Hacking: The Technology of Counter-culture
KHC, Spring 2017
KHC EK 102

Ari Trachtenberg, Ph.D.
Professor
Department of Electrical and Computer Engineering
Boston University College of Engineering
8 St. Mary’s St.
trachten@bu.edu
617-353-2811
Office Hours: TBD

Course Description
Formally, hacking describes the process of cutting irregularly or mangling. Less formally, it represents the creative art of exploring and exploiting features of a system that were not designed (or not documented) by its makers. Hacks include both the infamous and the famous: for example, in 2008 MIT students reverse engineered the MBTA “Charlie Card” in order to demonstrate how its poor security model allows easy forgery; John T. Draper, on the other hand, figured out that the toy whistle distributed through “Captain Crunch” cereals could be easily modified to emit a 2.6KHz tone used by AT&T to maintain long-distance lines, with a resulting ability to (illegally) make “free” phone calls.

Recent hackers include well-known personalities such as Stephen Wozniak and Steve Jobs (founders of Apple), Bill Gates (co-founder of Microsoft), Tim Berners-Lee (“inventor” of the World Wide Web), Linus Torvalds (creator of the Linux kernel), and a variety of unknown or unmentionable characters. Indeed, at some level, hacking is the driving force behind some of the most creative and original research in progress.

The main objective of this course is to expose students to the history and practice of hacking, through study of relevant texts and hands-on experiences. The course will open with an intensive review of the ethical and legal foundations and limitations of hacking. It will then proceed to survey a variety of well-known hacks, studying, in as much depth as possible, the technical elements and social ramifications of each hack, all with an eye towards understanding the counter-culture in which the medium thrives. Throughout, the course will involve hands-on experimentation and communication of a relevant project.

Course Objectives
1. Develop and awareness and understanding of the hacker mindset, including its positive and negative elements.
2. Understand some of the technical content underlying various hacks through hands-on activities, including development of research skills for finding missing technical background.
3. Develop best practices for critically evaluating technology and human behavior for design loopholes and fallacious assumptions.

Course Requirements

**Required Reading (preliminary)**

Many of these texts are available free on-line or through the library:

- Technical background content available on the Internet.

**Course Website:**

All course material will be managed on a learning management system maintained and run by the instructor.

**Course Grading:**

There will be roughly 5-6 homeworks based on course content, in-class laboratory exercises, and one final project.

Relative contributions to the final grade are roughly:

- 5-6 homeworks: 40%
- 8-10 graded in-class labs: 30%
- final project: 30%

**Course Outline**

This is the first time the course is being taught in its current incarnation, so weekly content may shift (even dramatically) based on class background.

**Weeks 1 and 2. Ethics, laws, and counterculture**

Introduction to the various ethics and laws related to hacking, and the hacker view of these principles.

**Readings:**

- Texts of laws and ethical guidelines
- Cypherpunks by Julian Assange: Transcription of a discussion between some known hackers about nation-states, and the control and power of the Internet age.
- Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw-By the Man Who Did It by T. Shimomura and J. Markoff: Describes the capture of the previously mentioned hacker from law enforcement's perspective.

Weeks 3 and 4. Social Engineering
Elements of social engineering used in hacking, including perceptual, technical, cognitive, physical, and psychological tools.

Readings:

Weeks 5 - 7. Technical Fundamentals
A survey of the technical fundamentals of a variety of computer-oriented hacks, including the basics of networking and the Linux operating system.

Readings:
- Technical documentation and tutorials from the Internet.

Weeks 8 - 10. Hacking Attacks
Hacking attacks, their methodologies and implementations, including passive and fingerprinting tools, password cracking and privilege escalation, and common web-based attacks.

Readings:
- Mikko Hypponen, Policy: Governments As Malware Authors The Next Generation, Blackhat 2014.

Weeks 11 - 13. Hacking Defenses
Defenses against hacking, including technical defenses such as those based on cryptography and operating system features, and socio-legal defenses based on laws, economics, or hack-back.

Readings:

**Weeks 14 and 15. Project presentations**

Presentations of final projects in class.