History of Hacking

Part 1: Phone Phreaking

Bruce Nikkel

Published in HISTEC Journal, a publication by the Swiss computer museum Enter (https://enter.ch).

This is part one of a four part series on the history of computer hacking.

The words "hacker" and "hacking" in the context of technology was first used in the Tech Model Railway club at the Massachusetts Institute of Technology (MIT) in the 1950s. A “hack” by students referred to a clever technical or engineering achievement (sometimes in the form of pranks) for the purpose of fun and learning. Early hackers and hacking were not associated with criminal activity.

To begin this series we start with hacking activity on the earliest public global network, the original telephone system. In this article we explore early hackers known as "phone phreaks" or “phreakers” and the technical methods they used. Before home computers or the Internet became popular, a hacking technique called "phone phreaking" was used to exploit weaknesses in the global telephone system. The word "phreak" is an English misspelling of "freak" using the "ph" from the word phone (the switching of "f" with "ph" for hacking is also used today with the word phishing). Phone phreaks learned how telephone networks functioned and manipulated central switching infrastructure by generating tones and pulses. Unlike the hacks from MIT students, phone phreaking was considered criminal activity in many countries where wire fraud laws prevented unauthorized misuse of network systems and bypassing telephone billing to make free calls.

When phone companies started to transition from human switchboard operators to automated dialing and switching systems they needed a way to pass signals from the customer's phone to the telephone switching infrastructure. They also needed signaling protocols between local and international telephone exchanges for long distance dialing. Telephone devices dialed numbers using a sequence of pulses or multi-frequency tones which were interpreted directly by the exchange infrastructure (in-band). Telephone exchanges also used in-band signaling to route calls to other exchanges and internationally. Because the signals were sent in-band over the same channel as the voice audio, the signals could be generated independently by anyone and injected into the system. This vulnerability led to

the growth of the phone phreaking community of hackers who discovered how to produce the sounds needed to control the exchange infrastructure. They did this by manually whistling into the phone lines or building electronic devices to generate the correct frequencies.

Human operators before automated phone switching

Information about phone company infrastructure was usually not public and difficult to find. Some information was published in technical journals (academic or industry). Some information was found by testing and experimenting with the systems (adhoc). One method of finding information was called “trashing” or “dumpster-diving” where hackers searched through the garbage of phone companies looking for printed technical material that was thrown out. Another way to get information was from social engineering, where hackers phoned employees of the phone company and tried to get information verbally. When phone phreaks found new technical information it was shared in the phreaking community.

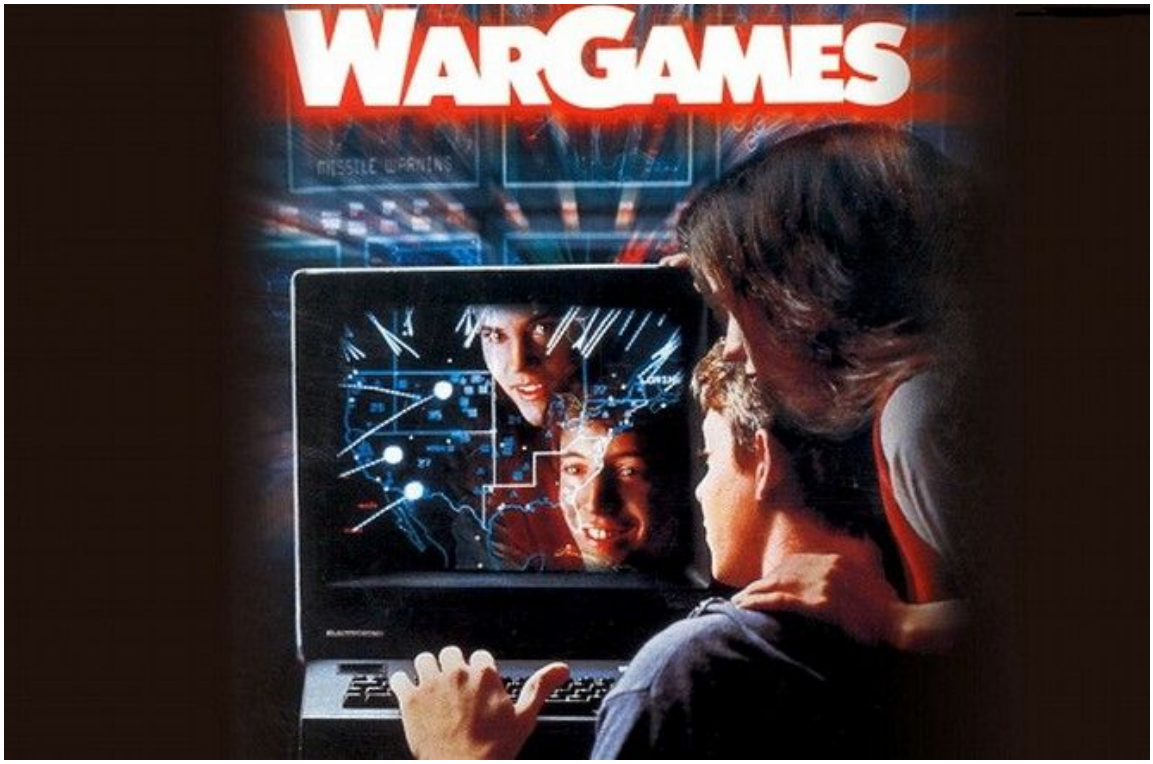
A famous phone phreak called "Captain Crunch" (real name John Draper) discovered the children's toy whistle in the Cap'n Crunch breakfast cereal produced a 2600hz tone. This tone would signal the telephone network's trunk infrastructure to partially drop a connection and accept other tones to control the system. This was used to route calls via any phone exchange in the world and it let phreakers make free long distance calls. Phone phreaking attracted blind hackers because it was not a visual activity, and people with sensitive hearing abilities had a skillful advantage. Phone phreaking mostly involved talking, whistling, and careful listening to frequencies, clicking, and other sounds over the phone.

Cap’n Crunch breakfast cereal with a toy whistle that generates 2600hz

Producing the correct tones needed to manipulate the in-band signaling was a challenge. To solve this problem an electronic device called a "blue box" was used to generate the right sounds (DTMF tones and others) at the push of a button. Before starting Apple Computer, Steve Wozniak and Steve Jobs developed and sold a Blue Box to the phone phreaking community. Other devices were built for generating multi-frequency tones to represent codes for diagnostics and testing. These devices also had color names like blackbox, redbox, silverbox, and more. The names did not describe to the color of the device, it was just a name to assigned to the device functionality.

The Bluebox created and sold by Steve Wozniak and Steve Jobs

There are many references to phone phreaking in public culture. In the Hollywood movie "War Games", the main character (David Lightman) uses phone phreaking techniques to make long distance calls from his computer, and from a pay phone. In the movie "Hackers" phone phreaking is used to make long distance calls and to wiretap the FBI.



Hollywood film War Games

Phone companies around the world viewed phone phreaking as a threat to their business. Bluebox devices started to become popular and available to the public for making free long distance phone calls. Over time phreaking was used more for financial profit and criminals were selling services for cheap calls that exploited the in-band signaling weaknesses. In most countries phone phreaking activity was considered fraud and a theft of service - a criminal offense. Law enforcement worked together with fraud investigation teams at the phone companies to identify phreakers and make arrests. The phone phreaking community started with curious people only wanting to have fun and learn about the phone system but later evolved into financially motivated criminal activity.

A Bluebox app available on the Apple Appstore

To prevent abuse of the system phone companies started building frequency filters into the customer lines to prevent the use of special tones like 2600hz. The fundamental weakness that allowed phreaking was the in-band signals to control the phone system. The phone companies recognized this and developed new infrastructure that used out-of-band signaling which could not be directly manipulated. Over time most of the world’s public switched telephone systems were moved away from legacy in-band signaling systems. Phone phreaking does not work on modern phone infrastructure today and is a hacking technique that is only of historical interest.

Resources:

The famous Esquire article that made phone phreaking public:
http://www.historyofphonephreaking.org/docs/rosenbaum1971.pdf

Historical information about early telephone switches:
https://strowger-net.telefoniemuseum.nl/tel_hist_index.html
https://strowger-net.telefoniemuseum.nl/tel_tech_index.html

A collection of recorded phone phreaking calls:
http://evan-doorbell
http://elmercat.org/ld-calls/

Different kinds of Phone Phreaking boxes:
https://en.wikipedia.org/wiki/Phreaking_boxes

HOWTO articles written by phone phreaks:
http://www.textfiles.com/phreak/