Critical analysis on the concept of Cyber Phreaking as a Cyber Crime in the Cyber World-A Glimpse

Dr.J.Star
M.L., Ph.D., Assistant Professor of Law, CDAGLC, Thiruvallur

Abstract: Phreaking is a routine word for breaking into a secure telecommunications network without the proper authorization. The word "phreaking" was first coined that, it referred to the act of investigating and manipulating phone networks by simulating calling tones in order to activate automated switches with whistles or special blue boxes created specifically for that purpose. Phreaks were often motivated by a desire to learn more about how phone networks worked rather than a goal to cheat telecommunications providers, according to most phone contact accounts. With the proliferation of mobile networks and the need to breach them via more blatantly illicit means, the term "phreaking" has come to be synonymous with "hacking". In India the legal provisions related to hacking/ phreaking is covered under IT Act and Indian Penal Code. The main objective of this paper is to explain the phreaking as a cybercrime. This study also focussed through a light on theoretical framework on phreaking, and the legislations in India also what are the measures are needful to prevent the crime.

INTRODUCTION

The term *phreak* comes from a combination of the words *phone*, *free*, and *freak*. Phone-freaks, or Phreaks as they were known in the 1970s, were an identifiable sub culture. Phreaks maintained a social network akin to that of ham radio enthusiasts with low-tech hacks like the plastic whistle from Captain Crunch boxes and the do-it-yourself blue boxes. To continue phreaking, more clear borders have to be crossed because of the increasing complexity of network security. Switch-hooking was maybe one of the earliest phreaking techniques employed. It enables calls to be made from a phone that has had its rotary dial or keypad removed. To mimic the rotary dial's pulses, a switch hook is quickly depressed and released to open and shut the circuit. For many years, phreakers were seen as 'hackers of the cellular telephone network', engaged in such activities as 'bluehacks', 'network mimicry', and 'bluecloning'.

Phreaking -meaning

It is the practise of breaking into a telecommunications system in order to make free calls or contact high-cost lines. In order to make long-distance or high-cost calls using your phone lines, you must unlawfully hack a telephone network. Firms with extended periods of absence, such as schools, would be most affected; nevertheless, all businesses face some risk over weekends or long periods of absence, such as bank holidays[1]. The most significant effect on a firm is the expense; once a phone line is hacked, it may be utilised to make a series of high-priced calls. A few days worth of long-distance phone calls may cost a corporation thousands of dollars. You have no legal recourse after the calls have been made, therefore you are responsible for the costs, no matter how high they are. In many circumstances, bankruptcy may have a severe consequence[2]. VoIP phone lines, which are powered by computers, are the most vulnerable to "phreaking" or telephone hacking. VoIP allows users to relocate or transfer their phone lines, reduce their call expenses, and so on, but they also come with the risk of having their personal information stolen from an online account[3]. The account is hacked, authenticated, and then used to make a series of long-distance telephone calls.

1Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Wolfe, S. E. (2014). Hacking in high school: Cybercrime perpetration by juveniles. Deviant Behavior, 35(7), 581-591.

2Crosston, M. (2014). Phreak the speak: the flawed communications within cyber intelligentsia. In Cyberspace and International Relations (pp. 253-267). Springer, Berlin, Heidelberg.

3Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society. Sage.

Historical Background of the study

Phone phreaking began in the late 1950s in the US. Late 1960s and early 1970s were its peak. People who were interested in phreaks spent a lot of time dialling around the phone network, figuring out how calls were routed,[4] reading obscure telephone company technical journals, learning how to impersonate operators and other telephone company personnel, digging through trash bins to find 'secret' documents, sneaking into telephone company buildings at night, and so on[5]. Prior to 1984, long-distance phone calls were expensive and regulated. Calling across the street was considerable distance in certain places[6]. The fact that a phone call was long-distance has extra weight since the caller pays by the minute. Phreaking is a method of avoiding long-range charges. This is termed 'toll fraud'[7]. The pager cloning method was employed by law enforcement in 1990[8].

Position in UK

The situation was much different in the UK owing to the lack of tone dialling and signalling, especially in the 1950s and 1960s. The tone system has been nearly fully superseded in the US, although it still exists in certain nations, such as Italy. It's possible that switch-hooking was the first phreaking technique. It permits making calls from phones that have had their rotary dial or keypad disabled. Simulating the rotary dial's pulses by quickly pushing and releasing the switch hook opens and closes the subscriber circuit. Even modern telephone exchanges use this strategy to handle older subscriber gear. The caller may dial numbers by clicking the hook repeatedly between 5 and 10 times per second, separated by around one second intervals. The exchange's pulse counter counts pulses or clicks and interprets them in two ways. To calculate the number of clicks before an interval, divide the number of clicks by the continent and nation. Ten consecutive clicks are therefore "zero" or "nine". Some exchanges offer[9] extra clicks for specific controls, but 0-9 now fall into one of two categories. It's conceivable but difficult to reproduce the "flash" code.

Rotary Dial Era

During the rotary dial era, almost identical phone sets were sold all over the globe, with the exception of country-specific plugs and dials. An DTMF tone dialer can employ key-locked telephones to create the DTMF tones used by current keypad devices. These signals are now globally standardised. Even if the exchange does not support DTMF, the key lock may be bypassed via switch-hooking, allowing the tone dialer to run automated DTMF controlled services that cannot be utilised with rotary dial. The approaches employed in the UK were different since the post office network (excluding Kingston upon Hull) relied on Strowger switches. Due to the way the exchange functioned, tone signalling was useless. The methods depended on peculiarities in the exchange wiring or technical facilities. Typical 1950s-1970s gimmicks included: By calling 9-1-10 from the caller's phone and touching the phone rest to add an additional pulse, irregular subscriber trunk dialling (STD) access may be gained. It was sometimes possible to discover a nearby local exchange that allowed free STD connection by dialling the local code + 0. The post office phone might be modified with a diode and a push button. This enabled one to receive a call yet not charge the calling party. The disadvantage was that the system only let the caller five or six minutes before terminating it. It was also wise to phone the receiver beforehand to make sure he was anticipating the call.

Role of unused number

The most common of them was the usage of an unused number. It would return a "number unobtainable" tone for a few seconds before clearing and allowing STD access. Also, technicians had to be aware of the Post

4Smith, A. R., & Hurley, D. L. (1992). A photon phreak digs the LDEF happening.

5Hakim, M., Jais, J., Azlan, Y., & Zuraidah, S. Phreakers in Higher Learning Institution in Malaysia: A Comparative Study on Harmful Phreaking v. Harmless Phreaking.

6Harry, M. (1985). The Computer Underground: Computer Hacking, Crashing, Pirating, and Phreaking. Loompanics Unlimited.

7Donn B. Parker, Fighting Computer Crime (Charles Scribner's Sons, New York, New York, 1983).

8Brenner, S. W. (2007). History of computer crime. In The history of information security (pp. 705-721). Elsevier Science BV.

9Schwartau, W. (2000). Cybershock: Surviving hackers, phreakers, identity thieves, internet terrorists, and weapons of mass disruption (p. 470). New York: Thunder's Mouth Press.

Office Special Investigation Branch. Phone phreaking began with AT&T's introduction of completely automated switches. These switches utilised tone dialling, an in-band signalling method, with certain tones reserved for internal use only. 2600 Hz internal-use tone triggers telephone switch to assume conversation has finished, leaving open carrier line for free long-distance and international calls. Long-distance calls were more costly back then. Blind seven-year-old Joe Engressia discovered the tone in 1957. stopped Engressia's phoned phone recording. Engressia phoned the phone provider, asking why the recordings had ceased. Joe Engressia is the phreaking father. Other early phreaks, including "Bill from New York", started to grasp the basics of phone network operation. Bill learned that a recorder he possessed could produce the same effect at 2600 Hz. By blowing on the complimentary whistles in Cap'n Crunch cereal boxes, John Draper detected a 2600 Hz tone (providing his nickname, "Captain Crunch"). This provides control of single frequency (SF) phone networks. It takes a lengthy whistle to reset the line, then a series of whistles.

Use of Phone line controller

While single-frequency operated on certain phone lines, multi-frequency (MF) controllers were the most popular. "Marty Freeman" was the colloquial name for these tones. Before 1954, the public was unaware of the requisite frequencies until the Bell System released an article in the Bell System Technical Journal outlining the processes and frequencies utilised for inter-office signalling. In October 1971, Ron Rosenbaum's piece "Secrets of the Little Blue Box" appeared in Esquire magazine[10]. This piece heavily highlighted Engressia and John Draper, phreaking their names. With the publication of the controversial "Regulating the Phone Company in Your Home" in June 1972, phreaking gained popularity. This article publishes basic schematic drawings for a "black box" used to make free long-distance phone calls, along with a components list. But not before several copies were sold and many regular subscribers got them.

Notion of Toll fraud

The notion of toll fraud became highly frowned upon among professional phreakers when the website Phone Trips was created by second generation phreakers Mark Bernay and Evan. These little phone businesses had no method of identifying the hackers[11]. They did not have access to local phone company records of calls made to their access lines, and getting such data would be costly and time consuming. While significant progress was made in the early 1990s, the issue did not go away until most long-distance operators could offer basic 1+ dialling without an access number. Diverters are another way to get free phone calls. Many company phone lines did not have call forwarding capabilities in the late 1980s and early 1990s, forcing them to purchase manual call forwarding equipment. When the company closed, they would pick up another phone line, contact their answering service, and bridge the two lines together. The caller was led to believe they were immediately connected to the company's answering service[12]. So, once the answering service terminated, the caller could simply wait until the second line had a useful dial tone. Phreakers took advantage of this by manually phoning establishments after hours to find malfunctioning diverters.

Role of phreaker

A phreaker might employ one of these lines for a variety of reasons. They might use the phone line to harass their adversaries and make international calls at the cost of the companies. They had to pay for long-distance calls since their own equipment, not phone company security weaknesses, permitted such fraud to occur. This was outdated by 1993, when almost every business line subscriber had call forwarding. So hackers stopped looking for the last handful, and this technique of toll fraud ended. Many (various sorts) of diverters still exist and are actively "phreaked" in the United States as of 2020. Pre-BBS phone phreaking was more of an individual endeavour due to the

10Rosenbaum, R. (1971). Secrets of the little blue box. Esquire Magazine, 76, 117-125.

11Ross, A. (1990). Hacking away at the counterculture. Postmodern Culture, 1(1).

12Alexander, J. C. (2018). The societalization of social problems: Church pedophilia, phone hacking, and the financial crisis. American Sociological Review, 83(6), 1049-1078.

difficulty of connecting with other phreaks[13]. Aside from BBSs, phone phreaks use voice mail boxes and party lines to network and stay in contact. They frequently take over disused commercial or cell phone boxes. When a phreak community discovers a susceptible mailbox system, they flock to it in droves[14]. They utilise these systems to communicate until the rightful owners detect the incursion and wipe them out. Because home phone numbers and personal mobile phone numbers may be traced back to the phreak's name (and address), voice mailboxes also act as a safe phone number[15]. This is crucial because phone phreaks contravene the law.

Commission of phreaking

Phreakers utilise "bridges" to converse live. Initial definition: A set of telephone company test lines linked together to provide the illusion of a party-line. Party-lines became bridges if they were mostly frequented by hackers and/or phreakers. The Internet's growth in the mid-1990s, together with increased awareness of voice mail by company and mobile phone users, made voice mailbox theft less common[16]. Even while bridges are still popular among phreakers, the usage of telephone company-owned bridges has dwindled in favour of phreaker-owned conferences. By the late 1990s, phreaking had lost its fraudulent character. There were flat-rate long-distance plans giving unlimited home phone long-distance for as low as $25 per month in the United States. Rates for international calls have also fallen. Because of the increased danger of getting detected and the reduced benefit of free phone calls, toll fraud has become a notion less connected with phreaking. On June 15, 2006, the final exchange in the continental United States to employ a "phreakable" MF-signalled trunk replaced the aged (but still well preserved) N2 carrier with a T1 carrier. Northern Telephone Company of Minnesota operated this exchange in Wawina Township, Minnesota. Recent examples of phreaking include VOIP PBX hacking[17]. In 2011, the Philippines and the FBI arrested four hackers for PBX hacking[18]. In 2015, Pakistani authorities apprehended a notorious hacker who had collected over $50 million via PBX hacking.

Legal provisions for hacking in India

In India, Theft of data and hacking are both criminal and civil violations under the Information Technology Act, 2000. For an offence to be considered hacking, as defined by Section 66 of the IT Act: The accused must have a harmful intent to tamper with or breach into the computer of the other person and steal or damage its data or sources. For an act to be considered illegal, it needs a nefarious motive. It's vital to note that Section 379 of the Indian Penal Code,1860, which deals with "theft" of moveable goods, also covers "theft" of data, whether it's online or off. A person may be charged with theft under Section 379 of the Indian Penal Code (IPC) if he or she removes or steals information from the authorised user's possession. If a theft is conducted in accordance with the IPC's definition of theft, the crime will also be punished.

Law of Torts

There is also the possibility that other laws of torts, such as those governing trespass to the person and property may be used, as the computer system is an intangible property that has been violated. As a result, any unauthorised access to computer sources motivated by malice may be seen as criminal trespass, putting the perpetrator at risk of civil responsibility as well. Section 66 of the Information and Technology Act states that a fine of up to 2 lakh rupees or imprisonment for up to three years may be imposed, or both. According to Section 43, damages have to be paid to the individual who was harmed as a result of the theft of the data. Section 66B imposes a penalty on anybody who receives stolen data or computer resources. A year in jail or a fine of one lakh rupees, or both, may be imposed as punishment. It is possible to be sentenced to up to three years in jail for stealing under Section 379 of the Indian Penal Code.

13Jain, A. (2005). Cyber Crime: Cyber crime: issues and threats. Gyan Publishing House, Delhi.

14Jorgensen, N. (2022). Contentious expertise: Hacking mobile phones, changing mobile technology. First Monday.

15Jacobs, S. L. (1976). Blue Boxes Spread From Phone Freaks To the Well-Heeled. The Wall Street Journal.

16Brenner, S. W. (2010). Cybercrime: criminal threats from cyberspace. ABC-CLIO.

17Shinder, D. L., & Cross, M. (2008). Scene of the Cybercrime. Elsevier.

18Gold, S. (2011). The rebirth of phreaking. Network security, 2011(6), 15-17.

CONCLUSION

From the begining of 1960s, phreaking was traditionally a challenging process which involved hacking the signal used by a phone network. The dawn of the internet, broadband, VoIP phones and new technology means that Phreaking is now more commonly associated with computer hacking and is simpler and quicker to do. The process of phreaking is relatively simple with the right circumstances, and can be completed in a matter of minutes. This means any business is technically at risk of Phreaking, if they haven't taken the right precautions. The ultimate aim of the hacker is usually free calls, so your risk is increased if your business has long absences, is closed at weekends, has multiple phone lines, or uses part-time staff. Particularly favourable targets are Schools, Universities and colleges, whose long holiday periods reduce the risk of immediate detection, although they are not exclusive targets. Companies may considerably minimise their vulnerability to cybercriminals by working with a vendor that adheres to industry standards for security, putting in place sound procedures, and putting its employees through regular security training. Hence, 'fraud detection' may immediately notify or even stop phone connections if hacking is detected. Otherwise the loss could not be liquidated.