Computing as a profession

Roles

The Computer Science discipline provides a scientific foundation for topics such as computer design, programming, information processing and algorithmic solutions.

The field of Computer Science is ever-expanding and so are the many roles and responsibilities for a Computer Scientist. There are many specialized disciplines within Computer Science and computer scientists work in a wide variety of industries from pharmaceutical to finance. Regardless of the discipline or field, computer science professionals will need technical, cognitive and leadership skills.

Because of their roles in developing software systems, software engineers have significant opportunities to do good or cause harm, to enable others to do good or cause harm, or to influence others to do good or cause harm. (https://ethics.acm.org/code-of-ethics/software-engineering-code/)

Contributing to their domain computer scientists undertake; applied, theoretical, practical and technical tasks.

A few of the available roles for a computer scientist are; Applications developer, Cybersecurity analyst, Data analyst, Database administrator, Games developer, IT consultant, Software engineer or Web developer.

New fields and trends in computer science are emerging all the time and along with them come new roles.

Responsibility's

Computer Scientists have responsibilities to a number of bodies including the; public, product, employer, self and profession.

Challenges and threats

New technologies have always ushered in new threats and challenges.

In the 19th century, the advance of new textiles machines meant the many skilled textile workers were being replaced by machines that could be operated by a small number of unskilled workers. A formation of textile workers called the Luddites rebelled against the machines and tried to stop their introduction. Inevitably they could not stop the march of the industrial revolution and many of those who tried to where executed.

Once a technology has been introduced to the world it is all but impossible to stop. This idea is very relevant to the many developments in Computer Science such as Big Data and Cloud computing and perhaps most frightening; Artificial Intelligence.

Ethics

Many questions in Computer Science are ethical, for example:

- Should websites that host other people's content be the responsibility of the site owner?
- Is it a good thing for machines to replace jobs that previously required human intervention?

- Should private data be handed to governments if they think it could help prevent crime?
- Should social media platforms allow freedom of speech if that enables the bullying of vulnerable users?

Some of the most recent technology advances have raised new issues:

Cloud computing – Can you ensure that users data is kept secure on machines you will never see?

Mobile Computing – Constant access to work emails breaks down the work-life barriers.

Artificial Intelligence – Should artificial intelligence be used to makes decisions where there was previously human intervention?

Cybersecurity

Computers connected to any network are potentially at risk of cybercrime.

Cybersecurity is the study of how to protect computers from such cybercrime.

A number of cyber-attacks are committed by running malicious software on a computer. Among these types of attack are:

- Viruses – software that inserts itself in existing applications on a computer. When the application is run so is the virus along with it.
- Worms – Programs that traverse through networks spreading through connected machines
- Trojan Horse – A program that disguises itself as a desirable application
- Spyware – Software that collects information from an infected PC and transfers it to the attacker

As well as cybercrimes that are executed on by running software on a computer there are types of attack which are run externally and attack over a network.

Such attacks include

- Denial of Service – Attacks which involve overwhelming a server with messages so it cannot operate correctly. A variant of this attack is the Distributed Denial of Service attack where the attack software first spread like a worm to sit in waiting on infected PC's before being invoked and all running synchronously to attack the target.
- Spam and phishing attacks. These attacks involve sending messages to people instead of machines to attempt to overwhelm them or trick them into providing information.

Protection from cybercrime

There are a number of protections that can be used to help protect against cybercrime. It is important to note that these are preventative measures and need to be in place before a cyber-attack.

A firewall can be installed on a network to filter messages in and out of the network by doing so they can stop messages from entering the network

Proxy servers can be used to hide the details of a network by routing all traffic through its interface.

Anti-virus software can be installed on computers to identify and remove malware

Cryptography

Cryptography is a method of protecting messages through the use of codes that obfuscate the message in the eyes of all but the recipient. Data transferred that is not encrypted using cryptography can be easily read and therefore expose sensitive information such as passwords.

Nowadays cryptography is commonly used to protect data transferred over networks. The HTPPS protocol demands all HTTPS data to be encrypted.

Keys are used in encryption to encrypt and decrypt data.

Only by knowing the appropriate key can you encrypt and decrypt a message for the given protocol. Encryptions keys are of a chosen length. Brute force can be used to obtain a key by attempting all possible combinations.

Two popular encryption methods are public-private key encryption and symmetric key encryption. Both have positive and negative attributes,

Symmetric key encryption is faster than public-private key encryption but both sides need to know the key for messages to be transferred. Therefore transferring the key without another method of encryption means the key can be intercepted and then the following messages left exposed.

Public-private key encryption is a slower technique.

Social impact of database technology

Database technology makes access to meaningful insight easier than ever. Newer practices such as Big data can provide insight to political parties, law enforcement and other bodies. This insight grants a level of power that can be used to shape society. What's more data collection is not always obvious or avoidable.

Professional ethics and code of conduct

British Computer Society

The BCS aims to promote the study and application of computing technology and advance the knowledge of professionals for their own and society benefit.

There are four key principles to the BCS code of conduct.

- Public Interest – Members should have due regard for public health. Members should abide by relevant laws and should not discriminate against others.
- Professional competence and integrity – Members should only undertake work within their level of competence. Developers should always aim to improve their skills. Developers should reject bribery.
- Duty to relevant authority's – Members should follow the law of relevant authority's and should accept responsibility for their actions.
- Duty to the profession – Members should uphold the reputation of the profession. Members should seek to improve professional standards and should act with integrity.

The role of law

Laws can provide legal recourse against cybercrime, but in themselves cannot prevent the crime.

Cybercrime

The international nature of cybercrime makes prosecution of criminals difficult as the attackers may launch attacks in other countries.

The right to cyber privacy is a contentious issue in law. While it is generally agreed that users have the right to privacy, there are many cases where this does not apply. For example, employees have a legal right to monitor the usage of their equipment.

Removing people's right to privacy can be seen as creating a big brother state, but on the other hand, transparency can make it easier to prevent crime. A reduction in rights in the name of protection has been common throughout history and it is worth bearing in mind it has been used to consolidate power.