, and when that was abused they merely changed their procedures to check that the number existed – without establishing ownership. Reputable providers now require faxed copies of telephone bills to establish *bona fides*, although forging a phone bill is hardly a significant obstacle for the wicked to overcome.

CLI "spoofing" on VoIP services is essentially the same problem just discussed with PABXs, except that one no longer needs access to any expensive hardware, but can just

[4] In this particular case, it may not have been obvious to the caller either. Without being able to interrogate them, it is hard to say whether their anonymity occurred by design or through chance.

[5] `asterisk` (`www.asterisk.org`) is an open source program that provides Linux users with a full-featured PABX. With appropriate hardware for interfacing to ISDN it will set appropriate CLI information on an outgoing call.

sign up to a service on a website. Any organisation that relies on CLI as an authenticator for signing up for, or reconfiguring, one of their services could be misled into believing that the request was traceable. Furthermore, the traceability of any request coming over the Internet ultimately relies upon the originating ISP being able to determine which of their customers was using an IP address at a particular time. Although dial-up Internet access can be problematic over VoIP services, it can work – so the ISP itself may ultimately be relying on CLI to identify its own interactions with its own customers.

In all of these cases, although the CLI for the call is bogus, there may well be traceability information at the SS7 level (in the telco switches) and so, in principle, the call can be traced back to where it entered the public telephone network. That location could, again in principle, hold details of the true caller so they would be traceable. However, when one is talking about VoIP calls then the gateway into the network will only hold the IP address of the origin of the call – and that, as just noted, may only be traceable if CLI can be trusted, and as the process recurses back, the trail gets ever colder. In practice of course, all is not lost. The VoIP service is unlikely to be free, and the payment can be traced back through financial systems. Nevertheless, the apparently trustworthy CLI from the fixed-line telephone era is suddenly exposed to the vagaries of traceability on the open Internet.

5. Legal Issues

The legal issues relating to CLI fall into two distinct areas. One deals with data access and processing. The other relates to whether or not spoofing CLI may be illegal.

5.1. *Legal restrictions on access to CLI data*

At present, in the UK, the regulations governing the use of CLI [11] permit "Electronic Communications Networks" to use received CLI data for "network/account management purposes" and "in co-operation with the relevant authorities, for emergency calls and the tracing of malicious calls and similar activities". However, an ISP that wanted to use the received CLI data (viz: overriding the user's request that it be withheld) would also have to meet the test that access to CLI data was "essential to the provision of an Electronic Communications Service", which would mean arguing that dial-up Internet access could not be offered unless the source of all calls could be traced. Although this might seem hard to argue in the general case, it is more plausible for "free" services where nothing is known about the user and for some time, the regulator has encouraged subscriptionless ISPs to take this approach [16].

CLI data relating to individuals is of course personal data within the meaning of the Data Protection Act 1998 and similar legislation throughout Europe. This restricts the way in which it can be processed, and in particular, access to CLI data by law enforcement must be by the serving of notices under s22 of the Regulation of Investigatory Powers Act 2000. At present, logs of CLI data must be discarded once there is no further business use for them, but this will change by October 2007 with the implementation of the Data Retention Directive [6] for telephone company datasets.

Outside of Europe, the situation is mixed. In Australia, which has a similar legislative framework in its Privacy Act 1988 [3] and Calling Number Display Industry Code [1], a number of telephone call carriers (including Telstra, Optus and Comindico) have been providing CLI to some ISPs since 2002, as requested by the Internet Industry Association of Australia (IIA). Electronic Frontiers Australia argues that this is "overkill" and unlawful [4].

Meanwhile, in New Zealand, an internal memo from Telecom New Zealand [12] states that ISPs will not be given withheld CLI, but that the telco records will have this information if the police require it.

A 2000 working group on Computer Related Crime in Hong Kong concluded [8] that forcing ISPs to record CLI for all calls should be put on hold. They were concerned about cost, likely effectiveness and the inability to deal with calls from abroad.

In India the authorities have taken the view that CLI is a necessity and should not be suppressed by individual users. In their 11 May 2004 Licence Agreement for telcos [7] it says at s41.19(iv):

> *"Calling Line Identification (CLI) shall never be tampered as the same is also required for security purposes and any violation of this amounts to breach of security. CLI Restriction should not be normally provided to the customers. Due verification for the reason of demanding the CLIR must be done before provision of the facility. It shall be the responsibility of the service provider to work out appropriate guidelines to be followed by their staff members to prevent misuse of this facility. The subscribers having CLIR should be listed in a password protected website with their complete address and details so that authorized Government agencies can view or download for detection and investigation of misuse. However, CLIR must not be provided in case of bulk connections, call centres, telemarketing services."*

5.2. *Legality of spoofing CLI*

In the US, where CLI is commonly used by consumers to filter calls and, it is claimed, as an authenticator for incoming calls from banks, there has been some concern about misuse of CLI spoofing to commit frauds.

In 2006 the "Truth in Caller ID Act" (HR 5126) passed Congress, with almost no discussion, but stalled in the Senate and fell at the end of the session. It has been reintroduced at the start of 2007 as HR 251 [5].

The main provision is:

> `It shall be unlawful for any person within the United States, in connection with any telecommunications service or VOIP service, to cause any caller identification service`

to transmit misleading or inaccurate caller identification information, with the intent to defraud or cause harm.

In the UK, the relevant legislation will now be found in s2 of the recently passed Fraud Act 2006.

s2 Fraud by false representation

(1) A person is in breach of this section if he--

(a) dishonestly makes a false representation, and

(b) intends, by making the representation--

(i) to make a gain for himself or another, or

(ii) to cause loss to another or to expose another to a risk of loss.

(2) A representation is false if--

(a) it is untrue or misleading, and

(b) the person making it knows that it is, or might be, untrue or misleading.

(3) ''Representation'' means any representation as to fact or law, including a representation as to the state of mind of--

(a) the person making the representation, or

(b) any other person.

(4) A representation may be express or implied.

(5) For the purposes of this section a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention).

This appears to cover the same ground as HR251 so far as fraud goes, but not so far as "harm" goes. However, s127(2) of the Communications Act 2003 says:

A person is guilty of an offence if, for the purpose of causing annoyance, inconvenience or needless anxiety to another, he--

(a) sends by means of a public electronic communications network, a message that he knows to be false,

(b) causes such a message to be sent; or

(c) persistently makes use of a public electronic communications network

which would cover cases where CLI spoofing causes "annoyance, inconvenience or needless anxiety" – and presumably in any case where people were looking for a law to employ, then doubtless "inconvenience" must have occurred.

It still seems worth considering whether there is a need for an explicit offence of spoofing CLI, to cover the cases where the spoofing is self-evident, but there is no convincing evidence of fraud, inconvenience or the "needless" type of anxiety. Is perhaps there sufficient flexibility in, say, the Criminal Attempts Act 1981, to deal with a CLI related fraud that just didn't come off as it was intended? Of course one might rely on a civil case for breach of contract with a telecommunications provider, but this might look like insufficient protection to a third party who might rely upon forged CLI.

6. Conclusions

In his book "The Art of Deception" [9] (essential reading for every security professional) Kevin Mitnick presents numerous examples of how humans can be tricked into compromising security. He has several stories that show how incorrect CLI can be used as part of the process of getting people to trust you enough to let you in to their systems. If someone spoofs the CLI for the Queen or the Prime Minister then it's unlikely that most people would recognise the number or be fooled for more than a moment. Yet, if the CLI says that the call is coming from the accounts department in Manchester, then a great many people will treat that as a solid means of authenticating the call.

Hollywood insists the hero can only catch the villain in the final dramatic shootout, without the benefit of successful call tracing in the second reel. In real life as well, CLI cannot be relied upon, either for proof of which landline is being used or increasingly – as VoIP is deployed – for proof of anything at all, when the source of a phone-call can only be determined by Internet traceability techniques. Businesses and others whose security policies place significant faith in CLI validity need to urgently re-examine their basic assumptions.

Acknowledgments

Richard Clayton is currently working on the spamHINTS project, funded by Intel Research.

References

[1] Australian Communications Industry Forum: Industry Code – Calling Number Display. ACIF C522, Feb 2003. http://www.acma.gov.au/acmainterwr/telcomm/industry_codes/codes/c522c.pdf

[2] K. Belson: Citing Threats, Entrepreneur Wants to Quit Caller ID Venture. New York Times, 4 Sep 2004. http://www.nytimes.com/2004/09/04/technology/04caller.html?ex=1252123200&en=68bab740982a4cb1&ei=5088

[3] Commonwealth of Australia: Privacy Act 1988. http://scaleplus.law.gov.au/html/pasteact/0/157/pdf/Privacy1988.pdf

[4] Electronic Frontiers Australia: Privacy invasions: Blocked Calling Number Disclosure to ISPs. EFA, 5 Jul 2003. http://www.efa.org.au/Issues/Privacy/cndnomand.html

[5] E.L. Engel: Truth in Caller ID Act of 2007. US House of Representatives, H.R. 251, 2007. http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.00251:

[6] European Union: Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Official Journal of the European Union, L 105, 54, 2006. http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2006/l_105/l_10520060413en00540063.pdf

[7] Government of India, Ministry of Communications and IT: Licence Agreement for Provision of Unified Access Services After Migration. 11 May 2004, 79pp. http://www.dotindia.com/basic/FINAL%20UASL%20MIGRATION%20metro(%2011.05.2004).doc

[8] Inter-departmental Working Group on Computer Related Crime: Report. Security Bureau, Hong Kong, Sep 2000, 138pp. http://www.hkispa.org.hk/pdf/ComputerRelatedCrime.pdf

[9] K. Mitnick and W.L. Simon: The Art of Deception. Wiley, 2002. ISBN 0-471-23712-4.

[10] Ofcom Network Interoperability Consultative Committee: Requirements on Communications Providers in Relation to Customer Line Identification Display Services and Other Related Services. ND1016:2004-09, PNO-ISC/SPEC/016, Ofcom, Sep 2004, 27pp. http://www.nicc.org.uk/nicc-public/Public/interconnectstandards/spec/nd1016_2004_09.pdf

[11] Oftel: Guidelines for the provision of Calling Line Identification Facilities and other related services over Electronic Communications Networks Version 2. Office of Telecommunications, 11 Dec 2003. http://www.ofcom.org.uk/telecoms/ioi/orp/cli/

[12] Telecom New Zealand: Calling Station ID/Calling Line ID. Informer WS 2003-02-10, Telecom New Zealand, 10 Feb 2003, 2pp. http://www.telecom.co.nz/binarys/ws_2003-02-10.pdf

[13] Telecommunication Standardization Section of the International Telecommunications Union: ITU-T Recommendation Q.763. Signalling System No. 7 – ISDN user part formats and codes. International Telecommunication Union, Dec 1999, 122pp. Not available online. [6]

[14] Telecommunication Standardization Section of the International Telecommunications Union: ITU-T Recommendation Q.931. Digital Subscriber Signalling System No. 1 – Network Layer, ISDN user-network interface layer 3 specification for basic call control. International Telecommunication Union, May 1998, 329pp. Not available online. [6]

[15] Telecommunication Standardization Section of the International Telecommunications Union: ITU-T Recommendation Q.951. Digital Subscriber Signalling System No. 1 – Stage 3 Description for Supplementary Services Using DSS 1. Clauses 3–6. International Telecommunication Union, Mar 1999, 34pp. Not available online. [6]

[16] P. Walker: Re: BT CLI availability ? 22 Jan 1999. http://www.google.com/groups?selm=789a0I$8sl$1@plug.news.pipex.net

[6] Note that although the ITU publications are not openly available online, it is currently possible to download a small number of documents from their electronic bookshop without charge.