Overview

- Concepts of CIA: confidentiality, integrity, and availability
- Confidentiality: concealment of information
  - The need arises from sensitive fields (military, industry)
  - Examples: encryption (protect the key), access control, existence of the data, resource hiding (configuration, google 1.7 – 2.4 M servers.)
- Integrity: prevent unauthorized or improper changes, is directly related to trustworthiness of data and sources
  - Include data integrity and origin integrity (has impact on trust), therefore, related to credibility
  - Prevention:
    - prevent unauthorized changes
    - changes in unauthorized ways
  - Detection
    - Report integrity violation (confine dirty data??)

Overview

- Concepts of CIA: confidentiality, integrity, and availability (continued)
- Availability: ability to use the data or resources
  - Example of highway
  - DoS or DDoS attacks (SMS for cell phone)
  - Very difficult to detect
    - Is it attack or we are unlucky today
    - Attacker will mess with the security methods as well (packet tracing)

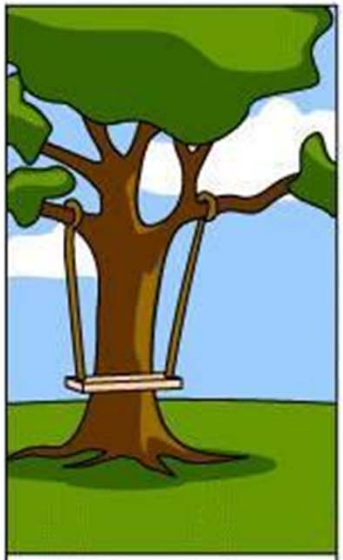
- Threats:
  - A potential violation of security (not necessarily occur at this moment).
    - The actions that cause such violations are called attacks.
    - 4 classes of threats:
      - Disclosure: unauthorized access to data
      - Deception: acceptance of false data
      - Disruption: interruption or prevention of correct operation
      - Usurpation: unauthorized control of the system

- Examples of threats:
  - Snooping: unauthorized interception, is a kind of disclosure (eavesdrop on wireless). Countered by confidentiality or other information hiding methods.
  - Modification: unauthorized change of data, may lead to deception, disruption, and usurpation. Countered by integrity.
  - Spoofing: impersonation, may lead to deception and usurpation. Countered by integrity.
    - Difference b/w impersonation and delegation
  - Denial of receipt or origin: is a kind of deception
    - Interesting questions: simultaneous contract signing

- Policy and mechanism
  - Policy is a statement of what is and what is not allowed.
    - Can be presented formally (in mathematical way)
    - Can be described in plain English
    - When two communicating parties have different policies, they may need to compromise (example b/w univ. and industry)
  - Mechanism is a method to enforce a policy.
    - May impact the system performance
    - Prevention: to fail an attack
    - Detection
    - Recovery: fix not only data, but also vulnerabilities
    - Tolerance

- Assumptions:
  - Security rests on assumptions of the required security and application environments
  - Assumptions of a security policy
    - A policy can correctly and unambiguously partitions system states into secure and insecure
    - A security mechanism will prevent a system from entering a insecure state
    - Define a security mechanism as secure, precise, or broad (the example of highway)
    - In real life, security mechanisms are usually broad (Why?)

How the customer explained it

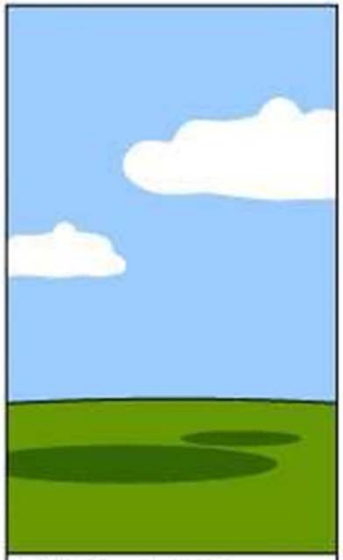


How the Project Leader understood it

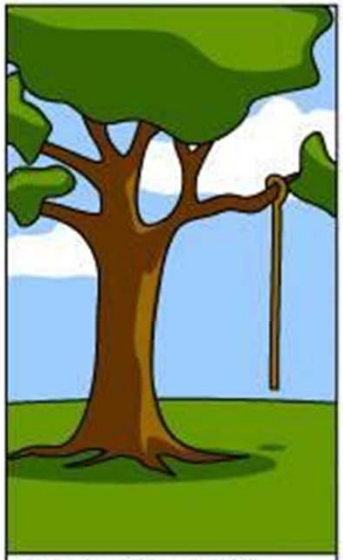
How the Analyst designed it

How the Programmer wrote it

How the Business Consultant described it

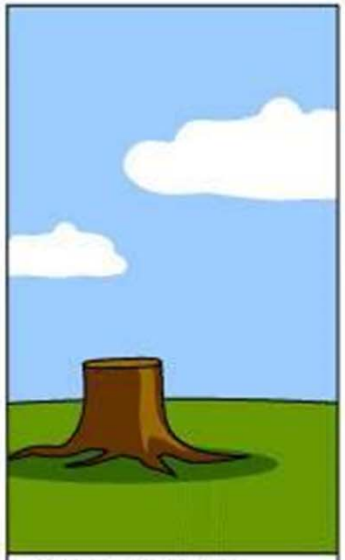


How the project was documented



What operations installed

How the customer was billed



How it was supported

What the customer really needed

- Operational issues:
  - An isolated PC will not be attacked through network, but it cannot access network either
  - We must balance the benefit of protection against the cost of designing, implementation, and usage of a system
  - Cost-benefit analysis:
    - Protect data or regenerated data? Which is cheaper?
    - There are after-impacts as well. (view of company?)

- Operational issues (continued):
  - Risk analysis:
    - We must understand the kinds and levels of threats, and their likelihood to happen to determine the levels of protection
    - Risk is a function of environment
    - Risk changes with time
    - Low probability attacks still exist
    - You must act on the analysis results

- Human issues:
  - Get the security tools from right hands, and put them into right hands
  - Organizational issues:
    - Security does not directly generate profit, but reduce potential losses
    - It often reduces performance
    - Power and responsibility must be properly linked
    - Shortage in people and resources

- Human issues (continued):
  - People issues:
    - People is heart of any security system
    - Attacks from outsider and insiders
    - Under trained workers and administrators
    - Social engineering based break-ins (in a bar at SV you can learn a lot)
    - The problem of misconfiguration (Example of SigComm)