

ETHICS OF

HACKING

&

CRACKING

What are ethics?

- It is **impractical to have laws** to describe all forms of acceptable behaviour in society. Instead, we rely on **ethics** to prescribe **generally accepted standards of proper behaviour**.
- An ethic is a **standard of right and wrong** defined by societal norms.
- **Subject to change** with change in the times.

Need and Importance of Ethics in Computer Science

The field of Computer Science hasn't yet faced consequences at a massive scale.

Events that changed how people approached the fields.

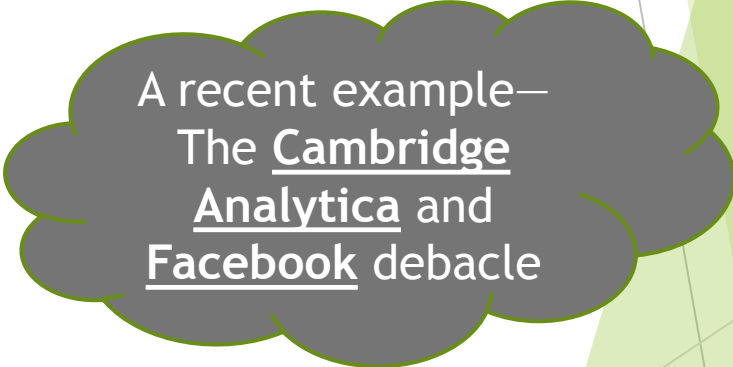
- Chemistry -> Dynamite & Chemical Weapons
- Physics -> Atomic Bomb
- Civil engineering -> Bridge collapses etc



- Before these, “hope” and “optimism” dominated and drove all kinds of innovation.
- After these, everyone became aware of the potentially destructive nature.

There hasn't been a particularly noteworthy event that seared the importance of **ETHICS** and consequences in computer science!

Young professionals(especially engineers) often see ethics as a speciality -something that need not be worried about too much. The **primary goal is to code and create and change the world, with no thought to the possible disruption or moral consequences.**



A recent example—
The Cambridge Analytica and Facebook debacle

However, in a field as relatively young as Computer Science—
You can NEVER stop thinking about how your work might be used and its possible consequences.

Hacking vs Cracking

Both have extensive knowledge of the working of a computer system/network. The **difference** lies in their **interests**.

Hackers identify flaws in security systems and work to improve upon them on behalf of an organisation.
(**white hats**)



Crackers use flaws in security systems as advantage to break into private data systems for personal gain.
(**black hats**)

Ethics of Hacking: A Case Study



This is Gun-gun, a computer security consultant.

In her spare time she,

1. **Attacks commercial products** for vulnerabilities and finding flaws.
2. Probes accessible sites on the Internet, **finds vulnerabilities and contacts owners** to offer her services in fixing the problems.
3. Being a pastry lover, **plants programs to slow performances** in the web sites of pastry shops that do not use good quality butter in their pastries.

1. Vulnerabilities in Commercial Products

Top **priority is given to users'** interests. Not attacker, vulnerability finder or vendor.
Options available to vendor are

- Full disclosure
- Partial disclosure
- No disclosure

2. Searching for Vulnerabilities & Customers

On the positive side, Gun-gun may **find and fix major vulnerabilities**.

On the negative side, there is a **risk of system failure** caused by Gun-gun's probing for vulnerabilities.

The *ethical* question posed is

Which is greater --the potential for good or harm?

3. Attacks based on personal views

- Is there a **universal appreciation** for butter in pastry-making?
- Is the good-ness of using butter to make pastries greater than the **good-ness of virtues** like honesty and fairness?
- Is it fair to harm others just because they **disagree** with us?

The answer **almost always** is ----- **NO.**

Ethical questions related to Cracking

Cracking is defended as a completely acceptable practise because lack of protection means that the owners of systems do not really value them.

The fallacy in this logic is made clear by the following analogy:

Most people would never find it acceptable to walk down a street, trying every door to find an unlocked one. Then enter the house and look around all the rooms and search through the drawers. It would be considered a criminal act even if no harm was done.

UNIX / LINUX

Security

Design Concepts:

Permissions

All files in a typical Unix-style filesystem have permissions set enabling different access to a file.

User Groups

This enables users to be grouped by the level of access they have to this system.

Root Access

Most Unix and Unix-like systems have an account or group which enables a user to exact complete control over the system.

User and Administrative Techniques:

1. Passwords

Unix security. In Unix systems, the essential information about users is stored under the file `/etc/passwd`. This file keeps track of the users registered in the system and their main definitions. Passwords, or more correctly, the hash of the password, can also be stored in the same place.

2. Users and Accounts

Administrators should delete old accounts promptly.
Su, sudo, ssh only , no remote root logins.

Software Maintenance:

Patching

Patching the operating system in a secure manner requires that the software come from a trustworthy source and not have been altered since it was packaged.

Source Distributions

Source distributions include the ability to examine the code for suspicious content.

RPM Packages

Linux distributions which use the RPM Package Manager format for providing base functionality and software updates make use of MD5 and GPG to ensure content integrity.

Debian Packages

Linux distributions which use the Debian.deb package format for providing base functionality and software updates make use of GPG signatures to ensure content integrity

File Systems:

1. File System Security

File system security within UNIX and Unix-like systems is based on 9 permission bits, set user and group ID bits, and the sticky bits for a total of 12 bits. These permissions apply almost equally to all filesystem objects such as files, directories and devices.

2. Root Squash

Root squash is a reduction of the access rights for the remote superuser (root) when using identity authentication (local user is the same as remote user). It is primarily a feature of NFS but may be available on other systems as well.

SELinux

SELinux is the set of kernel extensions to control access more precisely, strictly defining both if and how files, folders, network ports and other resources can be accessed by the confined process. This system is mostly used to restrict processes (database, server) rather than human users. It can also limit processes that run as root. Other distributions use comparable alternatives like AppArmor.

Viruses and Virus Scanners

Unix-like operating systems are immune to most Microsoft Windows viruses because binaries created to run on Windows generally won't run on other platforms.

Firewalls

Network Firewall protects systems and networks from network threats which exist on the opposite side of the firewall. Firewalls can block access to strictly internal services, unwanted users and in some cases filter network traffic by content.

Vulnerabilities in Windows 2000/xp/2003

- Passwords
- Default account
- File sharing
- RPC SERVICE FAILURE
- TELNET service
- IP fragments reassembly

Passwords as vulnerabilities

- ▶ The easiest way to break the password in windows 2000 or later is to use password burning program - which can set the admin password to blank
- ▶ Windows 2000 and later store the password in the form of hash values in a data base called SAM(SECURITY ACCOUNTS MANAGER)

os locks the SAM database which makes it difficult for access it from inside , nevertheless hackers are able to crack the password using password cracking tools

- ▶ A program name pwdump3 gives remote access to SAM database in computer in which SYSKEY(128 -bit algorithm) utility is active , however person need to have admin priviliges on the target computer

Default accounts

- ▶ Win2000 makes a default account named 'administrator', by default the password is blank. Nobody can delete this account, but it is possible to change password at the time of installation
- ▶ To acquire access to a target computer that is running, hackers attempt to access account named administrator, user can change the name to minimize the vulnerability
- ▶ By changing the username, makes hackers life more difficult as they have to think for both username and password

File sharing

- ▶ The default setting for sharing over network is “all access” so there is a definite risk , full control can allow other users to fabricate the file or modify it as they want to , access can be restricted based on user or group for the sake of maintaining security , it is important to leave access rights rather than leaving it at default settings

RPC service failure

- ▶ The remote procedure call service of windows system does not validate the inputs that are submitted to its processing . This vulnerability permits hacker to deny legitimate services of the system to users
- ▶ Hackers can easily send RPC requests with invalid inputs to computer , when computer receives invalid inputs, the os processes it and depending on their nature, invalid inputs lead to system services stopping for the period of time

Telnet Vulnerabilities

- ▶ The telnet service of win2000 os lets user to access commands that can cause denial of service
- ▶ Hackers can use this feature to perform denial of service attacks against the telnet services
- ▶ another vulnerability is that it can help the unauthorized user to access the target computer ,telnet generates a named pipe , it uses that for initialization process , however if telnet finds existing pipe than it uses existing one for initialization, vulnerability in this process is that hackers can predict the name of the pipe and can replace it with new pipe with some specific malicious code which can help them access to target system remotely

IP fragments reassembly

- ▶ A bug in the windows 2000 code component that handles the reassembly of the ip fragments causes the target system to spend all the cpu time to process ip packets that have been modified by hackers , the processing of such packets can deny the services of the system for some time , in some critical stages it can even cause a system to crash
- ▶ This vulnerability can be minimized by the use of firewalls and proxy