Definition of Terms

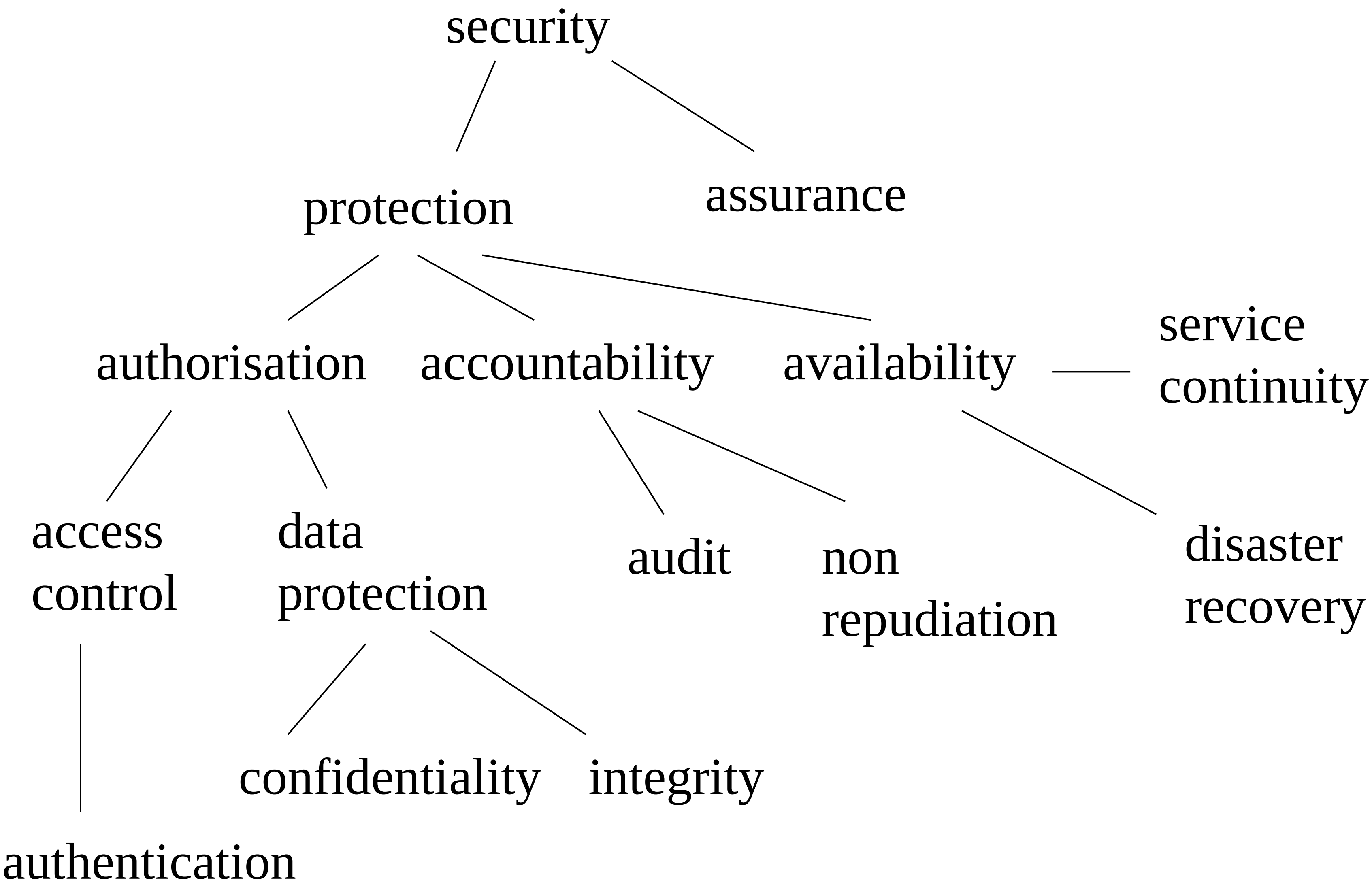
Definitions

- Collins Dictionary :-
- Secure
  - 1. Freedom from danger, damage etc.
  - 2. Free from worry, care, etc.
- Computer Security - Safety and freedom from worry when using a computer.

Alternative Definitions

- “Security is confidentiality, integrity and availability.”
- “Security is identification and authenticity, access control, audit and assurance.”

- Really security is what you get as a result of the above.



security

protection

assurance

authorisation

accountability

availability

service continuity

access control

data protection

audit

non repudiation

disaster recovery

confidentiality

integrity

authentication

Security - Safety

- Safety is provided by protection.
- Protection provided by a series of mechanisms (or countermeasures) designed to prevent a threat.
- Three main kinds of protection
  - authorization
  - accountability
  - availability

Authorisation

- User can not break the rules.
- Resources protected by authorization rules are called protected resources.

- Two categories of authorisation mechanisms:-
  - Access Control
  - Data Protection

Authorisation - Access Control

- Used in environments where it is feasible and practical to run a program to check if rules are being followed.
- Heavily dependent on authentication, i.e. being sure that someone is who they claim to be.
- Authentication for Access control often supported using user name and password.

Authorisation – Data Protection

- When it is not possible/practical to run a program to check if rules are being followed.
- For example, data over a telephone wire.
- Two types
  - confidentiality (read protection)
  - integrity (write protection)
- Normally implemented using encryption.

Accountability

- What happens when authorised users (you have got to trust somebody) break the rules.
- Accountability means you can find out who did what.
- Two possibilities
  - Audit
  - Non-repudiation (stronger form)

Accountability - Audit

- Users actions are recorded in an audit log.
- But audit logs themselves can be tampered with.
- Clever users would be able to impersonate other users.
- Hence provides only a weak form of accountability.

Accountability - Non-repudiation

- Requests for resources are digitally signed by users.
- Again actions are stored in an audit log, but now along with digital signatures.
- It is then not possible to deny having made the request.
- Several governments have brought in laws recognizing digital signatures as legally binding.

Availability

- Bombarding services with requests.
- Two approaches
  - service continuity
  - disaster recovery
- Service continuity can be obtained by keeping a number of active copies of services.
- Disaster recovery provided by keeping backup copies of everything and activating them after a problem.

Assurance

- What an organisation does to provide freedom from worry is called assurance.
- The theory is the organisation
  - knows what should be done.
  - can prove/demonstrate that they have been done
  - can convince you that doing those things will make the system secure
- An assurance argument is made to convince you that the system is secure.

Assurance Argument

- Tries to prove
  - the protection mechanisms are correct
  - the system uses the protection mechanisms when they are needed
  - no way to circumvent the protection mechanisms (i.e. no back doors)

Assurance Throughout the System Lifecycle

- The system should be designed, built, delivered, installed configured and is operated correctly.
- Record must be kept throughout the system lifecycle to demonstrate this.