Instituto Politécnico Nacional
"La Técnica al Servicio de la Patria"

CIC
Centro de Investigación en Computación

Laboratorio de Ciberseguridad

Centro de Investigación en Computación(CIC)
Instituto Politécnico Nacional - México.

Cyber security A-15

Dr. Ponciano Jorge Escamilla Ambrosio
pescamilla@cic.ipn.mx
http://www.cic.ipn.mx/~pescamilla/

Cyber security

2.3. Professional Ethics

2.5. Fair User and Ethical Hacking

Professional Ethics

- Professional ethical code (ISSA)
  - Perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles.
  - Promote generally accepted information security current best practices and standards.
  - Maintain appropriate confidentiality of proprietary or otherwise sensitive information encountered in the course of professional activities.

ISSA = Information Systems Security Association

Professional Ethics

- Professional ethical code (ISSA)
  - Discharge professional responsibilities with diligence and honesty.
  - Refrain from any activities which might constitute a conflict of interest or otherwise damage the reputation of employers, the information security profession, or the Institution.
  - Not intentionally injure or impugn the professional reputation or practice of colleagues, clients, or employers.

Ethical Challenges in InfoSec

- Misrepresentation of certifications, skills
- Abuse of privileges
- Inappropriate monitoring
- Withholding information
- Divulging information inappropriately
- Overstating issues
- Conflicts of interest
- Management / employee / client issues

Ethical Challenges – example issues

- “Consultants" who profess to offer information security consulting, but offer profoundly bad advice
- "Educators", both individuals and companies, that offer to teach information security, but provide misinformation (generally through ignorance, not intent)
- "Security Vendors", who oversell the security of their products

Ethical Challenges – example issues

- "Analysts", who oversimplify security challenges, and try to upsell additional services to naive clients
- "Legislators", who push through "from-the-hip" regulations, without thoughtful consideration of their long-term impact

Some Resource Links

- http://ethics.csc.ncsu.edu/
- http://www.ethicsweb.ca/resources/
- http://ethics.iit.edu/index.html
- http://onlineethics.org/

On the development of a personal code of ethics...

- http://www.domain-b.com/management/general/20060401_personal.html

Fair User and Ethical Hacking

Fair User and Ethical Hacking

The earliest known incidents of modern technological mischief date from 1878 and the early days of the Bell Telephone Company.

Teenage boys hired by Bell as switchboard operators intentionally misdirected and disconnected telephone calls, eavesdropped on conversations, and played a variety of other pranks on unsuspecting customers.

The term “Hack”

A kind of shortcut or modification—a way to bypass or rework the standard operation of an object or system.

The term “Hack”

- In the 1960s, the term originated with model train enthusiasts at MIT who hacked their train sets in order to modify how they worked

- Back then hacking was merely intended to quicker evaluate and improve faulty systems that had to be optimized.

Fair User and Ethical Hacking

- Hacker ethic is the generic phrase which describes the moral values and philosophy that are standard in the hacker community.
- The hacker culture and resulting philosophy originated at the Massachusetts Institute of Technology (MIT) in the 1950s and 1960s .
- The key points within this ethic are access, free information, and improvement to quality of life.

Fair User and Ethical Hacking

- Ethics is about how we ought to live. The purpose of Ethics in Information Security is not just philosophically important, it can mean the survival of a business or an industry.

Early "Hacker Ethics"

- 1984, MIT, Steven Levy, "hacker ethics"
  - 1. Access to computers - and anything which might teach you something about the way the world works - should be unlimited and total.
    - It is asserted to be a categorical imperative to remove any barriers between people and the use and understanding of any technology, no matter how large, complex, dangerous, labyrinthine, proprietary, or powerful.

Early "Hacker Ethics"

- 1984, MIT, Steven Levy, "hacker ethics"
  - 2. All information should be free.
    - Free might mean without restrictions (freedom of movement = no censorship), without control(freedom of change/evolution = no ownership or authorship, no intellectual property), or without monetary value (no cost.)

Early “Hacker Ethics”

- 1984, MIT, Steven Levy, “hacker ethics”
  - 3. Mistrust authority - promote decentralization.

    Promote decentralization. This element of the ethic shows its strong anarchistic, individualistic, and libertarian nature. Hackers have always shown distrust toward large institutions, including but not limited to the State, corporations, and computer administrative bureaucracies (the IBM 'priesthood'). Tools like the PC are said to move power away from large organizations (who use mainframes) and put them in the hands of the 'little guy' user.



4. Hackers should be judged by their hacking, not

Early “Hacker Ethics”

- 1984, MIT, Steven Levy, “hacker ethics”

  4. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.

  Nowhere is this ethos more apparent than in the strong embrace by most hackers of the levelling power of the Internet, where anonymity makes it possible for all such 'variables' about a person to remain unknown, and where their ideas must be judged on their merits alone since such contextual factors are not available.

Early "Hacker Ethics"

- 1984, MIT, Steven Levy, "hacker ethics"
  - 5. You can create art and beauty on a computer.

    Hacking is equated with artistry and creativity. Furthermore, this element of the ethos raises it to the level of philosophy (as opposed to simple pragmatism), which (at least in some quarters) is about humanity's search for the good, the true, and the beautiful.

Early “Hacker Ethics”

- 1984, MIT, Steven Levy, “hacker ethics”
  - 6. Computers can change your life for the better.

    In some ways, this last statement really is simply a corollary of the previous one. Since most of humanity desires things that are good, true, and/or beautiful, the fact that a computer can create such things would seem to mean that axiomatically it can change peoples' lives for the better.

Some more definitions

- **Phreaks** (Phone Phreakers, Blue Boxers) - These are people who attempt to use technology to explore and/or control the telephone system. Originally, this involved the use of "blue boxes" or tone generators, but as the phone company began using digital instead of electro-mechanical switches, the phreaks became more like hackers.

Some more definitions

- **Virus writers** (also, creators of Trojans, worms, logic bombs) - These are people who write code which attempts to a) reproduce itself on other systems without authorization and b) often has a side effect, whether that be to display a message, play a prank, or trash a hard drive.

Some more definitions

- **Pirates** - Piracy is sort of a non-technical matter. Originally, it involved breaking copy protection on software, and this activity was called "cracking." Nowadays, few software vendors use copy protection, but there are still various minor measures used to prevent the unauthorized duplication of software. Pirates devote themselves to thwarting these things and sharing commercial software freely with their friends.

Some more definitions

- **Cypherpunks** (cryptoanarchists) - Cypherpunks freely distribute the tools and methods for making use of strong encryption, which is basically unbreakable except by massive supercomputers. Because the NSA and FBI cannot break strong encryption (which is the basis of the PGP or Pretty Good Privacy), programs that employ it are classified as munitions, and distribution of algorithms that make use of it is a felony.

Some more definitions

- **Anarchists** - are committed to distributing illegal (or at least morally suspect) information, including but not limited to data on bombmaking, lockpicking, pornography, drug manufacturing, pirate radio, and cable and satellite TV piracy. In this parlance of the computer underground, anarchists are less likely to advocate the overthrow of government than the simple refusal to obey restrictions on distributing information.

Some more definitions

- **Cyberpunk** - usually some combination of the above, plus interest in technological self-modification, science fiction of the *Neuromancer* genre, and interest in hardware hacking and "street tech." A youth subculture in its own right, with some overlaps with the "modern primitive" and "raver" subcultures.

Two meanings of Hacker

- Traditionally, hackers like to tinker with software or electronic systems. **Hackers enjoy exploring and learning how computer systems operate.** They love discovering new ways to work — both mechanically and electronically.
- In recent years, hacker has taken on a new meaning — someone who maliciously breaks into systems for personal gain. Technically, these criminals are *crackers* (criminal hackers). **Crackers break into, or crack, systems with malicious intent.** The personal gain they seek could be fame, profit, and even revenge. They modify, delete, and steal critical information, often making other people miserable.

Hacker

- **Hackers** (or external attackers) try to compromise computers and sensitive information for ill-gotten gains — usually from the outside — as unauthorized users.
- Hackers go for almost any system they think they can compromise. Some prefer prestigious, well-protected systems, but hacking into anyone's system increases an attacker's status in hacker circles.

Malicious users

- **Malicious users** (or internal attackers) try to compromise computers and sensitive information from the inside as authorized and “trusted” users.
- Malicious users go for systems they believe they can compromise for ill-gotten gains or revenge.

Ethical Hackers

- **Ethical hackers** (or good guys) hack systems to discover vulnerabilities to protect against unauthorized access, abuse, and misuse.
- Information security “researchers” typically fall into this category.

Ethical Hacking

- Encompasses formal and methodical penetration testing, white hat hacking, and vulnerability testing — involves the same tools, tricks, and techniques that criminal hackers use, but with one major difference: **Ethical hacking is performed with the target's permission in a professional setting.**

Ethical Hacking

- The intent of ethical hacking is to discover vulnerabilities from a malicious attacker's viewpoint to better secure systems.
- Ethical hacking is part of an overall information risk management program that allows for ongoing security improvements.
- Ethical hacking can also ensure that vendors' claims about the security of their products are legitimate.

Modern Hacker Ethic

- **"Above all else, do no harm"** Do not damage computers or data if at all possible. Much like the key element of the Hippocratic Oath.
- **Protect Privacy** People have a right to privacy, which means control over their own personal (or even familial) information.

http://www2.fiu.edu/~mizrachs/hackethic.html

Modern Hacker Ethic

- **"Waste not, want not."** Computer resources should not lie idle and wasted. It's ethically wrong to keep people out of systems when they could be using them during idle time.
- **Exceed Limitations** Hacking is about the continual transcendence of problem limitations.

Modern Hacker Ethic

- **The Communicational Imperative** People have the right to communicate and associate with their peers freely. The United Nations International Telecommunications Union (ITU) has stated in many conferences that this should be a fundamental human right, with which no nation should ever interfere.

Modern Hacker Ethic

- **Leave No Traces** Don't leave a trail or trace of your presence; don't call attention to yourself or your exploits. Keep quiet, so everyone can enjoy what you have. This is an ethical principle, in that the hacker follows it not only for his own self-interest, but also to protect other hackers from being caught or losing access.

Modern Hacker Ethic

- **Share!** Information increases in value by sharing it with the maximum number of people; don't hoard, don't hide. Just because it wants to be free, does not mean necessarily you must give it to as many people as possible.

Modern Hacker Ethic

- **Self Defense** against a Cyberpunk Future
  Hacking and viruses are necessary to protect people from a possible 1984/cyberpunk dystopian future, or even in the present from the growing power of government and corporations.

Modern Hacker Ethic

- **Hacking Helps Security** This could be called the "Tiger team ethic": it is useful and courteous to find security holes, and then tell people how to fix them. Hacking is a positive force, because it shows people how to mend weak security, or in some cases to recognize and accept that total security is unattainable, without drastic sacrifice.

Modern Hacker Ethic

- **Trust, but Test!** You must constantly test the integrity of systems and find ways to improve them. Do not leave their maintenance and schematics to others; understand fully the systems you use or which affect you.

In short, the new hacker ethic suggests that it is the ethical duty of new hackers to : 1) protect data and hardware 2) respect and protect privacy 3) utilize what is being wasted by others 4) exceed unnecessary restrictions 5) promote peoples' right to communicate 6) leave no traces 7) share data and software 8) be vigilant against cyber-tyranny and 9) test security and system integrity of computer systems.

Certified Ethical Hacker (C|EH)

- www.eccouncil.org
- C|EH certification has become a well-known and respected certification in the industry.
- Accredited by the American National Standards Institute (ANSI 17024)

Colour-Coded Hacking

- White hackers
  - A so-called “white-hat” will inform an organisation if a security weakness is found in that organisation’s systems.
- Grey hackers
  - Often, they act on the spur of the moment. Depending on the situation, they might exploit or warn an organisation if a weakness is found in their system.
- Black hackers
  - These will act to exploit any weakness in a network or an organisation’s systems for gain. This could mean collecting and selling intellectual property or personal information.

Hacktivism

- Hacktivism is the term used to describe hacking activity that's typically for political and social purposes, attacking corporations, governments, organizations and individuals.
- Hacktivist groups may deface websites, redirect traffic, launch denial-of-service attacks and steal information to make their point.

Hacktivism

- A hacktivist group dominated headlines in 2011 with attacks on Sony, PBS, the U.S. Senate, the CIA, FBI affiliate InfraGard and others.
- Another group released 90,000 email addresses of U.S. military personnel in an attack on a federal government contractor.

Hack Attacks

- Distributed Denial of Service or DDoS
  - Simply, this involves hackers overloading a site's server with too many requests.
- Website hacking
  - This involves hackers bypassing the security parameters of a website, gaining access to its administrator panel, then adding or removing information (e.g. adding a page that carries a personal message from the hacker, or adding sexually explicit images on a site's landing pages).

Hack Attacks Examples

- Stuxnet
  - This highly sophisticated computer worm infection infiltrated systems in Iranian nuclear plants, halting scheduled operations between June and September.

Ethical Hacking vs. Unethical Hacking

- **Ethical Hacking:** Ethical hacking is always carried out by ethical hacker (or the so-called "white hat"). Ethical hackers are a gang of computer security expert who "specializes in penetration testing and in other testing methodologies to ensure the security of an organization's information systems“.
- These ethical hackers "have the ability to harm your system but they chose to make the choice to help uncover security failings in your system and then help you to find ways to protect your company from other hackers" .

Ethical Hacking vs. Unethical Hacking

- For ethical hackers, they will only hack and test on a system when they are authorized by the owner of the system in order to find a security flaws or to detect the cause after an attack. ethical hackers always do the hacking work under the permission of the system's owner. They will only hack as deep as the owner of the system specifies. For ethical hacking, it will be helpful to find out the system security holes, potential system vulnerabilities and the fact that whether a system is under attack.

Ethical Hacking vs. Unethical Hacking

- **Unethical Hacking:** Unethical hacking is a malicious hacking activity carried out by malicious hacker. Malicious hackers are also a group of computer security experts but their general purpose for hacking is to steal secret information from a system, corrupt a system or leave back doors to a compromised system in order for the future access.

Ethical Hacking vs. Unethical Hacking

- **Unethical Hacking:** For malicious hacking, the hackers are not authorized to access the information that they grab from the system. Malicious hacking may cause unpredictable economical loss to a corporation since the business strategy and product information stolen. So, here is the other point, malicious hackers carry out malicious hacking without the permission and authorization from the owner of the system.

Hacking remarks

There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again.

—FBI Director Robert Mueller RSA conference (March 1, 2012).

Hacking remarks

The attack surfaces for adversaries to get on the Internet now include all those mobile devices. The mobile security situation lags. It's far behind.

—Army Gen. Keith Alexander, Director of National Security Agency and Commander of U.S. Cyber Command DEF CON 20 (July 27, 2012).