Security:
It's hard to measure.
We hear of security features when they fail, not when they work.
Situation dependent. No universal approach.
Evaluation of tradeoffs.
Has costs. Open costs: locks, fences. Hidden costs: locking the door requires you to carry a key.
Both a feeling and reality.

"Security is about preventing adverse consequences from the intentional and unwarranted actions of others"

A security system is designed to prevent these adverse consequences. Lock on door.

Prevention:
Technology: metal detector, authentication systems.
People: military, guards.
Systems can be attacked and used for their flaws.

Protection against unintentional acts is "safety" not "security".

Safety is often more important. Accidents, thoughtlessness etc. Weak password.

Unwarranted actions are not justified or authorized. Doesn't have to be illegal, can be immoral.

Attacker:
Attackers have values
Attacks are ways to break the security of the system or a component of the system.
The objects of the attacks are assets.

Five step program:
What assets are you trying to protect?
What are the risks to those assets?
How well does the security solution mitigate those risks?
What other risks does the security solution cause? (Unintended consequences)
What costs and trade-offs does the security solution impose? (Balance pros and cons)

Trade offs are subjective.
How do we protect against air plane hijackings? Ground all the air planes. Doesn't really work.

A threat is a way an attacker can attack a system.
Risk is often calculated R = F * C which means likelihood * consequence.
If you suffer loss 500kr every 2 years. R = 0.5 * 500 = 250kr.
Also: Risk = Threat x Vulnerability x Asset

Agenda - why an attacker do something. Moral gain? Economical gain? White hat, black hat, grey hat.

Why wasn't lighters and tobacco banned from air planes when tweezers were? Tobacco lobby is stronger, has more money.

Security policy:
Who is authorized to do what?
Policies govern the security levels chosen by management   Based on risk analysis
  Policy says what is, and is not, allowed
  This defines "security" for the site/system/etc.
  Mechanisms enforce policies

If policies conflict, discrepancies may create security vulnerabilities

Important when writing policies

No attackers? —> No security problem. A security problem needs two players.

Proxy: someone who acts on the behalf of someone else.

Security theatre. The feeling of security vs actual security.

Externality: when security doesn't make financial sense. If the security system is going to work, there must be NO externality.

Security is a state of mind, security is a process, it is not a product

All security involve trade-offs, trade-offs are subjective

Risk = likelihood x consequences

Everybody makes those trade-offs differently esp. proxies

Externalities explain much of why security is the way it is

Traditionally, security deals with these actions:

Prevention (e.g., locks on doors)

Detection (e.g., burglar alarms)

Response/recovery (e.g., dial 911, replace locks)

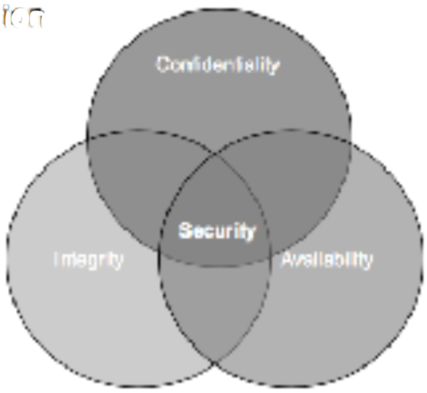
"Computer security deals with the prevention and detection of unauthorized actions by users of a computer system."

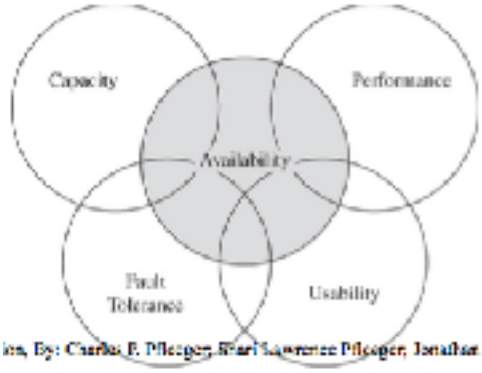
"Computer security is the protection of the items you value, called the assets of a computer or computer system."

Must be maintained in case of intentional and unwarranted actions:
Confidentiality: Data. Who can access, how can access and what can access.
Integrity: Data, systems, services. Make sure data is just the way it is supposed to be.
Availability: -II-
Accountability: actions. Be able to ensure who did what.
Nonrepudiation: actions. Ability to tell if something happened.
Reliability: systems, services. Must be able to function correctly. Manage accidental failures.

CIA Triad - security triad
Confidentiality: Prevention of unauthorised disclosure of information
Only authorized people or systems can access protected data
Keeping data and resources "hidden"
A good example is cryptography
Integrity: Prevention of unauthorised modification of information
Data integrity (integrity)
Origin integrity (authentication)
Availability: Prevention of (unauthorised) withholding of information or resources
Enabling access to data and resources
In other computer science area this property relate to "quality of service"

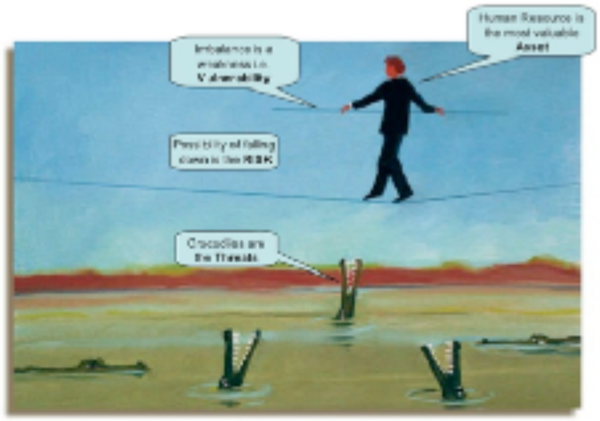
CIA is a balance of the terms.





ion, By: Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan

Computer security seeks to prevent unauthorized viewing (confidentiality) or modification (integrity) of data while preserving access (availability).


Imbalance is a weakness i.e. Vulnerability
Human Resource is the most valuable Asset
Possibility of falling down is the RISK
Crocodiles are the Threats

Risk analysis:
1. Identify the assets to protect
2. Find the threats for each asset
3. Prioritize each of these risks (asset x vulnerability x threat)

4. Implement controls for each risk, or accept it
5. Monitor the effectiveness of these controls and re- iterate

1. Fire stations
    1. Safety: set the proper number of fire station in a town
    2. Security: a pyromaniac set more fires than fire station can handle
2. Knives
    1. Safety: accidentally left knives in a luggage
    2. Security: an attacker try to sneak a knives fabricated in a material hard to detect
3. Fire exits
    1. Safety: calculate the right number of fire exits
    2. Security: attackers barricade fire exits

Passive failure
When they fail to prevent the unwanted action
The lock is successfully picked
Active failure
When they activate and stop wanted action
The lock jams and now you can't get in even though you have the key

To get digital identities (or non digital personal information) to access cyber systems
Social Engineering   Phishing
Pharming
Trojan
Spyware
Keylogging
Spoofing
Man in the middle   Vishing
Trashing
To disrupt services
Botnet
Warm
APT
DDoS

Systems are the source of many problems
Whether we attack them or try to use them to protect us
Without them we would be a lot more secure, but less happy...
The tripple 'a' – assets, attackers, attacks
Attackers – Know what types there are and guess who will be the most interesting for you application
Motives, opportunity, funding etc.
Attacks – Bad things are mostly the same but there are constantly new ways of bringing them about
Even though most attackers can't figure out a new way, once it's out there they can follow directions

Also hard to   Keep
Many criminals get caught because they brag   Generate
What's a “random” key?   Destroy
You can't tell when someone's copied it
But change the default password, safe combination etc. as these aren't really “secret” at all

Technology creates imbalances that usually favour the attacker

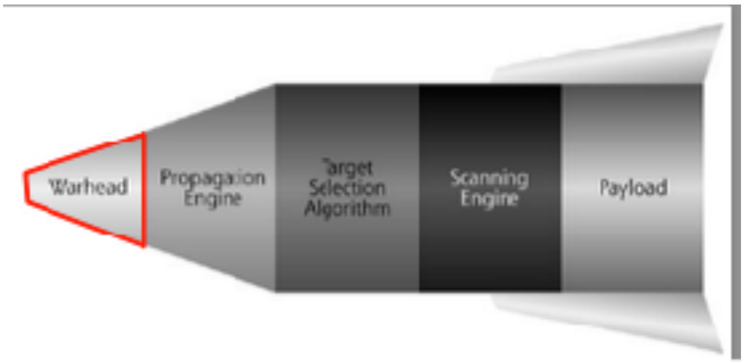
However, we can't do without

Security is a weakest link problem

Employ defence in depth, compartmentalization and choke points

A systems that fails badly is said to be brittle

Automation, static nature, having unnecessary secrets is bad – dynamic, heterogeneous and flexible is good.



Warhead - vulnerability to breaking in to a system - buffer overflow - email - file sharing

Propagation engine - way to transfer the rest of the worm / body to the target

Target selection algorithm - looking for new computers to infect

Scanning engine - looking for vulnerabilities in those targets

Payload - action on behalf of the attacker

there are various ways for an attacker to get malicious code to execute on remote computers

A virus ... self-replicating piece of code ... attaches itself to other programs ... requires human interaction to propagate

A worm ... self-replicating piece of code ... spreads via networks and ... doesn't require human interaction to propagate

A backdoor ... allows attackers to bypass normal security controls on a system, gaining access on the attacker's own terms

A Trojan horse ... appears to have some useful or benign purpose, ... masks some hidden malicious functionality¨

Emanation: the sound / electro magnetic radiation of something

1. The access points broadcast its availability by sending a beacon (invitation to connect)
2. A device responds with a request to authenticate, which the access point accepts
3. The device request establishment of an association which the access point negotiates and accepts.

In 1 anyone can reply to this invitations.

In 2 the authentication is not rigorous specially in open wifi (accept all).

In 3 any device can be accepted.

Lucky for us, We can counter these attacks at any of these steps