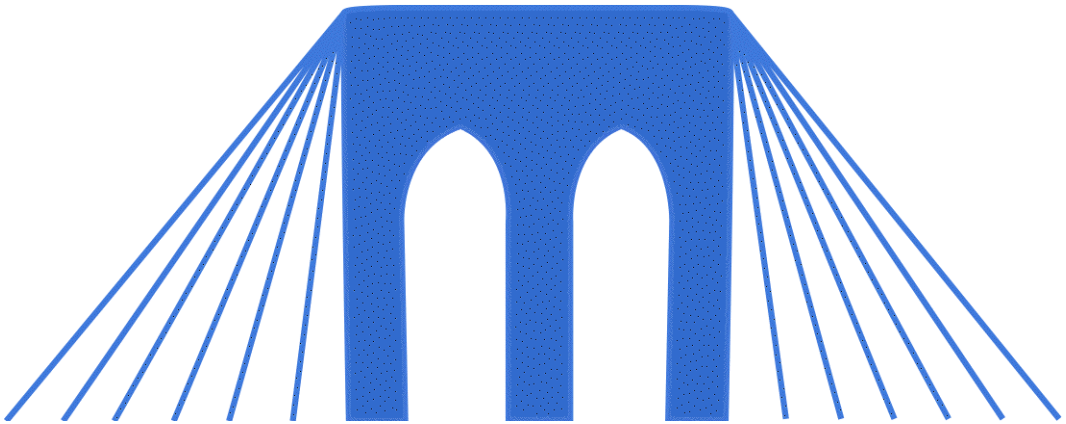
Bridges To Computing



General Information:

- This document was created for use in the "Bridges to Computing" project of Brooklyn College.
- You are invited and encouraged to use this presentation to promote computer science education in the U.S. and around the world.
- For more information about the Bridges Program, please visit our website at: http://bridges.brooklyn.cuny.edu/

Disclaimers:

- All images in this presentation were created by our Bridges to Computing staff or were found online through open access media sites and are used under the Creative Commons Attribution-Share Alike 3.0 License.
- If you believe an image in this presentation is in fact copyrighted material, never intended for creative commons use, please contact us at http://bridges.brooklyn.cuny.edu/ so that we can remove it from this presentation.
- This document may include links to sites and documents outside of the "Bridges to Computing" domain. The Bridges Program cannot be held responsible for the content of 3rd party sources and sites.

Introduction to Network Security

Lecture 1:

A short history of hacking.

M. Meyer
Bridges To Computing
2010

The first hacker?

- The telegraph was a device used in the 1800's and early 1900's to send messages over long distances.
- In 1903, magician Nevil Maskelyne interrupted John Ambrose Fleming's public demonstration of a new wireless telegraph technology, by sending insulting Morse code messages through the auditorium's projector.

Content

- What is a "hacker"
- Phreakers
- Hackers
  - History
  - Notable events in hacking.
- What is a hacker revisited

What is a hacker?

- You may already have your own understanding of the word.
- The reality is that the word hacker currently has several different definitions and has changed significantly over time from it's original definition.
- For the moment, let's leave out a "formal" definition… what do YOU think a hacker is?

Phreakers

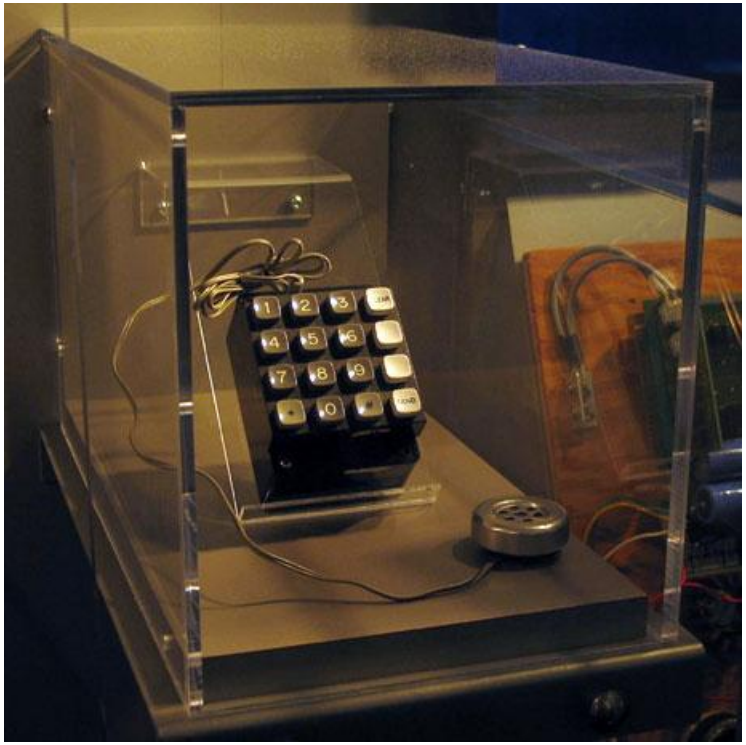
- In the 1940s making a phone call from the east coast to the west coast literally involved hundreds of people.
- Starting in the 1950's Telephone switch operators (on the right) began to be replaced with new electronic switchboards.
- The general population was, for the first time, exposed to computing power on a large scale.

Phreakers (2)

- Early automated switchboards communicated with one another using pulses and tones over the same lines that people talked on.
- In 1957 Joe Engressia, a blind seven-year old boy discovered that whistling a particular frequency (2600 Hertz) would cause a telephone switch to think a call was over.
- In 1964 Bell Systems published an article describing the methods and frequencies used by their switchboards. This manual found it's way into the publics hands.
- In 1972 John Draper discovered that a whistle from the Captain Crunch cereal could create the precise frequency needed to authorize Bell System long distance calls, thus making them free.

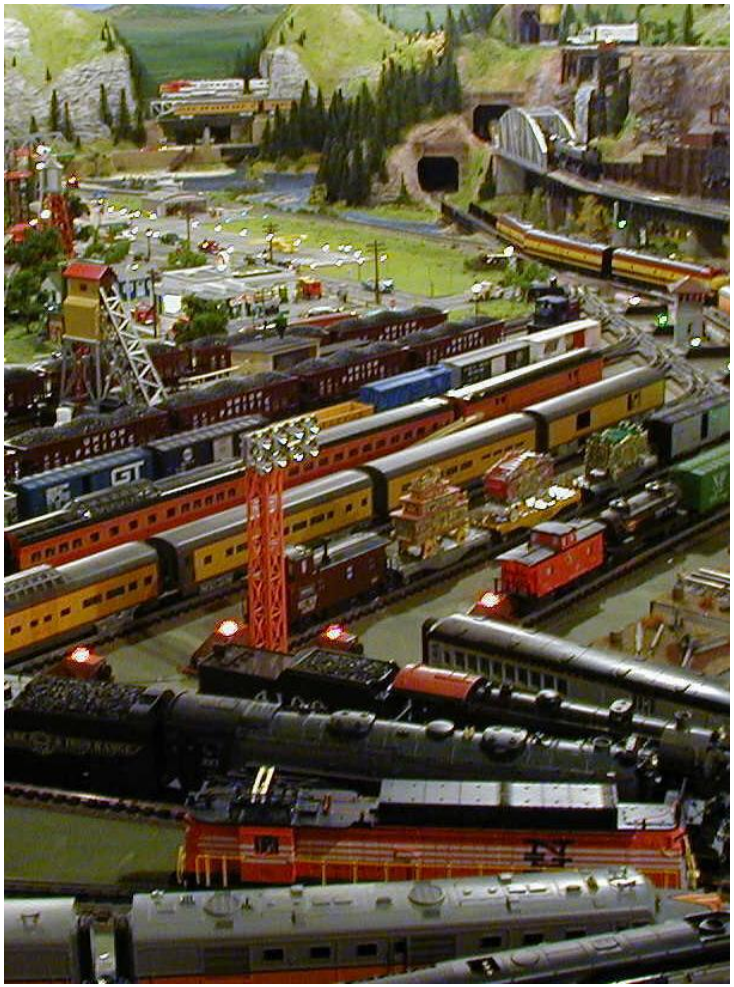
Phreakers (3)

- John Draper went on to create the "blue box“. A tool that, when sounded into a phone receiver, allows phreakers to make free calls.
- Among the early phreakers were college kids Steve Wozniak and Steve Jobs, future founders of Apple Computer.
- Phone phreaking came to an end in the late 80’s early 90’s as phone carriers moved to systems that did not send “control signals” over the same wires as the sound signals.



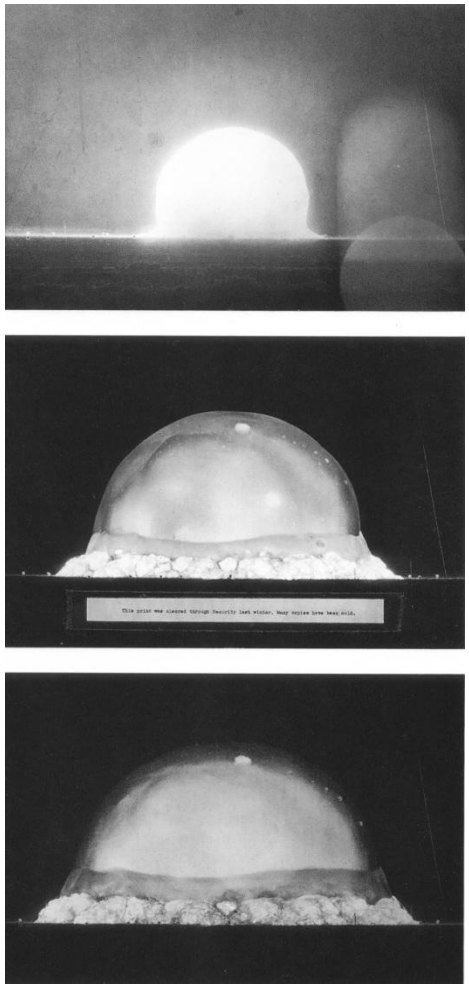
Hackers

- It is generally accepted that the first (self-described) hackers emerged at MIT in the 1960's.
- The term "hacker" came from the members of the model train group at the school who "hacked" their electric trains, tracks, and switches to make them perform faster and differently.
- A few of those club members transferred their curiosity and engineering skills to the new mainframe computing systems being developed on campus.



Early Hackers

- Early hackers were principally concerned with how to crack the password codes and encryption algorithms used by early computers.
- However as dial-up **modems** and eventually dedicated internet access connections became more widespread hackers switched to attempting to remotely compromise computer systems.
- In 1983, the FBI busted six teen-age hackers from Milwaukee (known as the 414s - after the local area code) for some 60 computer break-ins including the Los Alamos National Laboratory.



WarGames

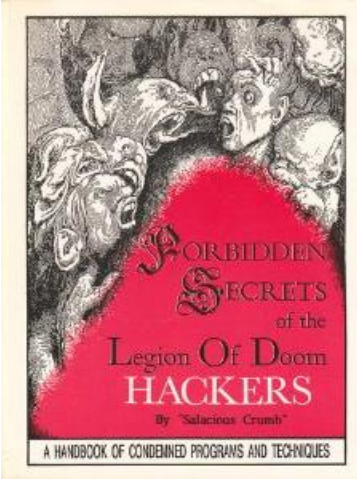
- In 1983, the movie "War Games" introduced the public to computer hacking.
- In the movie the film's main character (Matthew Broderick) accidently breaks into the military's nuclear combat simulator computer, nearly starting WW3.
- Broderick's character gets access to the military computer using a dial-up modem.

Hackers and Viruses

- In 1988 Robert T. Morres, Jr., a graduate senior at Cornell University "accidently" releases a self-replicating "worm" program on the government's ARPAnet (an early version of the Internet).
- The program spreads to some 6 thousand networked government computers disabling countless university and government systems.
- Morris is fined $10,000

Early Hacker Communities

- In 1990 the US Secret Service arrested prominent hackers in 14 U.S. cities including the entire "Legion of Doom" (an early hacker organization).
- The arrests are aimed at cracking down on criminal activity like credit-card theft and telephone and wire fraud as well as stopping the publications created by the hacking community.
- The result is a breakdown in the early hacking community, with members informing on each other in exchange for immunity.



NewsMakers in the 90's

- 1994 -> Russian hackers siphon $10 million from Citibank and transfer the money to bank accounts around the world.
- 1996 -> Hackers alter Web sites of the United States Department of Justice, the CIA, the U.S. Air Force.
- 1998 -> Seven members of the hacker think tank known as L0pht testifie in front of the US congressional Government Affairs committee on "Weak Computer Security in Government".

More recent events

- 2000 -> The ILOVEYOU worm infects millions of computers worldwide within a few hours of its release; considered to be one of the most damaging worms ever. It originated in the Philippines; made by an AMA Computer College student for his thesis.
- 2006 -> North Korea successfully attacks South Korean, Japanese, and US computer systems.
- 2008 -> Chinese hackers gain access to some of the world's most sensitive sites, including The Pentagon.
- 2010 -> Stuxnet a computer virus developed by the US is used to attack Iran's nuclear facilities.
- 2012 -> Foxconn is hacked by rising hacker group, Swagg Security, releasing bank account credentials of large companies like Apple and Microsoft.

Looking at history…

1. Hackers have very high-level skills in:
    1. Computer hardware
    2. Computer programming
    3. Computer Networks (Internet)
2. Hackers work as individuals, in groups, and sometimes even as government employees.
3. Some hackers commit crimes, and some commit crimes but claim to be doing so in pursuit of the greater good.
4. Other hackers work to stop illegal computer activities and protect the general public from cyber threats.
5. Hackers have had, and will continue to have a profound effect on society.

Hacker…

- is not a dirty word!
- has no agreed upon definition.
- at best describes a skill-set, not a behavior.

RFC 1392: A hacker is a "person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular."

My definition: A hacker is someone with a black-belt in computer science. There is nothing wrong with knowing **how** to do something…

What color is your hat?

To differentiate between the motivations of different types of hackers, different terms have entered the hacker lexicon:

- Black Hat Hackers: Those who perpetrate crimes.
- White Hat Hackers: Those who fix security problems.
- Grey Hat Hackers: Those who act illegally, but claim to do so in good will and in service of the general public (Hacktivists, Anonymous, Swagg Security)?
- Script Kiddies: Those who (lacking high-level CS skills of their own) use scripts or programs developed by others to attack computer systems and networks and deface websites

Use your powers for good

In the future we will concentrate on the problems faced by "white hat" hackers. That is, we will examine what a **network security specialist** needs to be aware of in order to prevent malicious theft of information from his/her company.

There is nothing wrong with being a hacker. There is nothing wrong with having those skills… but you should always endeavor to use your powers for good.

The End