Caller ID spoofing

From Wikipedia, the free encyclopedia

Caller ID spoofing is the practice of causing the telephone network to indicate to the receiver of a call that the originator of the call is a station other than the true originating station. For example, a Caller ID display might display a phone number different from that of the telephone from which the call was placed. The term is commonly used to describe situations in which the motivation is considered malicious by the speaker or writer.

Example of Caller ID spoofed via orange boxing, both the name and number are faked to reference "leetspeak".

Contents

- 1 History
- 2 Technology and methods
  - 2.1 Voice over IP
  - 2.2 Service providers
  - 2.3 Orange box
- 3 Caller name display
- 4 Legal considerations
  - 4.1 India
  - 4.2 United Kingdom
  - 4.3 United States
- 5 References
- 6 Further reading

History

Caller ID spoofing has been available for years to people with a specialized digital connection to the telephone company, called an ISDN PRI circuit. Collection agencies, law-enforcement officials, and private investigators have used the practice, with varying degrees of legality.

The first mainstream Caller ID spoofing service, Star38.com, was launched in September 2004. Star38.com was the first service to allow spoofed calls to be placed from a web interface. It stopped offering service in 2005, as a handful of similar sites were launched.

In August 2006, Paris Hilton was accused of using caller ID spoofing to break into a voicemail system that used caller ID for authentication.[1] Caller ID spoofing also has been used in purchase scams on web sites such as Craigslist and eBay. The scamming caller claims to be calling from Canada into the U.S. with a legitimate interest in purchasing advertised items. Often the sellers are asked for personal information such as a copy of a registration title, etc., before the (scamming) purchaser invests the time and effort to come see the for-sale items. In the 2010 election, fake caller IDs of ambulance companies and hospitals were used in Missouri to get potential voters to answer the phone.[2] In 2009, a vindictive Brooklyn wife spoofed the doctor's office of her husband's lover in an attempt to trick the other woman into taking medication which would make her miscarry.[3]

Frequently, caller ID spoofing is used for prank calls. For example, someone might call a friend and arrange for "The White House" to appear on the recipient's caller display. In December 2007, a hacker used a Caller ID spoofing service and was arrested for sending a SWAT team to a house of an unsuspecting victim.[4] In February 2008, a Collegeville, Pennsylvania man was arrested for making threatening phone calls to women and having their home numbers appear "on their caller ID to make it look like the call was coming from inside the house."[5][6]

In March 2008, several residents in Wilmington, Delaware reported receiving telemarketing calls during the early morning hours, when the caller had apparently spoofed the Caller ID to evoke the 1982 Tommy Tutone song "867-5309/Jenny."[7] By 2014, an increase in illegal telemarketers displaying the victim's own number, either verbatim or with a few digits randomised, was observed as an attempt to evade caller ID-based blacklists.[8]

In the Canadian federal election of May 2, 2011, both live calls and robocalls are alleged to have been placed with false caller ID, either to replace the caller's identity with that of a fictitious person (Pierre Poutine of Joliette, Quebec)[9] or to disguise calls from an Ohio call centre as Peterborough, Ontario domestic calls. See Robocall scandal.

In June 2012, a search on Google returned nearly 50,000 consumer complaints by individuals receiving multiple continuing spoofed Voice Over IP (VoIP) calls on lines leased / originating from "Pacific Telecom Communications Group" located in Los Angeles, CA (in a mailbox store), in apparent violation of the FCC. Companies such as these lease out thousands of phone numbers to anonymous voice-mail providers who, in combination with dubious companies like "Phone Broadcast Club" (who do the actual spoofing), allow phone spam to become an increasingly widespread and pervasive problem. In 2013, the misleading caller name "Teachers Phone" was reported on a large quantity of robocalls advertising credit card services as a ruse to trick students' families into answering the unwanted calls in the mistaken belief they were from local schools.[10]

On January 7, 2013, the Internet Crime Complaint Center issued a Scam Alert for various telephony denial of service attacks by which fraudsters were using spoofed caller ID to impersonate police in an attempt to collect bogus payday loans, then placing repeated harassing calls to police with the victim's number displayed.[11] While

impersonation of police is common,[12][13] other scams involved impersonating utility companies to threaten businesses or householders with disconnection[14] as a means to extort money,[15] impersonating immigration officials[16] or impersonating medical insurers to obtain personal data for use in theft of identity.[17] Bogus caller ID has also been used in grandparent scams which target the elderly by impersonating family members and requesting wire transfer of money.[18]

Technology and methods

Caller ID is spoofed through a variety of methods and different technology. The most popular ways of spoofing Caller ID are through the use of VoIP or PRI lines.

Voice over IP

In the past, Caller ID spoofing required an advanced knowledge of telephony equipment that could be quite expensive. However, with open source software (such as Asterisk or FreeSWITCH, and almost any VoIP company), one can spoof calls with minimal costs and effort.

Some VoIP providers allow the user to configure their displayed number as part of the configuration page on the provider's web interface. No additional software is required. If the caller name is sent with the call (instead of being generated from the number by a database lookup at destination) it may be configured as part of the settings on a client-owned analog telephone adapter or SIP phone. The level of flexibility is provider-dependent. A provider which allows users to bring their own device and unbundles service so that direct inward dial numbers may be purchased separately from outbound calling minutes will be more flexible. A carrier which doesn't follow established hardware standards (such as Skype) or locks subscribers out of configuration settings on hardware which the subscriber owns outright (such as Vonage) is more restrictive. Providers which market "wholesale VoIP" are typically intended to allow any displayed number to be sent, as resellers will want their end user's numbers to appear.

In a rare few cases, a destination number served by voice-over-IP is reachable directly at a known SIP address (which may be published through ENUM telephone number mapping, a .tel DNS record or located using an intermediary such as SIP Broker). Some Google Voice users are directly reachable by SIP, as are all iNum Initiative numbers in country codes +883 5100 and +888. As a Federated VoIP scheme provides a direct Internet connection which does not pass through a signaling gateway to the public switched telephone network, it shares the advantages (nearly free unlimited access worldwide) and disadvantages (ernet applications.)

Service providers

Some spoofing services work similarly to a prepaid calling card. Customers pay in advance for a personal identification number (PIN). Customers dial the number given to them by the company, their PIN, the destination number and the number they wish to appear as the Caller ID. The call is bridged or transferred and arrives with the spoofed number chosen by the caller—thus tricking the called party.

Many providers also provide a Web-based interface or a mobile application where a user creates an account, logs in and supplies a source number, destination number and the bogus caller ID information to be displayed. The server then places a call to each of the two endpoint numbers and bridges the calls together.

Some providers offer the ability to record calls, change the voice and send text messages.[19]

Orange box

Another method of spoofing is that of emulating the Bell 202 FSK signal. This method, informally called orange boxing, uses software that generates the audio signal which is then coupled to the telephone line during the call. The object is to deceive the called party into thinking that there is an incoming call waiting call from the spoofed number, when in fact there is no new incoming call. This technique often also involves an accomplice who may provide a secondary voice to complete the illusion of a call-waiting call. Because the orange box cannot truly spoof an incoming caller ID prior to answering and relies to a certain extent on the guile of the caller, it is considered as much a social engineering technique as a technical hack.

Other methods include switch access to the Signaling System 7 network and social engineering telephone company operators, who place calls for you from the desired phone number.

Caller name display

Telephone exchange equipment manufacturers vary in their handling of caller name display. Much of the equipment manufactured for Bell System companies in the United States sends only the caller's number to the distant exchange; that switch must then use a database lookup to find the name to display with the calling number. Canadian landline exchanges often run Nortel equipment which sends the name along with the number. Mobile, CLEC, Internet or independent exchanges also vary in their handling of caller name, depending on the switching equipment manufacturer. Calls between numbers in differing country codes represent a further complication, as Caller ID often displays the local portion of the calling number without indicating a country of origin or in a format that can be mistaken for a domestic or invalid number.

This results in multiple possible outcomes:

- The name provided by the caller (in the analog telephone adapter configuration screen for voice-over-IP users or on the web interface on a spoofing provider) is blindly passed verbatim to the called party and may be spoofed at will
- The name is generated from a telephone company database using the spoofed Caller ID number.
- A destination provider may display no name or just the geographic location of the provided telephone area code on caller ID (*e.g.*, "ARIZONA", "CALIFORNIA", "OREGON", or "ONTARIO"). This often occurs where the destination carrier is a low-cost service (such as a VoIP provider) running no database or outdated data in which the number is not found.
- If the displayed number is in the recipient's address book, some handsets will display the name from the local address book in place of the transmitted name. Some VoIP providers use Asterisk (PBX) to provide similar functionality at the server;[20] this may lead to multiple substitutions with priority going to the

destination user's own handset as the last link in the CNAM chain.

Legal considerations

India

According to a report from the India Department of Telecommunications, the Government of India has taken following steps against the CLI spoofing Service Providers:

- Websites offering caller-ID spoofing services are blocked in India as an immediate measure.
- ILDOs, NLDOs and Access Service Providers have been alerted to the existence of such spoofing services, and shall collectively be prepared to take action to investigate cases of caller-ID spoofing as they are reported.[21]

As per DOT, Using spoofed call service is illegal as per Indian Telegraph Act, Sec 25(c). Using such service may lead to fine or 3 years imprisonment or both

United Kingdom

In the U.K., the spoofed number is called the "presentation number". This must be either allocated to the caller, or if allocated to a third party, it is only to be used with the third party's explicit permission.[22]

United States

Caller ID spoofing is generally illegal in the United States if done "with the intent to defraud, cause harm, or wrongfully obtain anything of value". The relevant federal statute, the Truth in Caller ID Act of 2009, does make exceptions for certain law-enforcement purposes. Callers are also still allowed to preserve their anonymity by choosing to block all outgoing caller ID information on their phone lines.

A detailed discussion of the legislative process that gave rise to the applicable law now follows.

On April 6, 2006, Congressmen Eliot Engel (D-N.Y.) and Joe Barton (R-Tex.) introduced H.R. 5126, a bill that would have made caller ID spoofing a crime. Dubbed the "Truth in Caller ID Act of 2007", the bill would have outlawed causing "any caller identification service to transmit misleading or inaccurate caller identification information" via "any telecommunications service or IP-enabled voice service." Law enforcement was exempted from the rule. Three weeks later, an identical bill was introduced in the Senate.[23] On June 6, 2006, the House of Representatives passed the Truth in Caller ID Act, although no Senate action was taken on either the House or Senate bill. At the end of the 109th Congress, the bill expired (all pending legislation not voted into law at the end of the House term, a.k.a. end of a session of Congress, is dead).

On January 5, 2007, Congressman Engel introduced H.R. 251, and Senator Bill Nelson (D-Fla.) introduced a similar bill (S.704) two months later. On June 27, 2007, the United States Senate Committee on Commerce, Science and Transportation approved and submitted to the Senate calendar S.704, a bill that would have made caller ID spoofing a crime. Dubbed the "Truth in Caller ID Act of 2007", the bill would have outlawed

causing "any caller identification service to transmit misleading or inaccurate caller identification information" via "any telecommunications service or IP-enabled voice service." Law enforcement was exempted from the rule. Engel's bill passed in the House of Representatives. Nelson's bill was referred to the same Senate committee that approved S.704.[24][25] The Senate again passed neither version of the legislation.[26]

In the 111th Congress, Congressman Engel and Senator Nelson once again introduced similar versions of the Caller ID legislation, H.R. 1258. The bill was reintroduced in the Senate on January 7, 2009, as S.30, the Truth in Caller ID Act of 2009, and referred to the same committee.[27] The Senate and the House both passed their respective versions of the legislation, but on December 15, 2010 the House passed S.30 and sent the legislation to the President for a signature. On December 22, 2010, President Obama signed the bill into law.[28]

Under the act, which also targets VOIP services, it is illegal "to cause any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value...." Forfeiture penalties or criminal fines of up to $10,000 per violation (not to exceed $1,000,000) could be imposed.[19] The law maintains an exemption for blocking one's own outgoing caller ID information, and law enforcement isn't affected.[29][30]

The New York Times sent the number 111-111-1111 for all calls made from its offices until 15 August 2011. The fake number was intended to prevent the extensions of its reporters appearing in call logs, and thus protect reporters from having to divulge calls made to anonymous sources. The *Times* abandoned this practice because of the proposed changes to the caller ID law, and because many companies were blocking calls from the well-known number.[31]

References

1. Robert McMillan (25 August 2006). "Paris Hilton accused of voice-mail hacking". *InfoWorld*. Retrieved 14 June 2015.
2. Kansas City Star, "Fake called IDs used in Missouri elections" David A. Lieb, Associated Press. Sun. Nov. 14, 2010.
3. "Enraged Brooklyn wife Kisha Jones stole doc's Rx pad to prescribe drug to abort baby of hubby's lover". *Daily News* (New York).
4. Hacking caller id systems on the rise - FOX16.com (http://www.fox16.com/news/local/story.aspx?content_id=d7b03762-7dd1-41e9-8d9d-2ff1f8754b18&rss=315)
5. KYW Newsradio 1060 Philadelphia - Man Pleads Guilty to Making Scary Phone Calls (http://www.kyw1060.com/Man-Pleads-Guilty-to-Making-Scary-Phone-Calls/1614501) (link rot)
6. "Dodge SRT Forum". Retrieved 14 June 2015.
7. *Telemarketer's Call Invokes Old Hit Song* (http://news.technology.findlaw.com/ap/o/1110//03-11-2008/20080311073507_23.html), (Associated Press, March 11, 2008)
8. "The Caller ID Scam You Must Know About". *The Fiscal Times*. Retrieved 14 June 2015.
9. Payton, Laura (February 28, 2012). "Robocalls phone number registered to 'Pierre Poutine'". *CBC News*. Retrieved March 11, 2012.
10. "Robocallers Impersonate Teachers On Caller ID, Scare Parents". *Consumerist*. Retrieved 14 June 2015.
11. http://www.ic3.gov/media/2013/130107.aspx
12. Carmen Duarte Arizona Daily Star. "Pima County Sheriff's detectives alert public about scam". *Arizona Daily Star*. Retrieved 14 June 2015.
13. "Authorities Warn About Scam Artists Posing As Law Enforcement Officers In Camden

County". Retrieved 14 June 2015.
14. "FTC asked to probe fraudulent calls to restaurants".
15. Nick Sloan. "Kansas City Kansan: BPU warns customers of phone-scam". Retrieved 14 June 2015.
16. "Beware: widespread immigration-related fraud schemes currently on the rise!". Retrieved 14 June 2015.
17. "Scammers busy under guise of Obamacare". *CBS News*.
18. "Fort Stockton resident latest victim of Grandparent Scam". *The Fort Stockton Pioneer*. Retrieved 14 June 2015.
19. http://www.nysba.org/AM/Template.cfm?Section=Home&CONTENTID=46713&TEMPLATE=/CM/HTMLDisplay.cfm#_ftn2 "Don't Believe Your Eyes: Spoofing"
20. http://wiki.voip.ms/article/Phone_book
21. Harish Kumar Gangwar,ITS. "Call Spoofing Services , Modus Operandi ,Regulatory framework and impact on society".
22. Director General of Telecommunications (11 December 2003, amended 26 April 2007). "Guidelines for the provision of Calling Line Identification Facilities and other related services over Electronic Communications Networks Version 2". ofcom. Retrieved 2012-01-09. Check date values in: `|date=` (help)
23. "Truth in Caller ID Act of 2006 (2006; 109th Congress H.R. 5126) - GovTrack.us". *GovTrack.us*. Retrieved 14 June 2015.
24. Senate Bill *S.704*. Retrieved from http://thomas.loc.gov/cgi-bin/bdquery/z?d110:s.00704:.
25. House Bill *HR251*. Retrieved from http://thomas.loc.gov/cgi-bin/bdquery/z?d110:HR251:.
26. "Truth in Caller ID Act of 2007 (2007; 110th Congress S. 704) - GovTrack.us". *GovTrack.us*. Retrieved 14 June 2015.
27. "Truth in Caller ID Act of 2010 (2010; 111th Congress H.R. 1258) - GovTrack.us". *GovTrack.us*. Retrieved 14 June 2015.
28. "Truth in Caller ID Act of 2009 (2010; 111th Congress S. 30) - GovTrack.us". *GovTrack.us*. Retrieved 14 June 2015.
29. "Congress outlaws all Caller ID spoofing (VoIP too)". *Ars Technica*. Retrieved 14 June 2015.
30. "Caller ID and Spoofing". Retrieved 14 June 2015.
31. Peters, Jeremy W. (12 August 2011). "At The Times, Era of '111-111-1111' Nears Its End". *The New York Times (Media Decoder* blog*)*. Retrieved August 12, 2011.

Further reading

- BBC News (http://news.bbc.co.uk/2/hi/technology/4482139.stm)
- California State Senate Bill SJR15-Florez (http://info.sen.ca.gov/pub/07-08/bill/sen/sb_0001-0050/sjr_15_bill_20070725_introduced.html)
- October 29, 2004 *Washington Post* article (http://www.washingtonpost.com/wp-dyn/articles/A10597-2004Oct29.html)
- *Wired* news report of FCC investigation (http://www.wired.com/news/technology/0,70320-0.html)
- Arstechnica: Congress outlaws all Caller ID spoofing (VoIP too) (http://arstechnica.com/tech-policy/news/2010/04/congress-outlaws-all-caller-id-spoofing-voip-too.ars)
- Largest Caller ID Spoofing Tool (http://www.spoofcard.com)
- How to Unmask Spoofed & No Caller ID Calls (http://www.trapcall.com/blog/no-caller-id-how-to-unmask-hidden-calls-on-iphone/)

Categories: Deception | Caller ID
