History of Hacking

Part 2: Dial-up Modems

By Bruce Nikkel

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

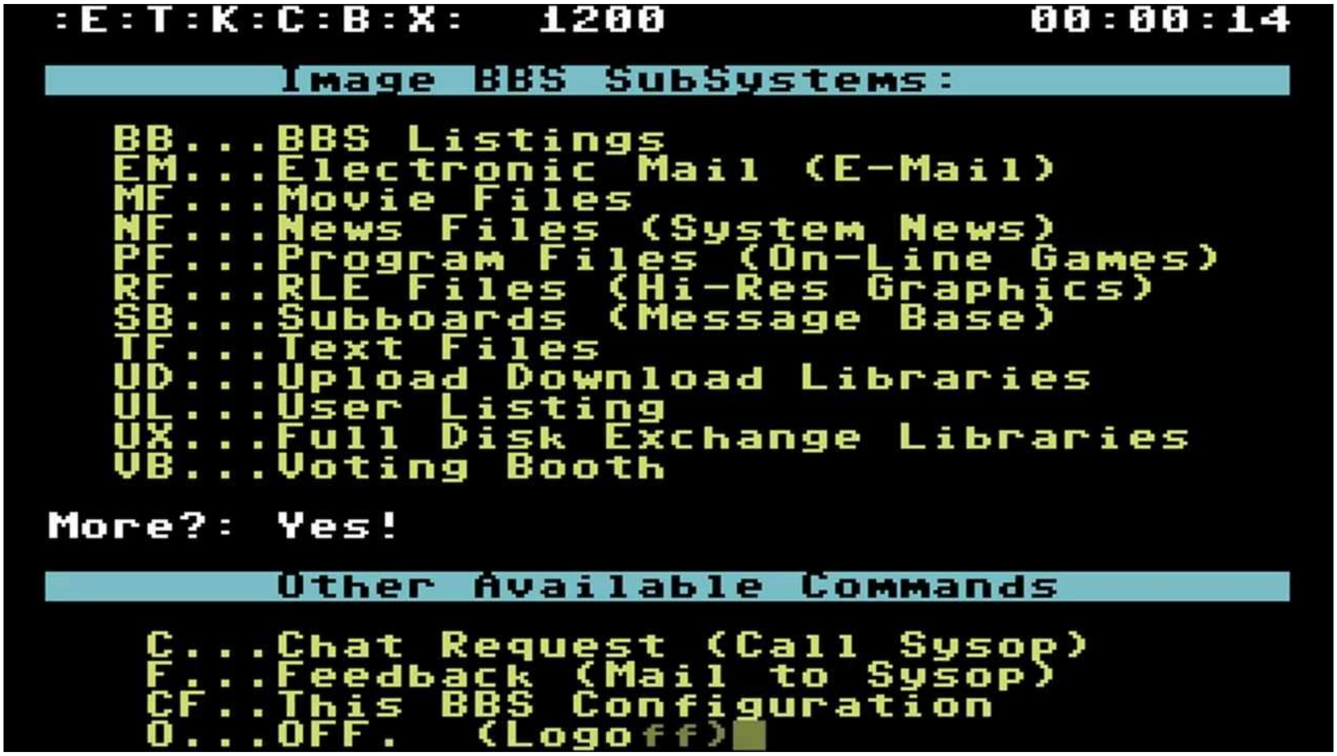
This is part two of a four part series on the history of computer hacking. In the first article we covered the early hacking of global telephone switching systems. This article describes the hacking scene with home computers, modems, and dial-up services.

Early computer networking leveraged the existing voice lines provided by the telephone companies. This communication required a conversion between analog audio sounds and digital data bits using signal *modulation* and *demodulation*. The origin of the word "modem" is derived from this process. Most telephone companies strictly regulated what equipment was allowed to attach to the phone network. Early "acoustic coupler" modems used audio sounds to communicate with the telephone's microphone and speaker. This was not a direct electrical connection ("air-gapped") and didn't require phone company approval, so hobbyists were free to build and use their own acoustic coupling modems. Modems directly connected (electrically) to the phone system were much faster and had less errors than acoustic modems, but these required phone company certification. Acoustic coupler modems could also be used with pay-phones where no direct cable was available. Over time, directly connected electronic modems became cheap and replaced the acoustic coupler technology. The use of the public telephone network for computer networking made it easy for hackers to exploit.

Acoustic coupler modem and telephone

Initially, dial-up modems were used to connect remote terminals to large mainframes and mini-computers running Unix or other time-sharing systems. Terminals and modems used a special sequence of characters called "escape codes" or an "escape sequence" to control the session and the modem. Escape sequences were used to send special commands to the system or the modem for file transfers, local printing, configuration, diagnostics, and other control functions. Escape sequences were especially interesting for hackers because they allowed more control over a system, and could be used to break out of programs or menu systems to access system command prompts and shells. More advanced modems had full featured command sets built into their firmware, and could be manipulated with complex "AT Commands" (originally invented by the Hayes modem company). Hackers also used dialing functionality to forward local calls to long distance numbers, allowing access to remote computer systems.

Access to large companies or networks was either restricted or expensive. This led to the proliferation of free Bulletin Board Systems (BBS) run by private "sysops" or system operators. Any computer enthusiast with a modem could create a BBS and publish the number (in local newspapers, computer magazines, or other BBS's). BBS's were text-based systems used for chat, forum discussions, electronic mail, games, news, uploading and downloading files, and for gateway access to other BBS's or networks. The BBS hacker scene included sharing "warez" or copyrighted hacked/cracked software, stolen credit cards and long distance calling cards, stolen passwords and access codes, and stolen proprietary source code and documentation. BBS's were also a popular way to distribute virus infected programs.



```
 :E:T:K:C:B:X:   1200              00:00:14

             Image BBS SubSystems:

   BB...BBS Listings
   EM...Electronic Mail (E-Mail)
   MF...Movie Files
   NF...News Files (System News)
   PF...Program Files (On-Line Games)
   RF...RLE Files (Hi-Res Graphics)
   SB...Subboards (Message Base)
   TF...Text Files
   UD...Upload Download Libraries
   UL...User Listing
   UX...Full Disk Exchange Libraries
   VB...Voting Booth

 More?: Yes!

             Other Available Commands

    C...Chat Request (Call Sysop)
    F...Feedback (Mail to Sysop)
    CF..This BBS Configuration
    O...OFF.  (Logoff)
```

Bulletin Board System (BBS)

Networks of computer systems around the world began growing in popularity. Some networks were commercial dial-up providers like Compuserve or AOL, where a monthly fee was charged for services. National telephone/post organizations also provided commercial services like Minitel in France, or BTX (Bildschirmtext) in Germany. Non-commercial networks like FidoNet connected BBS systems together from around the world, and UUCPNET connected Unix systems together using UUCP. There were also regional networks like MausNet (http://maus.de) in the German speaking countries of Europe. These networks were based on dial-up technology and the hacking was mostly non-malicious activity to gain access to systems or explore other networks (via gateways) because it was interesting or a learning experience.

French Minitel terminal

Finding computers with modems was a challenge because the phone numbers were not listed in a phone book, and the phone companies didn't know who had modems connected to their phone lines. A technique called "war-dialing" was used to search for computers with modems connected to the telephone network. A computer was programmed to repeatedly dial every phone from a range of numbers (usually a local area code to avoid long distance charges, or a range of numbers belonging to a company). If a human answered, the computer would hang up and dial the next number in the sequence. If a computer answered, a modem carrier signal was detected and the war-dialer software would save the phone number and other connection information for later analysis. War-dialing a large block of numbers could take a few days to complete, but at the end the hacker had a list of all the computers that answered the phone. Finding computer modems was interesting because many early systems didn't use passwords, and simply knowing the number was the only access control.

War-dialing was used in the movie War Games

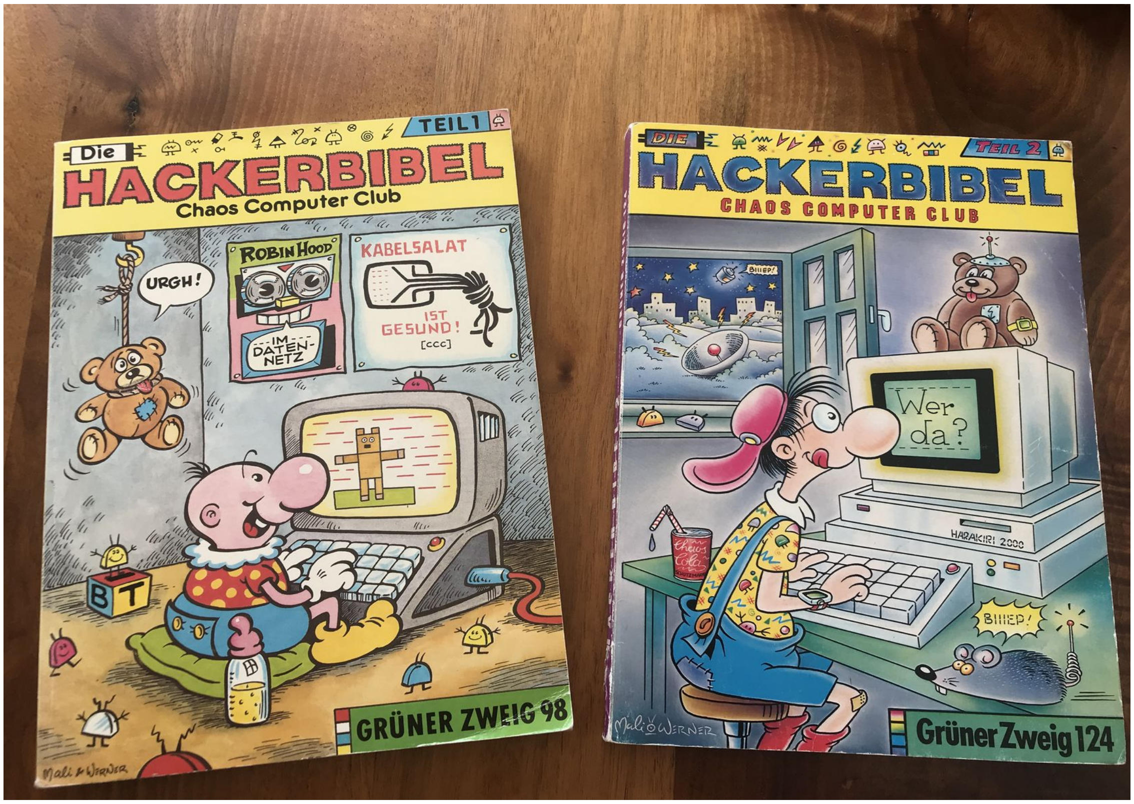
Other methods to find modem numbers and passwords included "social engineering" and "dumpster diving" (also mentioned in the last article). Social engineering (still very popular with cyber criminals today) is where people are deceived or tricked into doing things or revealing information. Hackers phoned or visited different people in a large company posing as other employees or technical support. They had a friendly interaction with a plausible story, asking for help to find phone numbers and passwords of computer modems. Dumpster diving (also called "trashing") is where hackers looked through the company's garbage for computer printouts or company phone lists that might have computer modem numbers, passwords, and other technical information. To avoid detection, dumpster diving was done at night when the office was closed. This was back in the days before recycling was common, and paper was thrown in the trash.

Another attack used against dial-up systems was "demon-dialing". A "demon dialer" was an electronic device (controlled by DTMF tones) connected to a telephone line or a software program controlling a modem, that continuously called a single number. This was originally created to speed dial a busy BBS or ISP until a connection was successful. Hackers also used demon-dialing for "Denial of Service" (DoS) attacks and brute-forcing access. A DoS attack involved keeping the modems busy so no other users could dial into the service. If the attacker could dial, hangup and re-dial faster than the provider could re-initialize the modems, it created a successful DoS. Another use for demon-dialing was to repeatedly test different usernames and passwords (brute force). A demon-dialer program with a list of common usernames and passwords was run against a company's dial-up system to attempt unauthorized access.

A demon-dialer box

For additional security, some organizations used a method called "dial-back" or "call-back" authentication. When a user wanted to connect to the company, they called, identified themselves, and then disconnected the call. The company's dial-up system had a pre-defined list of phone numbers for authorized users and called the identified user back. The user's computer then answered the phone and finished setting up the connection. There was a simple way to hack poorly designed dial-back systems. If the attacking modem refused to hangup the line, some dial-back systems didn't notice, and started sending the dialing codes (pulse or DTMF tones) over the still connected phone line. Without disconnecting, the attacker "answers" the dialing modem, the company system thinks the dial-back was successful, and an unauthorized connection is established.

Access to hacking tools and techniques started growing with popular hacker resources like the Chaos Computer Club (CCC), 2600 Magazine, Phrack e-zine, and other online hacker communities. Unauthorized access and intrusions to computer systems and networks via modem in the 1970s and 1980s became problematic for system owners. This resulted in new computer fraud and abuse laws in most countries to criminalize malicious hacking activity. These laws were created in the age of modem dial-up, but were intended to stay relevant as technology changed.



Chaos Computer Club Hacker Bibles

The dial-up modem has mostly disappeared today. Internet has replaced the BBS and other dail-up networks, broadband and fibre has replaced dial-up Internet, even analog phone lines are becoming obsolete, being replaced with Voice-over-IP (VoIP). The Enter Museum in Solothurn has an excellent collection of historical modems and telecommunications equipment, and I can highly recommend visiting.

Resources:

The Chaos Computer Club:
https://www.ccc.de/

2600 Hacker Quarterly:
https://2600.com/

The Phrack e-zine:
http://phrack.org/

List of Internet accessible BBS systems:
https://www.telnetbbsguide.com/