Exploiting "Ma Bell"

In the USA, in the 60's,   there was just ONE phone company.   Ma Bell.   Because of this,   the cost of phone calls were very unreasonable, almost as bad as the cellular companies "roaming charges",   so when someone comes along, and "airs" their dirty laundry, and finds some serious security holes in their network,   it really got their attention.

You have to really understand...

- How many knows my story?
- The political situation In the USA at that time.
- Watergate
- Viet nam protests.
- Set the stage for some really interesting times.
- I had been offered a high paying job.
- Turned it down because they were building technology to kill people.

Phone Phreaking

- What is a Phone Phreak?

- Most are blind… their world is Audio.

- Their hearing is excellent.   Most have perfect pitch.

- They know every click and pop, and where it comes from.

- With their intuition and super hearing, they could understand how calls originate and work throughout the vast ATT network.

ATT's Serious flaw.

- Using voice circuits for internal switching is a BAD IDEA.

- It's like leaving the keys to your house outside.

- 2600 was the magic frequency that opened the gate.

- The Cap'n Crunch Whistle did it.   Thus how I got the name.   Oscar Meyer wiener whistles worked also.

- On earlier equipment, just "pulsing" 2600 was all you needed to "divert" a call.

- Later on, they used Multi-Frequency, not touch tones.

- I couldn't believe it was that easy

- And it worked everywhere.

Demo

- Recorded in 1975

- Full description of each click

- Demo

Stories

- Scanning

- Hacking the white house

- Hacking the prison phone and radios

- Gave phone Phreaking lessons.

- Woz pranks, calling the pope, McDonalds

- Phone company should have hired me.

Evolution of hacking

- Phone Phreaks were the first hackers.

- Definition: Chopping up program, putting it together in a different way.

- Public access to modems spawned more hackers.

- Published on BBSs, Fidonet, Compuserve, WELL.

- Hacking took on a new direction. Became mainstream

- More news articles on hacker busts, and BBS busts.

- Internet became "commercial" in 90's. Totally changed the game.

- Viruses, Trojans, 419 scams, and spamming becomes serious problem.

How these flaws relate to systems today

- People overlooking the obvious

- Happens all too often these days.

- People "click happy", and just love to click those links.

- It takes a hacker to secure computer systems.

- Corporations afraid of pen testing their systems.

- Afraid their weaknesses may become public.

- Would YOU bank at a bank that wasn't secure?

- People don't pay attention to security alerts

- All systems prone to attack.. Mac, Windows, Linux

What can YOUR company do?

- Should they monitor their employees mail

- New employees should be required to orientate their new employees on security issues.

- Company IT staff should have at least one security expert.

- Network monitoring important... Snort, IPS's

- Browsers should be "hardened"

What I'm currently doing

- Starting a new LLC, http://crunchcreations.org
- Building specialized teams we can call on when needed.   Most already employed elsewhere.
- Writing my book – Signed a book/Movie deal
- Ecoviso
- Social networking.
- CrunchTV

How to contact me

- jdcrunchman@gmail.com
- Facebook.com/jdcrunchman
- Skype: jdcrunchman
- AIM: jdcrunchman
- Google+: jdcrunchman
- Twitter: @jdcrunchman
- LinkedIn: jdcrunchman
- Phone: +1 818-253-9102
- See a pattern there?