Phone Phreaking

Sam Wolfson

CSE 120, Winter 2020

Administrivia

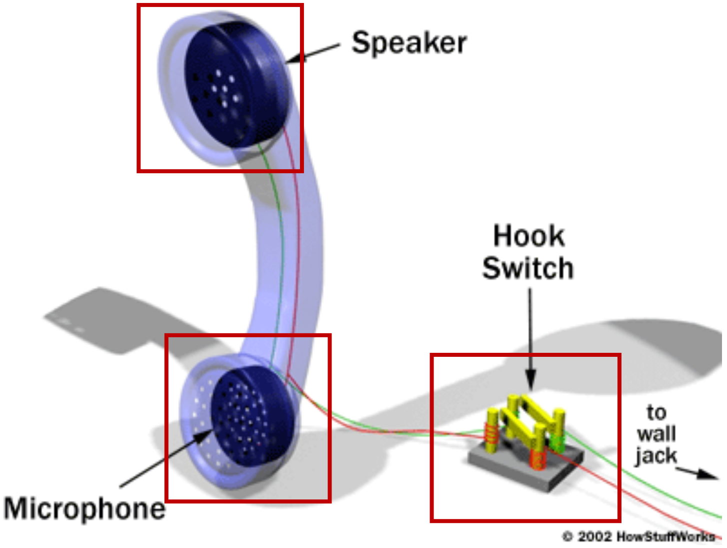
- Tic-Tac-Toe due tonight!
  - Checkoff during office hours, or submit on Canvas
- LCM Report due Monday
- Final Project Design Document due Monday
  - Talk to course staff if you'd like help brainstorming
  - Work with a partner!!!!
- Next week in section: Innovation Exploration
  - Presentations will take place both Tues and Thurs
  - The rest of section will be project work time 🙂

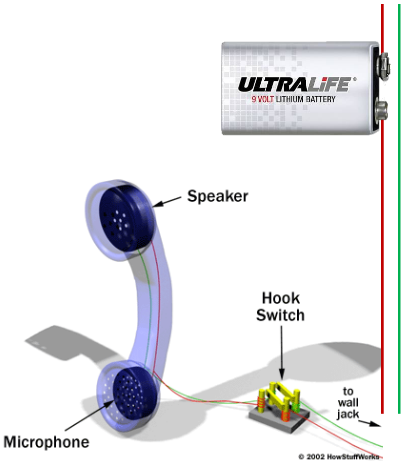
Who are the phone phreaks?

- People who study, explore, and experiment with telecommunications equipment.
  - Listen to patterns and tones on telephone lines and attempt to decipher them
  - Read obscure technical journals about the inner workings of the telephone system
  - Impersonate operators or other telco employees
  - Build devices to make the telephone network act in ways not intended by the designers
- For the most part, primarily interested in knowledge, but sometimes ended up in legal trouble…

How Do Phones Work? (Part 1)

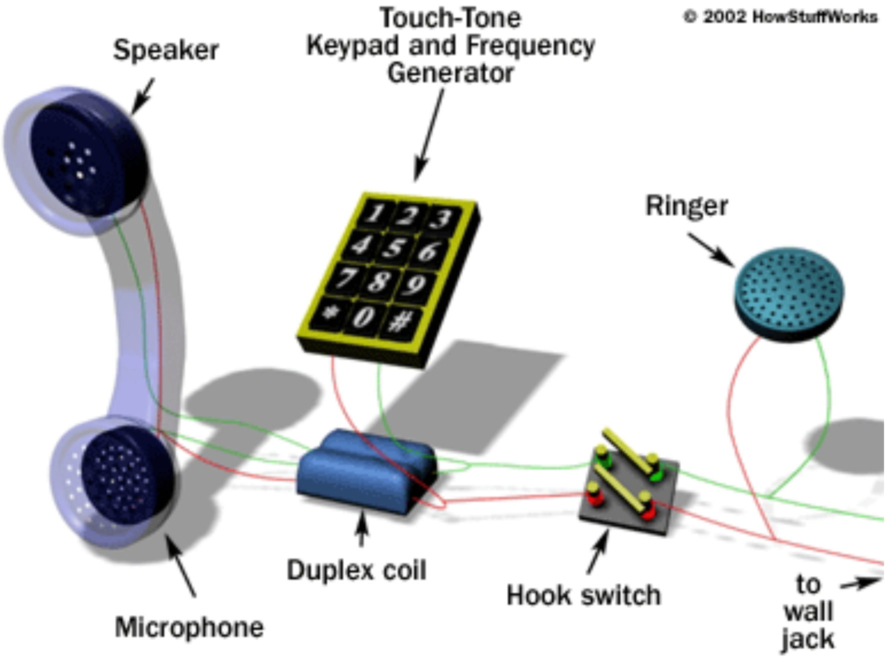
- Picking up the phone closes the hook switch, connects the phone to the other person
- Vibrations from speaking into the microphone change the resistance and the current flowing in the wires
- When the other person speaks, their microphone vibrates your speaker





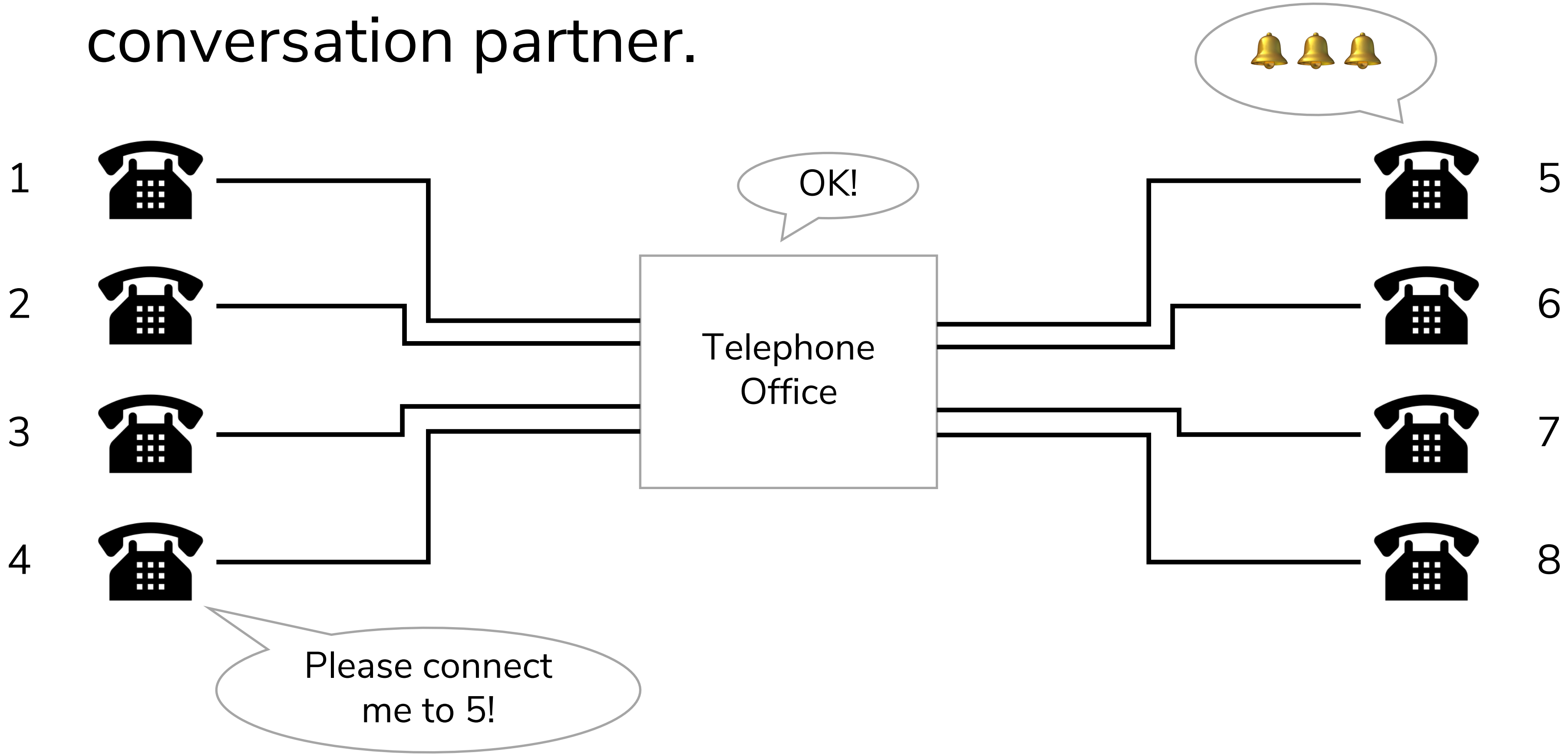
How Do Phones Work? (Part 2)

- Phones include a few other parts to make them easier to use
  - Duplex coil prevents you from hearing your own voice over the speaker
  - **Ringer and keypad – how do they work??**



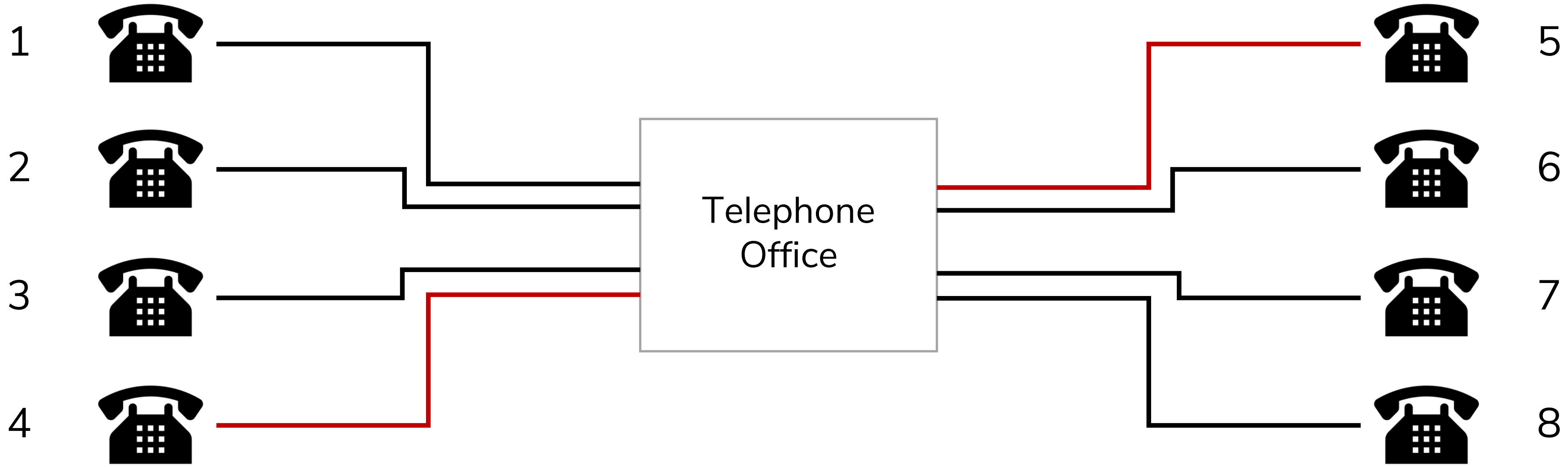
The Phone Network

- In reality, you are not *directly* connected to your conversation partner.



The Phone Network

- In reality, you are not *directly* connected to your conversation partner.



- The telephone office makes connections based on how you dial the keypad.

Telephone Signaling

- How do you tell the telephone office who you'd like to be connected to?
    - Talk with your neighbor!

Rotary Phones

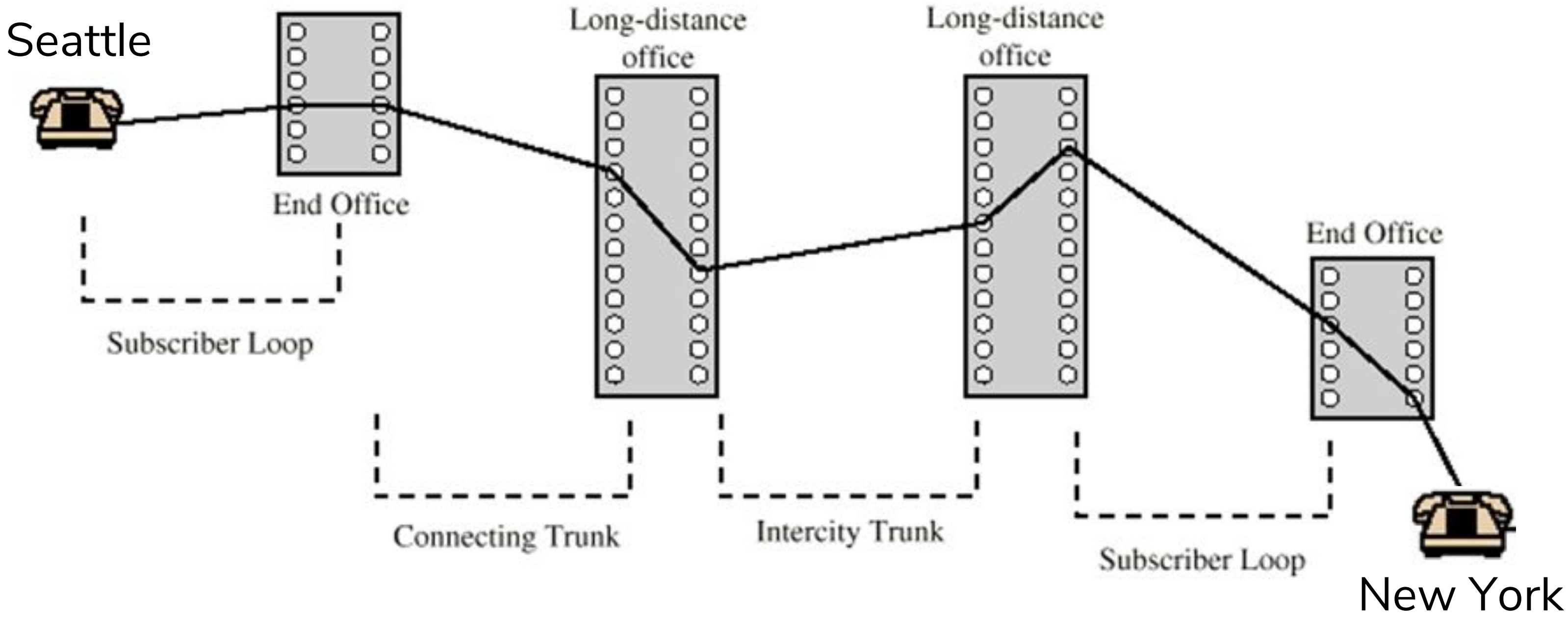
Pulse Dialing: Rotating the dial to a certain number sends that number of short pulses down the telephone line by disconnecting and reconnecting the hook switch.

Multi-Frequency Signaling

- **Idea:** have phones communicate with the network using tones, over the same wires!
  - The phones "sing" to the receivers inside the telephone office, which direct the call accordingly.
    - Your cell phone still makes these tones!
  - Internally, the phone network also uses tones to communicate (but over different frequencies)

- **In-Band Signaling**: happens over the *same connection* as your voice.

Long Distance Connections



- Long distance calls travel through multiple offices that need to find unused lines through which connections can be made.

Long Distance Connections

- How can the offices figure out whether a long-distance telephone line is free?
  - Play a tone over unused lines (typically 2600 Hz).
- When you dial a long-distance number…
  - Your local office looks for an unused long-distance line (i.e., one with a 2600 Hz tone).
  - It then plays the tones for the phone number you want to call over the line so that receiving office knows where to connect you.
  - The receiving office finishes the connection.

Long Di$tance Connection$

- Long distance calls were *expensive.*
- Your local telephone office kept track of how much you use the long-distance telephone lines and charged you accordingly.
- How might you trick this system into making these calls for free?
  - Talk with your neighbor!
  - **Hint:** think about toll-free numbers.

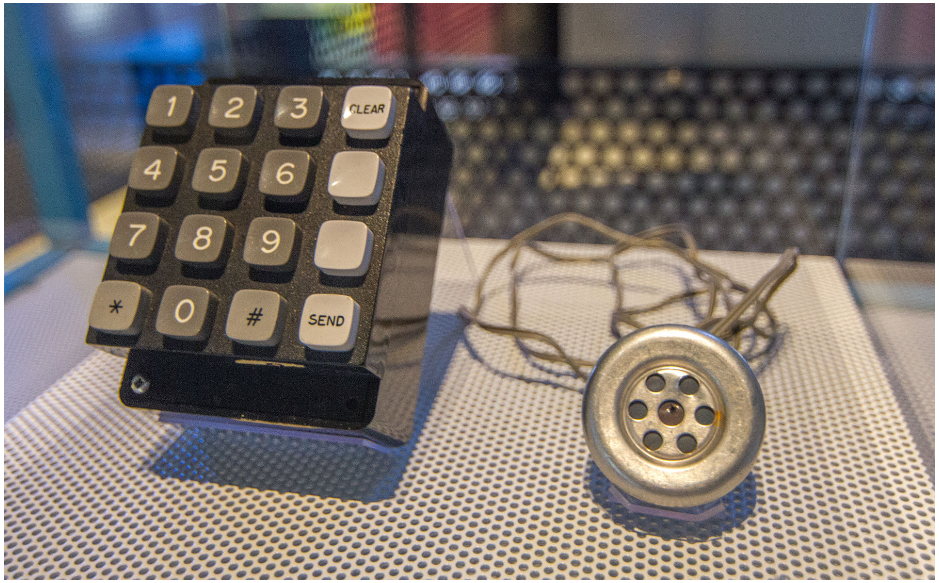
How To Make Free Calls

- Call a toll-free (1-800) number that connects you somewhere outside of your local telephone office.
- Play a 2600 Hz tone over the phone line, causing the receiving office to think that you’ve hung up.

- Somehow play the tones for the number you *actually* want to call, and the receiving office will connect you (but the local office will still think your call is toll-free!)

The Blue Box

- A device that could generate the tones used internally by the telephone network to connect long-distance lines.



- Also the first product that Steve Jobs and Steve Wozniak ever sold together.

How did they figure this out?

- Lots and lots of experimentation, reading found technical manuals, and some good luck.
  - Calling random phone numbers and trying to decipher the “beeps and boops” that went on inside the network as the call travelled through it.
  - Playing certain tones into the handset microphone and seeing what happened.
  - Intentionally trying to route calls through obscure offices to learn about different switching equipment.
- Later: using early computers to automatically call lots of phone numbers, play tones, and see what happened.

Phone Phreaking & Hacker Culture

- Phone phreaking was closely intertwined with the hacker culture of the later 20th century.
- Many of the important figures were in Silicon Valley around the time that computers and computer kits were becoming accessible.
- Used their skills with building & experimenting around electronics.

- Did phone phreaking indirectly lead to the creation of Apple? Maybe…

Mitigations

- “Blue boxing” techniques no longer work 😞
- Modern phone networks bundle together many signals and send them digitally over fiber optics.
- In-band signaling has been replaced with out-of-band signaling (i.e., over different wires than the voice signals), making this kind of interference impossible.
- Few people even have landline phones anymore.
- But the legacy of the phone phreaks lives on in modern hacker culture.

Learn More

- There are other, lesser-known techniques for phone phreaking that I didn’t have time to talk about
  - The rabbit hole goes deep…

- “Exploding The Phone” http://explodingthephone.com
- “How Telephone Phreaking Worked” https://www.youtube.com/watch?v=4tHyZdtXULw
- “Ghost In The Wires” https://www.amazon.com/dp/B0047Y0F0K/