NORTH DAKOTA CYBER SECURITY CONFERENCE

# Lies, Telephony, & Hacking History

Matt Scheurer

## Social Engineering Timeline

- Pre-1940's +
- 1950's +
- 1970's +
- 1990's +
- 2000's +

PDF http://slides.dfirmatt.com

Username:

Password:

Submit

# About Me

**I work for a big well-known organization...**

**As Vice President (VP) of Computer Security and Incident Response (IR). However, I have many years of hands-on technical experience, including Digital Forensics & Incident Response (DFIR).**

**I am also a Podcast Host for**

ThreatReel

https://threatreel.com

**Connect / Contact / Follow Matt:**

https://www.linkedin.com/in/mattscheurer

https://twitter.com/c3rkah

# Where I volunteer...

**I am an Official**


**Advocate**
**https://www.hackingisnotacrime.org**


**Advisory Board: Information Technology and Cybersecurity**
**https://www.mywccc.org/**


**Women's Security Alliance (WomSA) Technical Mentor**
**https://www.womsa.org**

# Disclaimer!

Yes, I have a day job. However…

Opinions expressed are based solely on my own independent security research and do not express or reflect the views or opinions of my employer.

# Origins of Social Engineering

Some believe that Social Engineering dates all the way back to the “Garden of Eden”.

# Whatever you believe...

Deception and trickery have likely been with us for a very, very long time!

# Social Engineering & Technology

- Social Engineering intertwined with Technology by telephony inspiring “Phone Phreaking”
  - The telephone system blossomed into the World’s first inter-connectable global network
    - Built by Telephone Companies (a.k.a., “Telcos” for short)
  - Phone Phreaking
    - We’ll dive into this topic momentarily...

# A note about Telecom History

- These may be somewhat fluid timelines...
  - Telcos were often slow to replace or upgrade otherwise adequately functioning equipment
    - Especially when systems exceeded utilization needs
    - Geo’s, metros, demographics and their respective local branch equipment often happened on different timetables
  - A local community’s telecommunication stack varied greatly at any given time based on a variety of market and other conditions

# 19th Century and Onward

- Telephone companies hired Switchboard Operators to assist customers and route calls
  - These individuals handled call routing by plugging physical cables into switchboard jacks
  - Many early phone subscribers communicated over shared “party lines”, with no real assurance of privacy

# Late 19th and Early 20th Centuries

- Electromechanical switches
  - The late 19th Century introduced Strowger "Step By Step" (SXS) switches
  - These SXS switches continued growing in footprint during the early 20th century
  - This was the beginning of automation in the burgeoning telecommunications industry

# 1940's to the 1950's

- AT&T developed automation using audible tones for long-distance call routing
  - Multi-Frequency (MF) signals were assigned to telephone number digits
  - Single-Frequency (SF) tones were used for line status signaling
- These advancements paved the way for Phone Phreaking “Blue Boxes” in the future

# 1950's and 1960's

- Beginning around the mid-20th Century
  - Telephone companies began more widely deploying advanced circuit switching technologies such as “Panel" and "Crossbar"
  - These switches along with reliable transistors paved the way for viable dual-tone and multi-frequency (DTMF) support, often referred to as “touch tones”, on phones

# 1970’s to Present

- Electromechanical switches were slowly being phased out in favor of newer Digital Switches (i.e., Electronic Switching Systems / ESS)
  - The migration to digital switching was the beginning of phasing out analog telephony in favor of digital telephony
- Voice-over-Internet Protocol (VoIP) technology is now largely displacing electronic switches

# Phone Phreakers

- Who are/were the Phone Phreaks?
  - People who enjoy exploring phone systems
  - Those who enjoy experimenting with technology
  - Some were obsessed with learning the science and technology behind telephones and phone networks
  - Phone Phreaking often became a gateway or bridge towards becoming a computer hacker, or vice-versa; and "War Dialing"

# Objectives of Phone Phreaking

- Some Phone Phreaker motivations include
  - Learning (Thirst for knowledge)
  - Meeting and talking with other Phone Phreaks
  - Pranks and mischief
  - Making free phone calls to anyone, anywhere

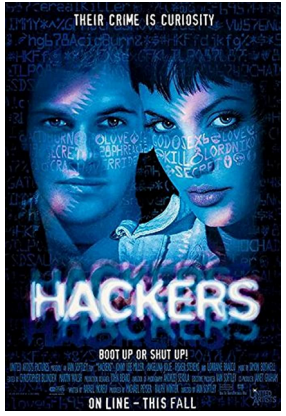
# Phone Phreaking in Film


## Three Days of the Condor

Released: 1975

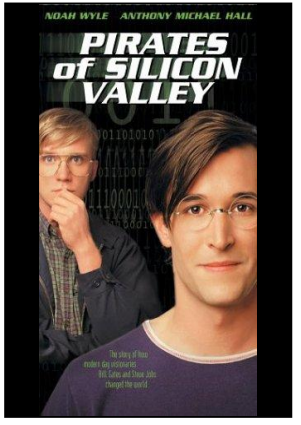

## WarGames

Released: 1983




## Hackers

Released: 1995




## Pirates of Silicon Valley

Released: 1999

# Classic “Phone Phreak” Tools

- Musical Instruments & Whistles
- Phreaker Boxes
  - Blue boxes, Beige boxes, Red boxes, etc.
- Payphones
- Tape Recorders
- Scanners and Radios

# Phone Switching and Tones

- Early phone systems used audible control tones
  - Some musical instrument notes could pass as recognizable telephone switch signal tones
- Whistles / whistling
  - Cap'n Crunch breakfast cereal once included a free whistle as an in-box toy giveaway, capable of producing a perfect 2600Hz tone
  - Some people could whistle the tones by themselves

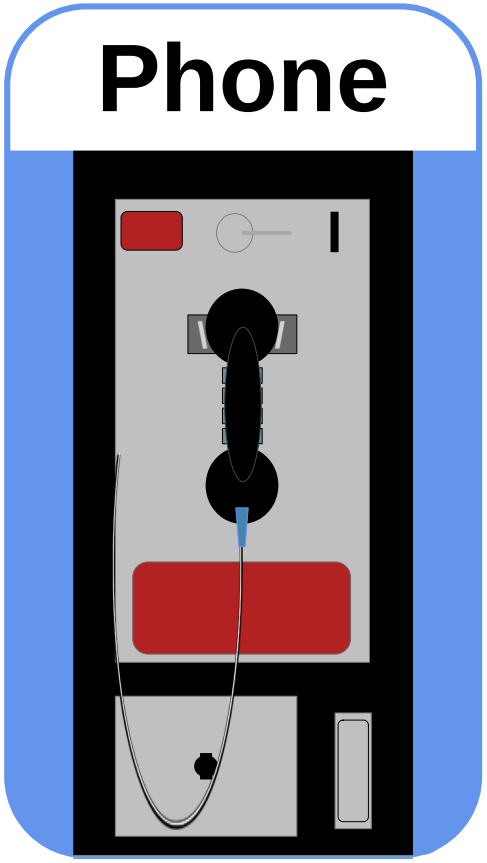
# Blue Boxes

- Generated 2600Hz tones among others
- Used for controlling phone switches
- Gave users the ability to place free phone calls

# Beige Boxes

- Beige box
  - A lineman’s handset
  - Or a homemade variety thereof
- Connects to a phone wiring block
- Used to “tap” into a phone line or connect a new extension onto a discovered phone block

# Payphones




- Once very commonplace
- Provides a physical layer of separation from home
- Offered a level of anonymity to their users
- Some level of deniability for callers

# Red Boxes

- Red boxing
  - Used by phone phreaks to load fake money into payphones by playing tones into the handset’s mouthpiece
  - Thus enabling users to place free phone calls from Telco owned and operated payphones

# Tape Recorders

- For those not adept at building electronic tone generators and circuits, using a tape recorder and playback was a viable alternative
  - Often combined with a telephone recording device adapter
  - Or by using universal telephone pick-up coils
    - Useful when no modular jacks are present

# Scanners and Radios

- Scanners and radios were capable of listening into wireless communications and eavesdropping on conversations
  - Many people unwittingly “bugged” themselves
    - Cordless Phones (43–50 MHz and 900 MHz)
    - Early Cellular Phones (800 MHz)
    - Baby Monitors

# Private Branch eXchange (PBX)

- A Private Branch eXchange (PBX) system is a comparatively smaller (to Telco exchanges) telephone exchange and switching system
- Typically owned and operated by organizations and private businesses
  - Providing interconnected phone services to them

# PBX Abuse and Hacking

- Enumerating company employee phone directory abuse
- Compromising voice mailboxes and listening to saved messages
- Setting up unauthorized voice mail boxes
- Transfers to extension 91 and other 9 + Country Codes (socially engineered people or switched methods)
- Call-Forwarding, Diverters, and other routing tricks

# Phone Phreak Tradecraft

- Dumpster Diving (a.k.a. “Trashing”)
- Call routing loops and 3-way calling used for eavesdropping and/or pranks, what we now often think of as “Man-in-the-Middle” or “Adversary-in-the-Middle” (MitM or AitM)
- Socially engineering phone operators and other Telco employees
- Calling card fraud and abuse

# Telco Countermeasures

- Telcos implemented various fraud controls to detect and flag, or block phone phreaking efforts by the early 1980's
  - Old phone phreaking methods and the various color boxes became obsolete and unusable
  - These countermeasures forced Phone Phreaks to continually adjust their tactics midst the changing times

# Ch-ch-ch-ch-changes

- Switchboard operator career opportunities were mostly displaced by technology in recent decades
- The market saturation of mobile phones made deploying and maintaining payphones financially infeasible for Telcos in North America
  - Consequently, payphones have largely disappeared from the landscape in most first-world countries

# Nowadays

- The proliferation of “unlimited” and “flat-rate” cellular calling plans eliminated the incentive to steal phone service for the purpose of making free phone calls
- Most new telecommunication deployments favor using Voice over IP (VoIP) technologies, platforms, and services
- Calling Card fraud (once very prevalent) has given way to Credit Card fraud

# The New Underground

- Phone Phreak "Bridges" (conference call party lines, and virtual meeting places) have largely been abandoned in favor of newer technologies
  - Web conferencing platforms
  - Encrypted Communication mobile apps
  - Darknets
    - Including the dark web

# The New Frontier

- Data dumps and dark marketplace use today is more prevalent than old school dumpster diving
- Mobile malware is an ongoing threat
- Proxy servers, VPN services, and TOR are mostly used to cloak communication source endpoint origins today

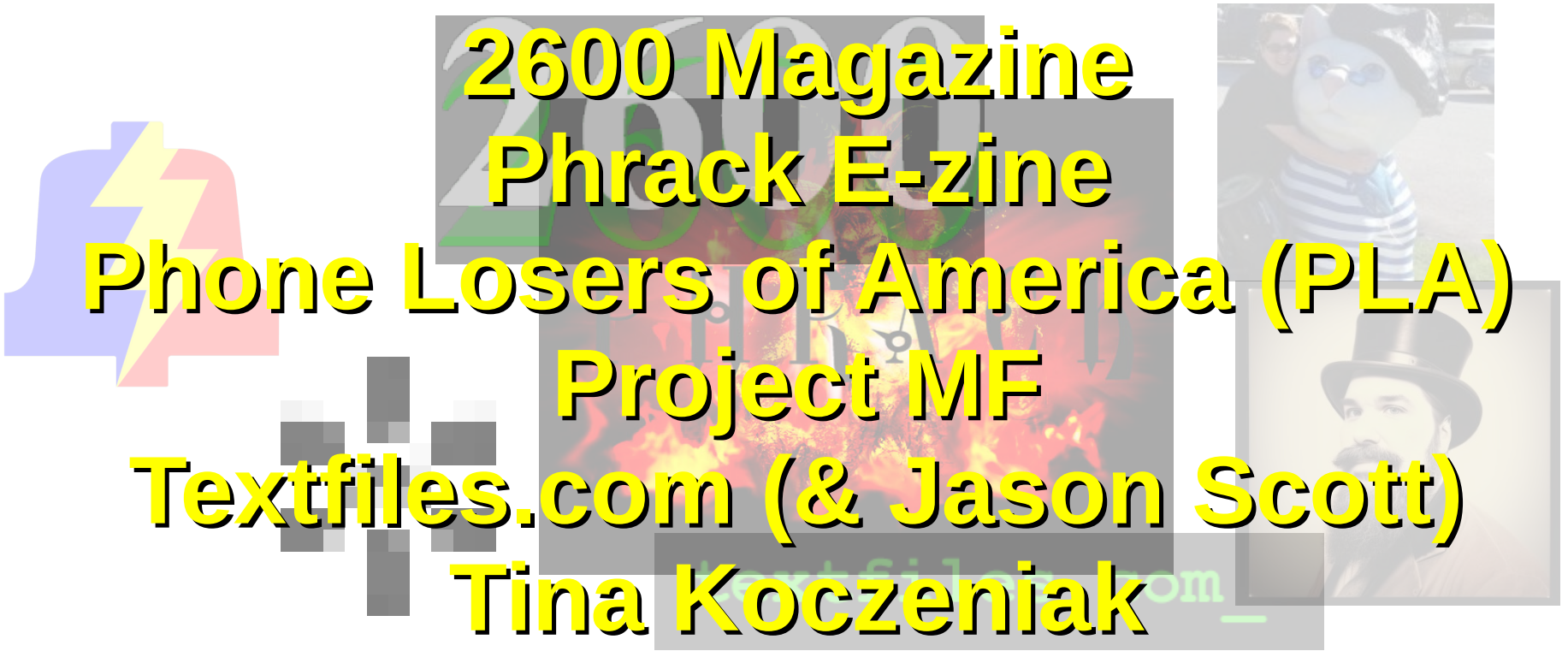
# Epilogue

- Technology and telephony abuse is less of a technology hobbyist, enthusiast, and prankster activity now
  - Modern abusers often comprise of...
    - Advanced Persistent Threats (APT's) & Threat Actor (TA) groups, Hacktivists, Financially-motivated actors, Organized Crime, and Nation-states

# Modern Phone Phreaking

- Reverse toll-fraud
  - International and other high-toll or pay-per-minute numbers
- Web conference calls
  - Eavesdropping, call bombing, raiding, and hijacking attacks
- Vishing and SMiShing
- Porting (a.k.a. “Port-out”) fraud
  - Migrating a mobile phone number to a different service provider
- Mobile phone SIM swapping

# Shout Outs for this talk



2600 Magazine
Phrack E-zine
Phone Losers of America (PLA)
Project MF
Textfiles.com (& Jason Scott)
Tina Koczeniak

# Questions

Who?

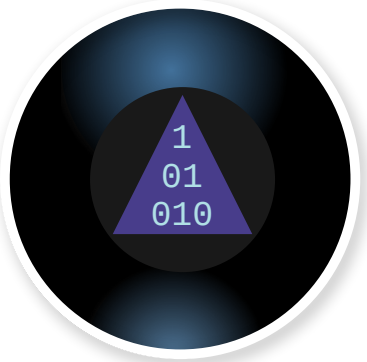
What?

When?

Where?

Why?

How?

NORTH DAKOTA CYBER SECURITY CONFERENCE

## Social Engineering Timeline

**Pre-1940's +**

**1950's +**

**1970's +**

**1990's +**

**2000's +**

Matt Scheurer

**Thank you for attending!**

Username:

Password:

Submit

PDF http://slides.dfirmatt.com