Nuisance calls and CLI spoofing – progress to date and the way forward

Huw Saunders, Director, Network Infrastructure

12th November

Agenda

- Nuisance calls and spoofed CLI – metrics, motives and policy actions
- Mitigating the risk through regulatory and industry initiatives
- Longer term technical solutions and implementation challenges

False CLIs are often associated with nuisance calls

- 80% of UK consumers report receiving nuisance calls and volumes are again increasing
- Many have spoofed CLI – deliberately malformed or a legitimate, but incorrect, CLI, so as to disguise the callers identity and location
- Network traffic sampling suggests that overall call attempts from such sources may be of the order of **1 – 2 billion** per annum across all networks in the UK
- Most such calls are unsolicited live marketing calls or automated messages from "lead generators"
  - Little evidence to date of "Voice Denial of Service" attacks seen in North America
- Calls create significant consumer concern and undermine trust

Nature of some calls is becoming more overtly criminal but action is being taken

- Increasing number of cases where there is exploitation for fraud through “social engineering” (using faked CLI, for example for the consumers bank) to gain trust. Such “vishing” techniques may be replacing “courier fraud” as a focus of criminal activity as a result of co-ordinated industry action to reduce the “Called Party Held” duration that is necessary for that scam to work

- Both general “nuisance” and “vishing” calls represent clear breaches of regulation and law
  - Coordinated action being taken on nuisance calls by Ofcom and ICO, and a UK Government Action Plan was announced by DCMS in March, 2014
  - We are restricted to our regulatory remit so law enforcement have to take the lead in the case of fraud but we are liaising with them and the anti-fraud organisations

- The problem is international in scope, both in terms of impact and sources of problem traffic – cooperation with US FTC/FCC, Canadian CRTC, Australian and Indian authorities is already in place

- We asked NICC to aid our regulatory actions through the agreement of cross industry processes and revised CLI technical guidelines

The ease of CLI spoofing is inherent in IP telephony, now ubiquitous in businesses and CPs

- The problem is due to the transition from traditional Time Division Multiplexing (TDM) and Signalling System 7 (SS7) to all-IP-based technologies such as the Session Initiation Protocol (SIP) and the IP Multimedia System (IMS)
  - In addition, liberalisation and de-regulatory initiatives have encouraged many new entrants into the voice marketplace

- This evolution has benefitted consumers, but also undermined the “Circle of Trust” among the small group of providers of traditional voice communications

- In the world of the PSTN, CLI was implicitly linked to the physical topology of the switched network and controlled by the CP so could be “trusted”

- VoIP includes the source address of each packet, and a “From” CLI but it provides no validation of this, since it is carried as plain text and can be set as any value by the user, if using appropriate CPE or application software

- As the Internet Architecture Board (IAB), noted with regard to SIP, “*Without any form of cryptographic identity assertion, the ‘From’ header can be easily forged, and headers are often stripped or modified by intermediaries in transit.*”

Short term mitigation approaches

- **Aim to stop Nuisance Calls at source**

- Requires an agreed call tracing process and appropriate action when the source has been identified – NICC ND1437 delivered, tested and now in BAU use by Ofcom and, shortly, the ICO, with a number of successful outcomes in nuisance calls cases but unlikely to be effective against most fraudsters

- **Use clear regulatory guidelines on CLI to identify calls which are problematic**

- NICC producing revised rules dealing with VoIP and VoIP to SS7 transition (ND1016)

- We have a short term focus on ensuring our CLI Guidelines (ND1016 + Ofcom policy) are fit for purpose in the VoIP age and that CPs police best practice through commercial agreements, potentially allowing the most egregious originators of spoofed CLI nuisance calls traffic to be discouraged.

ND1437 tracing process

Stage 0

Basic data to trace call is assembled

- Ofcom obtains information required for a call trace from the terminating CP, e.g.
  - Time of call, CLI of calling/called parties, presentation number, incoming route id etc

Stage 1

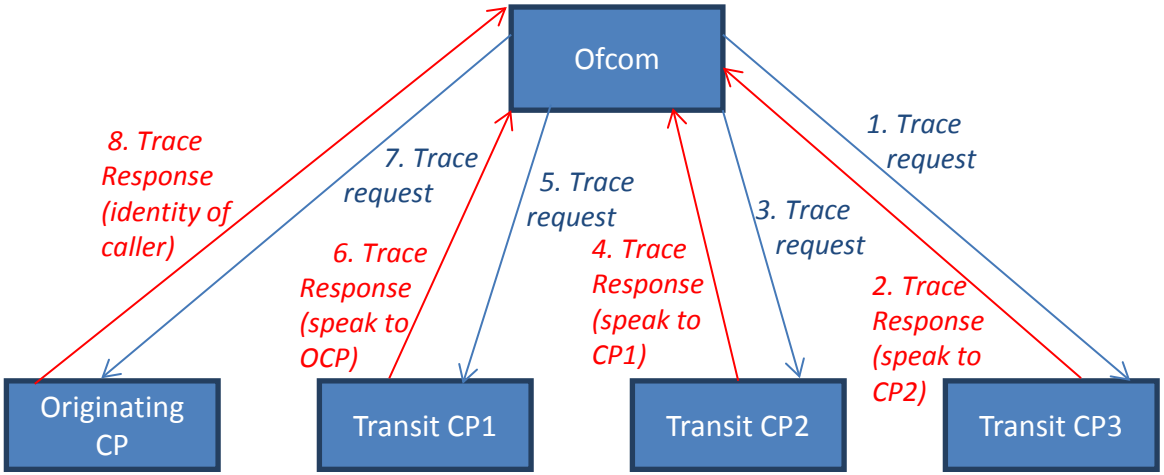
Contact the CP hosting the calling CLI (i.e. the originating CP) for caller information

- If CLI is missing/inaccurate, this step will definitely/probably fail
- Even with valid CLI, it may be international, subcontracted to a reseller, ported out, misallocated – all of which may lead to failure of this step

Stage 2

Trace the call through the upstream networks

- This step occurs if Step 1 fails

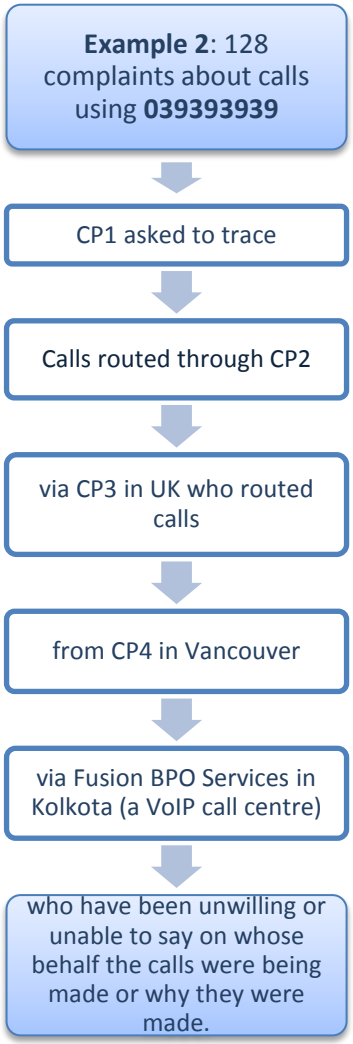


Stage 3

Obtain caller information from originating CP

- If this network CP is also retail CP, then customer identity = caller identity
- If there is a reseller then a further request(s) may be needed to obtain caller identity

A sample trace



ND1016 - Requirements on Communications Providers in relation to Customer Line Identification display services and other related services

- CLI needs to be handled correctly, principally to maintain the protection for two different groups:

- Calling parties – for example if the desire to withhold CLI is asserted this needs to be conveyed across networks and respected on termination
- Called parties – need to see accurate CLI and have the ability to manage calls based on presence or absence of CLI to minimise nuisance calls

- The current focus on nuisance calls has put particular emphasis on the second of these

- The growth of SIP has made it increasingly straightforward for callers to spoof their CLI
- The standards adopted for CLI by overseas callers and/or CPs may not match our own
- SIP also creates interworking challenges with ISUP/IUP in maintaining accurate CLI and CLI markings across networks

- The work of updating ND1016 has proven complex. Ofcom would like the thank NICC members for their positive engagement with this difficult work. This is an important element of the ongoing effort to reduce the harm of nuisance calls.

Other consumer protection options

- **Call screening** may have some value but “black list” approaches may have limited relevance given the ease of changing the spoofed CLI being used. This is the main some CPs are resistant to the approach adopted by TalkTalk who have implemented a network wide “black list”

- “White list” based approaches are available, both as CPE and as network overlay/adjunct systems – **TrueCall** are the leading vendor for the former (although they have licenced their IPR to BT for an own brand device that is selling fast) and have recently demonstrated a “carrier class” adjunct that could in principle be implemented on even legacy networks

- We are exploring this type of approach via the Industry Working Group to identify costs and practicalities – because of altered routing and OSS/BSS issues, CPs would have to make potentially major investments to enable availability to any significant proportion of their customer base

- We also need to understand the policy implications of moving to an environment where not answering unsolicited voice calls becomes the norm

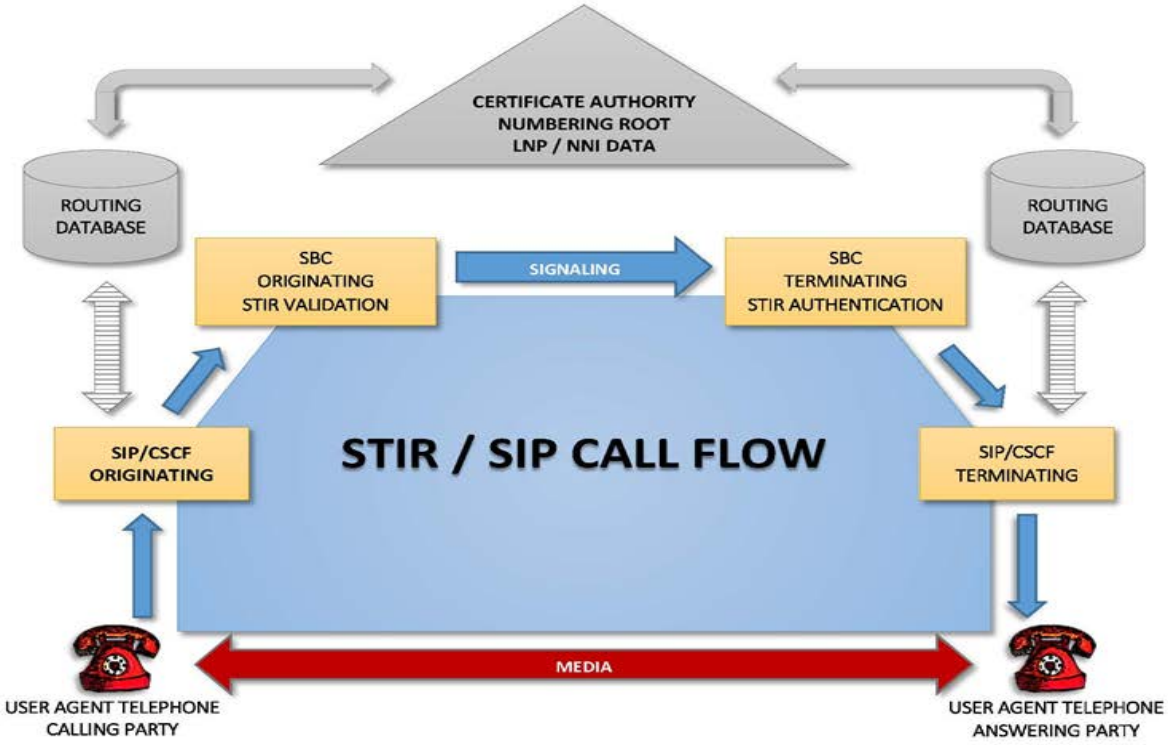
Technical standards are being developed to verify CLIs but implementation will be protracted

- Whilst greater regulatory clarity over acceptable practice and effective regulatory and law enforcement will help, a more systemic means of providing **caller identity assurance** is needed

- This problem is international in scope and requires international resolution on a technical level – key leadership being given by US FCC CTO, Henning Schulzrinne, one of the original authors of SIP

- The IETF is the international body responsible for standardising SIP telephony
  - Its STIR Working Group has been seeking to apply existing internet *authentication/authorisation* principles to phone numbers
  - This is possible because the assignment of E.164 phone numbers by national authorities is hierarchical, thus somewhat similar to assignment of IP addresses by regional or national bodies

Securing VoIP: STIR and RPKI in practice



CSCF = Call Session Control Function | SBC = Session Border Control

STIR builds on existing work but is complex

- Verification lends itself to end-to-end solutions:
  - On an end-to-end basis, *authentication* (providing assurance that the source of a communication is as claimed) and the closely related problem of *authorisation* (providing assurance that the party seeking services is entitled to them) are routinely verified using public key cryptographic techniques

- The IETF has turned to such public key technology (more specifically RPKI) already in use in other areas for potential solutions to ensuring verification for VoIP voice calls
  - The early work centres on a major rewrite of "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474

- STIR is a 'Work in Progress' and at a very early stage
  - It may be **18 to 24 months before technical standards work is complete** and **up to a further 3 years for actual implementation in major CP networks**

We may be able to implement a national solution that could deliver real benefits

- If Ofcom were successful in getting most or all UK network operators, including VoIP operators, on board with a validation scheme, it might be possible to validate at least UK numbers with moderate confidence
  - Off-shore operators could still falsify the Caller ID, but might have difficulty falsifying a UK Caller ID without detection
  - For consumers, this would at least limit the scale of the problem

- A UK-only solution might have substantial effect if supported not only by networks but also by consumer education and perhaps by intelligent handset or network screening software

- Conversely contractual mechanisms could be used to enforce a more prescriptive regulatory position on trusted CLI
  - Failure to use STIR based authentication or provide equivalent assurance could lead to refusal to carry traffic or termination of interconnect

- Ofcom could encourage support for a collaborative industry approach on adoption, but may need to consider intervention if progress is slow – **we will need to assess feasibility when standards work is more complete – mid 2015 for a possible start but could take 3 years+ for implementation**.

- Clearly, NICC and its members will have a key role in this process and we would welcome your support