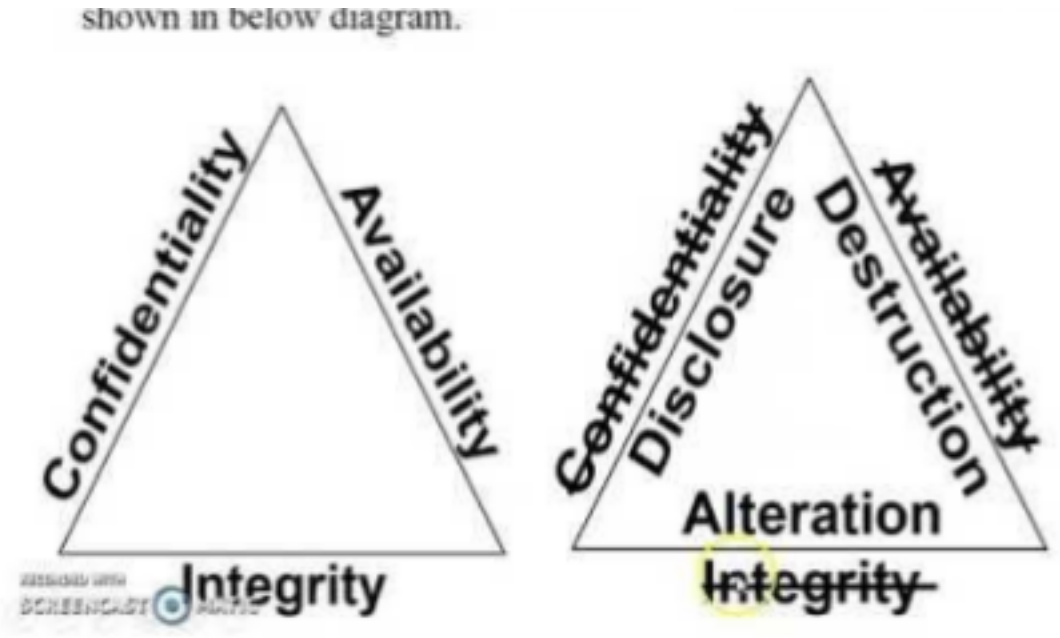
Basic Understanding

White hats, Good guys, Ethical hackers
Black Hats, Bad guys, Malicious hackers
Gray Hats, Good or bad hacker, depends on the situation

Security consists of four basic elements

1. Confidentiality
2. Authenticity
3. Integrity
4. Availability

A hackers goal is to exploit vulnerabilities in a system or network to find a weakness in one or more of the four elements of security



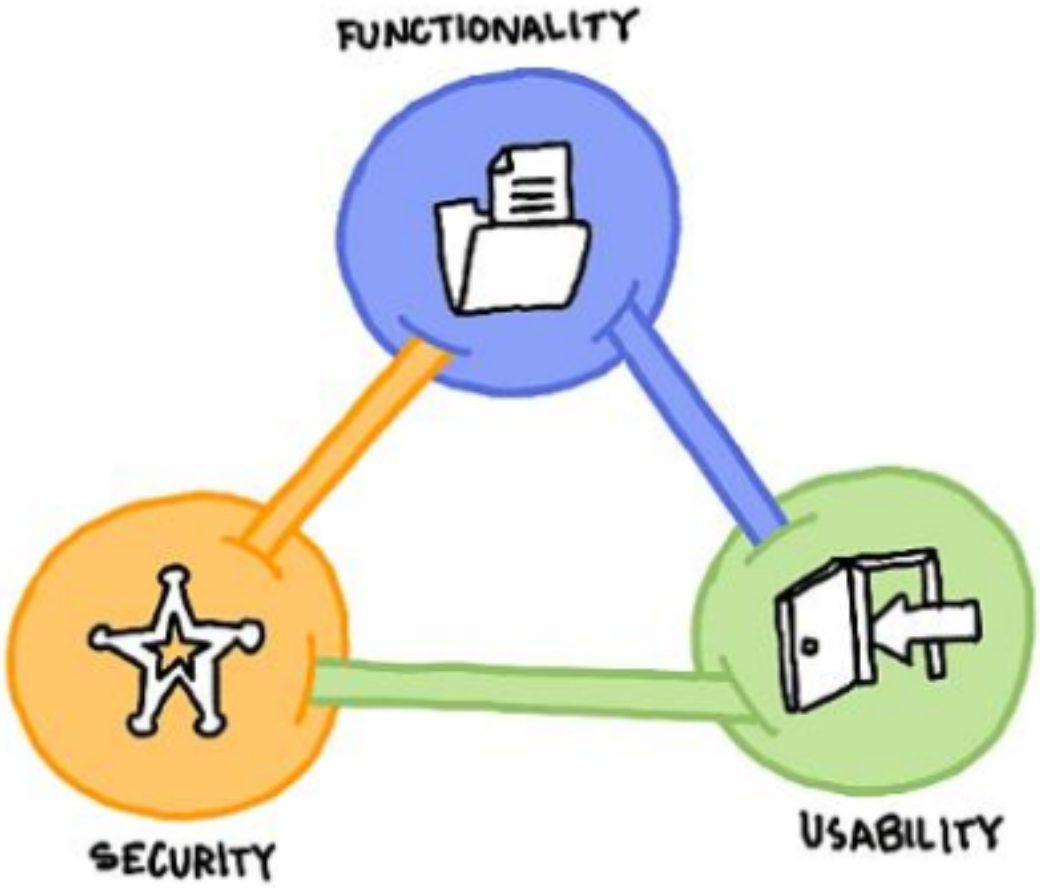
For example,

Confidentiality keeping systems and data from being accessed, seen, read, to anyone who is not authorized to do so.

Integrity. Protect the data from modification or deletion by unauthorized parties and ensuring that when authorized people make changes that shouldn't have been made the damage can be undone.

Availablity, Systems, access channels and authentication mechanisms must all be working properly for the information they provide and protect to be available when needed.

Ethical Hacking involves the hacking tools, tricks, techniques to identify vulnerabilities and ensure system security.



There is an inter dependency between these three atttributes. When security goes up, usability and funcationality come down.

The most hacking tools exploit weakness in one of the following four areas:

1. *Operating systems*, Many sys admins install OS with the default settings, resulting in potential vulnerabilities that remain unpatches.
2. *Applications*, usually aren't thoroughly tested for vulnerabilities when developers are writing the code, which can leave many programming flaws that a hacker can exploit.
3. *Shrink-Wrap Code*, many off the shelf programs come with extra features the common user isn't aware of, and these features can be used to exploit the system.
4. Misconfigurations, Systems can also be misconfigured or left at the lowest common security settings to increase ease of use for the user, this may result in vulnerability and an attack.